Proposition de nouveaux mécanismes de protection contre l'usurpation d'identité pour les fournisseurs de services Internet

Aroua Biri

Ecole Doctorale EDITE

Thèse présentée pour l'obtention du diplôme de Docteur de Télécom & Management SudParis

Doctorat conjoint Télécom & Management SudParis et Université Pierre et Marie Curie

Spécialité : Informatique

Par Mlle. Aroua BIRI

Titre

Proposition de nouveaux mécanismes de protection contre l'usurpation d'identité pour les fournisseurs de services Internet

Soutenue le 25 février 2011 devant le jury composé de :

Rapporteur : Pr. Bernard COUSIN, professeur à l'université RENNES 1

Rapporteur : Dr. Hasnaa MOUSTAFA, ingénieur de recherche senior, Orange labs

Examinateur : Pr. Guy Pujolle, professeur à Paris VI

Examinateur : M. Olivier MARY, associé de la société OPPIDA

Directeur de thèse : Pr. Hossam AFIFI, professeur à Telecom Sud Paris

Thèse n° 2011TELE0009

Résumé

De plus en plus d'organisations sont informatisées et plus une organisation est grande, plus elle peut être la cible d'attaques via Internet. On note également que les internautes utilisent de plus en plus Internet pour faire des achats sur des sites de commerce électronique, pour se connecter à l'administration en ligne, pour voter de manière électronique, etc. Par ailleurs, certains d'entre eux ont de plus en plus d'équipements électroniques qui peuvent être raccordés à Internet et ce dans divers sites (domicile, voiture, lieu de travail, etc.). Ces équipements forment ce qu'on appelle un réseau personnel qui permet la mise en place de nouvelles applications centrées sur l'internaute. Les fournisseurs de services Internet peuvent ainsi étoffer leurs offres de services en présentant une offre de sécurisation de ce genre de réseau.

Selon le rapport du cabinet « Arbor Networks » intitulé « Worldwide Infrastructure Security Report », les menaces identifiées comme les plus sévères sont relatives aux attaques de déni de service distribué. Ce type d'attaque a pour but de rendre indisponible un service en empêchant les utilisateurs légitimes de l'utiliser. Il utilise la technique de l'usurpation d'identité qui consiste en la création de paquets (de type IP, ARP, etc.) avec une adresse source forgée et ce dans le but d'usurper un système informatique ou d'usurper l'identité de l'émetteur. La technique de l'usurpation d'identité permet ainsi de rendre un service indisponible, d'écouter, de corrompre, de bloquer le trafic des internautes ou de nuire au bon fonctionnement des protocoles de routage et des réseaux personnels des clients. De plus, la technique de l'usurpation d'identité est également utilisée pour des activités interdites par la loi « Hadopi » en rigueur en France comme le téléchargement illégal. De ce fait, les fournisseurs de services Internet se doivent de prémunir leurs clients des attaques basées sur la technique de l'usurpation d'identité.

Ces dits fournisseurs comptent sur les protocoles de routage qu'ils déroulent pour participer au bon acheminement des données de leurs clients. Cependant, le protocole intra-domaine OSPF et le protocole inter-domaine BGP sont vulnérables aux attaques utilisant la technique de l'usurpation d'identité qui peuvent conduire à l'acheminement des paquets vers des destinataires non légitimes ou au déni de service. Nous proposons donc deux mécanismes dédiés respectivement au protocole intra-domaine OSPF et au protocole inter-domaine BGP. D'une part, afin de protéger les routeurs OSPF contre les attaques utilisant la technique d'usurpation d'identité, nous avons préconisé le stockage de l'identité et du matériel cryptographique dans un coffre-fort électronique que sont les cartes à puce. Les cartes déroulent ensuite un algorithme de dérivation de clés avec les cartes des routeurs voisins ainsi qu'avec celle du routeur désigné. Les clés dérivées entre les cartes à puce servent à signer les messages OSPF et à authentifier le niveau MAC. Nous avons décrit par la suite la plateforme du démonstrateur et les scénarios de tests adoptés pour évaluer les performances de notre prototype et les comparer avec ceux du logiciel Quagga sur la base de trois critères : le temps requis pour traiter une annonce d'état de liens, le temps de convergence ainsi que le temps de re-calcul d'une table de routage après un changement. Ces temps augmentent peu avec l'introduction de la carte à puce implémentant les fonctions de sécurité proposées. Ainsi, cette solution permet de renforcer la sécurité du protocole OSPF avec un impact raisonnable sur les performances. D'autre part, afin de protéger les routeurs BGP contre les attaques utilisant la technique d'usurpation d'identité, nous avons préconisé la « clustérisation » des domaines Internet et la sécurisation des liens entre les clusters ainsi qu'au sein de chacun d'eux grâce aux paradigmes de « web of trust » et de la cryptographie sans certificats. Le but étant de former au niveau de chaque chef de cluster le graphe actuel d'Internet. Chaque message de

rafraîchissement BGP sera ensuite vérifié à l'aide de ce graphe qui sera mis à jour grâce à des messages de rafraîchissement émis par les routeurs. En plus de se protéger contre les attaques au niveau des protocoles de routage, les fournisseurs de services Internet se doivent d'octroyer à leurs clients des adresses IP dont l'usurpation peut être détectée, neutralisée et tracée. L'attribution des adresses IP se fait lors de la connexion du client au fournisseur de services Internet. Il est donc crucial de repenser le mécanisme d'octroi des adresses IP. Nous avons ainsi proposé une nouvelle extension pour DNSSEC pour assurer la correspondance entre l'adresse IP du client et sa clé publique. Nous avons également évalué de manière formelle la réduction de dommages obtenue avec notre mécanisme et appliqué les formules obtenues au contexte d'Internet.

Les mécanismes de protection contre les attaques d'usurpation d'identité dans un contexte privé ainsi que dans un contexte public sont aussi cruciaux pour l'adoption par les clients des nouvelles applications offertes par les fournisseurs de services Internet. En effet, dans un contexte privé, la communication entre les équipements personnels des utilisateurs véhiculent des données qui peuvent être confidentielles. Il ne faut donc pas qu'un équipement n'appartenant pas à l'utilisateur légitime puisse accéder à son réseau personnel. De ce fait, nous avons proposé deux mécanismes de protection contre les attaques basées sur l'usurpation d'identité afin qu'un équipement illégitime ne soit pas en mesure d'usurper l'identité d'un équipement légitime. Le premier sera dédié à la phase de formation et d'utilisation des réseaux personnels et le second sera dédié au cas particulier des réseaux médicaux. Concernant le mécanisme dédié au réseau personnel, nous avons préconisé l'utilisation d'un protocole basé sur les canaux hors bande en vue d'attribuer des certificats aux capteurs biomédicaux. Nous dérivons par la suite des clés bilatérales entre les équipements du réseau personnel du même site ainsi qu'entre des équipements sur des sites distants. Concernant le cas particulier des réseaux médicaux, nous avons proposé de couvrir leurs phases de déploiement ainsi que leurs phases opérationnelles. Le protocole proposé exige peu de participation de la part des utilisateurs et respecte les capacités limitées de calculs des capteurs biomédicaux. Dans le contexte d'accès d'un équipement de l'utilisateur au réseau d'un fournisseur de services Internet depuis un lieu public, nous avons proposé un protocole inter-couche basé sur les principes de la théorie de l'information. Ce protocole fixe la faille de sécurité non abordée dans les autres propositions qu'est l'attaque de l'usurpation d'identité qui survient au début de la communication et protège donc les utilisateurs contre les attaques de type « homme du milieu ». Nous avons proposé que la personne qui désire avoir un accès sécurisé à Internet doit être sur un cercle spécifique qu'on a nommé « RED POINT » de telle façon que l'attaquant n'est pas en mesure d'être sur le même cercle au même moment. Le protocole inter-couche proposé se déclinent en trois phases: la phase de vérification de la position de l'utilisateur, la phase d'extraction du secret partagé de la couche physique et la phase de la dérivation de la clé partagée au niveau de la couche MAC. Nous avons par la suite validé formellement notre solution grâce à l'outil AVISPA et présenté les résultats de son implémentation.

Summary

More and more organizations are computerized and more an organization is great, plus it can be the target of Internet attacks. Moreover, some of them have a growing number of electronic equipments that can be connected to the Internet from various locations (home, car, workplace, etc.). These devices form a so-called personal area network that allows the development of new applications centered on users. The ISPs can then expand their service offerings by providing a secure supply of such networks.

According to the report of the firm “Arbor Networks”, entitled "Worldwide Infrastructure Security Report ", the most severe threats are related to distributed denial of service. This type of attack aims to make available a service by preventing legitimate users from using it. It uses the technique of identity theft that involves the creation of packages (like IP, ARP, etc.) with a forged source address and that in order to usurp the Identity of the issuer or of the computer system.

Thus, the technique of identity theft allows to render a service unavailable, to listen, to corrupt, to block traffic from Internet users or to undermine the legitimate operation of routing protocols and personal networks. Moreover, the technique of identity theft is also used for prohibited activities by "HADOPI" law in France and related to illegal downloading issues. Thus, the ISPs have a duty to protect their customers from attacks based on the technique of identity theft.

The mechanisms of protection against spoofing attacks for access networks are crucial for customer adoption of new applications offered by Internet service providers. This part of the doctoral thesis is part of the European project “MAGNET Beyond" whose vision is to put into practice the concept of personal networks, with the ultimate objective to design, develop, prototype and validate the concept.

In the context of user equipment’s access to the network of an Internet services provider from a public place, we proposed a cross-layer protocol based on the principles of information theory. This protocol fixes the security hole not addressed by other proposals that is the attack of identity theft that occurs at the beginning of communication and thus protects users against the middle man attacks. We proposed that the person who wants to have secure access to the Internet must be on a specific circle has been called "RED POINT" so that the attacker is not able to be on the same circle at the same time. The proposed cross-layer protocol can be divided into three phases: the phase of checking the position of the user, the extraction phase of the shared secret of the physical layer and the phase of the derivation of the shared key at the MAC layer. We subsequently validated our solution through a formal tool AVISPA and presented the results of its implementation.

In a private context, communication between devices convey users' personal data which may be confidential, so we must prevent equipment not belonging to the legitimate user to access its network. Thus, we proposed two mechanisms of protection against attacks based on spoofing so that illegitimate equipment is unable to impersonate legitimate equipment. The first phase will be dedicated to personal networks and the second will be dedicated to the particular case of medical networks. Regarding the mechanism dedicated to personal networks, we have proposed the use of a protocol based on out-of-band channel in order to provide certificates to user equipments.

We derive bilateral key for personal network's equipments of the same site and between equipments at remote sites. Concerning the particular case of medical networks, we proposed to cover their deployment phases and their operational phases. This proposal was submitted to the IEEE 802.15.6 working group that conducts research for the standardization of medical networks. The proposed protocol requires little involvement from users and respects the limited capacity of calculations of biomedical sensors.

The mechanisms of protection against spoofing attacks are also needed in the framework of core networks. In fact, ISPs rely on routing protocols to participate in the smooth flow of customer data. However, the intra-domain protocol OSPF and inter-domain protocol are vulnerable to attacks using the technique of identity theft that can lead to routing packets to illegitimate recipients or to denial of service. We therefore propose two mechanisms dedicated respectively to inter-domain BGP protocol and intra-domain OSPF protocol. This part of the doctoral thesis is part of the ESTER project aimed at demonstrating the feasibility of an approach based on the integration of smart cards within the network nodes, thus acting as an electronic safe. On the one hand, to protect against attacks BGP routers using the technique of identity theft, we propose the "clustering" of Internet domains and securing links between clusters and within each of them through the paradigms of "web of trust " and certificateless cryptography. The goal is to form at each cluster head the current Internet graph. Each BGP refresh message will then be verified against this graph which will be updated through refresh messages sent by routers. On the other hand, to protect against OSPF routers attacks using the technique of identity theft, we propose to store the identity and the cryptographic material in an electronic safe that are smart cards. The cards then run a key derivation protocol with those of neighboring routers as well as with that of the designated router. The key derived between the smart cards is used to sign messages and to authenticate the OSPF MAC level. We then described the demonstrator's platform and the test scenarios adopted to evaluate the performance of our prototype and compared with those of the Quagga software based on three criteria: the time required to process a link state advertisement, the convergence time and the re-calculation time of a routing table after a change. In addition to protecting against attacks at routing protocols level, Internet service providers will have to grant their clients with IP address whose spoofing can be detected, neutralized and drawn. The allocation of IP addresses is done at the client's connection to the ISP. It is therefore crucial to rethink the IP addresses granting mechanism. We proposed a new extension to DNSSEC to secure correspondence between the client's IP address and public key. We also formally assessed the damage reduction obtained with our mechanism and apply obtained the formulas in the context of the Internet.

Sommaire

Table des figures

CHAPITRE 1

1 Introduction

1.1 Introduction générale

L'accès à Internet est réalisée grâce à un fournisseur de services Internet via divers moyens de communications électroniques : soit par des liens filaires (réseau téléphonique commuté, ADSL), soit par des liens sans fil (WI-FI, WiMAX, Internet par satellite).

De plus, certains internautes ont de plus en plus d'équipements électroniques qui peuvent être raccordés à Internet et ce dans divers domaines privés (domicile, voiture, bureau, lieu de travail, etc.). Ces équipements forment ce qu'on appelle un réseau personnel qui est une extension du concept du PAN (Personal Area Network)[1] et qui permet la mise en place de nouvelles applications centrées sur l'internaute. Les fournisseurs de services Internet peuvent ainsi étoffer leurs offres de services en présentant une offre de sécurisation de ce genre de réseau.

Selon le rapport de "Arbor Networks"[2] intitulé « Worldwide Infrastructure *Security* Report » [22], les menaces identifiées comme les plus sévères sont celles relatives aux attaques de déni de service distribué. Ce type d'attaque a pour but de rendre indisponible un service en empêchant les utilisateurs légitimes de l'utiliser. Elle utilise la technique d'usurpation d'identité [29], et consiste en la création de paquets avec une adresse source contrefaite et ce dans le but d'usurper un système informatique ou d'usurper l'identité de l'émetteur. La technique d'usurpation d'identité permet ainsi de rendre un service indisponible, d'écouter, de corrompre ou de bloquer le trafic des internautes ou de nuire au bon fonctionnement des protocoles de routage et des réseaux personnels des clients.

---

1 L'acronyme PAN désigne un réseau d'équipements personnels utilisant les technologies sans fil telles que Bluetooth, l'infrarouge (IR), ou le zigbee.

2 « Arbor Networks » est un fournisseur mondial de solutions de sécurité (en particulier contre les dénis de service).

La technique d'usurpation d'identité est également utilisée pour des activités interdites par la loi en rigueur en France comme le téléchargement illégal. Ainsi, le téléchargement des fichiers du site de partage de fichiers Emule peut impliquer l'utilisation de *70* IP sources, dont 65 sont des IP artificiellement injectées et dont certaines sont relatives à des clients actifs et en ligne mais qui n'ont aucune connexion sur un réseau pair à pair[3] [52]. Selon la loi Hadopi [45] en rigueur en France, un internaute peut être poursuivi si son adresse IP est impliquée dans une action illégale et les "victimes d'une usurpation d'adresse IP pourront faire valoir des observations auprès de la Haute Autorité, qui seront alors étudiées par le juge seul à même de prononcer une peine de suspension de l'accès à Internet".

De ce fait, les fournisseurs de services Internet se doivent de prémunir leurs clients des attaques basées sur la technique d'usurpation d'identité.

1.2 Présentation de l'usurpation d'identité

1.2.1 Description

Dans les systèmes informatiques, le terme usurpation d'identité réfère à la création de paquets (de type IP, ARP[4], etc.) avec une adresse source falsifiée et ce dans le but d'usurper l'adresse d'origine d'un serveur ou l'identité de l'émetteur. La figure 1 illustre le champ de l'adresse source à modifier dans le cadre de l'usurpation d'une adresse source de type IP. Cette technique peut permettre à l'attaquant de détourner des flux de communication, de les écouter, de les corrompre et de les bloquer. Ainsi, un attaquant peut forger l'adresse IP d'un paquet donné dans le but de leurrer le récepteur sur l'origine du paquet. L'attaquant peut ensuite récupérer les réponses aux paquets en les redirigeant vers sa propre ma-

---

[3] Le pair-à-pair est un modèle de réseau informatique proche du modèle client-serveur mais où chaque client est aussi un serveur.

[4] ARP est le protocole de résolution d'adresse le plus répandu dans les réseaux Ethernet

chine. Il peut également forger une requête ARP. Ainsi, il émet une requête en unicast vers la victime en spécifiant comme adresse IP émettrice, l'adresse IP qu'il veut usurper et en indiquant sa propre adresse MAC comme l'adresse MAC de l'émetteur. En conséquence, lorsque la victime reçoit la requête, elle enregistre la correspondance IP/MAC dans sa table ARP alors que celle-ci est erronée.

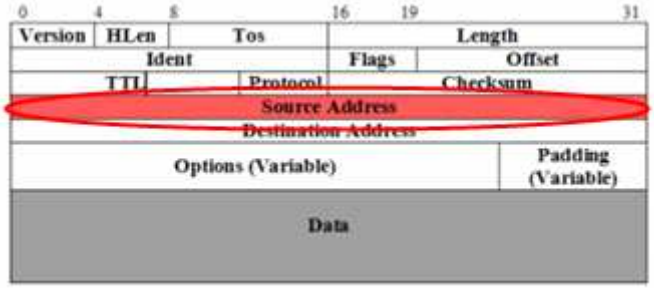


Figure 1: Champ impacté par l'usurpation d'adresse IP

La technique d'usurpation d'identité est le plus souvent utilisée dans les attaques par déni de service [15]. Ces attaques consistent en l'inondation de la victime par des quantités écrasantes de paquets dans le but de rendre indisponible un service en empêchant les utilisateurs légitimes de l'utiliser. Dans le cadre de ce type d'attaques, l'attaquant n'a pas besoin de recevoir des réponses à ses paquets. De ce fait, les paquets avec des adresses IP source usurpées sont adaptés à de telles attaques.

De plus, les paquets avec des adresses usurpées sont difficiles à filtrer. En effet, chaque paquet usurpé provient d'une adresse différente ce qui complexifie la détection de la véritable source de l'attaque. Les attaques par déni de service utilisent généralement au hasard des adresses à partir de l'espace des adresses IP. Les mécanismes d'usurpation d'identité sophistiqués se basent sur le mécanisme « Reverse DNS lookup » afin d'éviter les adresses non routables et les portions inutilisées de l'espace d'adressage IP. L'attaquant n'a pas forcément besoin de matériel

sophistiqué. Ainsi, ce type d'attaque peut être exécuté avec des ressources limitées contre un réseau beaucoup plus grand et plus moderne.

Les attaquants sont majoritairement des organisations criminelles, essentiellement motivées par l'argent. Ainsi, certaines d'entre elles se sont spécialisées dans le piratage d'un grand nombre de machines, qu'ils peuvent ensuite louer à d'autres pirates pour attaquer une cible particulière. Ainsi, un pirate est en mesure de lancer une attaque en déni de service contre une entreprise et de lui demander une rançon pour arrêter cette attaque [74].

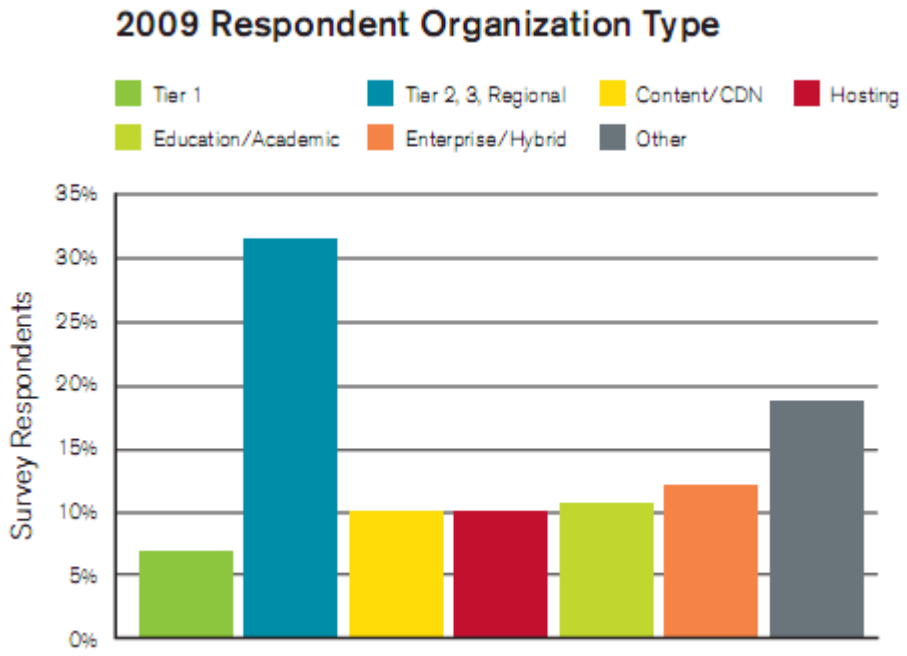
1.2.2 Les attaques d'usurpation d'identité en chiffres

Selon le cinquième rapport d' « Arbor Networks » intitulé « Worldwide Infrastructure Security Report », les menaces identifiées comme les plus sévères par les entreprises consultées - dont la répartition par organisations et par continent sont explicités par les figures 3 et 4 - sont celles relatives aux attaques DDoS[5] (35%) [15], suivie par les activités basées sur les bots[6] (21%). Ensuite, dans l'ordre décroissant, les menaces sont relatives au vol d'informations d'identification, à l'empoisonnement du cache DNS, au détournement de route, à la compromission des systèmes ou des infrastructures, et aux vers informatiques.

---

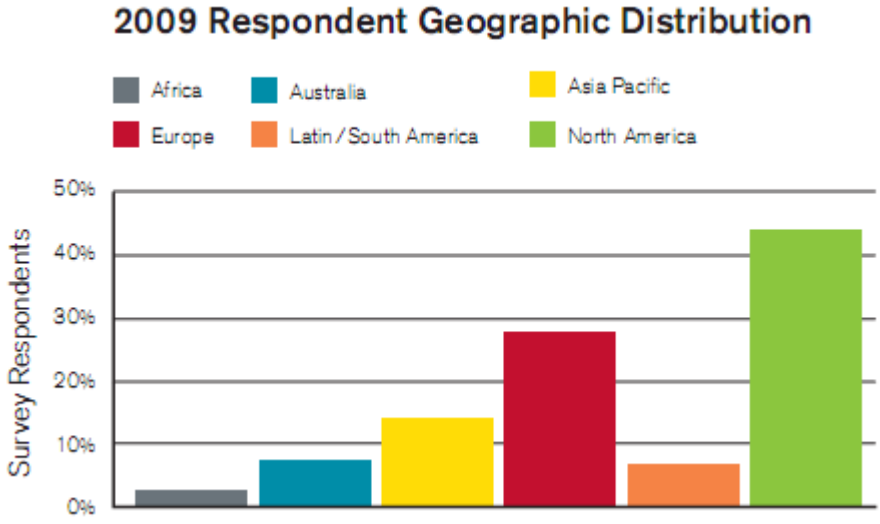
5 Il est nécessaire d'appliquer un effet multiplicateur à un simple déni de service au vue des performances actuelles des serveurs et de la généralisation des techniques de répartition de charge et de haute disponibilité. Ceci peut être réalisé grâce à la multiplication au sein des machines piratées de contrôleurs (nœuds maitres) de l'attaque.

6 Un bot est un ordinateur contrôlé à l'insu de son utilisateur par un pirate informatique.



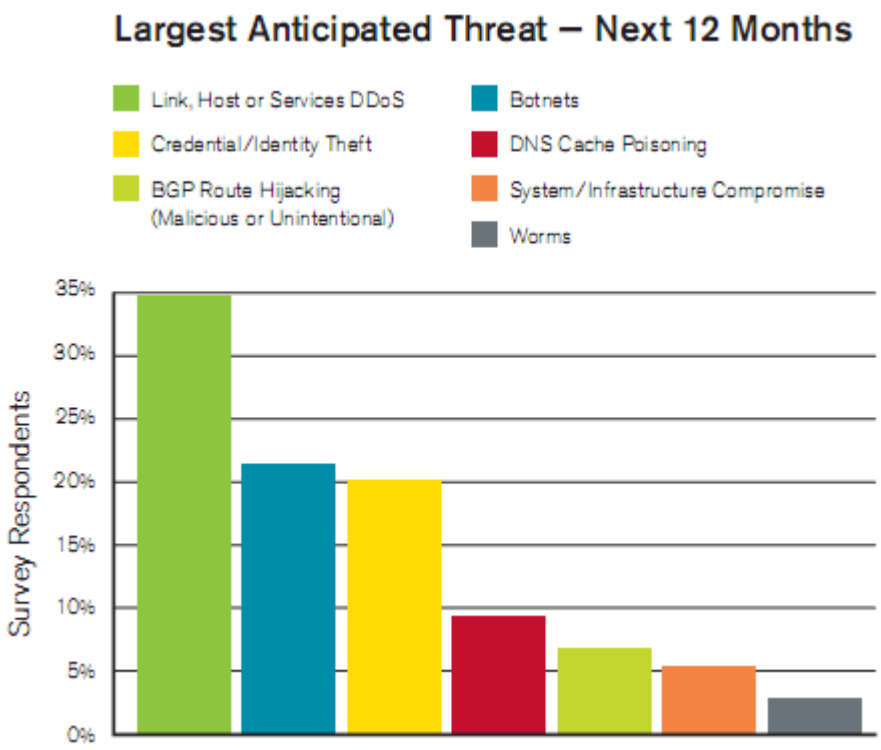
Source: rapport de "Arbor Networks" intitulée «5th Edition of the Worldwide Infrastructure Security Report»

Figure 2: Répartition des entreprises consultées par organisation



Source: rapport de "Arbor Networks" intitulée «5th Edition of the Worldwide Infrastructure Security Report»

Figure 3: Répartition des entreprises consultées par continent



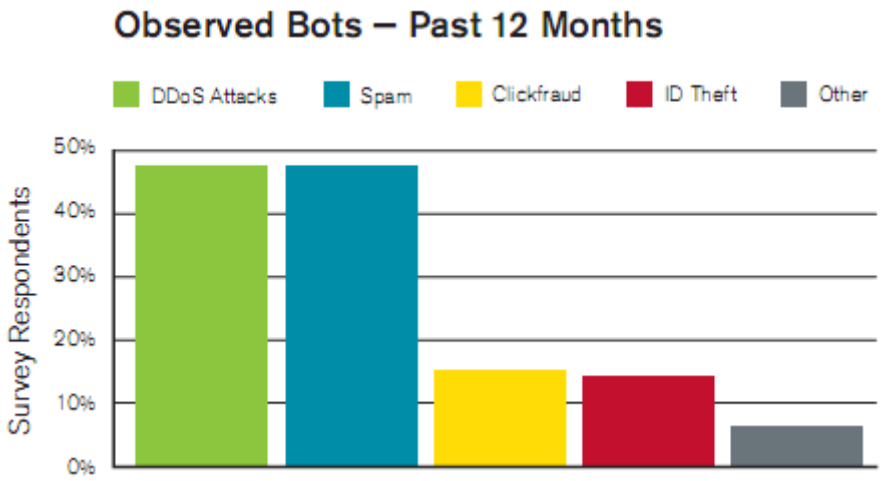
Source: rapport de "Arbor Networks" intitulée «5th Edition of the Worldwide Infrastructure Security Report»

Figure 4: Les plus grandes menaces anticipées

Les entreprises consultées ont été interrogées sur les activités qu'ils ont personnellement constatées au niveau des botnets[7]. Il en ressort que le DDoS et le spam se partagent la première place, suivie par la fraude par le clic[8], le vol d'identité et un éventail d'autres activités criminelles.

7 Un botnet est un ensemble de bots

8 La fraude au clic est une activité qui consiste à faire effectuer, par une personne ou un programme informatique, des clics sur des publicités afin de dilapider rapidement le budget publicitaire d'un concurrent.



Source: rapport de "Arbor Networks" intitulée «5th Edition of the Worldwide Infrastructure Security Report»

Figure 5: les activités des botnets

Les attaques DrDos[9] sont responsables des plus grandes attaques en termes de consommation de bande passante en 2007 et 2008. Les attaques de cette nature employées contre les racines Internet et les serveurs de noms au début de 2006 ont atteint un facteur d'amplification de 1 à 76. Les attaques signalées en 2008 auraient atteint un facteur d'amplification encore plus grand. Avec de tels niveaux d'amplification, un petit nombre d'hôtes liés entre eux sont capables de générer de grandes quantités de trafic, ce qui peut porter préjudice à la plupart des organismes reliés à l'Internet d'aujourd'hui.

Le but de cette thèse est de proposer des mécanismes de protection contre l'usurpation d'identité lors de la connexion aux FSI notamment depuis les réseaux personnels ainsi que des mécanismes de protection contre l'usurpation d'identité pour les réseaux de cœur. En effet, la technique d'usurpation d'identité peut être utilisée pour nuire aux particuliers et aux entreprises lors de la con-

[9] Une attaque distribuée réflective de déni de service (DRDOS) consiste à envoyer des messages forgés à un très grand nombre d'ordinateurs qui répondront à ces demandes. Ainsi, l'adresse source est réglée sur celle de la victime ciblée, ce qui signifie que toutes les réponses vont aller à la cible.

nexion des clients du FSI au service Internet ainsi que lors de la formation et l'usage de leurs réseaux personnels. Cette technique peut également nuire au bon fonctionnement des protocoles de routage et par la même du service Internet.

1.3 Organisation de la thèse

Ce manuscrit traite de la problématique de la protection des réseaux de cœur ainsi que celles des réseaux d'accès aux services Internet contre les attaques basées sur l'usurpation d'identité. Chacun des deux chapitres suivants propose des contributions pour prémunir les clients contre les attaques utilisant la technique d'usurpation d'identité. Par souci de lisibilité, l'état de l'art de chaque contribution est détaillé respectivement dans les sections des chapitres.

1.3.1 Mécanismes de protection contre l'usurpation d'identité au niveau des réseaux d'accès

Les mécanismes de protection contre les attaques d'usurpation d'identité dans le cadre des réseaux d'accès sont cruciaux pour l'adoption par les clients des nouvelles applications offertes par les fournisseurs de services Internet. Cette partie de cette thèse doctorale s'inscrit dans le cadre du projet européen [65] « MAGNET Beyond » [2006, 2008] dont la vision est de mettre en pratique le concept des réseaux personnels, l'objectif final étant de concevoir, développer, prototyper et valider ce concept.

Dans le contexte d'accès d'un équipement personnel de l'utilisateur au réseau d'un fournisseur de services sur l'Internet depuis un lieu public, nous proposons un protocole inter-couche basé sur les principes de la théorie de l'information. Ce protocole traite la faille de sécurité non abordée dans les autres propositions qu'est l'attaque de l'usurpation d'identité qui survient au début de la communication et protège donc les utilisateurs contre les attaques de type « homme du milieu ». Nous proposons que la personne qui désire avoir un accès sécurisé à In-

ternet se déplace physiquement vers une zone spécifique qu'on a nommé « RED POINT » de telle façon que l'attaquant n'est pas en mesure d'être sur le même cercle au même moment. Le protocole inter-couche proposé se décline en trois phases: la phase de vérification de la position de l'utilisateur, la phase d'extraction du secret partagé de la couche physique et la phase de la dérivation de la clé partagée au niveau de la couche MAC. Nous validons par la suite formellement notre solution grâce à l'outil AVISPA et présenté les résultats de son implémentation.

Dans un contexte privé, comme la communication entre les équipements personnels des utilisateurs véhicule des données confidentielles, il ne faut pas qu'un équipement n'appartenant pas à l'utilisateur légitime puisse accéder à son réseau personnel. De ce fait, nous proposons deux mécanismes de protection contre les attaques basées sur l'usurpation d'identité afin qu'un équipement illégitime ne soit pas en mesure d'usurper l'identité d'un équipement légitime. Le premier sera dédié à la phase de formation et d'utilisation des réseaux personnels et le second sera dédié au cas particulier des réseaux médicaux.

Concernant le mécanisme dédié au réseau personnel, nous proposons un protocole basé sur les canaux hors bande impliquant une intervention minime de la part des utilisateurs en vue d'attribuer des certificats à leurs équipements. Nous dérivons par la suite des clés bilatérales entre les équipements du réseau personnel du même site ainsi qu'entre des équipements sur des sites distants.

Concernant le cas particulier des réseaux médicaux, nous proposons d'étudier leurs phases de déploiement ainsi que leurs phases opérationnelles. Cette proposition a été présentée au groupe de travail IEEE 802.15.6 qui mène des travaux en vue de la normalisation de réseaux médicaux. Ce protocole proposé exige peu de participation de la part des utilisateurs et respecte les capacités limitées de calcul des capteurs biomédicaux ainsi que leurs puissances électriques très limitées.

1.3.2 Mécanismes de protection contre l'usurpation d'identité au niveau du réseau de cœur

Les mécanismes de protection contre les attaques d'usurpation d'identité sont également nécessaires dans le cadre des réseaux de cœur. En effet, les fournisseurs comptent sur les protocoles de routage qu'ils déroulent pour participer au bon acheminement des données de leurs clients. Cependant, le protocole intra-domaine OSPF et le protocole inter-domaine BGP sont vulnérables aux attaques utilisant la technique de l'usurpation d'identité qui peuvent conduire à l'acheminement des paquets vers des destinataires non légitimes ou au déni de service. Nous proposons donc deux mécanismes dédiés respectivement au protocole inter-domaine BGP et au protocole intra-domaine OSPF. Cette partie de cette thèse doctorale s'inscrit dans le cadre du projet ESTER qui vise à démontrer la faisabilité d'une approche basée sur l'intégration de cartes à puces au sein des nœuds de réseaux agissant ainsi comme un coffre-fort électronique. D'une part, afin de protéger les routeurs BGP contre les attaques utilisant la technique d'usurpation d'identité, nous préconisons la « clustérisation » des domaines Internet et la sécurisation des liens entre les clusters ainsi qu'au sein de chacun d'eux grâce aux paradigmes de « web de confiance » et de la cryptographie sans certificats. Le but étant de former au niveau de chaque chef de cluster le graphe actuel d'Internet. Chaque message de rafraîchissement BGP sera ensuite vérifié à l'aide de ce graphe qui sera mis à jour grâce à des messages de rafraîchissement émis par les routeurs.

D'autre part, afin de protéger les routeurs OSPF contre les attaques utilisant la technique d'usurpation d'identité, nous préconisons le stockage de l'identité et du matériel cryptographique dans un coffre-fort électronique que sont les cartes à puce. Les cartes déroulent ensuite un algorithme de dérivation de clés avec les cartes des routeurs voisins ainsi qu'avec celle du routeur désigné. Les clés dérivées entre les cartes à puce servent à signer les messages OSPF et à authentifier le niveau MAC. Nous décrivons par la suite la plateforme du démonstrateur et

les scénarios de tests adoptés pour évaluer les performances de notre prototype et les comparer avec ceux du logiciel Quagga sur la base de trois critères :

- le temps requis pour traiter une annonce d'état de liens ;
- le temps de convergence ;
- le temps de re-calcul d'une table de routage après un changement.

En plus de la protection contre les attaques au niveau des protocoles de routage, les fournisseurs de services Internet se doivent d'octroyer à leurs clients des adresses IP dont l'usurpation peut être détectée, neutralisée et tracée. L'attribution des adresses IP se fait lors de la connexion du client au fournisseur de services Internet. Il est donc crucial de repenser le mécanisme d'octroi des adresses IP. Nous proposons ainsi une nouvelle extension pour DNSSEC afin d'assurer la correspondance entre l'adresse IP du client et sa clé publique. Nous évaluons également de manière formelle la réduction de dommages obtenue avec notre mécanisme et appliqué les formules obtenues au contexte d'Internet.

CHAPITRE 2

2 Mécanismes de protection contre l'usurpation d'identité pour les réseaux d'accès des fournisseurs de services Internet

2.1 Introduction

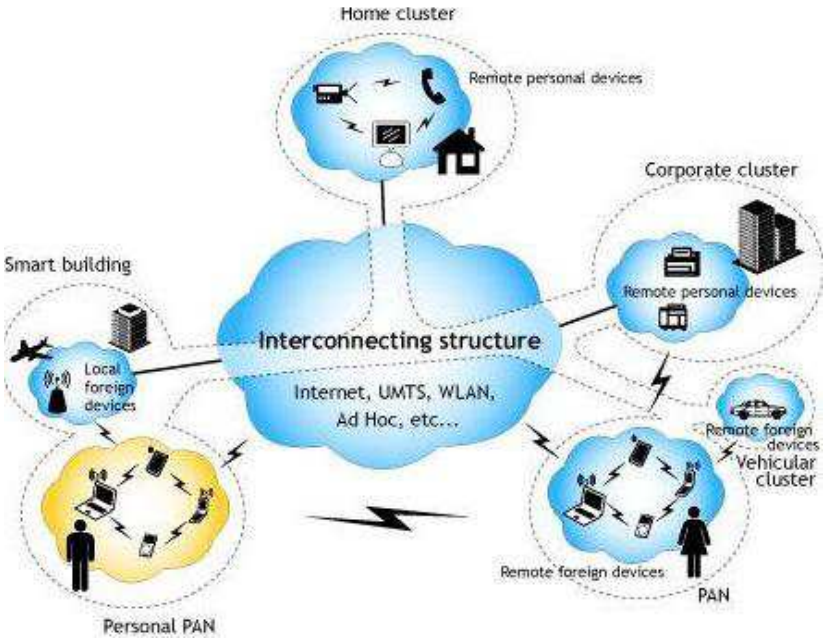
Ce chapitre s'inscrit dans le cadre du projet européen « MAGNET Beyond » dont la vision est de mettre en pratique le concept des réseaux personnels [5], l'objectif final étant de concevoir, développer, prototyper et valider ce concept. Le Réseau Personnel (RP) réfère à une collection d'équipements personnels qui ont la capacité d'établir une ou plusieurs connexions réseaux avec d'autres équipements et qui sont situés à la proximité de l'utilisateur (en termes de couverture radio) soit dans son réseau local personnel[10] soit dans d'autres réseaux qui lui sont rattachés. Un RP est donc une extension dynamique du réseau local personnel en termes de connectivité, de services potentiels et de configurations réseaux. Cette extension est réalisée physiquement via des infrastructures réseaux tel que les réseaux véhiculaires, les réseaux domestiques ou les réseaux ad hoc multi-sauts. Le RP d'un utilisateur donné est configuré pour permettre la mise en œuvre des applications de l'utilisateur et tient compte de son contexte et des possibilités de communication. Un RP doit s'adapter aux changements des environs, être auto-configurable et supporter de nombreux types de réseaux et appareils. Comme le RP se doit d'assurer à l'utilisateur tous ses besoins de communication, un RP inclut non seulement les appareils portables et sans fil de l'utilisateur mais aussi des dispositifs relatifs à la maison, à la voiture et au bureau, etc.

La mise en pratique du concept des réseaux personnels permet ainsi la mise en place de services sûrs, robustes et de manière omniprésente pour les utilisateurs mobiles et itinérants. Ces services peuvent être fournis par les fournis-

---

10 Un réseau local personnel désigne un réseau d'étendue restreinte d'équipements informatiques habituellement utilisés dans le cadre d'une utilisation personnelle

seurs de services Internet. Les mécanismes de protection contre les attaques d'usurpation d'identité dans un contexte privé ainsi que dans un contexte public sont cruciaux pour l'adoption par les clients des nouvelles applications offertes par les fournisseurs de services Internet.



Source: magnet.aau.dk/

Figure 6: Illustration du concept du réseau personnel

Les équipements personnels des utilisateurs comportent des données privées dont certaines peuvent être confidentielles. Il ne faut donc pas qu'un équipement n'appartenant pas à l'utilisateur légitime ou appartenant à l'utilisateur mais contrôlé par l'attaquant puisse accéder à son réseau personnel. De ce fait, il ne faut pas qu'un équipement illégitime soit en mesure d'usurper l'identité d'un équipement légitime.

Les FSI peuvent profiter du paradigme de réseau personnel pour jouer le rôle de fournisseur de services centrés sur l'internaute. Le FSI peut ainsi proposer une offre de mécanismes de protection contre l'usurpation d'identité pour la mise en place et le fonctionnement des RPs.

Dans ce chapitre, nous allons proposer un mécanisme de protection contre l'usurpation d'identité pour l'accès d'un équipement personnel depuis un lieu public. Nous allons par la suite proposer un mécanisme de protection contre l'usurpation d'identité pour les réseaux personnels et nous allons également traiter le cas particuliers des réseaux médicaux des patients.

La section 2.2 présente le mécanisme de protection contre l'usurpation d'identité pour l'accès d'un équipement personnel depuis un lieu public. La section 2.3 présente des mécanismes de sécurité basés sur les canaux hors-bande et dédiés aux réseaux locaux personnels. La section 2.4 présente le protocole « Elliptic Curve Diffie-Hellman ». La section 2.5 décrit par la suite notre solution. La section 2.6 présente le cas particulier des réseaux médicaux des patients et nous concluons dans la section 2.7.

2.2 Accès d'un équipement personnel depuis un lieu public

2.2.1 Introduction

Les accès Internet depuis les réseaux publics se font généralement depuis les hotpots. Les hotspots sont des zones géographiques couvertes par un groupe de points d'accès sans fil Wi-Fi (802.11). Dans ces zones, le public peut utiliser un ordinateur portable, un téléphone Wi-Fi ou tout autre appareil portatif approprié permettant l'accès à Internet. Les hotspots se trouvent souvent dans des restaurants, gares, aéroports, bibliothèques, cafés, librairies et autres lieux publics.

La plupart des hotspots ne sont pas sécurisés et les clients sont vulnérables aux attaques de type « homme au milieu » et aux points d'accès clandestins[11]. La

[11] Un point d'accès clandestin est un point d'accès sans fil qui a été soit installé sur un réseau d'entreprise sans l'autorisation explicite d'un administrateur de réseau local, ou a été créé pour permettre à un pirate de mener une attaque de type « homme de milieu »

protection contre l'usurpation d'identité peut être assurée grâce à une clé secrète partagée entre le point d'accès et le client. Cette clé sera associée à l'adresse IP du client ainsi qu'à l'adresse IP du point d'accès. Ainsi, l'attaquant ne pourra pas se faire passer pour le client ou le point d'accès légitime vu qu'il ne possède pas cette clé.

L'utilisation de l'infrastructure à clé publique est lourde et inappropriée dans ce cas parce que a) La gestion des certificats des utilisateurs et leurs révocations seront difficiles à mettre en œuvre en raison du grand nombre de clients occasionnels qui peuvent être impliqués dans ce processus et b) le service Internet est généralement gratuit et les clients l'utilisent de manière anonyme.

Un moyen classique de sécurisation du lien entre le point d'accès et l'équipement du client serait d'utiliser un algorithme d'appariement. L'objectif de l'appariement est de permettre à deux dispositifs de convenir, sans aucune connaissance préalable, d'un secret partagé qui peut être utilisé pour protéger leur communication ultérieure, même en présence d'un attaquant type « homme au milieu ».

Le concept d'appariement a d'abord été évoqué par Stajano et Anderson [25], dans leur modèle de sécurité « Resurrecting Duckling ». Le modèle préconise l'utilisation d'un canal de courte portée pour dériver leur secret partagé. Un canal physique supplémentaire est donc utilisé et est appelé canal hors bande. L'adversaire est supposé incapable de modifier les messages sur ce canal bien qu'il puisse l'écouter. Le canal hors-bande peut être un canal visuel comme celui proposé par McCune, et al [48]. Dans le cadre de leur proposition, le canal visuel se compose de deux codes-barres, affiché par un dispositif A, qui représentent des informations de sécurité propres à A. L'utilisateur peut positionner un autre appareil B contre le code à barres afin que B puisse lire le code-barres visuel, et utiliser cette information pour mettre en place un canal authentifié avec A. La série de protocoles MANA (Manuel d'authentification)

considère, quant à elles, l'utilisateur comme un canal hors bande confidentiel et authentifié. Selon le type des interfaces disponibles sur les appareils aux extrémités du canal hors-bande, Gehrmann C. et al. [13] décrivent trois protocoles possibles, à savoir MANA I, II et III. Ces protocoles correspondent respectivement à input/input (I / I), output/input (O / I) et output/output (O / O). MANA I et II sont basés sur la comparaison de codes d'authentification de message dérivés de données. Selon Mana III, un mot de passe secret partagé est saisi sur les deux appareils à la fois et une vérification aléatoire est ensuite réalisée sur le canal non sécurisé. Toutefois, partant de l'observation que si les procédures de sécurité ne peuvent pas être mises en place facilement, ils ne seront souvent pas utilisés, nous devons proposer des solutions simples de sécurité pour les clients.

Dans ce sous-chapitre, nous proposons un mécanisme permettant la dérivation d'un secret partagé entre le point d'accès et le client. Ce mécanisme inclut un protocole inter-couche qui fait usage des caractéristiques du canal physique et qui ne nécessite pas de secret partagé au préalable.

La section 2.6.2 présente l'état de l'art de la sécurité basée sur la théorie de l'information. Nous présentons dans la section 2.6.3 notre solution et dans la section 2.6.4 la validation formelle. La section 2.6.5 décrit l'implémentation et les résultats associés.

2.2.2 Etat de l'art

La sécurité basée sur la théorie de l'information est l'une des deux principaux axes de la cryptographie moderne [46].

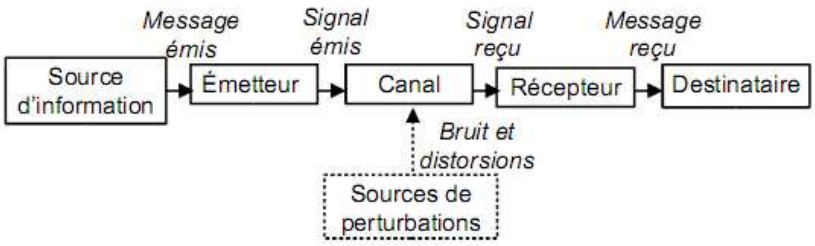


Figure 7: Modélisation d'un canal

Les systèmes sécurisés basés sur la théorie de l'information sont impossibles à briser, même pour les adversaires avec une puissance de calcul illimitée. Les lois de la physique imposent en effet une borne, dans certains contextes, sur la quantité d'information qu'un adversaire peut obtenir. Le bruit dans les canaux de communication garantit qu'un adversaire reçoit les bits transmis avec une probabilité d'erreur minime. L'étude de la communication sécurisée des informations à partir d'un point de vue théorique a été initiée par Shannon [12].

Wyner [3] a établi la possibilité d'assurer une communication entre une source A et un récepteur B sans besoin d'un secret partagé au préalable. L'attaquant E et le récepteur B observent sur le canal d'écoute le message de la source à travers des canaux bruités. L'idée principale est que le flux d'information soit caché dans le bruit ce qui le rendra inaccessible à l'attaquant. En fait, la source utilise un encodeur stochastique qui relie chaque message à de nombreux mots codés selon une distribution de probabilité appropriée. Il a été montré que si le canal d'A-E est une version dégradée du canal d'A-B, il existe un taux en dessous duquel un secret parfait est possible. La notion de capacité de secret a été présentée pour mesurer le taux maximum pour des communications secrètes. Les généralisations ultérieures apportées par Csiszar et Korner montrent que la capacité positive du secret est possible aussi longtemps que le canal d'A-B est meilleur que celui du canal d'A-E [32].

Li et al [77] proposent une approche pratique pour les protocoles de partage de clés qui assurent un secret absolu fondé sur les techniques de traitement du signal de la couche physique. Des études approfondies sur les canaux MIMO montrent que les canaux A-B et A-E peuvent être considérés comme complètement différents aussi longtemps que la distance entre eux excède quelques longueurs d'onde. Ainsi, les auteurs exploitent la différence de canal plutôt que la différence de bruit afin d'obtenir des informations secrètes. Cette procédure empêche l'attaquant d'estimer le canal, tout en permettant la réception des signaux par B avec succès.

Goel et al [59] affirment qu'en général il n'y a aucune garantie que le récepteur aura un meilleur canal que l'attaquant. Ils proposent donc d'utiliser des antennes multiples pour produire du «bruit artificiel». Ce bruit dégrade seulement le canal de l'attaquant donc il n'affecte pas le canal de B, permettant ainsi une communication parfaitement sécurisée dans des conditions génériques de canaux. L'idée clé de cette étude est que l'émetteur peut utiliser des antennes multiples pour ajouter du bruit généré artificiellement au signal de l'information, de telle manière qu'il se trouve dans l'espace nul du canal du récepteur. Ainsi, des opérations au niveau du canal du récepteur annulent le bruit artificiel et donc le récepteur n'est pas affecté par le bruit. Par contre, le canal de l'attaquant sera dégradé.

Li et al [81] propose d'établir de nouvelles formes d'authentification et de confidentialité qui opèrent au niveau de la couche physique basée sur le fait que les lois de propagation radio entre les deux entités sont uniques et décorrèlent rapidement avec la distance. Les techniques de sondage de canal, comme les impulsions à large bande et sondages multi-tons sont utilisées pour vérifier l'authenticité d'un émetteur. Les canaux Multiple-Input Multiple-Output (MIMO) sont appropriés pour de telles techniques. Ils valident la faisabilité de l'utilisation des techniques de couche physique pour la sécurisation des sys-

tèmes sans fil en présentant les résultats d'expériences réalisées grâce au logiciel de plateforme radio USRP / GNU. Notons que Miao [27] a estimé les paramètres MIMO à large bande et leurs applications aux estimations de canal MIMO-OFDM.

Même si les solutions décrites ci-dessus sont novatrices, elles souffrent toutes d'une faille sérieuse de sécurité car elles font l'hypothèse que ni l'identité de la source ni celle du récepteur ne peuvent être usurpés au début de la communication. En effet, ces solutions n'incluent pas des mécanismes d'authentification mutuelle au début de la communication. Elles sont donc vulnérables à l'attaque de type usurpation d'identité qui – rappelons-le – fait référence à une situation dans laquelle un appareil se fait passer avec succès pour un autre par la falsification des données et acquière ainsi un avantage illégitime.

Quant à la sécurité Wi-Fi actuelle, elle est basée sur le protocole IEEE 802.11i qui est un amendement à la norme 802.11 spécifiant les mécanismes de sécurité pour les réseaux sans fil [76]. Comme Wired Equivalent Privacy (WEP) a montré des failles de sécurité sévères[12], l'association « Wi-Fi Alliance » a préconisé l'utilisation du WPA « Wi-Fi Protected Access » en tant que solution intermédiaire. WPA est mis en œuvre comme un sous-ensemble de 802.11i. La mise en œuvre de l'ensemble des mécanismes du 802.11i est réalisée par le WPA2. L'architecture 802.11i contient les composants suivants: l'authentification 802.1X (ce qui nécessite l'utilisation du protocole EAP), RSN pour garder la trace d'associations et la norme de chiffrement avancé (AES) sur la base CCMP pour assurer la confidentialité, l'intégrité et l'authentification de l'origine. L'échange EAP fournit le secret partagé PMK (Pairwise Master Key)

12 Le WEP utilise l'algorithme de chiffrement par flot RC4 qui implique l'utilisation d'une clé différente à chaque envoi de données. De ce fait, la clé comporte une partie dynamique nommée vecteur d'initialisation (24 bits). Toutefois, la taille de ce vecteur d'initialisation n'empêche pas la répétition de l'utilisation des clés surtout lorsque l'utilisateur télécharge un volume conséquent de données en un court laps de temps. De plus, ce mécanisme nécessite l'utilisation d'une clz partagée par tous les équipements connectés au réseau sans-fil. Ainsi, la connaissance de la clé permettrait de déchiffrer toutes les communications.

qui sert à calculer la PTK (Pairwise Transient Key) et GTK (Group Temporal Key). La Figure 8 illustre l'architecture 802.11i. Comme le déploiement d'un serveur d'authentification tel qu'un serveur RADIUS ne peut être pas recommandé dans un hotspot public, nous avons besoin d'obtenir la PMK par un autre moyen. Notre solution permettra également de fournir cette clé.

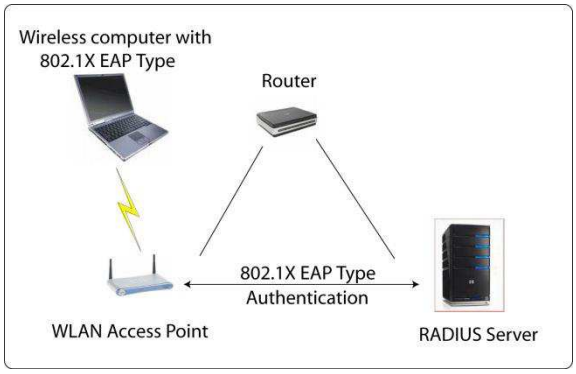


Figure 8: L'architecture 802.11i

2.2.3 Solution proposée

- Description:

Un cas d'utilisation du protocole proposé est illustré par la figure 9. Le client désireux de se connecter à Internet est positionné sur une des zones rouges se trouvant dans le hotspot. Notre but dans la suite de cette section est de fournir une clé partagée entre le Point d'Accès (PA) et l'équipement du client qui les protégera contre les attaques d'usurpation d'identité.

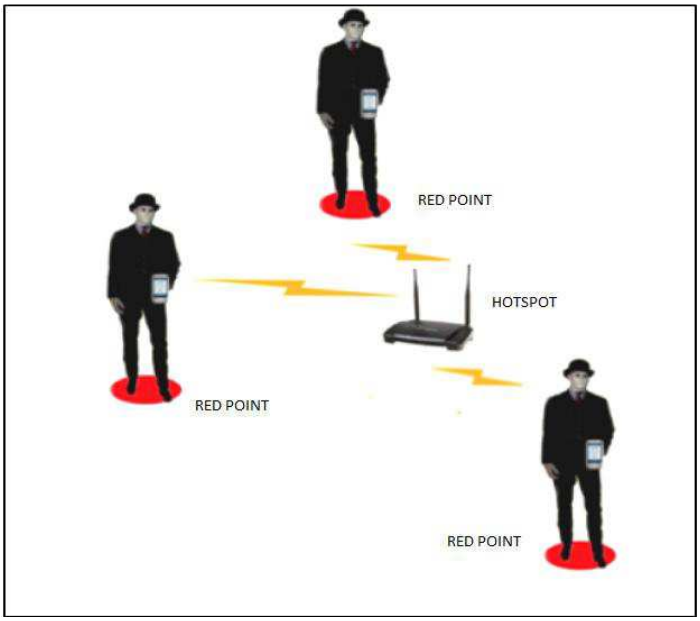


Figure 9: Cas d'utilisation du protocole proposé

Notre protocole est basé sur les principes de la théorie de l'information et en outre, il résout la faille de sécurité non abordée dans la littérature qu'est l'attaque d'usurpation qui peut survenir au début de la communication. Notre protocole protège ainsi contre les attaques de type « homme au milieu ».

Nous proposons le rajout de zones rouges comme décrit dans la figure 9 dans le hotspot, où l'utilisateur doit se placer quand il veut se connecter à Internet. Cette condition permet de résoudre le problème d'un utilisateur malveillant qui désire usurper l'identité de l'utilisateur légitime. En effet, toutes les méthodes expliquées dans la section précédente présupposent que la communication est établie entre les parties légitimes. Le PA ne peut pas cependant supposer qu'il communique avec l'équipement appartenant à la personne légitime. C'est pourquoi nous proposons que la personne qui désire avoir un accès sécurisé à Internet doive être sur un cercle spécifique de telle façon que l'attaquant n'est pas en mesure d'être sur le même cercle au même moment. Dans notre solution, les points d'accès

sont muti-faisceaux[13]. Ainsi, ils peuvent offrir plusieurs connexions sécurisées simultanément. Notons que le client doit télécharger la clé publique des hotspots avant de s'y rendre (par exemple celle de l'aéroport) ainsi que des paramètres de sécurité p (nombre premier) et g (base) qui satisfont la propriété suivante : g est inférieur à p et pour tout n entre 1 et p-1, il existe un exposant k de g tel que $n = g^k \bmod p$.

Les paramètres p et g vont permettre à l'utilisateur de générer une clé publique K à partir d'une clé secrète S qu'il aura choisi préalablement et ce comme suit : $K= G^S$.

Ces dites clés seront ensuite utilisés pour dériver des clés partagées avec les PA des hotspots en question. Par ailleurs, la clé publique des hotspots permettra à l'équipement du client d'authentifier le hotspot et d'ainsi s'assurer qu'il communique bien avec des hotspots légitimes.

L'équipement du client voit tous les points d'accès disponibles dans les hotspots et choisit l'un de ces points d'accès. Il déclenche ensuite la procédure d'envoi d'une demande d'association au PA. Le PA doit ensuite vérifier que l'utilisateur est sur une des zones rouges spécifiées. Après vérification de la position de l'utilisateur (via le concours de capteurs de mouvement), un premier secret est extrait par le PA et l'équipement Wi-Fi à partir du lien physique. Comme l'utilisateur est sur une zone rouge, l'AP est sûr que le secret qu'il reçoit du canal physique est bien partagé uniquement avec la personne légitime. Ensuite, un protocole de dérivation de clés se déroule au niveau MAC en se basant sur le secret partagé obtenu dans la phase précédente.

Ainsi, un attaquant n'est pas en mesure d'usurper ni l'identité de l'équipement du client ni celle du point d'accès au début de la communication. En effet, ce mécanisme protège les clients contre un attaquant ayant configuré son PDA ou

---

13 Un point d'accès « muti-faisceaux » forme des faisceaux multiples pour optimiser la gestion de plusieurs connexions simultanées. La formation de faisceau est réalisée par le contrôle les caractéristiques de chaque émetteur au sein d'un groupe d'émetteurs de sorte que le signal global soit optimisé pour atteindre un récepteur dans une direction donnée.

son ordinateur portable de telle manière qu'il apparaisse comme un point d'accès légitime. De plus, la clé obtenue servira alors de PMK pour d'autres procédures de sécurité Wi-Fi.

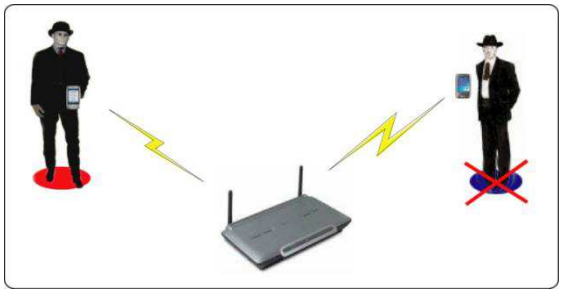


Figure 10: Illustration du rejet de l'équipement non légitime

- Le modèle du canal physique:

Nous choisissons d'adopter l'environnement multi-canal dans notre protocole car il est typique des scénarios sans fil. Pour un scénario spécifique émetteur-récepteur, l'effet de la propagation par trajets multiples peut être représenté comme un système où l'entrée u (t) est le signal transmis et le signal reçu est :

$$r(t) = \int_{-\infty}^{\infty} h(t,\tau) \cdot u(t-\tau) d\tau \qquad (1)$$

Dans ce système, la réponse du canal est la fonction variable dans le temps h(t,τ). La réponse du canal peut être modélisée (dans le sens du domaine temporel) comme un « tapped-delay line ». En outre, avec l'hypothèse supplémentaire d'un modèle de Rayleigh fading, le ***hi(t)*** devient un processus complexe gaussien stochastique avec une moyenne nulle. Ainsi, la réponse du canal peut être interprétée comme la somme des N versions retardées, atténuées et déphasées du signal original.

$$h(t,\tau) = \sum_{i=1}^{N} h_i(t)\delta(t-\tau_i) \qquad (2)$$

Notons que la caractérisation de canaux dé-corrèle d'un chemin de communication à un autre si les chemins sont séparés par l'ordre d'une longueur d'onde RF ou plus [72].

- Proposition du protocole inter-couche (couche physique, couche MAC) :

Le protocole inter-couche proposé se déclinent en trois phases: la vérification de la position de l'utilisateur, l'extraction du secret partagé de la couche physique et la dérivation de la clé partagée au niveau de la couche MAC.

- **Vérification de la position de l'utilisateur et de l'authenticité du point d'accès**

Lorsque le client se positionne sur une zone rouge, il reçoit des trames balises (beacons) chiffrés avec la clé publique (récupérée du certificat) partagée par tous les points d'accès appartenant à un aéroport par exemple. L'équipement est ainsi en mesure de vérifier la légitimité du point d'accès.

L'équipement envoie par la suite sa requête d'association au point d'accès. Ensuite, le capteur de mouvement Wi-Fi, qui se trouve au niveau de la zone rouge et ayant un faisceau très étroit centré sur l'utilisateur, reçoit ce paquet et l'envoie chiffré avec sa clé partagée avec le point d'accès. Ainsi, le point d'accès s'assure du fait que la demande d'association qu'il a reçu provient bien de l'utilisateur placé sur une des zones rouges.

- **Extraction du secret partagé de la couche physique**

Dans notre proposition, le canal physique joue le rôle d'un canal hors-bande sécurisé. Nous avons choisi la méthode de Li et al. [81] pour l'extraction du secret partagé de la couche physique qui consiste à extraire le secret partagé à partir de l'estimation de l'état du canal qu'on note $K_{lien\_physique}$. En effet, cette méthode est selon nous la plus simple proposée afin de partager un secret entre A et B. Comme A et B pourraient avoir des estimations du canal légèrement différentes, toutes les données chiffrées par $K_{lien\_physique}$ doit être traité par un code correcteur

d'erreur [14] avant leurs envois [46]. Pour obtenir $K_{lien\_physique}$, A et B estiment l'état du canal et obtiennent approximativement la même valeur (vu que l'estimation de l'état du canal peut différer de très peu selon que c'est A ou B qui la réalise). Puis, ils convertissent les valeurs obtenues en une représentation binaire à l'aide d'un processus de quantification obtenant ainsi approximativement la même valeur de $K_{lien\_physique}$.

- **La dérivation de la clé partagée au niveau de la couche MAC**

Nous utilisons la syntaxe suivante pour décrire les messages échangés au niveau MAC: le point d'accès PA et l'équipement de l'utilisateur sont désignés respectivement par A et B.

MAC_x	Adresse MAC de X
K_{xy}	Secret partagé entre X et Y
H (M)	Hachage du message M
{M}_K	Message M chiffré par la clef K
N_A	Nombre aléatoire généré par X
M.N	M concaténé à N
HMAC (M, k)	calculé en utilisant une fonction de hachage cryptographique en combinaison avec une clé secrète.

Tableau 1: Syntaxe adoptée

[14] Un code correcteur d'erreur est un système consistant dans l'ajout de données redondantes, ou de données de parité, à un message, de sorte qu'il peut être récupéré par un récepteur, même si un certain nombre d'erreurs ont été introduits, soit pendant le processus de transmission, ou suite au processus de stockage.

Les messages échangés sont comme suit:

A->B: $MAC_{A.}K_A$. HMAC ($K_{lien\_physique}$, K_A)

B-> A: MAC_B. $K_{B.}$HMAC ($K_{lien\_physique}$, K_B). $\{N_B\}\_ TK_{AB}$

A->B: MAC_A. $\{N_{A.}N_B\}\_ TK_{AB}$

B-> A: MAC_B. $\{N_A\}\_ TK_{AB}$

Puis A et B calculent $PK_{AB} = H (N_{A.}N_B, TK_{AB})$

Dans le message 1, l'équipement A envoie son adresse MAC, sa clé publique ainsi que le HMAC de la clé $K_{lien\_physique}$ et de sa clé publique. Le point d'accès B vérifie l'authenticité de la clé K_A à partir de la valeur HMAC ($K_{lien\_physique}$, K_A) reçue de l'équipement et de la clé $K_{lien\_physique}$ qu'il a en sa possession. En effet, il calcule de HMAC de K_A avec la valeur $K_{lien\_physique}$ et compare la valeur obtenue avec la valeur reçue. Ensuite, il calcule une clé partagée intermédiaire TK_{AB} ($K_B^{S_B}$ mod p) avec le paradigme de « Diffie Hellman » puis il génère un nombre aléatoire $N_{B.}$ Il envoie par la suite son adresse MAC, sa clé publique, son certificat, le HMAC de la clé $K_{lien\_physique}$ et de sa clé publique ainsi que le nombre aléatoire N_B chiffré par la clé TK_{AB}. L'équipement A récupère le nombre aléatoire N_B en utilisant sa clé $TK_{AB,}$ génère un nombre aléatoire N_A et envoie à A son adresse MAC ainsi que le résultat du chiffrement par la clé TK_{AB} des deux valeurs N_A et N_B.

Par la suite, A et B calcule $PK_{AB} = H (N_{A.}N_B, TK_{AB})$

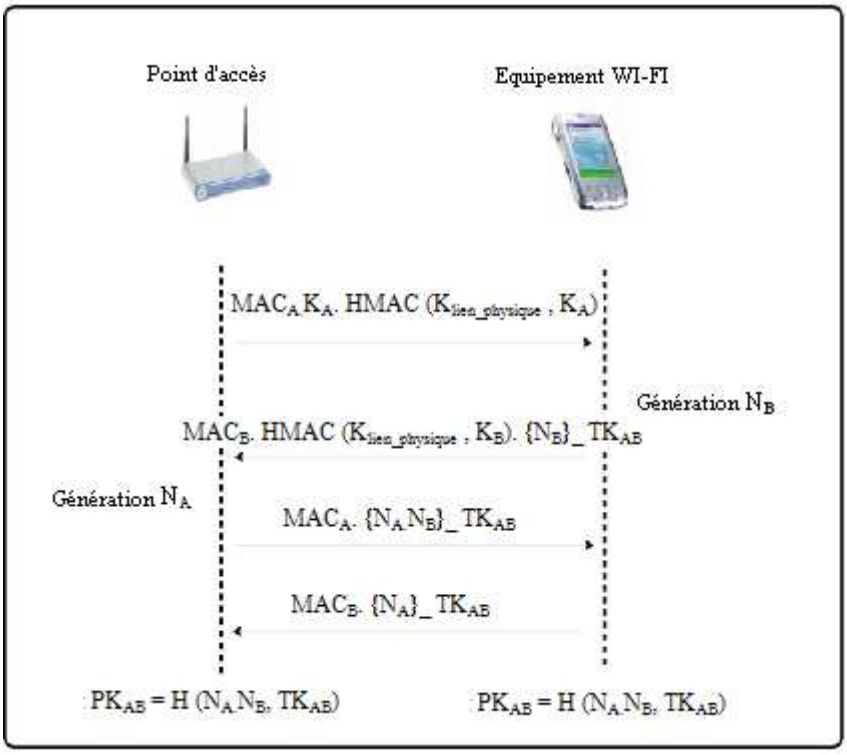


Figure 11: Illustration du protocole

2.2.4 Validation formelle

Dans cette section, nous validons formellement notre protocole grâce à l'outil AVISPA [64] qui est un analyseur de protocole de sécurité. Nous avons employé le modèle d'attaquant « Dolev-Yao » [44] représentant un attaquant qui peut écouter, intercepter, synthétiser un message et qui est seulement limité par les contraintes des méthodes cryptographiques utilisées. Nous avons également utilisé OFMC non seulement pour la détection rapide des attaques, mais aussi pour la vérification d'un nombre borné de sessions et ce sans limite sur le nombre qu'un attaquant peut générer [16]. Le code HLPSL correspondant est explicité dans l'annexe. Le code HSPSL décrit 4 types de rôle: « initiator » (correspondant au client A), « responder » (correspondant au client B), « session » (correspondant à la session entre A et B) et le rôle « environment ». Le rôle environnement décrit

trois sessions simultanées. La première est une session typique avec des agents légitimes A et B. La deuxième et la troisième session sont celles où l'intrus usurpe respectivement l'identité de A et B. Le résultat est que les objectifs de sécurité après le processus de validation sont atteints et que le protocole est sûr (pas d'attaques recensées). Ces objectifs étant l'authentification forte entre les deux équipements et la confidentialité des nombres aléatoires qu'ils ont échangés.

Notons que OFMC été exécuté avec succès avec l'option anti-replay, ce qui signifie que, même si l'attaquant a observé plusieurs instances de ce protocole, il reste dans l'incapacité de rejouer ou de falsifier des messages et de compromettre les objectifs de sécurité mentionnés ci-dessus.

2.2.5 Description de l'implémentation d'un « prototype »

Nous avons utilisé dans le cadre de cette implémentation des messages EAP over LAN sans fil (EAPoW) entre deux ordinateurs portables tournant sous Linux. Pour ce faire, nous avons adapté le logiciel Xsupplicant [69], qui est un client IEEE 802.1X léger et open-source afin d'encapsuler les messages du protocole dans les messages EAP. Nous avons également utilisé les librairies « Openssl » suivantes: une de cryptographie générale et une implémentant le protocole SSL [78]. Afin d'exécuter ce protocole dans la tablette Internet Nokia 770, nous avons eu recours à Scratchbox [67]. Scratchbox est un environnement de configuration et de compilation pour le développement de logiciels. L'idée de base dans Scratchbox est d'offrir aux développeurs un environnement qui fonctionne et qui ressemble à l'environnement cible avant que l'environnement cible soit disponible. La procédure complète prend presque 50 ms. Nous avons utilisé les paramètres suivants:

Taille du nombre aléatoire	32 bits

Type de chiffrement	AES-CBC-128
Fonction de hachage	SHA-1
Taille de PK_{AB}	128 bits

Tableau 2: Paramètres utilisés

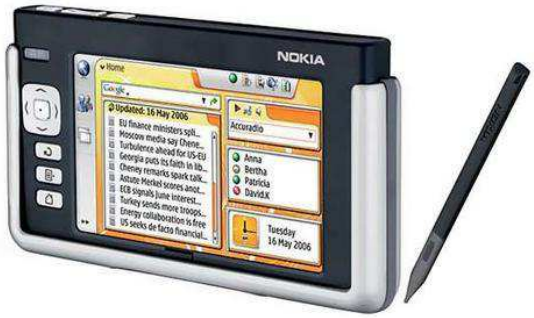


Figure 12: Illustration d'un NOKIA N770

2.3 Accès d'un équipement personnel depuis un lieu privé

Les fournisseurs de services Internet peuvent profiter du paradigme de réseau personnel pour jouer le rôle de fournisseur de services centrés sur l'internaute. Le FSI peut ainsi proposer une offre de mécanismes de protection contre l'usurpation d'identité pour la mise en place et le fonctionnement des RP.

Certaines des normes sans fil relatives à la connectivité personnelle locale fournissent leurs propres mécanismes pour établir des associations de sécurité en se fondant sur des canaux hors-bande.

2.3.1 Les modèles d'association « Wireless USB »

Les modèles d'association sont au cœur de la proposition du consortium « Wireless Universal Serial Bus » [68], qui indique que le mécanisme d'appairage peut être réalisé soit par le biais d'une connexion matériel soit par l'utilisateur qui agit comme un canal hors bande en entrant un numéro.

Les modèles d'association « Wireless USB » ciblent des scénarios d'usage à courte portée et se déclinent en deux modèles :

- modèle avec câble
- modèle numérique.

Le modèle avec câble utilise une liaison filaire USB comme canal hors bande pour transmettre une clé, tandis que le modèle numérique nécessite l'intervention de l'utilisateur pour vérifier visuellement des valeurs numériques et les valider en cas de correspondance.

2.3.2 Le mécanisme « Wireless Protected Setup » (WPS)

Le mécanisme « Wireless Protected Setup (WPS) » [76] vise à contrôler l'accès d'un dispositif donné dans un réseau local personnel sans fil et ce au niveau de la couche MAC. WPS définit un modèle logique au-dessus des entités classiques du Wi-Fi et ce pour sécuriser les réseaux personnels sans fil. Dans ce modèle, trois entités sont définies comme suit:

Contrôleur	Un équipement qui a le pouvoir dans le réseau local sans fil de fournir et de révoquer les jetons. Il peut être situé dans le point d'accès ou dans toute autre station sans fil.
Enrôlé	Un équipement qui vise à rejoindre le réseau personnel sans fil.
Authentificateur	Un point d'accès qui relaye les messages WPS entre un contrôleur et un enrôlé.

WPS exige l'identification des capacités des deux parties, nécessaire pour dérouler le protocole initié par l'utilisateur. Les valeurs des champs des messages du protocole dépendront des capacités et des méthodes de configuration. Trois méthodes sont prises en charge: « in-band », « hors-bande », et les configurations « push-button ». Le modèle « in-band » oblige l'utilisateur à saisir une

clé qui servira à authentifier un échange de clés Diffie-Hellman entre l'enrôlé et le contrôleur. Le protocole ressemble à MANA III [13] et permet l'utilisation de clés USB pour transmettre la clé d'authentification. Le modèle « hors-bande » définit trois scénarios possibles, la plus intéressante implique l'existence d'interfaces NFC[15] sur les deux appareils et ne nécessite aucune communication en bande. Enfin, la configuration « push-button » est essentiellement basée sur l'utilisateur et repose sur un échange de clé effectué par l'utilisateur et non authentifié. L'enrôlé cherche des points d'accès correctement configuré, et le protocole est déroulé seulement si le contrôleur est sollicité par un enrôlé. Notons que la méthode « push-button » est la plus conviviale. Toutefois, les modèles hors-bande restent les plus sûrs parce qu'ils fournissent un canal hors-bande protégé.

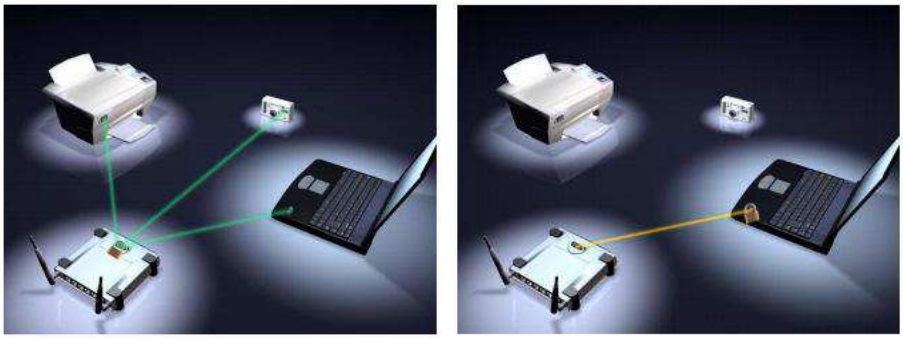


Figure 13: Illustrations du mécanisme "Wireless Protected setup"

2.4 Présentation du protocole Elliptic Curve Diffie-Hellman (ECDH)

Elliptic Curve Diffie-Hellman (ECDH) est un protocole de partage de secret qui permet à deux parties, chacune ayant préalablement une paire de clés (nécessaire pour l'authentification seulement), d'établir un secret partagé via un canal sécurisé [30]. Ce secret partagé peut être directement utilisé comme une clé, ou mieux encore, pour dériver une autre clé qui peut ensuite être utilisée

15 Le NFC est une technologie de communication sans-fil à courte portée et haute fréquence, permettant l'échange d'informations entre des périphériques sur une distance allant jusqu'à environ 10 cm

pour chiffrer les communications ultérieures en utilisant un chiffrement à clé symétrique. Il s'agit d'une variante du protocole « Diffie-Hellman » utilisant la cryptographie à courbe elliptique. Le protocole est sécurisé parce que rien n'est divulgué – sauf pour les clés publiques - et aucune partie ne peut déduire la clé privée de l'autre, sauf si elle peut résoudre le problème du logarithme discret des courbes elliptiques qui reste irrésolue à l'heure actuelle. Soit (d_A, Q_A) la paire de clés de A et (d_B, Q_B) la paire de clés de B.

Les étapes du protocole ECDH sont comme suit :

1. A calcule $(x_k,y_k) = d_A Q_B$.
2. B calcule $(x_k,y_k) = d_B Q_A$

La clé partagée est x_k vu que $d_A.Q_B = d_A d_B G = d_B d_A G = d_B Q_A$

2.5 Solution proposée

- Description:

Dans notre proposition, les nœuds au sein du réseau se décomposent en nœuds contrôleurs de sites de réseaux personnels qu'on nommera Contrôleurs Locaux de Réseaux Personnels (CLRP) et en nœuds contrôlés. Nous proposons un mécanisme comportant deux phases. Durant la première phase, chacun des contrôleurs remet des certificats à ses nœuds selon un mécanisme basé sur les canaux hors bande. Dans la seconde phase, chacun des nœuds dérivent des clés bilatérales avec les nœuds avec lesquels ils souhaitent communiquer et ce avec l'aide de l'utilisateur. Nous allons également proposer un mécanisme de protection contre l'usurpation d'identité pour les communications entre nœuds de sites distants appartenant au même RP ainsi qu'un mécanisme de protection contre l'usurpation d'identité pour la communication avec le fournisseur de services personnels.

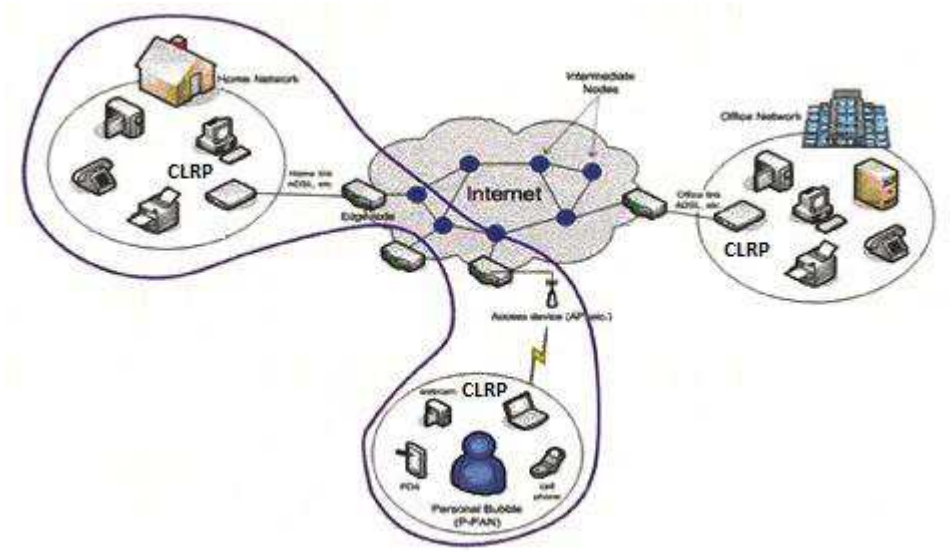


Figure 14 : Positionnement des CLRP au sein du réseau personnel

- Distribution sécurisée de certificats:

Nous préconisons dans le cadre de cette proposition la mise en place d'une autorité de certification au niveau du RP. Nos choix de paramètres et de fonctionnalités requièrent peu de ressources de calcul et de stockage.

La distribution sécurisée des certificats se fera en utilisant les canaux hors-bande. Les canaux hors-bande se déclinent en deux types : privé et public. Un exemple typique d'un canal hors-bande privé est réalisé par un utilisateur qui lit une chaine alphanumérique affichée par un équipement pour la recopier dans un autre équipement à l'aide d'un clavier. De ce fait, la longueur de la chaine alphanumérique doit correspondre à 4/5 caractères donc à 32/40 bits. En effet, les utilisateurs n'adopteront pas la solution s'il leur faut recopier de longues chaines de caractères. Les tags RFID et les communications infrarouges sont des exemples de canaux publics. Le protocole doit prévoir au moins 160 bits d'informations à transférer. On préconise également l'utilisation d'un PIN (stocké dans une puce électronique) pour lancer les opérations en attendant la démocratisation de

l'utilisation des outils biométriques tel qu'une clé USB contenant un lecteur d'empreinte digitale qui permettra d'assurer un plus haut niveau de sécurité.

Pendant l'initialisation, le contrôleur local du réseau personnel CLRP sélectionne une courbe elliptique et ensuite demande à l'utilisateur de rentrer un PIN de son choix. Le CLRP applique une fonction F1 à sens unique sur ce PIN et stocke le résultat FPIN. L'utilisateur doit entrer le PIN à chaque utilisation du CLRP et le CLRP est bloqué au bout de 3 essais infructueux. Ce procédé permet de s'assurer que le CLRP est lancé par l'utilisateur légitime.

Nous proposons deux méthodes de distribution sécurisée de certificats selon la nature du canal hors-bande (privé ou public).

- **Distribution sécurisée de certificats basée sur un canal hors-bande privé:**

Dans le cadre de ce type de distribution, un nouvel équipement E de l'utilisateur demande un certificat au CLRP en lui envoyant son identifiant et son adresse MAC. Le CLRP lui envoie alors les paramètres de la courbe elliptique et E lui renvoie sa clé publique. Le CLRP invite ensuite l'utilisateur à entrer les informations correspondantes au nouvel équipement. Ensuite, le CLRP envoie au nouvel équipement E sa clé publique et le certificat correspondant aux informations données par l'utilisateur sur E.

E->CLRP : $ID_E|MAC_E$

CLRP->E: param_courbe_elliptique

E->CLRP : K^E_{PUB}

CLRP->E : $K^{EC}_{PUB}|\ Cert_E$

Le CLRP génère par la suite une clé K et le HMAC du certificat à l'aide de la valeur K et l'affiche avec la valeur stockée K sous la forme : **K, HMAC (K, $Cert_E$)**

Les longueurs de K et le résultat de la fonction de HMAC doivent être assez raisonnable pour être transféré par l'utilisateur sur le canal hors-bande privé. Cela veut dire que le résultat du HMAC doit être réduit à 4 caractères. Il est possible à cette fin de garder les 32 bits les moins significatifs, de les convertir à un entier puis de prendre les 4 bits les moins significatifs.

Il y a deux scenarios possibles d'utilisation qui dépendent de la nature des interfaces disponibles.

Le CLRP a un afficheur et un clavier : si l'équipement E a un clavier alors les valeurs K et le MAC réduit sont affichées par le CLRP en vue d'être saisies sur E. L'équipement E utilise la clé K pour calculer le HMAC du certificat, réduit le HMAC puis compare le résultat avec la valeur reçue.

Si les deux valeurs ne correspondent pas, il émet un bip sonore à l'utilisateur pour qu'il rejette cette association et 2 bips dans le cas contraire. L'utilisateur saisit ensuite le résultat (oui ou non) sur le CLRP.

Le second scénario correspond au cas de figure où l'équipement et le CLRP ont des afficheurs. Dans ce cas, le CLRP envoie une clé K sur le canal non sécurisée à l'équipement, puis les deux équipements affichent K et le MAC réduit (8 caractères) à l'utilisateur qui va les comparer et qui indique à l'équipement et au CLRP le résultat de la comparaison.

- **Distribution sécurisée de certificats basée sur un canal hors-bande public:**

Dans le cadre de ce type de distribution, un nouvel équipement de l'utilisateur E demande un certificat au CLRP en lui envoyant son identifiant et son adresse MAC. Le CLRP lui envoie alors les paramètres de la courbe elliptique et E lui renvoie sa clé publique. Le CLRP invite ensuite l'utilisateur à entrer les informations correspondantes au nouvel équipement. Ensuite, le CLRP envoie au nouvel

équipement E sa clé publique et le certificat correspondant aux informations données par l'utilisateur sur E.

E->CLRP : $ID_E|MAC_E$

CLRP->E: param_courbe_elliptique

E->CLRP : K^E_{PUB}

CLRP->E : $K^{EC}_{PUB}|$ $Cert_E$

Ensuite, le CLRP applique la fonction HMAC sur le certificat et l'envoie à E sur le PAC public.

CLRP->E: K, HMAC (K, $Cert_E$)

Comme le canal hors bande public ne garantit que l'intégrité et l'authenticité, un attaquant peut soit bloquer les messages afin d'empêcher l'achèvement de la phase d'obtention du certificat soit remplacer la clé par une autre clé pour usurper l'identité du CLRP. Le remplacement ne reste indétectable que si la valeur de hachage reste la même. Toutefois, si la fonction de hachage est résistante à la collision, la probabilité d'usurpation d'identité est négligeable. Par ailleurs, le blocage des messages peut être détecté par l'expiration d'un « timeout » assigné à l'opération d'attribution de certificat. L'expiration de ce « timeout » enclenchera l'envoie d'une alerte à l'utilisateur.

- Appariement entre les équipements contrôlés et le CLRP et entre les différents équipements:

- **Phase 1:**

Cette procédure nécessite la communication par clavier avec le CLRP et dépend de la nature des interfaces des deux équipements E_A et E_B souhaitant dérivant une clé. Si les deux ont un clavier, alors l'utilisateur entre le PIN sur les deux équipements. Si aucun des équipements n'a de clavier, alors :

E_A->CLRP: $Cert_{EA}$

E_B->CLRP: $Cert_{Eb}$

L'utilisateur est alors invité à entrer le PIN sur le CLRP. Au bout de 3 essais infructueux, le CLRP est bloqué et la procédure s'arrête.

Si le PIN est correct:

CLRP-> E_B : $Cert_{EA}$

CLRP-> E_A: $Cert_{EB}$

- **Phase 2:**

Comme le protocole de partage de clés ECDH n'assure pas la propriété de « Perfect Forward Secrecy »[16], nous proposons les messages suivants pour générer une clé de session K_{AB} :

- E_A->E_B : ID_{EA}.[N_A] _(K)
- E_B->E_A : ID_{EB}.[N_B]_ (K)
- E_A->E_B : [N_B]_ (K)

Le secret partagé est K_{AB}= H (N_A, N_B, K)

A envoie son identifiant ainsi qu'un nombre aléatoire N_A chiffré par la clé K résultante du déroulement du protocole ECDH (vu que A possède la clé publique de B suite à la phase 1). A la réception de ce message, *B* envoie son identifiant ainsi qu'un nombre aléatoire N_B chiffré par la clé K. Ensuite, A renvoie N_B chiffré par la clé K. A et B calculent alors le secret partagé K_{AB}= H (N_A, N_B, K).

- <u>Le contact entre tous les composants du même RP ainsi qu'avec le FSI :</u>

Chaque CLRP envoie son adresse publique au serveur DNS et le protocole Dynamic DNS[17] veille à la mise à jour de l'adresse IP lors d'éventuels changements. Lors de l'établissement de la sécurité entre les CLRPs des différents PAN

---

16 PFS est la propriété qui assure qu'une clé de session dérivée d'un ensemble de paires de clé de long terme ne sera pas compromise même si la clé privée de long terme a été compromise

17 « Dynamic DNS » permet à des utilisateurs qui utilisent une adresse IP dynamique de disposer quand même d'un nom de domaine.

composant le RP, l'utilisateur entre son PIN pour démarrer la procédure. Chacun des CLRP cherche la clé publique de l'autre grâce à DNSSEC+ détaillé plu tard dans ce manuscrit et dérivent une clé partagée comme spécifié ci-dessus. Notons que les CLRP jouent le rôle de relais de confiance entre les équipements situés sur des sites distants.

Chacun des CLRP doit partager une clé avec le fournisseur de services personnels. L'accord des clients est sollicité au moyen de SMS par exemple sur leur PDA. Le client est ainsi invité à indiquer s'il est d'accord ou pas pour les opérations demandées par le CLRP.

- **Analyse de sécurité :**

Nous allons dans cette section analyser le rôle du CLRP ainsi que le mécanisme de révocation.

- Analyse du rôle du CLRP :

Même si le CLRP joue un rôle important pour la gestion des clés au sein du RP, il ne peut toutefois pas rajouter/révoquer des équipements sans l'aval de l'utilisateur. Il joue juste le rôle de relai et il ne peut donc pas initier de demande de sécurisation d'équipements. Si le CLRP venait à être hors service, on a juste besoin de la paire de clés de signature pour installer le CLRP sur un autre équipement. De plus, même si le CLRP est volé, il ne peut pas rajouter ou révoquer sans l'approbation de l'utilisateur légitime.

- Révocation

Dans le cadre de notre proposition, un équipement ne peut pas usurper l'identité d'un autre car les opérations d'attribution de certificats ainsi que les opérations d'appariement impliquent l'intervention de l'utilisateur qui est en mesure de reconnaitre l'équipement légitime. Ainsi, l'opération de révocation concerne uniquement la phase de retrait d'un équipement E du RP pour son remplacement par

exemple. L'utilisateur demande alors au CLRP de révoquer l'équipement qui va donc envoyer à chacun des équipements des notifications de révocation de l'équipement E chiffrées chacune avec la clé partagée entre l'équipement et le CLRP.

2.6 Cas particulier des MBAN

2.6.1 Introduction

Le paradigme des réseaux médicaux (MBAN) [62] réfère à une collection de nœuds de capteurs avec des antennes et des capacités de calcul limitées destinée à des applications médicales. Les capteurs MBAN sont soit collés soit incorporés sur le corps d'un patient. Le MBAN est donc un nouveau champ d'application pour les réseaux de capteurs. Il permet la réalisation dans le monde réel de concepts tels que l'informatique ubiquitaire. Parmi les projets dédiés à l'utilisation de capteurs sans fil à des fins médicales, on peut évoquer "CodeBlue" de l'Université Harvard. Ils ont ainsi développé des capteurs de signaux vitaux et une infrastructure logicielle évolutive pour les dispositifs médicaux sans fil. La sécurité des MBAN reste un domaine à explorer au vue du peu d'efforts de recherche ont peu abordé cette question.

Les capteurs sans fil de MBAN mesurent, collectent et envoient les données des signaux vitaux des patients à une entité, appelée serveur personnel (SP), qui peut être hébergé dans un assistant numérique personnel du patient comme par exemple son PDA.

Les données de signaux vitaux circulant dans les MBAN sont par nature critiques. Il faut donc s'assurer qu'un capteur non légitime ne puisse pas usurper l'identité d'un équipement légitime et véhiculer des données erronées.

Ainsi, il faut s'assurer que les capteurs qui communiquent avec le serveur personnel soient légitimes et attachés au corps du bon utilisateur.

L'utilisation de secrets pré-distribués n'est pas appropriée dans notre cas puisque nous souhaitons laisser la possibilité d'utilisation de capteurs de différents fabricants afin de maintenir le réseau aussi souple que possible. Cela signifie que les clés doivent être dérivées sans secret partagé au préalable entre les capteurs du MBAN.

Dans cette section, nous nous proposons de dériver des clés bilatérales entre certains capteurs du MBAN ainsi qu'entre chaque capteur du MBAN et le SP. Ainsi, les capteurs non légitimes ne peuvent pas usurper l'identité d'un équipement légitime et véhiculer des données erronées car ils n'ont pas le matériel cryptographique approprié. Cette procédure doit être réalisée en respectant les capacités limitées en termes de calcul et d'énergie des équipements du MBAN.

La section 2.5.2 passe en revue l'état de l'art en termes de sécurité de réseaux médicaux. La section 2.5.3 présente notre solution et la section 2.5.4 présente l'analyse de sécurité de notre solution. La section 2.5.5 présente par la suite son évaluation.

2.6.2 Etat de l'art

Cherukuri et al. [58] ont proposé une approche basée sur la biométrie pour sécuriser la communication dans un réseau sans fil de capteurs implantés dans le corps humain. Si un capteur souhaite envoyer des données à un autre, il génère une clé aléatoire nommé $K_{session}$ et chiffre les données avec cette clé. Puis, $K_{session}$ est protégée [4] par une autre clé, nommé K_{commit}, calculée à

partir des données biométriques mesurées à partir du corps. Par la suite, les données sont chiffrées et envoyées avec une valeur calculée à partir de K_{commit} et de la clé de session. A la réception du message, un capteur extrait la clé de session en utilisant son K_{commit} puis récupère les données. Ils suggèrent d'utiliser des clés pré-déployées pour communiquer avec le nœud du contrôleur qu'est le SP.

Bao et al. [60] décrivent une architecture de sécurité pour les réseaux de capteurs biomédicaux. Cette architecture se compose d'un nœud maître, qui est un capteur biomédical portable et de nœuds esclaves qui sont des biocapteurs implantés dans le corps humain. A la réception d'une indication de synchronisation à partir du nœud maître, les nœuds esclaves se partagent un secret partagé ASS (Auto-Shared Secret) à partir de valeurs extraites de données physiologiques recueillies simultanément pendant une certaine période de temps. Ensuite, le nœud maître utilise l'ASS dans le but de protéger la transmission d'une clé nommée K_{init} aux nœuds esclaves. K_{init} sera ensuite utilisée pour protéger la transmission des clés de session. Bao et al. [14] décrivent une étude de faisabilité de l'utilisation de caractéristiques intrinsèques d'un corps humain pour assurer la distribution de clés à des capteurs biomédicaux. Ces capteurs peuvent être soit portatifs soit implantés dans le corps. Ils utilisent l'intervalle entre les impulsions comme une caractéristique biométrique pour la génération de l'ASS. La méthode a été testée sur 99 sujets avec 838 segments d'enregistrements simultanés de l'électrocardiogramme et d'autres mesures vitales. Le système atteint un taux minimum d'erreur totale de 2,58%. En fait, ils montrent une bonne similitude entre les identités (données physiologiques capturés par un nœud) dans le même MBAN. Ils ont également prouvé qu'il existe une grande différence entre les deux identités de deux nœuds de capteurs de MBANs différentes. Les résultats des analyses statistiques suggèrent que les

mesures en question sont des caractéristiques biométriques adaptées à l'authentification au sein des MBANs.

Malasri et al [39] ont proposé une architecture à clé publique et un protocole de sécurité pour atteindre les exigences de sécurité d'un réseau de capteurs biomédicaux. La pierre angulaire de cette proposition est l'utilisation des empreintes digitales de l'utilisateur. En effet, les biocapteurs génèrent un nombre aléatoire et une clé maîtresse dérivée de l'empreinte digitale du patient. Ensuite, ils échangent des messages avec la station de base en utilisant ces valeurs afin d'obtenir un secret partagé avec la station de base. Ils ont évalué leur protocole en utilisant la cryptographie à clé publique sur une plate-forme « Sky Moteiv's Tmote ». Cette solution présente des failles de sécurité car il est clair aujourd'hui que les empreintes digitales peuvent être reproduites assez facilement.

Seo et al [56] utilisent les algorithmes de courbes elliptiques Diffie-Hellman (ECDH) et de courbes elliptiques Digital Signature Algorithm (ECDSA) [34] afin de sécuriser la phase de l'installation de clés bilatérales et la phase d'authentification. Ils préconisent l'utilisation du TinySec[18] afin d'assurer l'authentification et la confidentialité des données échangées entre les capteurs. De plus, ils ont mis en œuvre leur protocole sur des Mote MICAz 8-bit et 7.3828 MHz. Leurs résultats expérimentaux montrent la faisabilité de leur protocole pour les nœuds de capteurs sans fil.

Plusieurs solutions ont été proposées afin de dériver des clés dans le cas d'une combinaison de dispositifs de faible et de grande puissance. Le paradigme des puzzles de Merkle [54] est la solution la plus crédible dans ce domaine. Le

[18] TinySec est une architecture de sécurité mise en œuvre au niveau de la couche de liaison pour les réseaux de capteurs sans fil

puzzle de Merkle est l'un des premiers protocoles d'échange de clés sans secret partagé au préalable. Ce paradigme est utilisé entre un dispositif avec une faible puissance noté ici par A et un appareil plus puissant dénoté ici par B. Donc le puzzle de Merkle semble être un bon candidat pour générer des clés entre les capteurs biomédicaux dans le MBAN et le serveur personnel qui est hébergé par exemple par le PDA. Un puzzle consiste en un identifiant aléatoire de puzzle, une clé aléatoire de chiffrement K et quelques informations redondantes.

Les puzzles sont chiffrés par une clé k qui est plus petit que K. Le dispositif B envoie N puzzles à l'appareil A. L'appareil A choisit au hasard un puzzle, récupère le texte brut du puzzle par une attaque en force brute qui est faisable puisque k est plus petite que K et informe B de l'identifiant du puzzle qu'il a choisi. Le dispositif B utilise l'ID reçue de l'appareil de A pour connaître la clé choisie par A. L'attaquant ici peut être plus puissant que le capteur biomédical et pourrait donc effectuer les mêmes calculs que celui-ci en beaucoup moins de temps. C'est pour cela que nous n'avons pas considéré ce protocole dans notre solution.

2.6.3 Solution proposée

Nous proposons une solution de sécurisation de réseaux médicaux simple à mettre en œuvre et qui est la seule à prendre en compte à notre connaissance à la fois la phase de déploiement ainsi que la phase d'usage des réseaux médicaux. Ce protocole a été présenté au groupe de travail IEEE 802.15.6 qui mène des travaux en vue de la normalisation de réseaux médicaux.

Les capteurs du MBAN ont des ressources de calcul limitées et n'ont pas d'affichage. Ils envoient des données vitales et doivent pourvoir communiquer entre

eux et avec le SP de l'utilisateur. Par ailleurs, ils peuvent être dérobés par un attaquant.

Le cas d'utilisation d'un réseau médical est illustré par la figure 15: plusieurs capteurs biomédicaux recueillent des données sur le corps d'un patient. Les données sont envoyées vers un PDA, agissant comme le SP. Les données sont ensuite transmises vers un hôpital distant.

Notre objectif dans le reste de la section est de protéger les nœuds du réseau de capteurs contre les attaques d'usurpation d'identité en leur fournissant des clés robustes pour leurs communications bilatérales ainsi qu'avec le SP. Dans notre solution, nous respectons les capacités de calcul des nœuds puisque nous utilisons la cryptographie asymétrique uniquement pour dériver les clés. De plus, nous utilisons la cryptographie à courbes elliptiques qui propose une cryptographie asymétrique avec une moindre charge de calcul et des tailles de clé plus petites pour un même niveau de protection que celles de la cryptographie asymétrique traditionnelle et donc convient pleinement à un protocole impliquant un réseau de capteurs. Comme nous devons également optimiser la consommation de la batterie, nous allons clustériser[19] le MBAN.

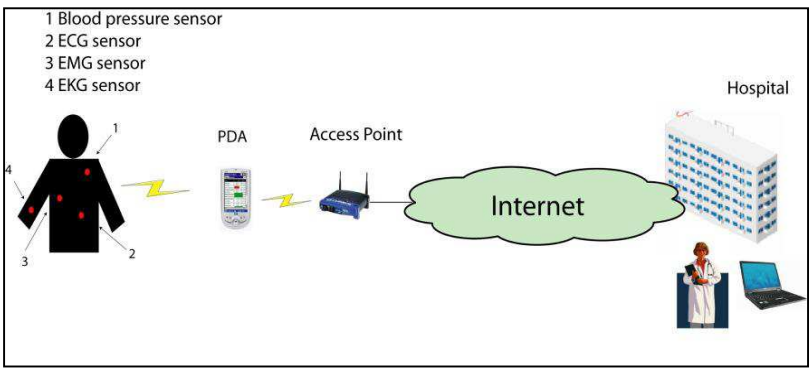


Figure 15: Cas d'utilisation des réseaux médicaux

19 Un cluster est un groupe de capteurs co-localisés qui délèguent à l'un d'eux, pour de courtes périodes de temps, la communication directe avec le serveur personnel.

Nous devons distinguer deux phases: la phase de déploiement et la phase d'usage. La phase de déploiement représente la phase où les capteurs biomédicaux sont placés sur le corps du patient. La phase d'usage commence au moment où se termine la phase de déploiement et correspond à la phase opérationnelle du MBAN. Dans les sections suivantes, nous allons décrire ces deux phases en détail.

- Phase de déploiement :

Nous supposons que le SP et un seul capteur S du MBAN ont une clé prépartagée. La phase de déploiement représente la phase où les capteurs biomédicaux sont fixés au corps d'un utilisateur et consiste en quatre étapes :

À l'étape 1, après la réception d'une indication de synchronisation à partir du SP, les nœuds de MBAN recueillent simultanément les données physiologiques du patient pendant une courte période de temps. Chaque nœud extrait ensuite des valeurs de ces données biométriques, afin d'obtenir la clé K_{BIO}. À l'étape 2, chaque nœud dérive une clé bilatérale avec le SP via S. À l'étape 3, nous proposons d'utiliser le processus sécurisé de formation de cluster décrit dans [41] afin d'organiser la MBAN en cluster. En fait, ils utilisent des valeurs physiologiques, afin d'assurer la sécurité du processus de la formation de clusters. À l'étape 4, les nœuds dérivent des clés bilatérales avec leurs chefs de cluster et le SP. La sécurité offerte par cette phase exige peu de participation de la part des utilisateurs.
La syntaxe utilisée est comme suit :

K_A	Clé publique de A
{M}_K	Message M Chiffré par la clé K
HMAC(M)	Fonction de HMAC sur message M
S	Secret

N_A	Nombre aléatoire généré par A

À l'étape 1, tous les capteurs du MBAN reçoivent une trame de synchronisation du SP afin de capturer les données physiologiques du patient et obtenir ainsi la clé K_{BIO}. La trame de synchronisation contient l'identité du SP et des informations concernant un paramètre de surveillance consistant en la périodicité de la capture des données physiologiques.

Le capteur biomédical S diffuse son secret s partagé avec SP ainsi que la clé publique de SP à l'aide de K_{BIO} aux autres capteurs biomédicaux. Ensuite, nous adoptons le même protocole de dérivation de clés proposé dans la première contribution de ce chapitre mais nous utilisons la cryptographie à courbe elliptique pour générer le secret intermédiaire afin d'optimiser l'utilisation des ressources de calcul des capteurs. Ainsi, les messages échangés entre le SP et un capteur biomédical A sont comme suit:

A -> SP: MAC_A. K_A. HMAC (K_A, s)

SP ->A: MAC_{SP}. K_{SP}. HMAC (K_{SP}, s). $\{N_{SP}\}_{\_K1}$

A -> SP: MAC_A. K_A. $\{N_A.N_{SP}\}_{\_K1}$

SP-> A: MAC_{SP}. $(N_A)_{K1}$

Par la suite, A et SP calculent HMAC(N_A.$N_{SP.}$ K_1).

Dans le message 1, l'équipement A envoie son adresse MAC, sa clé publique ainsi que le HMAC de sa clé publique avec le secret s. Le SP vérifie l'authenticité de la clé K_A en utilisant le secret s. Ensuite, il dérive une clé partagée intermédiaire K_1 puis il génère un nombre aléatoire $N_{SP.}$ Il envoie par la suite son adresse MAC, sa clé publique, le HMAC de sa clé publique avec le secret s ainsi que le nombre aléatoire N_{SP} chiffré par la clé K_1. L'équipement A récupère le nombre aléatoire N_{SP} en utilisant sa clé $K_{1,}$ génère un nombre aléatoire N_A et

envoie à SP son adresse MAC ainsi que le résultat du chiffrement par la clé K_1 des deux valeurs N_A et N_{SP}.

Par la suite, A et SP calculent H ($N_A.N_{SP}$, K_1).

Nous proposons par la suite d'organiser le MBAN en utilisant le processus sécurisé de formation de cluster décrit dans [39]. Puis, les capteurs biomédicaux utilisent les messages ci-dessus pour dériver les clés partagées avec leurs chefs de clusters.

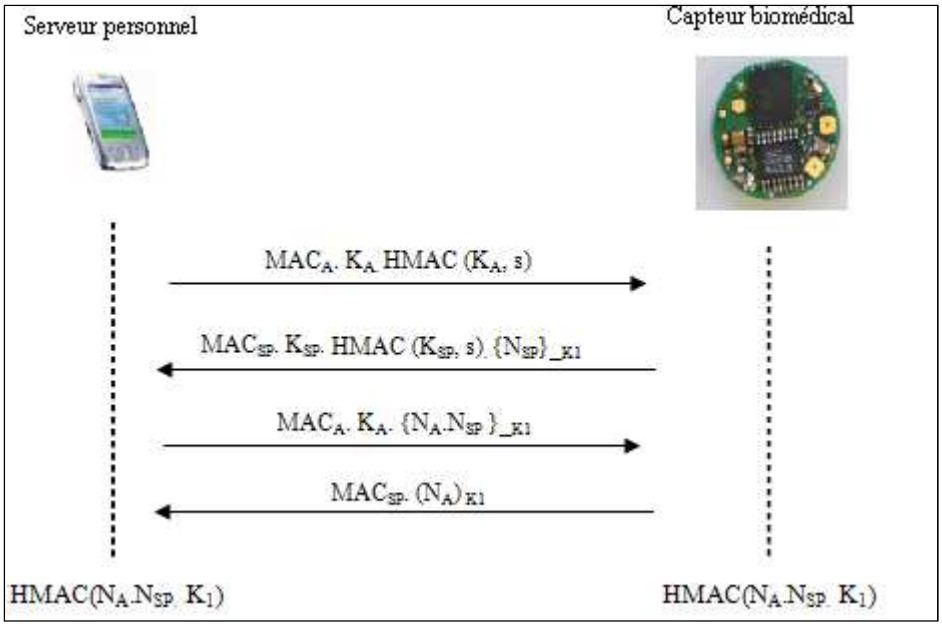


Figure 16: Illustration du protocole proposé

- Phase d'usage :

Lors de la phase d'usage du MBAN, le propriétaire du MBAN peut être amené à rajouter ou retirer un capteur biomédical. Il peut également avoir besoin de donner accès à ses capteurs biomédicaux à d'autres personnes, comme son médecin. Nous devons également assurer la sécurité au sein de chaque cluster et proposer des mécanismes permettant la détection et la révocation des nœuds compromis.

- Rajout et retrait de capteurs biomédicaux dans le MBAN :

Le propriétaire du MBAN peut avoir besoin d'ajouter un nouveau capteur biomédical pendant la phase d'utilisation, capteur désigné ici par S_N. L'utilisateur doit lancer le processus d'ajout dans le SP. S_N envoie à ses voisins S_{NJ} une demande de rajout chiffrée par K_{BIO}. Ensuite, S_N choisit au hasard un nœud S_{NJ}* entre les voisins qui lui ont répondu. Puis S_N envoie à la S_{NJ} * une demande de rajout. S_{NJ}* route la demande vers son chef de cluster auquel on réfèrera par la suite par CH qui la relaie au SP. Le SP va ensuite envoyer un secret au CH qui va le relayer au S_N chiffrée par $K_{BIO.}$ Le SP demande également au CH de rajouter S_N à son cluster. Ensuite, SP et S_N dérivent une clé partagée en se basant sur le protocole décrit dans la phase de déploiement.

Le retrait d'un capteur biomédical se fait au niveau du SP qui envoie un message de notification du retrait du capteur à tous les autres capteurs du réseau médical. Nous considérons également la mise hors service temporaire d'un capteur comme une opération de retrait. Sa remise en service impliquera ainsi une nouvelle opération de rajout.

- Octroi de l'accès à autrui :

Le propriétaire du MBAN peut être amené à donner l'accès à certains de ses capteurs biomédicaux à des personnes ayant sa confiance comme par exemple à son médecin. Donc, notre SP dérivera un secret avec l'équipement de la personne de confiance au moyen de mécanismes d'appairage comme celui décrit en [13]. Nous suggérons que la clé bilatérale doit être éphémère en raison de l'espace de stockage limité.

- Gestion de clés dans un cluster :

Chaque nœud du MBAN doit périodiquement rafraîchir la valeur K_{BIO} selon la périodicité spécifié par le SP. Chaque CH envoie périodiquement une clé commune à tous les membres de son cluster. Ainsi, chaque membre du cluster reçoit cette clé chiffrée par la clé bilatérale qu'il partage avec le CH. Les membres sont alors en mesure 1) de chiffrer leurs données avec la clé de paires partagées avec le SP puis 2) avec Kcluster_i puis d'envoyer le résultat au CH.

Afin d'optimiser la consommation d'énergie de tous les nœuds dans le MBAN, le CH changé périodiquement dans un cluster donné. La sélection du nouveau CH est hors de portée du présent document. Le CH actuel enverra l'identité du CH nouvellement élu au SP.

2.6.4 Analyse de sécurité

Notre solution est la première à adresser à notre connaissance la sécurisation de la phase de déploiement et d'usage des MBANs. Durant la phase d'usage, un adversaire peut ajouter un nœud malveillant sur le corps du patient afin d'envoyer des données erronées, mais ce nœud sera détecté comme un nœud non autorisé vu qu'il n'appartient à aucun cluster. En effet, rejoindre un groupe se fait soit dans la phase de déploiement soit à l'aide du SP dans la phase de rajout.

De plus, le vol d'un capteur biomédical et sa remise en service avec des données erronées sera détecté par le chef de cluster correspondant puisque les données qu'il envoie ne sont pas chiffrées avec le la clé courante Kcluster_i. De ce fait, un point d'attention particulier doit être porté sur la fréquence de changement de la clé Kcluster_i.

En outre, quand un adversaire vole un capteur qui joue le rôle de chef de cluster, le capteur sera détecté par le SP comme étant un capteur corrompu car ce nœud n'est pas en mesure de lui restituer les donnés sous la forme de concaténation des valeurs chiffrées des données vitales. Ceci est dû au fait que l'attaquant ne possède toutes les clés bilatérales des membres du MBAN avec le SP. Une alerte sera remontée à l'utilisateur en cas de détection d'un nœud corrompu.

2.6.5 Evaluation de la solution

Dans cette section, nous fournissons une évaluation de la performance en termes de temps de calcul. La longueur de clé utilisée ici est de 163 bits ce qui est la taille de clé recommandée par le NIST.

La génération du secret partagé intermédiaire est connue pour consommer 34,173 sec sur le MICA II 8-bits avec 7,38 Mhz CPU [19].

Figure 17: illustration d'un capteur MICAZ

Comme pour le chiffrement, nous avons trouvé 33,6 ms, 22,3 ms et 20 ms respectivement pour les messages 2, 3 et 4 illustrés dans la figure 16. La génération d'un nonce dans le nœud capteur prend presque 10ms.

Temps de génération du secret partagé intermédiaire	34,173 s
Temps de génération message 2	33,6 ms
Temps de génération message 3	22,3 ms
Temps de génération message 4	20 ms
Temps de génération d'un nonce	10ms

Tableau 3: Temps de calcul

Comme le temps de génération du secret partagé K_{ECDH} est prédominant, il faudra améliorer les performances de cette opération [56].

2.7 Conclusion

Dans ce chapitre, nous avons proposé trois mécanismes de protection contre l'usurpation d'identité: le premier troisième dédié à la connexion d'un équipement personnel depuis un lieu public, le second dédié aux réseaux personnels, le troisième dédié au cas particulier des réseaux médicaux.

Le mécanisme dédié à la connexion d'un équipement personnel depuis un lieu public consiste en un protocole inter-couche basé sur les principes de la théorie de l'information. Ce protocole résout la faille de sécurité non abordée dans la littérature qu'est l'attaque d'usurpation d'identité qui survient au début de la communication et protège donc les utilisateurs contre les attaques de type « homme au milieu ». Nous avons proposé que la personne qui désire avoir un accès sécurisé à Internet doit être sur un cercle spécifique qu'on a nommé « RED POINT » de telle façon que l'attaquant n'est pas en mesure d'être sur le même cercle au même moment. Le protocole inter-couche proposé se déclinent en trois phases: la phase de vérification de la position de l'utilisateur, la phase d'extraction du secret partagé de la couche physique et la dernière phase de la dérivation de la clé partagée au niveau de la couche MAC. Nous avons par la suite validé formellement notre solution grâce à l'outil AVISPA et présenté les résultats de son implémentation. Concernant le mécanisme dédié au réseau personnel, nous avons préconisé l'utilisation d'un protocole basé sur les canaux hors bande en vue d'attribuer des certificats aux nœuds du réseau personnel. Nous avons par la suite proposé la dérivation de clés bilatérales entre les équipements du réseau personnel du même site ainsi qu'entre des équipements sur des sites distants.

Concernant le cas particulier des réseaux médicaux, nous avons proposé de couvrir les phases de déploiement et d'utilisation des MBANs. Le protocole proposé exige peu de participation de la part des utilisateurs et respecte les capacités limitées de calculs de nœuds de capteurs.

CHAPITRE 3

3 Mécanismes de protection contre l'usurpation d'identité pour les réseaux de cœur utilisés par les fournisseurs de services Internet

3.1 Introduction

Les contributions de ce chapitre ont été effectuées dans le cadre du projet ANR ESTER. Ce projet vise à démontrer la faisabilité d'une approche basée sur l'intégration de cartes à puces au sein des nœuds de réseaux agissant ainsi comme un coffre-fort électronique. Cette solution assure un environnement de confiance pour la génération et la protection des clés cryptographiques, la signature des messages en vue de leur authentification mais aussi la protection des éléments sensibles du nœud (par exemple tables de routage). Cette approche permet également des avancées en vue de la résilience des réseaux, car les cartes à puces en protégeant les éléments de contrôle et de gestion du réseau permettront de se protéger contre des attaques visant à détruire et falsifier des éléments vitaux au fonctionnement du réseau.

Les fournisseurs d'accès Internet comptent sur l'infrastructure de routage pour acheminer les paquets de ses clients. Le rôle-clé d'une infrastructure de routage est de permettre à un expéditeur de trouver un chemin valide vers une destination aussi longtemps qu'un tel chemin existe. Ainsi, l'infrastructure de routage doit fournir un transfert sécurisé de données, même si certaines parties sont sous contrôle d'un attaquant. En effet, les attaques d'usurpation d'identité peuvent conduire à l'acheminement des paquets vers des destinataires non légitimes ou au déni de service. Il est donc essentiel de prémunir les infrastructures de routage contre les attaques d'usurpation d'identité. Le routage est effectué à deux niveaux, inter-domaine; généralement grâce au protocole BGP et intra-domaine; OSPF.

Les internautes ainsi que les entreprises raccordées aux réseaux des FSIs sont également vulnérables aux attaques d'usurpation d'identité. Ainsi, des attaquants peuvent utiliser cette technique en vue de réaliser des attaques de type déni de services. Le FSI se doit donc d'octroyer à ses clients des adresses IP dont l'usurpation peut être détectée, neutralisée et tracée. L'attribution des adresses IP se fait lors de la connexion du client au FSI. Il est donc crucial de repenser le mécanisme d'octroi des adresses IP chez le FSI.

Nous proposons dans la section 3.2 un mécanisme de protection contre l'usurpation d'identité pour le protocole de routage BGP. Nous proposons par la suite dans la section 3.3 un mécanisme de protection contre l'usurpation d'identité pour le protocole de routage OSPF. Ensuite, nous proposons dans la section 3.4 un mécanisme de protection contre l'usurpation des adresses IP des clients abonnés à un fournisseur de services Internet et nous concluons ce chapitre dans la section 3.5.

3.2 T-BGP

Dans cette section, nous présentons un nouveau mécanisme de protection contre l'usurpation d'identité pour le protocole de routage BGP.

3.2.1 Introduction

L'infrastructure de routage de l'Internet se compose d'un certain nombre de systèmes autonomes (AS), dont chacun se compose d'un certain nombre de routeurs sous le contrôle d'une administration unique (partage de la même politique de routage). BGP [51] est le protocole de routage standard IETF d'échange d'informations sur l'accessibilité des AS sur l'Internet. Un système autonome annonce ses préfixes IP[20] via BGP à ses AS voisins directs, qui vont

[20] Un préfixe IP identifie chaque destination de la couche réseau

les propager à leurs AS voisins. Ces annonces permettent de construire des routes pour le trafic à destination des adresses dans la plage d'adresses spécifiées par les préfixes. Un AS malveillant peut envoyer des annonces erronées au moyen de messages BGP UPDATE. Ainsi, il peut annoncer un préfixe appartenant à un autre AS et prétendre qu'il est le sien. Ce processus est appelé détournement de préfixe. Nous proposons un nouveau mécanisme de sécurité empêchant l'usurpation d'identité d'un routeur BGP. Pour ce faire, nous proposons une architecture simple qui ne requiert ni changements dans les messages BGP, ni d'énormes ressources de calcul au niveau des routeurs. De plus, ce mécanisme assure la validité du chemin et la disponibilité pour le protocole BGP.

La section 3.2.2 passe en revue les vulnérabilités du protocole BGP et la section 3.2.3 décrit les mécanismes de sécurité proposés dans la littérature. La section 3.2.4 présente les mécanismes cryptographiques que nous allons utiliser dans notre solution décrite dans la section 3.2.5. L'analyse de sécurité de cette solution ainsi qu'une comparaison avec d'autres mécanismes de sécurité sont explicitées dans la section 3.2.6.

3.2.2 Vulnérabilités du protocole BGP

Le protocole BGP est vulnérable aux attaques sur le détournement de préfixes et aux attaques sur l'attribut AS-PATH[21] et ce comme suit :

- Attaques sur l'AS-PATH

Dans les scénarios suivants, l'hypothèse est que l'attaquant a réussi à prendre le contrôle complet d'un ou de plusieurs routeurs BGP dans Internet. Cela peut être accompli par divers moyens, par exemple avec des sniffers de mot de

[21] L'attribut AS-PATH correspond à la concaténation des numéros d'AS qu'a traversé le paquet BGP avec le numéro d'AS du domaine source et permet d'éviter les boucles.

passe, par l'exploitation de failles d'implémentation dans les protocoles d'administration du routeur ou soit par le vol de mot de passe de l'opérateur de réseau.

La figure 18 permet d'illustrer les différentes attaques sur l'AS-PATH [1].

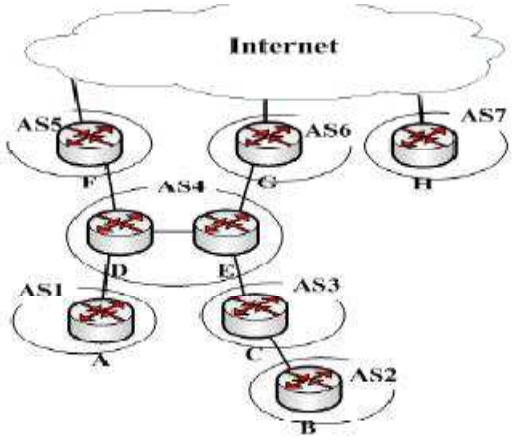


Figure 18: Illustration des attaques de modification de l'AS-PATH

Ces attaques peuvent être divisées en trois types:

- **L'attaque par raccourcissement de l'AS-PATH :** Supposons que le routeur G veut manipuler le trafic destiné à AS_2. Il envoie un itinéraire raccourci {AS_6, AS_2} annonçant qu'il a un lien direct vers AS_2. Le trafic destiné à AS_2 et provenant de AS_1 peut passer par G parce que les chemins corrects et manipulés de l'AS-PATH ont la même longueur. Toutefois, les trafics venus d'autres parties de l'Internet doivent passer par G parce que l'AS-PATH annoncé par le routeur compromis G est le plus court.
- **L'attaque par allongement de l'AS-PATH :** Supposons que le routeur D soit compromis, qu'il veuille amener tous les AS à utiliser le lien G-E pour le congestionner et qu'il veuille rendre le lien F-D inactif. A cette fin, D doit concaténer des numéros d'AS à l'attribut AS-dans les messages « BGP UPDATE » destiné à F. De ce fait, l'AS-

PATH impliquant le passage par F est plus long que celui impliquant le passage par G. Ainsi, les paquets provenant des AS souhaitant joindre AS_1, AS_2, AS_3 passeront par le lien G-E. Notons que la technique du remplissage peut aussi être légalement utilisée par le routeur D pour rendre inactif le lien F-D à des fins de sauvegarde ou parce qu'il est moins cher d'utiliser le lien G-E.

- **L'attaque par falsification de l'AS-PATH :** Soit F un routeur malveillant, et supposons que son objectif est de rendre AS_7 inaccessible à un ensemble de systèmes autonomes. Pour ce faire, F envoie une version modifiée du « BGP UDPATE » comprenant l'AS PATH modifié (AS_5, AS_4, AS_7). Le trafic vers AS_7 et à partir de cet ensemble d'AS passerait par AS_5 en utilisant le plus court chemin, et serait supprimé directement par le routeur F. En d'autres termes, le trou noir[22] se produit.

Ainsi, les attaques AS-PATH peuvent provoquer la compromission du trafic, sa redirection ou le trou noir, ce qui représente des menaces sérieuses pour l'infrastructure de l'Internet. Notons qu'il est très facile de lancer des attaques sur l'AS-PATH car le protocole BGP n'a pas de mesures de protection contre ce genre d'attaques; d'ailleurs tant que la connectivité est préservée, il est très difficile de détecter une attaque opérée pour un AS tiers car les relations de business et les politiques entre les fournisseurs sont largement tenues secrètes.

- Détournement de préfixes

Un système autonome peut envoyer des informations erronées au moyen de messages BGP UPDATE. Un système autonome malveillant peut annoncer un

22 Le trou noir est l'effet provoqué par la suppression de tous les paquets destinés aux adresses sur lesquelles porte l'attaque de l'AS malicieux.

préfixe possédé par un autre AS et revendiqué que c'est lui qui est à l'origine de ce message. Ce processus est appelé détournement de préfixe.

Les systèmes autonomes voisins qui reçoivent une annonce falsifiée penseront que l'AS malveillant est le propriétaire du préfixe et lui achemineront donc les paquets destinés à ce préfixe. L'AS légitime ne recevra donc pas le trafic qui est censé lui parvenir. Cette attaque rend les adresses falsifiées indisponibles. Notons que ce type de panne est souvent difficile à détecter.

Si l'AS malveillant choisit de falsifier toutes les adresses de l'AS victime avec un ensemble d'équipements sous son contrôle, l'effet peut être beaucoup plus sévère. On peut répliquer tous les services et les ressources de l'espace d'adressage de l'AS victime s'ils n'ont pas leurs propres mécanismes de sécurité. L'AS malveillant peut ensuite analyser le trafic qu'il reçoit et éventuellement récupérer des informations sensibles telles que les mots de passe. Une méthode particulièrement nuisible de propagation de fausses informations est la désagrégation des préfixes. Cela se produit lorsque l'annonce d'un grand préfixe est fragmentée ou reproduite par un ensemble d'annonces avec des préfixes plus petits. Par exemple, si les préfixes 12.0.0.0/8 et 12.0.0.0/16 sont annoncés, l'annonce correspondante au préfixe de 12.0.0.0/16 sera retenue. La désagrégation nuit aux performances de BGP et indirectement à celle des FSIs et ce en augmentant la taille des tables BGP et en inondant le réseau avec des mises à jour redondantes et parfois erronées. Ainsi, un AS peut détourner le trafic vers le préfixe le plus petit et non seulement les routeurs voisins adopteront cette mise à jour, mais ils inonderont aussi les mises à jour erronées à leurs pairs. Ces inondations propagent finalement au sein d'Internet.

3.2.3 Etat de l'art

Les attaquants peuvent compromettre la sécurité des communications sur deux plans: le plan de contrôle et le plan des données.

Dans la section suivante, nous présentons des propositions de sécurisation BGP au niveau des deux plans précités. Les protocoles Secure BGP (S-BGP) [43] Pretty Secure BGP (psBGP) [73] et SPV [79] sont des propositions de sécurisation relatives au plan de contrôle et les deux premiers protocoles utilisent une infrastructure à clé publique (PKI). Cette infrastructure publique peut être mise en place en adoptant une démarche de déploiement d'une infrastructure à clé publique au niveau d'Internet qu'on va décrire par la suite. Nous présentons ensuite SPV qui utilise la cryptographie basée sur l'identité et de simples primitives cryptographiques pour sécuriser BGP. Ces propositions de sécurisation du protocole de routage se concentrent sur l'authentification de l'origine et la validité du chemin, identifié comme nécessaires par l'IETF pour sécuriser BGP [8]. L'authentification de l'origine consiste en la validation des allégations de possession d'adresses par un AS. La validation de chemin garantit que le chemin est valide (chaque routeur BGP dans le chemin est accessible à partir du routeur BGP précédent), et que chaque AS sur le chemin d'accès est authentifié. Toutefois, Wendlandt et al [20] soulignent que vu que le plan de contrôle doit encore être augmenté avec des techniques de bout en bout pour garantir l'intégrité et la confidentialité, la seule propriété que le plan de contrôle doit garantir est la disponibilité. L'objectif étant de permettre aux équipements de communiquer de manière sécurisée, même si des portions de l'infrastructure du réseau sont contrôlées par un adversaire. Ainsi, nous présenterons « Stealth Probing » qui est un mécanisme permettant de surveiller la disponibilité en toute sécurité, puis le routage centrée sur la disponibilité (Availabity Centric Routing (ACR)).

Comme l'attaque de réinitialisation de TCP [40], le détournement de session implique une intrusion dans la session BGP en cours. Ainsi, l'attaquant se fait passer avec succès comme l'un des pairs lors d'une session BGP et ceci requiert les mêmes informations nécessaires à l'accomplissement de l'attaque de réinitialisation TCP. Par exemple, l'objectif est de modifier les itinéraires utilisés par les pairs, afin de faciliter l'écoute ou l'analyse du trafic. Les pairs eBGP[23] essaient par défaut d'ajouter toutes les routes reçues par un autre pair dans la table de routage et relaieront la quasi-totalité de ces routes à d'autres pairs eBGP.

L'attaquant visant à détourner des sessions BGP cherchent à localiser des FSIs qui n'appliquent pas le filtrage des annonces BGP (intentionnellement ou non) ou à repérer des FSI dont les sessions BGP sont sensibles à des attaques de type « homme au milieu ». Une fois ces FSI localisés, un attaquant pourrait annoncer le préfixe qu'il veut, impliquant le détournement d'une partie ou l'ensemble du trafic de la source légitime vers l'attaquant. Il n'est pas rare pour un attaquant de causer des pannes graves, y compris une perte complète de connectivité. Au début de 2008, au moins huit universités américaines ont vu leur trafic détourné vers l'Indonésie pendant 90 minutes durant une attaque très silencieuse, silence gardé par les intéressés. En outre, en février 2008, une grande portion d'espace d'adressage de YouTube a été redirigée vers le Pakistan. En effet, en bloquant l'accès vers le site de l'intérieur du pays avec la technique de détournement de préfixes, ce pays a causé la perturbation accidentelle du fonctionnement de BGP [7].

Nous classons les propositions selon les propriétés qu'ils remplissent :

- Authentification de l'origine et de la validité du chemin pour se défendre contre les attaques au niveau du plan de contrôle;

---

[23] eBGP (*Exterior Border Gateway Protocol*) correspond au déroulement du protocole entre les systèmes autonomes.

- Disponibilité pour se défendre contre les attaques au niveau du plan de données.

Propriétés : Authentification de l'origine et de la validité du chemin pour se défendre contre les attaques au niveau du plan de contrôle

- **S-BGP**

La proposition la plus complète et la plus concrète pour la sécurité de BGP est S-BGP. Elle propose l'utilisation d'une infrastructure à clé publique pour l'authentification des systèmes autonomes. Les infrastructures à clé publique sont ancrées à un bureau d'enregistrements Internet régional[24]. L'infrastructure à clé publique permet l'authentification des allocations d'adresses à travers une hiérarchie qui s'étend de l'organisation, des fournisseurs et des services d'enregistrements régionaux conduisant finalement à l'ICANN[25]. Ceci est accompli grâce à des certificats. Les attestations sont signées numériquement et sont utilisées pour affirmer l'authenticité de la propriété du préfixe et de l'itinéraire annoncé. Les attestations de route (une sorte de certificat numérique) sont distribuées avec S-BGP dans un nouvel attribut du message BGP UPDATE.

Pour simplifier, les attestations de route sont signées par chaque AS au fur et à mesure qu'il traverse le réseau. Par conséquent, cela permet au destinataire de valider non seulement la trajectoire, mais aussi le chemin a) parcouru entre les systèmes autonomes, dans l'ordre indiqué par le chemin AS PATH, et b) aucun des ASes intermédiaires n'ont été ajoutés ou supprimés par un attaquant malveillant.

---

24 Un bureau d'enregistrement Internet régional est l'organisme qui alloue les blocs d'adresses IP (adressage IPv4, IPv6) et des numéros d'Autonomous System dans sa zone géographique (dite régionale).

25 L'Internet Corporation for Assigned Names and Numbers (ICANN) est chargée d'allouer l'espace des adresses de protocole Internet (IP), d'attribuer les identificateurs de protocole, de gérer le système de nom de domaine de premier niveau pour les codes génériques et les codes nationaux, et d'assurer les fonctions de gestion du système de serveurs racines.

- **PsBGP**

PsBGP diffère de S-BGP dans le sens qu'il définit une nouvelle approche pour la vérification de l'authenticité de l'origine du préfixe par des informations recoupées provenant de multiples sources, de préférence indépendantes afin de vérifier l'AS PATH (intégrité). L'AS obtient tout d'abord un certificat de clé publique de l'une des autres autorités de certification, qui associe un numéro d'AS à une clé publique. Ensuite, chaque AS diffuse périodiquement un « Prefix Assertion List » (PAL) signé numériquement et composé d'un certain nombre de correspondances entre un numéro d'AS et des préfixes IP (zéro ou plus), une pour lui et une pour chacun de ses voisins. Le graphe de préfixes est construit de façon indépendante par chaque AS en se basant sur les PAL qu'il a reçus des autres systèmes autonomes et sur ses notations sur ces AS. Le graphe de préfixes est ensuite utilisé pour évaluer l'authenticité de l'origine d'un préfixe. PsBGP modifie l'approche S-BGP de la signature numérique en utilisant un mécanisme de notation et une approche graduelle pour la vérification de l'intégrité du chemin AS PATH. Chaque AS calcule un poids pour chaque chemin en fonction de la confiance accordée aux différents systèmes autonomes qui l'ont signés, et détermine sil accepte ou pas le chemin selon des critères tel que le Weight (Préférence administrative locale) ou AS-PATH (Préférence du chemin avec les moins d'AS traversés).

- **Le déploiement de la PKI**

Dans [36], les auteurs proposent de déployer progressivement une infrastructure à clé publique. Au cours de la phase d'initialisation, chacun des propriétaires des préfixes génère et signe son propre certificat. Lorsque de nombreuses parties s'impliquent dans ce processus, des partis dignes de confiance peuvent signer ces certificats. Enfin, il y aura un besoin d'authentification cen-

tralisée pour éviter les problèmes organisationnels qui peuvent être causés par des points multiples de confiance. Un draft propose une architecture permettant d'assurer le routage sécurisé dans Internet [9]. L'architecture est composée de trois éléments principaux:

- Une infrastructure à clé publique où des certificats X.509 attestent la correspondance entre les espaces d'adresses IP et les systèmes autonomes associés;
- Objets signés appelés autorisations de l'origine d'un chemin qui autorisent l'envoi de messages proclamant la possession de certaines portions de l'espace d'adressage IP ;
- Un système de stockage distribué qui rend ces objets disponibles pour les FSI afin de prendre des décisions de routage.

- **Secure Path Vector (SPV)**

Hu et al. proposent un protocole SPV [79] pour assurer la sécurité de BGP qui utilise de primitives cryptographiques, par exemple, les arbres d'authentification et les chaînes de hachage à sens unique pour la protection du chemin, et se veut plus efficace que le S-BGP. SPV met en œuvre la validation du chemin en utilisant une chaîne de signature à usage unique générée à partir d'une valeur racine unique. Aussi connues sous le nom de signatures hors ligne, les signatures à usage unique permettent au signataire d'effectuer en amont les lourdes opérations cryptographiques. SPV étend cette approche pour permettre à une signature hors ligne de générer potentiellement plusieurs signatures. Pour simplifier, selon SPV, l'initiateur d'un préfixe établit une valeur racine unique qu'il utilise pour la génération d'un ensemble de signatures à usage unique pour chaque tronçon dans le chemin. Les signatures et le matériel de signature sont transmis à chaque nœud suivant pendant la propagation de route. Les récepteurs utilisent un jeton de validation généré par l'initiateur

afin de vérifier les signatures à sens unique, et par conséquent le chemin. Le fonctionnement du SPV est léger grâce à l'utilisation du mécanisme du hachage. Cependant, cette efficacité a un coût; SPV est un protocole très complexe impliquant la manipulation et la communication d'un nombre important d'états.

Propriété : Disponibilité pour se défendre contre les attaques au niveau du plan de données

- **Le mécanisme « Stealth Probing »**

Les auteurs de [31] observent que la couche de contrôle du protocole de routage ne protège pas des retransmissions suspectes. Il ne protège pas non plus des perturbations au niveau de la couche Liaison, de la couche Réseau et de la couche Transport. L'objectif de ces auteurs est de permettre un contrôle de la disponibilité et de la localisation des pannes par le biais du mécanisme de « Stealth Probing » qui surveille la disponibilité en dissimulant le trafic de sondage. Ils visent à empêcher l'adversaire de traiter préférentiellement le trafic en rendant les données du trafic et les données de sondage indiscernables. L'hôte final doit créer un tunnel chiffré et rediriger les données ainsi que le trafic de sondage vers le tunnel. La taille du trafic de sondage doit correspondre à la taille du trafic de données et le calendrier des sondes doit être protégé. Cette approche est non-intrusive et permet de diminuer le nombre d'attaques exploitant les failles TCP.

- **Routage centré sur la disponibilité**

Les auteurs de [25] soutiennent que les propositions qui visent à protéger le plan de contrôle du protocole de routage sont soit lourdes soit insuffisantes. En fait, ils soutiennent que les modifications requises par ces protocoles augmente la complexité du protocole BGP et ne prévoient pas de toute façon ni la protection contre les attaques sur les données, ni celles de liens inutilisables à

cause de la congestion par exemple. Ils font observer que les hôtes / routeurs de bordure fournissent souvent déjà des mécanismes de sécurité de bout en bout comme SSL ou IPSec. Ils soutiennent que, par conséquent l'infrastructure de routage ne se doit de fournir que la disponibilité, c'est à dire la capacité de trouver et d'utiliser un chemin d'accès valide s'il existe. Alors, ils proposent un routage centré sur la disponibilité. Les clients peuvent apprendre de multiples chemins possibles vers une destination fournis par des fournisseurs de la disponibilité (FD), au lieu d'un seul «meilleur chemin». Les FDs peuvent être connectés densément avec des FSI tier-I et offrent aux utilisateurs des chemins de remplacement en plus de la voie normale annoncés via BGP. Ainsi, les clients peuvent utiliser des chemins adéquats et changer des routes si nécessaire. Selon la logique de l'ACR, une source tente de mettre en place un canal sécurisé en utilisant un chemin par défaut. Si la mise en place échoue, il peut demander d'autres chemins à son FD, tente de mettre en place un canal sécurisé avec chacun de ces chemins jusqu'à ce qu'il trouve un chemin adéquat. Les sources surveillent la performance du chemin et demandent les chemins alternatifs si le chemin actuel est inadéquat.

3.2.4 Mécanismes cryptographiques

- **Le « web de confiance »**

Le « web de confiance » est un modèle de confiance distribuée utilisée par PGP pour valider la possession d'une clé publique [50]. Le niveau de confiance est dépend de tiers faisant partie d'un réseau de confiance.

- **Cryptographie sans certificat**

La cryptographie sans certificat [23] est une variante de la cryptographie basée sur l'identité conçue pour se passer d'une entité de haute confiance. En effet, l'opération de la génération de la clé privée est partagée entre un utilisateur et

une tierce entité de confiance. Un utilisateur a besoin de trois informations pour chiffrer un message: 1) la clé publique de l'autre utilisateur, 2) son identité et 3) l'information publique de la tierce entité de confiance. Un utilisateur a juste besoin de sa clé privée pour déchiffrer un message. Ce système ne requiert pas de certificats car aucune clé valide ne peut être générée sans l'information secrète de la tierce entité de confiance.

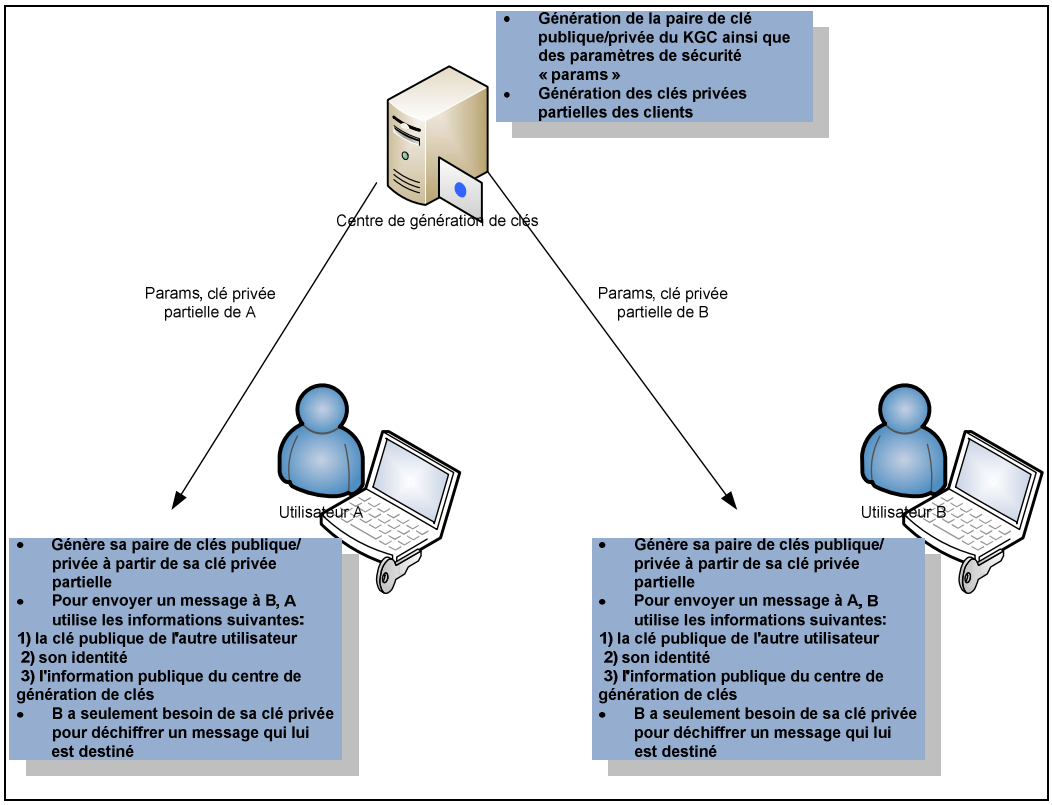


Figure 19: Illustration simplifiée du concept de la cryptographie sans certificats

3.2.5 Description de Trusted BGP (T-BGP)

Dans la section suivante, nous décrivons notre solution de protection des routeurs BGP contre les attaques basées sur l'usurpation d'identité. Notre solution de protection des routeurs BGP contre ce type d'attaques permet d'assurer à la fois les

propriétés d'authentification de l'origine et de validité du chemin pour se défendre contre les attaques au niveau du plan de contrôle ainsi que d'assurer la disponibilité pour se défendre contre les attaques au niveau du plan de données.

Afin de protéger les routeurs BGP contre l'usurpation d'identité, nous proposons dans un premier temps de clustériser les domaines Internet (tiers 1/2/3). Dans le cadre de notre architecture, Les domaines racine jouent le rôle de chefs de clusters. Les liens entre le chef de cluster et ses routeurs seront protégées grâce au paradigme de la cryptographie sans certificats et au concept de « web de confiance ». Les membres des clusters sont soit des routeurs normaux dans le cas des petits domaines soit des « Route Reflector »[26] dans le cas de grands domaines. Par commodité, nous allons noter les membres de cluster par RR^{AS}. Chacun des RR^{AS} au sein de chacun des clusters remontent ses préfixes actuels et ceux qu'il a délégués[27] ainsi que l'identité de ses voisins actuels à son chef de cluster. Chacun des chefs de cluster forme ensuite un graphe représentant son cluster dont les nœuds représentent les RR^{AS} et les liens représentent les adjacences actuelles entre les RR^{AS}. Ensuite, chacun des RR^{AS} envoie son graphe à autres clusters ce qui permet à chacun d'eux de former le graphe actuel d'Internet. Chaque message BGP UPDATE sera vérifié à l'aide de ce graphe. Le RR^{AS} envoie un paquet de rafraichissement à son chef de cluster CH s'il y a un changement au niveau des préfixes possédés ou ceux de son adjacence. Notons que les matériaux cryptographiques utilisés dans le cadre de ce mécanisme sont stockés dans des cartes à puces agissant ainsi comme un coffre-fort électronique.

- Formation et sécurisation du cluster :

---

26 Un « route reflector » propage les routes apprises par IBGP aux autres pairs. Cette approche diminue le nombre de sessions TCP dans l'AS et réduit donc le trafic associé.

27 Un AS est en mesure de déléguer l'utilisation d'un ensemble de préfixes à un autre AS

Chacun des centres de génération de clés (KGC : Key Generation Center) au niveau de chacun des chefs de clusters (CH) génère certains paramètres publics appelé params, puis les algorithmes « Probabilistic Polynomial-Time » (PPT) suivants sont déroulés:

- **KGC_MasterKeyGeneration:** comme entrée params et 1^y où $y \in N$ est un paramètre de sécurité, ensuite l'algorithme PPT génère les clés privées et publiques du KGC (msk, mpk).
- **KGC_certificate_sollicitation (par le biais du paradigme du "web de confiance") :** Chaque KGC envoie ses paramètres publics et sa clé publique <params, msk > aux autres KGCs et reçoit un certificat contenant la concaténation des signatures de chacun des KGCs de <params, msk >.
- **PartialKeyGeneration:** Avec comme entrée la clé privé msk ainsi que l'identité ID ∈ {1,0}* du routeur, l'algorithme PPT génère une clé partielle du routeur RouterPartialKey. Cette opération est réalisée par le KGC. Le chef de cluster envoie cette valeur et son certificat – obtenu grâce au paradigme de « web de confiance » - au routeur en question.
- **RouterKeyGeneration:** l'algorithme PPT est réalisé par le routeur. Il choisit un secret x and donne x, params, RouterPartialKey ainsi que son identité ID comme entrée à l'algorithme PPT qui génère une paire de clés secrètes et publiques.

- Formation du graphe de correspondance AS- préfixes IP

On suppose que chacun des CH dispose de clés partagées avec l'IANA et que toutes les communications entre chacun des CH et l'IANA seront chiffrées avec cette clé.

Initialement, chaque RR^{AS} envoie des informations sur les préfixes qu'il possède et les préfixes qu'il a délégué à son chef de cluster. Ces informations seront re-

layées par le chef de cluster à l'IANA, qui est une organisation dont le rôle est la gestion de l'espace d'adressage IP d'Internet, et des autres ressources partagées de numérotation requises soit par les protocoles de communication sur Internet, soit pour l'interconnexion de réseaux à Internet. L'IANA va recouper ces informations avec sa propre base de données et avec la base de données des RIRs, qui sont des organismes qui allouent les blocs d'adresses IP (adressage IPv4, IPv6) et des numéros d'AS dans sa zone géographique. Cette organisation va par la suite signifier au chef de cluster de prendre en compte ou pas ces dites informations (par un message contenant les chaînes de caractères suivantes : validation ou non validation). Les messages entre chaque RR^{AS} et son CH seront signés avec leurs clés obtenues lors de la phase de formation de clusters. Le message sera envoyé avec le certificat du CH correspondant à l'AS.

$$RR^{AS}\text{->CH} : [\{P\}_{P\subset AS} | \{Px\}_{Px\subset AS}] \_K^{RR}{}_{PRIV}$$

Où $\{P\}_{P\subset AS}$ représente les préfixes que RR^{AS} possède et $\{Px\}_{P\subset AS}$ les préfixes que RR^{AS} a délégués.

- **Envoi par des routeurs de leurs adjacences actuelles :**

Chacun des RR^{AS} envoie la liste de leurs voisins signée par sa clé.

$$RR^{AS}\text{->CH} : [\{Vo\}_{Vo\subset \text{voisinage}(AS)}] \_K^{RR}{}_{PRIV}$$

Où $\{Vo\}_{Vo\subset \text{voisinage}(AS)}$ représente la liste des voisins de RR^{AS}

Le chef de cluster correspondant va ainsi recouper les informations et obtenir une portion du graphe des ASes qu'il va envoyer aux autres chefs de cluster signé par sa clé. Ensuite, tous les chefs de cluster fusionnent leurs propres informations avec celles reçues par les autres chefs de cluster.

- **Formation du graphe : Matrice d'adjacence et fonctions associés :**

Dans cette phase, chacun des chefs de clusters forment un graphe G_{BGP} des systèmes autonomes avec les préfixes de chaque système autonome.

Soit $G_{BGP}= (V, E)$ où $|V| = n$. Supposons aussi que les sommets de G_{BGP} sont arbitrairement $v_1, \ldots, v_n$. La matrice d'adjacence A de G_{BGP} se rapportant à cet ensemble de sommets est la matrice $n \times n$ booléenne A avec :

$$a_{ij} = \begin{cases} 1 & \text{si } (v_i, v_j) \in E \\ 0 & \text{sinon.} \end{cases}$$

Nous définissons également trois fonctions comme suit:

F_1 : Cette fonction prend en entrée un numéro de domaine donné et retourne la liste de ses préfixes. Soit E^{AS} l'ensemble des systèmes autonomes et E^{PREFIX} l'ensemble des préfixes.

$$\mathbf{F_1 : E^{AS}} \rightarrow E^{PREFIX}$$

$$\mathbf{N_{AS}} \mapsto \{P\}_{P \subset AS}$$

F_2 : Cette fonction prend en entrée un AS-PATH et retourne 1 si cet AS-PATH existe et dans cet ordre et 0 (çà s'arrête à la première erreur) si cet AS-PATH n'existe pas dans le graphe reconstitué par le chef de cluster ou s'il détecte du « padding » d'AS (répétition du même AS).

Un AS-PATH peut être modélisé comme suit : $\prod_{a_{ij} \in AS-PATH} a_{ij}$

Soit $E^{\mathbf{AS\text{-}PATH}}$ l'ensemble des AS-PATH.

$$\mathbf{F_2 : } E^{\mathbf{AS\text{-}PATH}} \rightarrow \mathbf{\{0,1\}}$$

$$\prod_{a_{ij} \in AS-PATH} a_{ij} \mapsto \mathbf{V}$$

F_3: Cette fonction prend en entrée un AS-PATH et retourne l'AS qui a envoyé le message BGP.

- Fonctionnement

- **Vérification du BGP update :**

A chaque réception d'un BGP UPDATE, le RR le relaie comme à son habitude à son RR pour propager l'information. Nous ajoutons une fonctionnalité au RR.

Le RR extrait l'AS-PATH ainsi que la liste des préfixes spécifiés dans le message et l'envoient à son CH signée par sa clé K.

$$\mathbf{RR^{AS}\text{->}CH : [AS\text{-}PATH|}\{P\}_{P\subset AS}\mathbf{\ ]\ \_K}$$

Le CH effectue les opérations suivantes:

- Il déchiffre le message à l'aide de la clé publique et de l'identité du routeur ;
- Applique la fonction F_3 pour retrouver l'AS qui a envoyé le message ;
- Applique la fonction F_1 pour retrouver la liste des préfixes légitimes ;
- Compare la liste des préfixes légitimes avec celle reçue et retourne 0 si elles concordent et 1 sinon ;
- Applique la fonction F_2 pour vérifier l'existence du chemin ;
- Retourne 0 si les informations sont avérées et 1 sinon.

Puis le CH envoie au routeur RR^{AS} la réponse R (OK ou KO) chiffrée par la clé K comme suit :

CH-> RR^{AS}: [R] _K

- **Maintenance**

Le RR^{AS} envoie un paquet de rafraichissement à son chef de cluster s'il y a un changement au niveau des préfixes possédés ou de son adjacence actuelle.

3.2.6 Analyse de sécurité et comparaison de notre solution

L'utilisation de la cryptographie permet de renforcer la sécurité des échanges BGP et permet plus particulièrement l'authentification de l'origine ainsi que du chemin ce qui permet de se prémunir contre les attaques d'usurpation d'identité.

- Analyse de sécurité :

- **Attaques sur le champ AS-PATH:** Une attaque sur l'AS-PATH implique sa modification soit en ajoutant des systèmes autonomes qui ne sont pas normalement dans le chemin, soit en faisant du « remplissage », soit en supprimant des AS dans le chemin ou soit en modifiant un ou plusieurs identifiants d'AS. Cette attaque peut être déjouée grâce à notre proposition car la fonction F_2 prend en entrée un AS-PATH et retourne 0 si cet AS-PATH n'existe pas dans l'ordre ou si elle détecte du « remplissage ».

  En effet,

$$\prod_{a_{ij} \in AS-PATH} a_{ij} = 0 \; si \begin{cases} \exists a_{ij} = 0 : \text{lien n' existe pas} \\ \exists i = i+1 \text{ et } j = j+1 : \text{redondance} \end{cases}$$

- **Origine des données:** Une attaque sur l'origine des données implique qu'il existe dans le message « BGP UPDATE » des préfixes qui n'appartiennent pas à l'AS qui a émis le message. Ceci peut être déjoué grâce à notre proposition car la fonction F_1 prend en entrée un numéro de domaine donné et retourne la liste de ses préfixes à partir des données approuvées par l'IANA et donc le routeur est en mesure de détecter ce type d'attaque et en comparant la liste de préfixes légitimes avec ceux reçus dans le message.

$$\text{Si F2 } (\mathbf{N_{AS}}) = \{P\}_{P \subset AS} \neq \{P\}_{P \subset BGPUPDATE}$$

Alors le paquet BGP UPDATE n'est pas pris en compte et une alerte est remontée à l'administrateur du domaine.

- **Disponibilité:** Le graphe peut être utilisé pour surveiller le routage BGP. En effet, une condition essentielle pour assurer la disponibilité est la présence d'un fournisseur de disponibilité (AP), qui peut fournir de nombreux chemins vers une seule destination. Chaque chef de cluster peut alors agir comme fournisseur de disponibilité parce qu'il possède le graphe complet et actuel des systèmes autonomes.

- Comparaison

Le tableau suivant présente la comparaison de notre proposition avec les protocoles filtrage de route, S-BGP, SoBGP, SPV selon divers critères fonctionnels comme suit:

	En cours d'utilisation	Moyens utilisés	Authentification de la topologie[28]	Authentification du chemin	Authentification de l'origine
Filtrage de route	Oui (par certains Ases)	Anomalies	Faible	Faible	Faible
S-BGP	Non	Crypto	Crypto	Crypto	Crypto
SoBGP	Non	Crypto/Anomalies	Crypto	Non	Crypto
SPV	Non	Crypto	Crypto	Crypto	Non
T-BGP	Non	Crypto	Crypto	Crypto	Crypto

Tableau 4: Comparaison de notre proposition

28 L'authentification de la topologie revient à s'assurer que les chemins correspondent à la topologie actuelle de BGP

L'utilisation de la cryptographie permet de renforcer la sécurité des échanges BGP et permet plus particulièrement l'authentification de l'origine ainsi que du chemin ce qui permet de se prémunir contre les attaques d'usurpation d'identité.

3.3 Réseaux OSPF

Dans cette section, nous présentons un nouveau mécanisme de protection contre l'usurpation d'identité pour le protocole de routage OSPF.

3.3.1 Introduction

OSPF est un protocole de routage dynamique à état de lien utilisé au sein des réseaux IP [35]. Dans son mode de fonctionnement, OSPF recueille les informations d'état des liens depuis les routeurs disponibles et construit une carte de la topologie du réseau. La topologie détermine la table de routage utilisée par le plan de contrôle et est ainsi utilisée à postériori par le plan de transfert pour la transmission des paquets. OSPF détecte les changements de topologie comme ceux générés par les ruptures de liens et lorsque cela est possible, il fait converger la structure vers un nouvel arbre de routage sans boucle. L'arbre optimal pour atteindre un destinataire à partir de la racine (le nœud courant ou nœud de base) est calculé grâce à l'algorithme de Dijkstra. Les informations d'état des liens sont maintenues sur chaque nœud dans une base de données d'état des liens (Link-State DataBase **LSDB**) qui consiste en un graphe de la topologie réseau. Cette base est périodiquement répliquée sur l'ensemble des routeurs.

Au sein du protocole OSPF, les politiques de constitution des tables de routage sont influencées par des facteurs de coût associées à chaque interface. Ces facteurs de coût peuvent être :

- La distance d'un routeur (Round-trip time) ;
- La congestion du lien;

- La disponibilité du lien;

Ces facteurs permettent de répartir le flux entre des routes de même coût initial et d'influencer la répartition du trafic en cas de besoin.

Pour les réseaux OSPF, on choisit généralement un DR (routeur désigné) qui va recevoir toutes les informations sur l'état des liens et les retransmettra aux autres routeurs. Ce DR permet de réduire le trafic lié à l'échange d'informations sur l'état des liens et améliorera l'intégrité de la base de données topologique.

L'ensemble des fonctions complexes de construction des tables de routage et du maintien de la topologie réseau dans un état stable et fonctionnel repose sur l'intégrité des paquets de signalisation OSPF.

Le protocole OSPF n'a pas été conçu de manière sécurisée. Dans un mode basique sans authentification, la sécurité est « assurée » par le mécanisme de « Fight Back » mais ce dernier, davantage dédié à la correction d'erreur qu'à une réaction face à des attaques, est contournable. Elle est assurée également par l'authentification MD5 qui peut être contournée également. En effet, des travaux de recherche [71] ont permis de développer des algorithmes qui peuvent calculer les collisions de hachage.

Par ailleurs, OSPF est vulnérable à plusieurs attaques d'usurpation d'identité dont les attaques de « masquerading » et de substitution qui seront explicitées dans la section suivante. Ces attaques peuvent conduire à la perturbation du fonctionnement du réseau du FSI.

Dans ce chapitre, nous allons proposer un mécanisme de protection contre l'usurpation d'identité spécifique au protocole OSPF en utilisant un coffre-fort électronique qu'est la carte à puce.

La section 3.3.2 passe en revue les attaques au sein du réseau OSPF. La section 3.3.3 présente notre solution. La section 3.3.4 présente l'analyse de sécurité. La

section 3.3.5 présente la plateforme de tests ainsi que les résultats obtenus et leurs interprétations.

3.3.2 Les attaques au sein du réseau OSPF

- un attaquant isolé – Masquerading [11]: Une attaque de masquerading entreprise par un seul attaquant Rx se produit lorsqu'il se prétend à l'origine des informations censées provenir d'un autre routeur R_1.
- un attaquant isolé – Substitution [70]: Dans une attaque de substitution, un attaquant R_x tente de modifier des informations provenant de R_1 et retransmet le message modifié.
- Les attaquants multiples - Masquerading: Pour une attaque de « masquerading » impliquant de multiples attaquants, l'attaque se passe comme suit: les routeurs R_{X1}, R_{X2},. . . , R_{XI} génèrent des paquets supposés provenir de R_1.
- Les attaquants multiples - Substitution: Pour une attaque de substitution impliquant de multiples attaquants, les routeurs R_{X1}, R_{X2},. . . , R_{XI} tentent de modifier des informations provenant de R_1 et retransmettent les messages modifiés.
- Contournement du mécanisme « Fight back » : Le mécanisme de « Fight Back » est un comportement naturel des routeurs qui implémentent OSPF : il s'agit d'une réponse face à la détection d'une erreur. Ce mécanisme peut être utilisé en réaction à une attaque, par exemple lors d'une attaque par usurpation. Lorsqu'un routeur reçoit un paquet où il est spécifié comme la source (usurpation) et que les données sont incohérentes par rapport à sa base, ce dernier renvoie le paquet dans sa forme juste afin de corriger les informations transmises. Plusieurs possibilités visant à con-

tourner le mécanisme de « Fight Back » sont exposés dans [23] comme suit:

1. Lorsque le routeur usurpé n'existe pas réellement : aucune réaction n'est à prévoir. Les routeurs légitimes vont donc considérer l'attaquant comme l'un des leurs.
2. Lorsque le routeur attaquant est placé au centre d'un réseau partitionné de façon à ce que le routeur usurpé ne reçoive pas les messages de l'attaquant, ce qui inhibe sa faculté de réponse.
3. Lorsque le rythme d'envoi du routeur attaquant est inférieur à ceux du routeur légitime.

Sur la base de ces mécanismes de contournement, un attaquant peut rendre indisponible un routeur légitime en provoquant par exemple une saturation et réaliser en parallèle des attaques de modification de la topologie en usurpant son identité.

- Usurpation de l'identité d'un routeur au niveau MAC : Un attaquant usurpe l'identité d'un routeur au niveau deux du modèle OSI de façon à intercepter le trafic unicast entre les routeurs. L'attaque a pour effet de modifier la base de données, ce qui va entraîner l'envoi de paquets de mise à jour. Si le nombre de paquet à envoyer est important, la disponibilité du réseau pourrait être dégradée.
- Empoisonnement de la table de routage **:**

L'empoisonnement de la table de routage signifie qu'elle contient des informations qui ne reflètent pas la topologie actuelle du réseau. Un exemple d'empoisonnement de la table de routage est illustré par la figure 20. Supposons que le nœud A communique avec le nœud F à travers le nœud C. Si le nœud D souhaite avoir accès aux données échangées entre A et C, D pourrait se faire passer pour le nœud C en initiant un paquet de mise à jour d'état des liens qui semble provenir de C, en indiquant un lien (C, F) est indisponible. Cela risque de contraindre le nœud A à re-router le trafic destiné à F à tra-

vers le nœud D, lui donnant ainsi accès aux données. Ce scénario peut se produire parce que le nœud A n'a aucun moyen de connaître la véritable source de l'annonce falsifiée de l'état des liens.

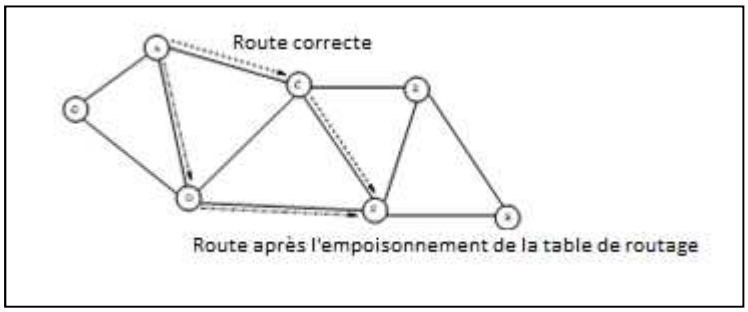


Figure 20: Illustration d'un exemple d'empoisonnement de la table de routage

3.3.3 Solution proposée

La figure suivante met en évidence les différentes entités de notre proposition :

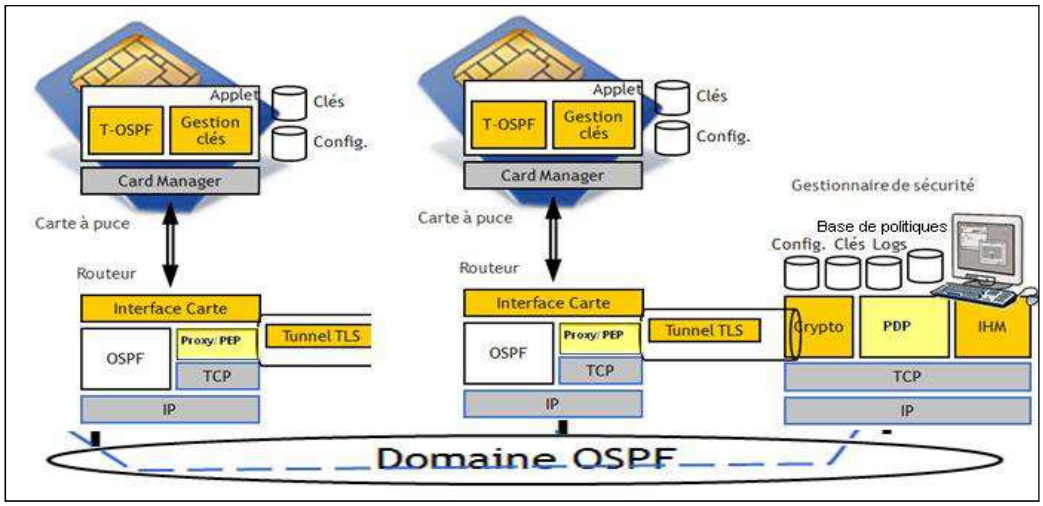


Figure 21: Architecture proposée

Le gestionnaire de sécurité contient la racine de confiance. A chacun des routeurs est raccordée une carte à puce. De plus, chacun des routeurs dispose d'une version modifiée d'OSPF. Ainsi, le module OSPF est décomposé en deux briques : une brique au niveau du routeur et une brique de la carte à puce. Par

ailleurs, chacune des cartes à puce contient également son matériel cryptographique, son adresse MAC ainsi que l'identité de son routeur (données chargées par l'administrateur au niveau de la station d'administration).

Le matériel cryptographique des routeurs peut être installé avec une clé USB afin d'éviter de faire transiter sur le réseau les clés privées des différents routeurs. Cette solution est toutefois contraignante pour l'administrateur car il doit se déplacer dans le datacenter et répéter l'opération au niveau de chaque routeur. Ensuite, chacun des routeurs dérive une clé partagée avec le routeur désigné (DR)[29]. Aussi, les cartes déroulent un algorithme de dérivation de clés avec les cartes des routeurs voisins ainsi qu'avec celle du routeur désigné.

Les clés dérivées entre les cartes à puce servent à signer les messages OSPF et à authentifier le niveau MAC. Les clés dérivées entre les routeurs servent à chiffrer les paquets IP contenant les messages OSPF. Le mécanisme d'authentification utilisé est l'authentification cryptographique utilisant une fonction de hachage à sens unique le SHA-1 (Secure Hash Algorithm) [18].

Les fonctions de hachage cryptographiques telles que le SHA-1 effectuent leurs opérations sur des blocs de 512 bits (64 octets). Elles requièrent par ailleurs une clé secrète pour le hachage. L'empreinte numérique (Authentication Digest) est ainsi générée sur le résultat de la concaténation entre le message OSPF (en-tête et corps OSPF), la clé secrète et les octets de remplissage permettent d'obtenir une chaîne d'une longueur égale à un nombre entier de blocs de traitement de 512 bits (64 octets). L'empreinte est ainsi ensuite ajoutée à la fin du message OSPF pour l'authentification. L'empreinte générée est de 20 octets (160 bits) pour le résultat de l'algorithme SHA-1.

---

[29] Le DR est un routeur qui sert de référent pour la base de données topologique représentant le réseau.

Dans le cadre de l'authentification cryptographique, une clé secrète partagée et un identifiant associé à cette clé (KeyID), sont définis pour chaque lien entre les deux interfaces de deux routeurs adjacents. La combinaison de l'identifiant et d'une interface permet d'identifier une clé. Pour chaque échange de message, cette clé secrète est utilisée pour générer ou vérifier une empreinte ajoutée au paquet OSPF.

A chaque clé est associée 4 constantes de temps qui peuvent être fixées en secondes:

- **KeyStartAccept:** date à partir de laquelle le routeur acceptera les paquets utilisant cette clé.
- **KeyStartGenerate:** date à partir de laquelle le routeur générera ses paquets en utilisant cette clé.
- **KeyStopGenerate:** date à partir de laquelle le routeur n'utilise plus cette clé pour les paquets générés.
- **KeyStopAccept:** date à partir de laquelle le routeur n'accepte plus des paquets reçus et qui ont été générés en utilisant cette clé.

Ainsi, la clé est localisée sur la carte à puce et est repérée par son identifiant KeyID. Les différents attributs qui caractérisent la clé (KeyStartAccept, etc.) sont toujours localisés sur le routeur. Notons que le routeur doit disposer de mécanisme de prévention contre les attaques sur l'horloge.

La génération de l'empreinte se déroule ainsi au sein de la carte, décrite ci-dessous.

- Génération des messages OSPF utilisant le mécanisme d'authentification cryptographique

Cette phase se décompose en plusieurs étapes comme illustré sur la figure 22.

1. **Etapes avant génération de l'empreinte :** Ces étapes se déroulent au sein du routeur. Une fois le contenu du paquet OSPF construits, les différents champs de l'en-tête sont déterminés et fixés. Puis, l'identifiant de la clé secrète à utiliser est déterminé en fonction des paramètres temporels définissant la clé. Etant donné que les fonctions de hachage citées précédemment opèrent sur des blocs de 512 bits (64 octets), le message OSPF (en-tête + corps) est divisé en blocs de 64 octets. Ces différents blocs sont hachés en suivant l'algorithme choisi jusqu'au dernier bloc complet de 64 octets. Les octets restants du message OSPF sont transmis en même temps que le résultat du hachage (empreinte intermédiaire calculée sans clé) des blocs précédents et l'identifiant de la clé à utiliser.
2. **Envoi de la commande vers la carte :** Une fois les étapes précédentes franchies, le routeur construit une commande APDU contenant l'instruction du calcul avec les données d'entrée.
3. **Génération de l'empreinte:** La génération de l'empreinte se déroule dans la carte. La carte sélectionne la clé correspondante à l'identifiant reçu. La clé est concaténée au bloc reçu et le remplissage est effectué afin d'avoir un ou des blocs complets de 64 octets. Ensuite, la fonction de hachage opère sur la concaténation obtenue en utilisant l'empreinte intermédiaire comme vecteur d'initialisation. L'empreinte est ainsi générée et a une taille 20 octets (160 bits) dans le cas de SHA-1.

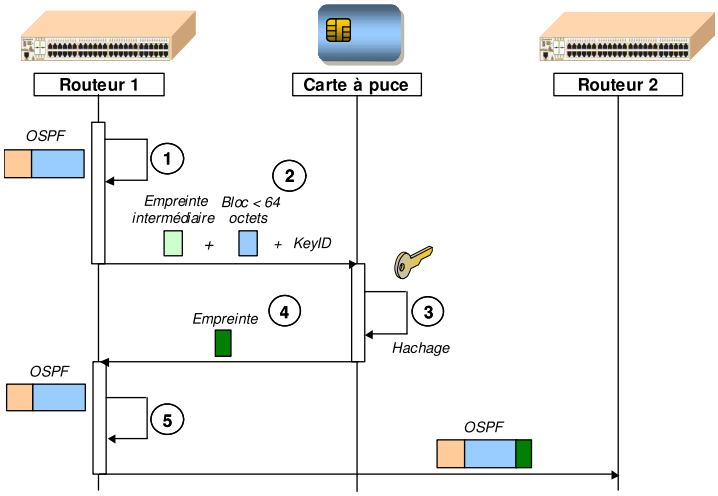


Figure 22: Génération des messages OSPF

4. **Envoi de la réponse vers le routeur:** L'empreinte est retournée en réponse vers le routeur. Notons que tous les paquets échangés entre routeurs sont numérotés séquentiellement (numéro de séquence : entier de 32 bits). Chaque coté de la connexion initialise et maintient la séquence des paquets envoyés.

5. **Génération du message OSPF final et l'envoi vers ses voisins :** L'empreinte est ensuite concaténée à la fin du message OSPF. Le message OSPF est ensuite chiffré par la clé privée du routeur. L'empreinte n'est pas comptabilisée dans la taille du paquet OSPF spécifiée par le champ Message Length de l'en-tête. Mais elle est comptabilisée dans le champ Length du paquet IP. Tout remplissage supplémentaire n'est pas comptabilisé ou transmis.

- Vérification des messages OSPF utilisant le mécanisme d'authentification cryptographique

Tout paquet OSPF reçu sur une interface est authentifié selon les étapes suivantes comme illustrée dans la figure 23:

Réception de message OSPF: Le routeur reçoit un message OSPF qui doit être authentifié.

Traitement du message OSPF: Le type d'authentification de l'interface est lu et confronté à celui du paquet (type 2 dans le cas de l'authentification cryptographique). Si le champ AuType du paquet n'est pas 2, celui-ci est rejeté.

Dans le cas où l'étape précédente serait franchie, la clé correspondant à l'identifiant de la clé lue dans le champ KeyID du paquet reçu, est recherchée.

Si on ne trouve pas de clé associée à ce KeyID ou si l'attribut de la clé KeyStopAccept est dépassé, le paquet est rejeté. Dans le cas où l'étape précédente serait franchie, si le numéro de séquence du paquet OSPF reçu est inférieur à au moins un de ceux qui ont été retenu par le routeur dans sa base de voisinage et provenant de ce même expéditeur, le paquet est rejeté. Dans le cas où l'étape précédente serait franchie, l'empreinte ajoutée à la fin du message OSPF est extraite.

Ensuite, le message est découpé en plusieurs blocs de 64 octets comme pour la phase de génération de signature, puis la fonction de hachage opère. Ensuite, les différentes données adéquates sont envoyées vers la carte.

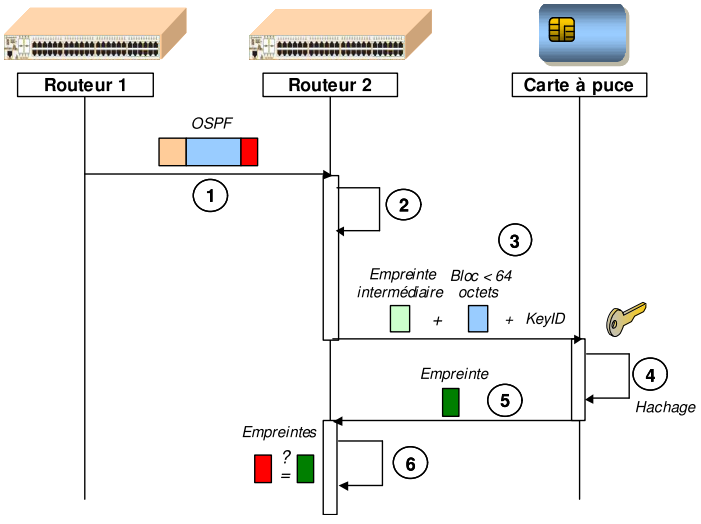


Figure 23: Vérification des messages OSPF

Envoi de la commande vers la carte : Le routeur construit une commande APDU contenant l'instruction du calcul avec les données adéquates en entrée et l'envoi vers la carte.

Génération de l'empreinte: La génération de l'empreinte se déroule dans la carte. L'empreinte finale est générée comme pour la phase de génération du message OSPF.

Envoi de la réponse vers le routeur : L'empreinte est retournée en réponse vers le routeur.

Comparaison des empreintes: Le routeur compare l'empreinte du message OSPF reçue à celle calculée par la carte. Si elles ne sont pas identiques, le paquet est rejeté. Si elles sont identiques, le paquet est authentifié, son numéro de séquence est ajouté dans la base de voisinage du routeur.

Notons qu'on rajoute une fonctionnalité au DR qui, en plus de recevoir toutes les informations sur l'état des liens et de les retransmettre aux autres routeurs, tient un tableau de correspondance entre les identifiants des routeurs et les identifiants de leurs voisins saisis par l'opérateur réseau et qui est rafraichi à chaque rajout ou changement de positions de routeurs.

3.3.4 Analyse de sécurité

- Les attaques de l'extérieur

Toutes les attaques extérieures sont contrecarrées par l'authentification entre voisins. Ainsi, le premier routeur qui reçoit les données de routage forgées n'est pas en mesure de les vérifier et le message est donc éliminé.

- Analyse des attaques au sein du réseau OSPF

Notons que la carte à puce joue le rôle d'un coffre-fort électronique et donc l'identité ainsi que le matériel cryptographique de chaque routeur ne peuvent ni

être modifiés ni être utilisés dans le cadre d'une attaque d'usurpation d'identité. Notons également que les cartes à puces sont localisés au niveau des routeurs situés datacenters donc ces cartes à puce sont protégés contre le vol.

Cependant, le routeur doit disposer des mécanismes de protection contre les attaques exploitant les failles spécifiques à l'utilisation des cartes à puce [24].

- **un attaquant isolé – Masquerading :** Un seul attaquant R_x ne peut pas se prétendre à l'origine des informations censées provenir d'un autre routeur R_1 car la signature dépend de l'identité du routeur.
- **un attaquant isolé – Substitution** : Un attaquant R_x ne peut pas modifier des informations provenant de R_1 et retransmettre le message modifié car il n'est pas en mesure de recalculer la signature.
- **Les attaquants multiples - Masquerading:** Les routeurs R_{X1}, R_{X2},. . . , R_{XI} ne peuvent pas générer des paquets supposés provenir de R1 car la signature dépend de l'identité du routeur.
- **Les attaquants multiples - Substitution:** Les routeurs R_{X1}, R_{X2},. . . , R_{XI} ne peuvent pas modifier et inonder des informations falsifiées provenant d'un seul routeur R_1 car des nouvelles signatures doivent être générées pour les données modifiées.
- **"Fight back":** L'attaquant ne peut plus encombrer le réseau par déclenchement de « Fight Back ». En effet, il ne peut plus forger un paquet LSA (de n'importe quel type) en rajoutant une information erronée du point de vu du routeur légitime car il n'a pas la bonne clé pour régénérer une signature valide.
- **Usurpation de l'identité d'un routeur au niveau MAC :** L'attaquant n'a pas la possibilité d'usurper l'identité MAC d'un routeur car il n'est pas en mesure de recalculer une signature valide. On évite donc la situa-

tion dans laquelle l'attaquant modifie à la volée des trames Unicast et qui a pour effet de modifier la base de données, ce qui pourrait entraîner l'envoi de paquets de mise à jour et l'indisponibilité du réseau si le nombre de paquet à envoyer est important.

- **Empoisonnement de la table de routage :** L'attaquant ne peut pas « empoisonner» la table du routage car un routeur ne pourra plus initier un paquet mise à jour d'état des liens semblant provenir d'un autre routeur.

3.3.5 Présentation du système

Notre démonstrateur se compose d'un ensemble d'ordinateurs dédié au projet ANR ESTER et reliée à la plateforme Percevale.

- La plateforme Percevale

L'infrastructure réseau Percevale reproduit un réseau métropolitain d'opérateur (MAN) et permet aux plates-formes d'études un accès au réseau interne INT et à l'Internet.

La plateforme PERCEVALE offre non seulement l'opportunité d'étudier et de valider des solutions techniques sur un réseau MAN mais il permet aussi de travailler sur un réseau indépendant des infrastructures techniques de TELECOM SudParis.

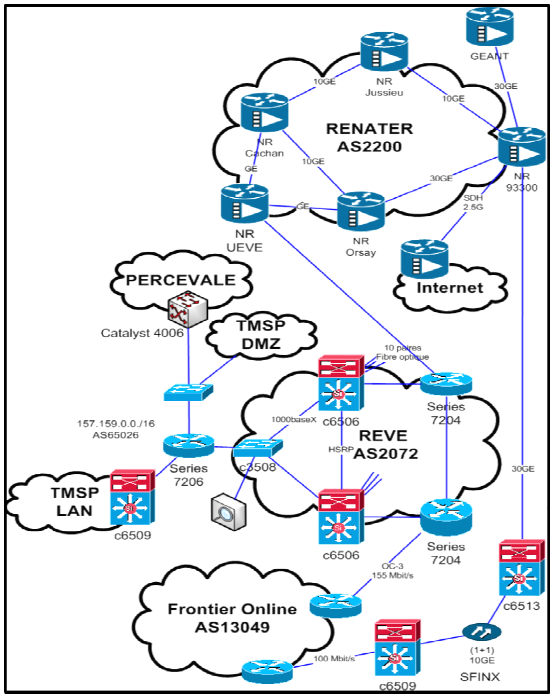


Figure 24: **La plateforme Percevale**

Le routage sur le réseau de cœur est contrôlé par une instance OSPF (area 0) présente sur chaque routeur PE.

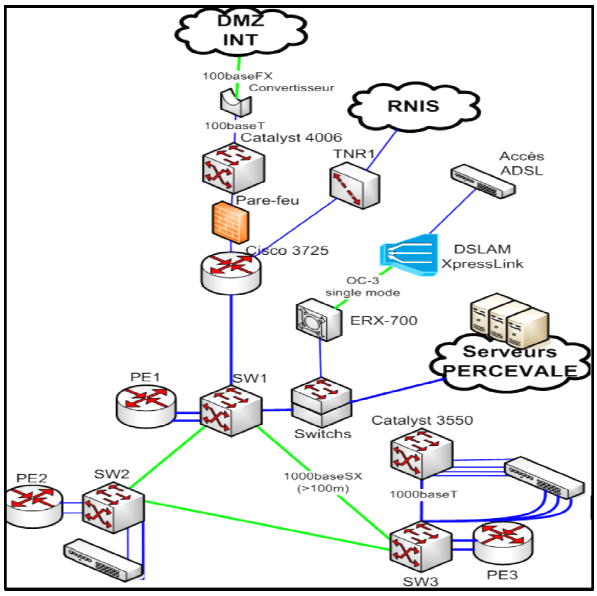


Figure 25 : Illustration de l'area 0 de la plateforme Percevale

- Description du démonstrateur

La figure 25 décrit le démonstrateur en explicitant les identifiants des routeurs ainsi que leurs interconnexions. Tous les routeurs sont connectés à travers des liens Point à Point.

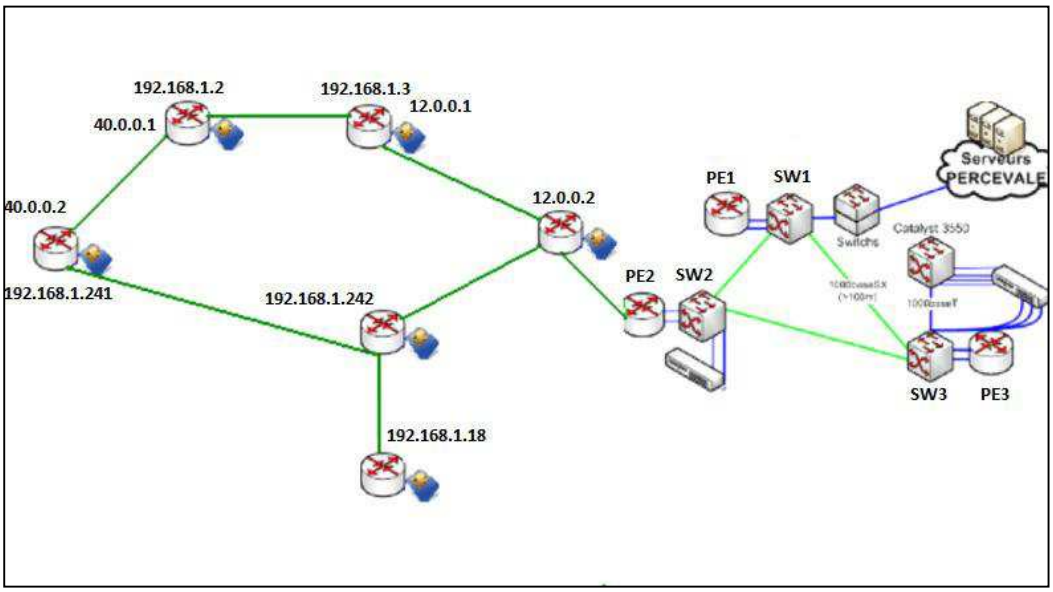


Figure 26 : Plateforme pour les tests de performance

- Présentation des tests

Les tests vont permettre les éléments suivants:

✓ Temps requis pour traiter une LSA[30]

✓ Temps de convergence

✓ Temps de re-calcul d'une table de routage après un changement.

- **Scénario 1**

- Description :

30 Chaque routeur communique la liste des réseaux auxquels il est directement connecté par des messages LSA (*Link-State Advertisement*) propagés de proche en proche à tous les routeurs du réseau.

Le scénario 1 décrit dans la RFC 4061 est conçu pour calculer le temps nécessaire pour le traitement d'un message LSA. Il sera exécuté en premier temps avec la version sans ESTER d'OSPF puis avec la version ESTER.

- Envoi d'un duplicata d'un LSA qui se trouve déjà dans l'équipement de test (Device Under Test- DUT).
- On note la différence de temps entre le moment où le LSA est envoyé et lorsque l'acquittement est reçu. Ainsi on mesure le temps nécessaire pour la propagation d'un LSA et l'acquittement et la durée du traitement des doublons LSA. Ce temps est appelé dupLSAprocTime.
- Envoi d'une nouvelle LSA de la génératrice au DUT, suivie par un duplicata LSA (LSA qui réside déjà dans la base des données du DUT, mais différente de celle envoyée précédemment)
- Le DUT accusera cette deuxième LSA immédiatement et note le temps de l'acquittement. Ce temps est appelé newLSAprocTime.

Le temps requis pour le traitement du nouveau LSA est calculé par soustraction de dupLSAprocTime de newLSAprocTime.

- Mise en œuvre du scénario 1 :

On exécute ces tests en utilisant les routeurs ayant comme router-id 192.168.1.2 et 192.168.1.241. On envoie un LSA qui correspond à un ajout de réseau à l'aire comme suit :

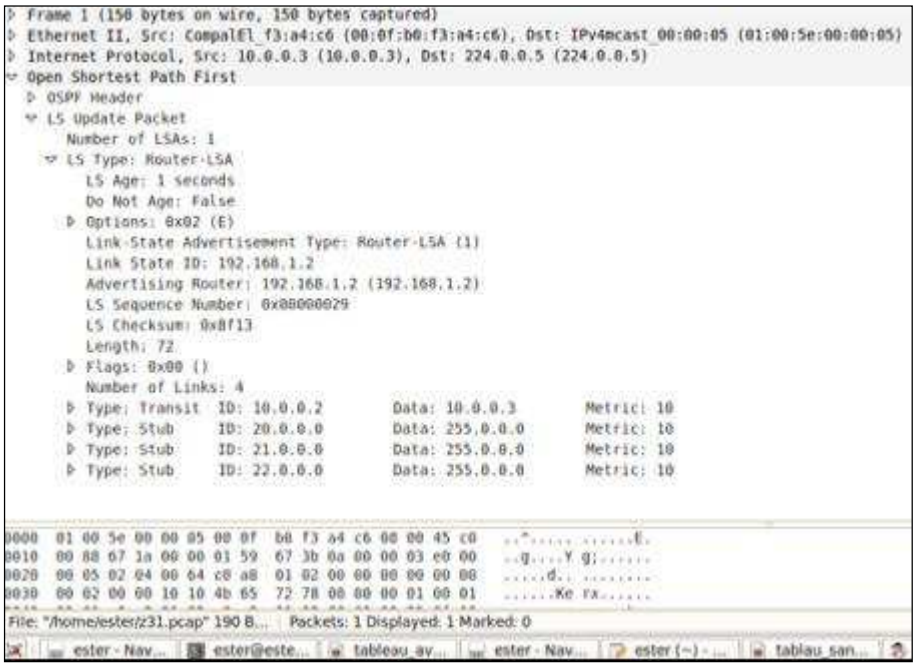


Figure 27: Illustration scénario 1 (1/3)

On enregistre le paquet correspondant au LSA avec la fonctionnalité offerte par Ethereal.

On rejoue ce paquet en utilisant la commande suivante:

sudo tcpreplay –i eth0 z31.cap (fichier contenant du paquet LSA qui correspond à un ajout de réseau à l'aire)

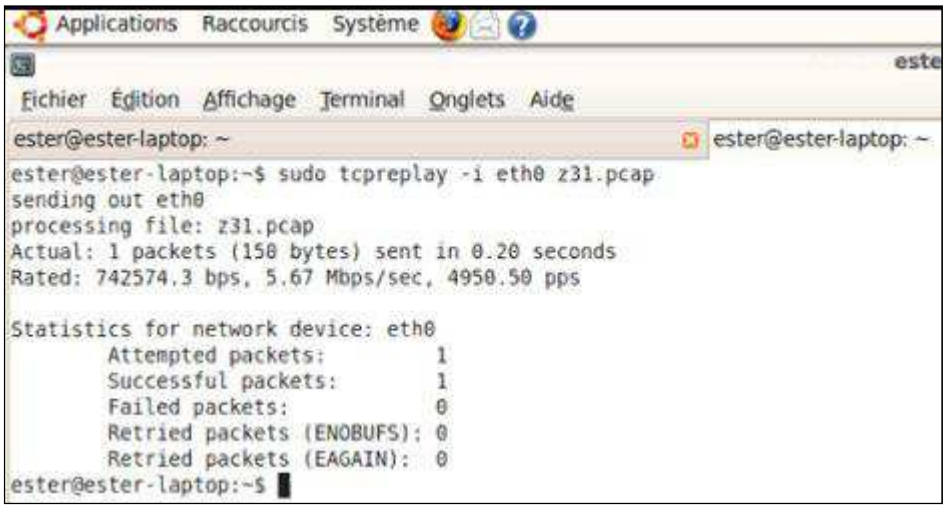


Figure 28: Illustration scénario 1 (2/3)

On calcule le temps T_1 correspondant au temps entre l'envoi du paquet et entre la réception de l'acquittement.

Ensuite, on envoie un nouveau LSA correspondant à l'ajout d'une nouvelle route. De plus, on renvoie par la suite le même paquet de la première étape et on calcule le temps T_2 entre l'envoi du paquet et la réception du LSA. Le temps requis pour le traitement du nouveau LSA est calculé par soustraction de T_1de T_2.

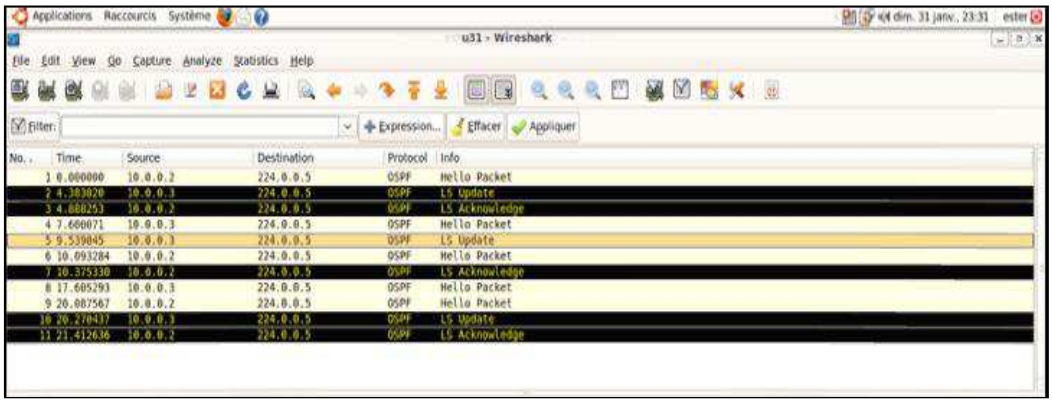


Figure 29: Illustration scénario 1 (3/3)

On répète la même opération avec des tailles de LSA différentes.

- **Scénario 2**

- Description :

Nous allons calculer le temps nécessaire pour un routeur pour prendre en compte les changements au réseau OSPF. Ainsi, nous allons changer le coût du lien au niveau du lien entre 192.168.1.241 et 192.168.1.2 et voir le temps nécessaire au routeur 12.0.0.2 pour prendre en compte ces changements.

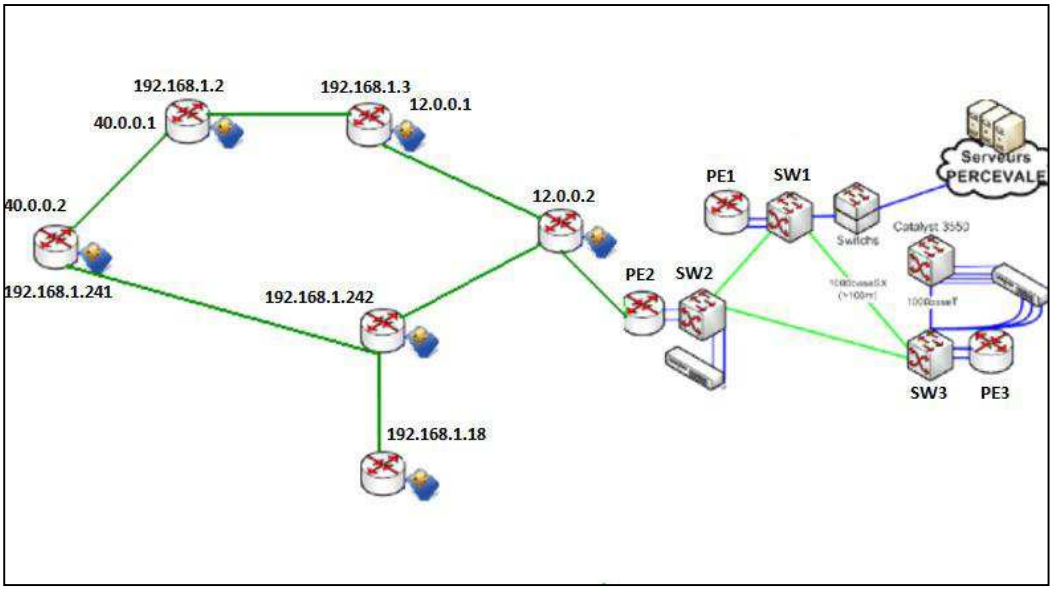


Figure 30: Illustration du scénario 2

- Mise en œuvre du scénario 2 :

Le scénario 2 est conçu pour calculer le temps nécessaire pour la convergence. Il sera exécuté en premier temps avec la version sans ESTER d'OSPF puis avec la version ESTER.

Nous générons du trafic depuis le routeur 12.0.0.2 à l'interface 40.0.0.2 qui existe sur le routeur 192.168.1.241.

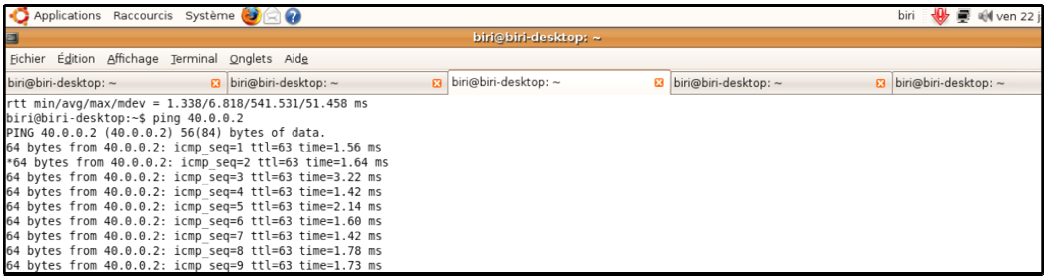


Figure 31: Illustration scénario 2 (1/5)

Le trafic passe au départ par le routeur 192.168.1.242. Voici le résultat de trace-path

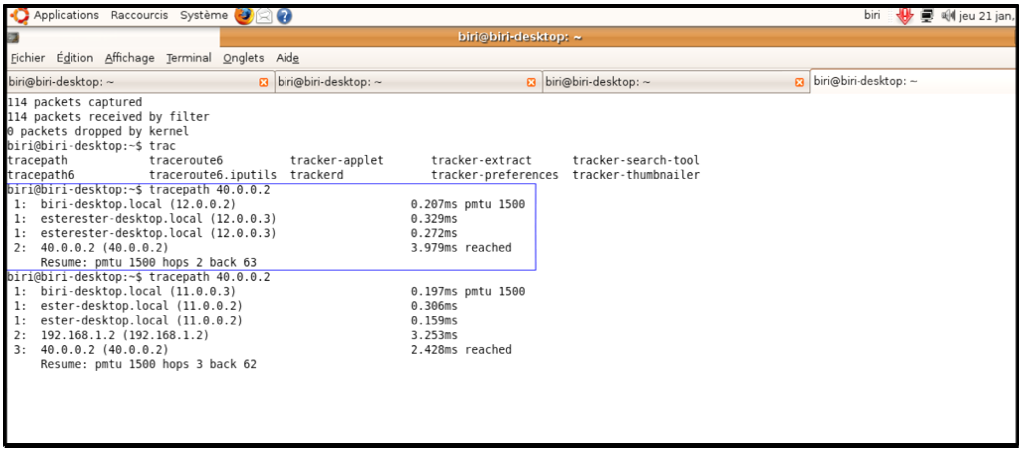


Figure 32: Illustration scénario 2 (2/5)

Ensuite on change fixe à 40 le lien entre 192.168.1.241 et 192.168.1.242 pour pouvoir faire changer le chemin du trafic depuis le routeur 192.168.1.2. Ainsi le trafic passe par le routeur 192.168.1.2 si le coût du chemin entre 192.168.1.2 est 192.168.1.241 est à 10 et ne passera pas s'il est à 40.

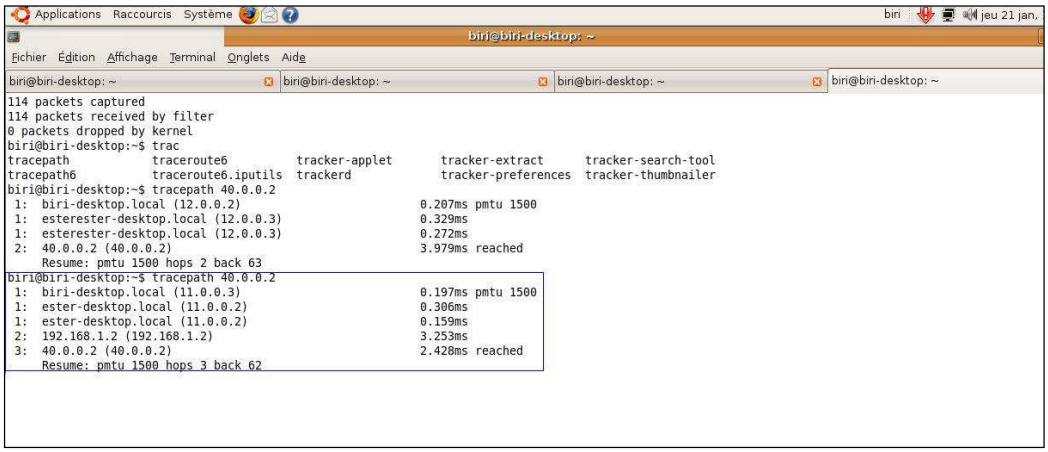


Figure 33: Illustration scénario 2 (3/5)

On procède de la manière suivante pour changer le coût au niveau de 192.168.1.2 du chemin entre 192.168.1.2 est 192.168.1.241

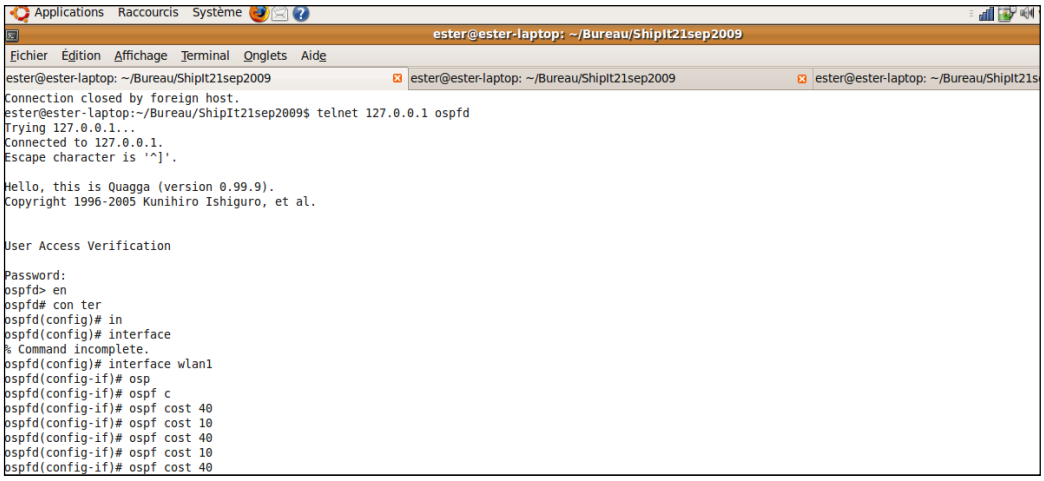


Figure 34: Illustration scénario 2 (4/5)

Lorsqu'on change le coût à 10, un LSA est envoyé et après un laps de temps le trafic repasse par ce routeur.

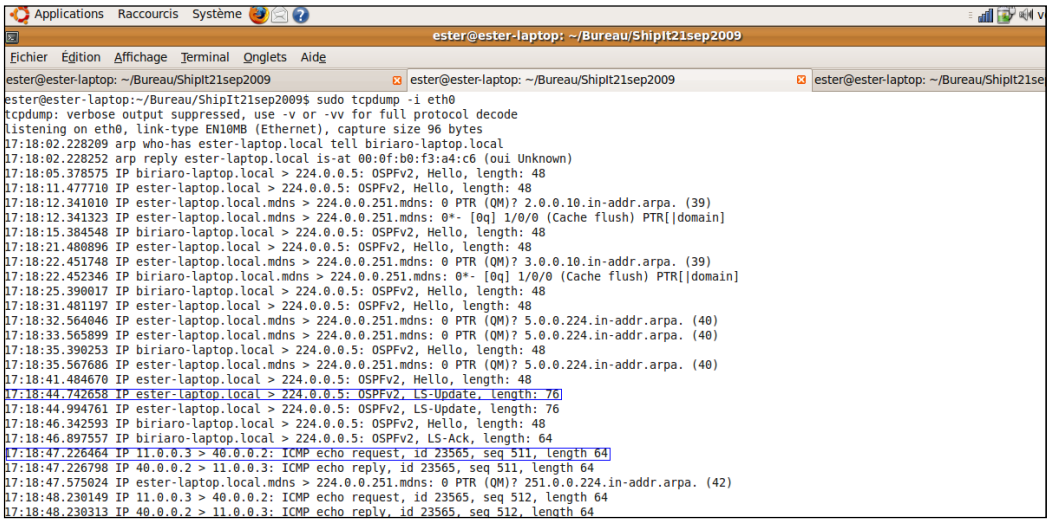


Figure 35: Illustration scénario 2 (5/5)

Le temps de convergence est donné par la soustraction du temps de changement de coût (donc d'envoi d'un LSA update) du temps de réception du trafic envoyé par le routeur 12.0.0.2.

- **Scénario 3**

- Description :

Nous allons calculer le temps nécessaire pour un routeur pour recalculer une table de routage après un changement de coûts. Ainsi, nous allons changer le coût du lien au niveau du lien entre 12.0.0.2 et 192.168.1.242 et voir le temps nécessaire au routeur 12.0.0.2 pour recalculer la table de routage selon le nombre de liens.

- Mise en œuvre du scénario 3 :

Le scénario 3 est conçu pour calculer le temps de re-calcul de la table de routage. Il sera exécuté en premier temps avec la version sans ESTER d'OSPF puis avec la version ESTER.
Nous le faisons pour un nombre de liens de 31, 36, 41, 46 et 51.

Nous envoyons du trafic du routeur 12.0.0.2 vers le routeur 192.16.1.241 comme suit :

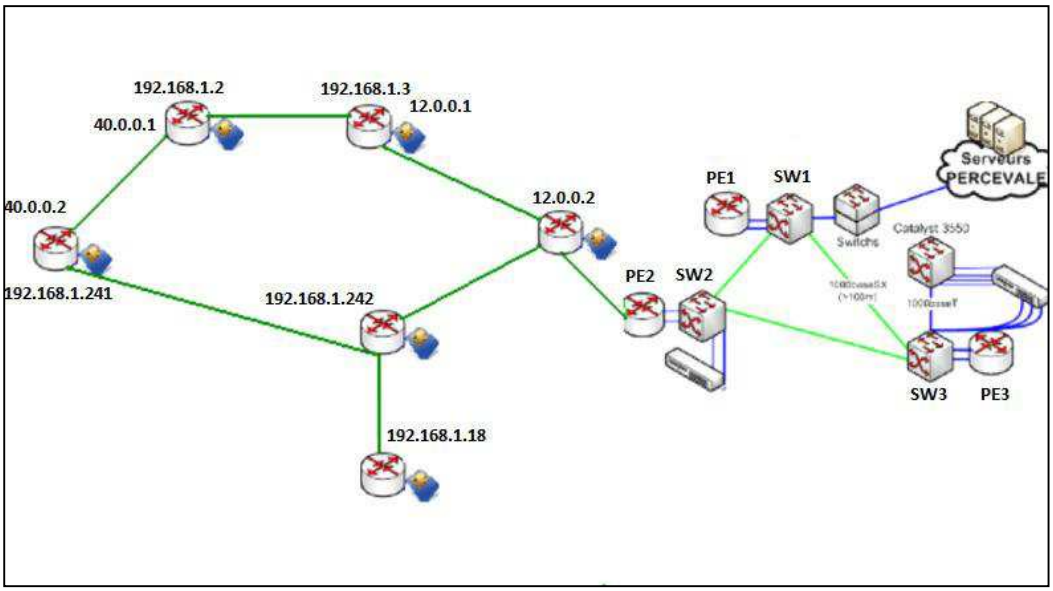


Figure 36: Illustration scénario 3 (1/4)

Ensuite, nous changeons le coût du chemin entre le routeur 12.0.0.2 et le routeur 192.168.1.242 :

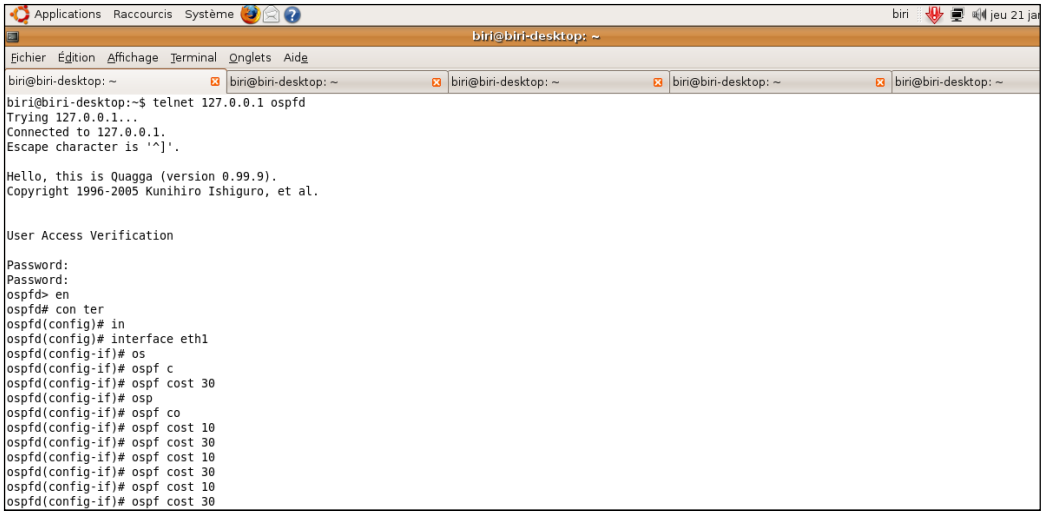


Figure 37: Illustration scénario 3 (2/4)

Le changement de coût provoque l'envoi de LSA. Le trafic passe par le routeur 192.168.1.3 lorsque le coût est à 30 et passe par le routeur 192.168.1.242 lorsque le coût est à 10.

La figure ci-dessous décrit la trace de tcpdump explicitant l'envoi du paquet LSA update et le passage du trafic par l'interface eth0 après le changement de coût à 30.

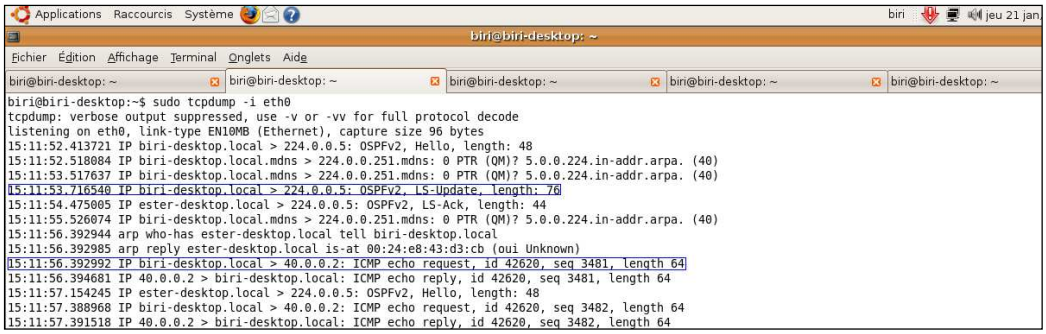


Figure 38: Illustration scénario 3 (3/4)

La figure ci-dessous décrit la trace de tcpdump explicitant l'envoi du paquet LSA update et le passage du trafic par l'interface eth0 après le changement de coût à 10.

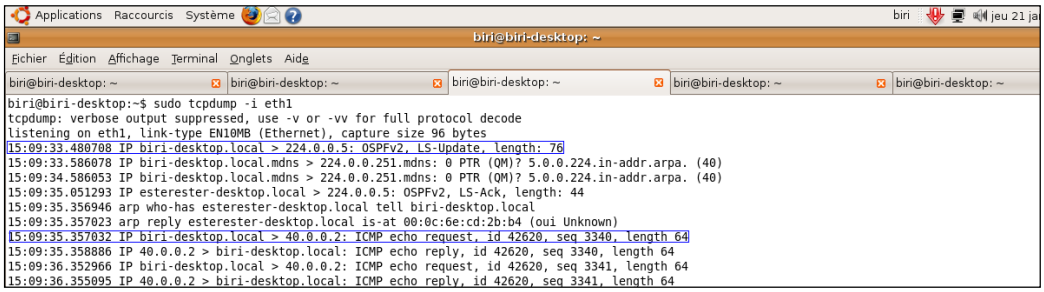


Figure 39: Illustration scénario 3 (4/4)

- **Résultats des tests**

On présente ci-dessous le temps d'exécution des composants participant à la fonction de routage. Les mesures sont en microsecondes.

- Calcul du temps de traitement d'un message LSA :

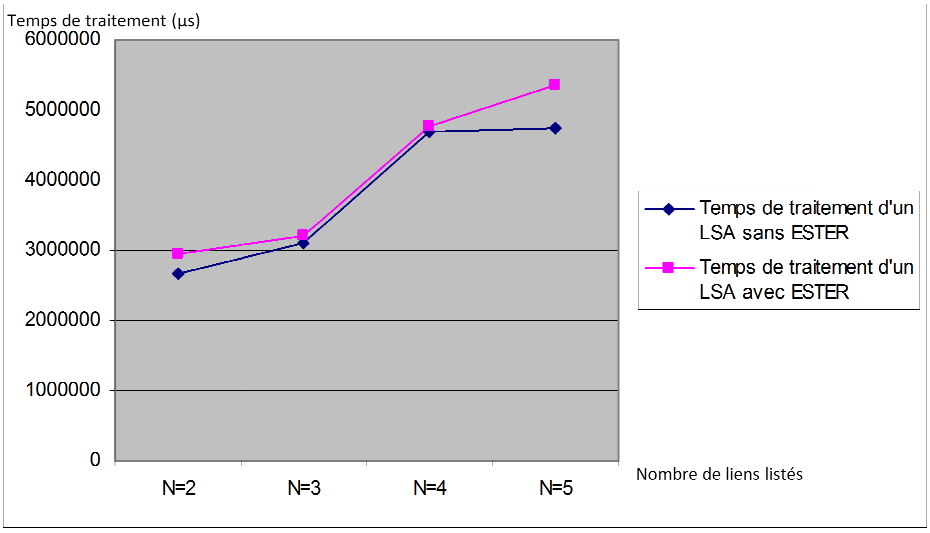


Figure 40 : Comparaison du temps de traitement LSA avec et sans le module ESTER

Le temps de traitement LSA augmente peu avec l'introduction du module ESTER. Cette augmentation est du au temps nécessaires aux opérations relatives à la vérification de la signature.

- **Calcul du temps de convergence :**

Le temps de convergence augmente également peu avec l'introduction du module ESTER. Le temps de convergence sans la solution ESTER est en moyenne 2545697 µs et 2603270 µs avec la solution avec ainsi une augmentation de 2% en moyenne. Cette augmentation est dû au fait que nous avons rajouté une partie dans le prototype pour protéger la table de liens comme décrit dans la figure 10 ainsi que le temps nécessaire pour les opérations dédiées à la vérification de la signature.

- Calcul du temps de re-calcul de la table de routage en fonction du nombre de liens :

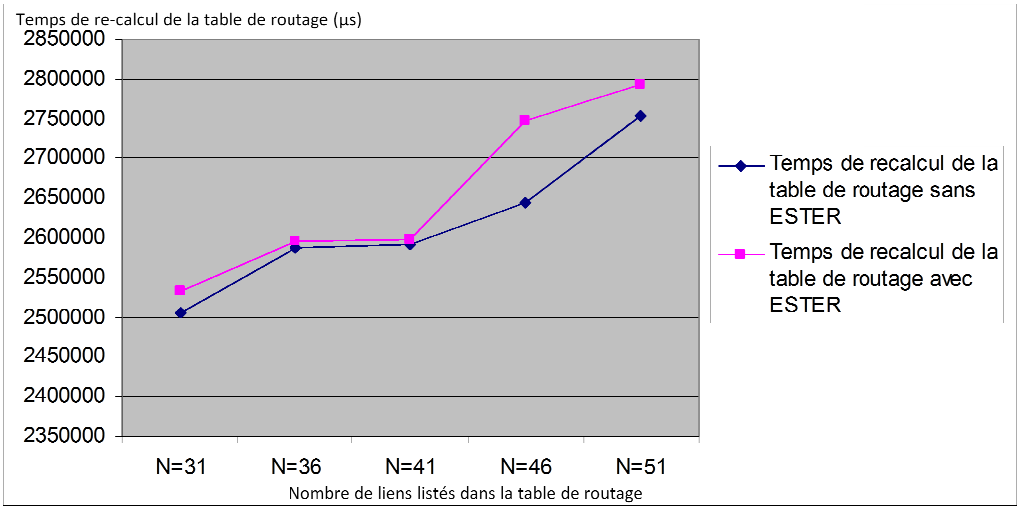


Figure 41 : Comparaison du temps de re-calcul de la table de routage avec et sans ESTER

Le temps de re-calcul de la table de routage augmente peu avec l'introduction du module ESTER. Cette augmentation est dû au fait que nous avons rajouté une partie dans le prototype pour protéger la table de liens.

Nous avons décrit dans ce document la plateforme du démonstrateur et les scénarios de tests adoptés pour évaluer les performances de notre prototype et les comparer avec ceux du logiciel Quagga[31]. Ils ont permis de mesurer les éléments suivants:

- ✓ Temps requis pour traiter une LSA
- ✓ Temps de convergence
- ✓ Temps de re-calcul d'une table de routage après un changement.

[31] Quagga est une suite de routage implémentant les protocoles OSPF (v2 & v3), RIP (v1, v2 & v3) et BGP (v4)

Le temps de traitement LSA augmente peu avec l'introduction du module ESTER. Cette augmentation est due au temps nécessaire pour les opérations dédiées à la vérification de la signature. Le temps de convergence augmente également peu avec l'introduction du module ESTER. Le temps de convergence sans la solution ESTER est en moyenne 2545697 µs et 2603270 µs avec la solution avec ainsi une augmentation de 2% en moyenne. Cette augmentation est dû au fait que nous avons rajouté une partie dans le prototype pour protéger la table de liens ainsi que le temps nécessaire pour les opérations dédiées à la vérification de la signature.

Le temps de re-calcul de la table de routage augmente également peu avec l'introduction du module ESTER. Cette augmentation est dû au fait que nous avons rajouté une partie dans le prototype pour protéger la table de liens. Ainsi, la solution ESTER permet de renforcer la sécurité du protocole OSPF avec un impact raisonnable sur les performances.

3.4 Mécanisme de protection contre l'usurpation des adresses IP des clients abonnés à un fournisseur de services Internet

3.4.1 Introduction

Les fournisseurs de service Internet n'offrent pas de mécanismes permettant de vérifier si un client est bien en droit d'utiliser une adresse IP donnée.

En effet, les fournisseurs de service Internet utilisent, généralement en Europe comme indiqué dans les tableaux suivants, le protocole PPPoA [26] (Point-to-Point Protocol over ATM) qui est un protocole d'encapsulation de PPP sur ATM décrit dans le RFC 2364, utilisé par les connexions haut débit ADSL et câble

Carriers and ISP	**connexion mode**
AOL France	PPPoE / RFC 1483 bridge mode
AOL UK	PPPoA mode
BT	PPPoA mode
Belgacom / Skynet	PPPoE / RFC 1483 bridge mode
France Telecom / Wanadoo France	PPPoA mode PPPoE / RFC 1483 bridge mode
Freeserve	PPPoA mode
Portugal Telecom / Telepac	PPPoE / RFC 1483 bridge mode
Telecom Italia	PPPoA mode PPPoE / RFC 1483 bridge mode
Telecom Italia Business	Fixed IP / RFC 1483 router mode
Telefonica	Fixed IP / RFC 1483 router mode
Tiscali France	PPPoA mode
Tiscali Italia	PPPoA mode

Pays	**Réseau**	**VPI**	**VCI**	**Encapsulation**
France	FT	8	35	PPPoA VCmux
United Kingdom	BT	0	38	PPPoA VCmux
Germany	DT	1	32	PPPoE LLC
Spain	Telefonica	8	32	RFC1483 routed or PPPoE LLC
Spain	Retevision	8	35	PPPoA VCmux
Belgium	Belgacom	8	35	PPPoA VCmux
Netherlands	KPN	8	48	PPPoA VCmux
Italy	Telecom Italia	8	35	PPPoA VCmux
Portugal	PT	0	35	PPPoE LLC

Tiscali UK	PPPoA mode
Wanadoo Espana	Fixed IP / RFC 1483 router mode

Tableau 5: Mode de connexion par FSI

destinées aux particuliers. Ce protocole offre des fonctionnalités PPP standards telles que l'authentification, le chiffrement et la compression. La configuration PPP utilise généralement des informations sur des clients (identifiant et mot de passe) et est unique à chaque utilisateur. La configuration ATM inclut des liens virtuels (identifiant du chemin virtuel et identifiant du circuit virtuel (VPI/VCI)), la modulation G.DMT et l'encapsulation VC-MUX.

Comme le protocole PPPoA ne permet pas de vérifier si un client est en droit d'utiliser une adresse donnée, un attaquant peut par exemple se connecter frauduleusement à son réseau WI-FI et donc utiliser l'adresse IP du client légitime pour effectuer des activités interdites.

De ce fait, nous allons proposer dans ce sous-chapitre un mécanisme permettant de faire la correspondance entre l'adresse IP d'un client et son matériel cryptographique. Ainsi un attaquant n'aura pas la possibilité d'usurper son adresse IP.

Nous allons classer, passer en revue et évaluer dans la section 3.4.2 les différentes méthodes permettant la prévention contre les attaques utilisant la technique d'usurpation d'identité. La section 3.4.3 décrit le protocole « Domain Name System Security Extensions » (DNSSEC). Nous présentons par la suite dans la section 3.4.4 notre solution. La section 3.4.5 présente l'évaluation formelle de notre solution et les résultats obtenus.

3.4.2 Les méthodes de prévention contre les attaques d'usurpation d'identité

Nous passons en revue et évaluons dans cette section les différentes méthodes permettant la prévention contre les attaques utilisant la technique d'usurpation d'identité. Ces méthodes sont classées en quatre familles distinctes selon qu'elles se basent sur :

- ✓ Le contrôle de certaines valeurs au niveau des paquets ;
- ✓ La collaboration entre les domaines de l'émetteur et du destinataire ;
- ✓ La génération de paquets de contrôle et de surveillance ;
- ✓ Le contrôle de l'accès au réseau.

- **Méthodes basées sur le contrôle de valeurs au niveau des paquets :**

Les mécanismes de protection contre l'usurpation d'identité basée sur le contrôle de valeurs au niveau des paquets sont comme suit :

- **La méthode « Distance Vector Filtering » (DVF)**

- **Description**: La méthode « Distance Vector Filtering » (DVF) [33] est basée sur l'observation qu'un routeur de bordure en cours d'exécution dans des échanges de routage intra-domaine peut facilement connaître le nombre de sauts le séparant de tout autre routeur dans le même domaine. Dans le cadre de cette méthode, les paquets sont filtrés en se basant à la fois sur l'interface d'arrivée des paquets et sur la valeur du TTL (Time-To-Live) du paquet pour savoir si ce paquet est passé par le bon nombre de sauts et si les paquets arrivent bien à l'interface appropriée.

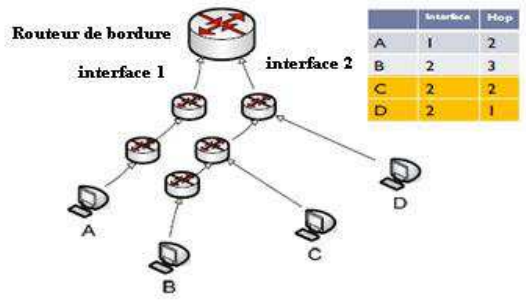


Figure 42: Illustration de la méthode DVF

La figure 41 décrit un exemple de table de correspondance obtenu suite l'application par le routeur de bordure de la méthode DVF.

Ainsi, cette table de correspondance décrit le nombre de hop séparant chacun des routeurs A, B, C, D du routeur de bordure ainsi que l'interface d'arrivée au niveau du routeur de bordure des paquets issues de chacun de ces routeurs.

- **Evaluation :**

▪ **Le protocole « Source Address Validity Enforcement Protocol » (SAVE):**

- **Description**: Pour valider la légitimité d'une adresse IP source d'un paquet donné, le protocole SAVE [38] construit une table de correspondance qui associe chacune des interfaces d'arrivée d'un routeur avec un ensemble d'adresses IP. Le protocole SAVE s'exécute sur chaque routeur IP et vérifie si un paquet IP arrive à la bonne interface ou pas. En faisant correspondre les adresses IP entrantes avec des interfaces, l'ensemble des adresses IP source qu'une personne malveillante pourraient être usurpées est considérablement réduit. Un routeur de bordure doit disposer d'un espace d'adresses source couvrant les adresses d'un réseau local, afin de transmettre ses paquets de données. L'espace d'adressage source d'un système autonome est donc géré par le(s) routeur(s) de bordure. Un routeur de transit sans aucun hôte a un

espace d'adressage source constitué par l'ensemble de ses propres adresses IP. La mise à jour SAVE est soit générée périodiquement par un routeur SAVE pour chacune des entrées de la table de transfert du routeur ou soit provoquée par des changements au niveau de la table de transfert.

- **Evaluation**: L'avantage de ce protocole est qu'il ne génère pas de faux positifs. Les inconvénients sont qu'il peut générer des faux négatifs et qu'il est difficile de concevoir un protocole de mise à jour des tables de correspondance qui associe chacune des interfaces d'arrivée d'un routeur avec un ensemble d'adresses IP.

▪ **La méthode « Passeport de paquets »**

- **Description**: Le concept de « passeport de paquets » [65] fait référence à une séquence de numéros de systèmes autonomes et de valeurs cryptographiques correspondantes consistant en des Codes d'Authentification de Messages (CAM ou MAC (Message Authentication Code) en anglais). Chaque valeur MAC est calculé en utilisant une clé secrète partagée entre le domaine source et un domaine par lequel transite le paquet. Un hôte envoie un paquet sans passeport. Le paquet est vérifié par le routeur de bordure comme étant originaire d'un hôte dans le domaine et si c'est le cas, il lui rajoute un passeport. Lorsqu'un domaine de transit reçoit un paquet, il valide la valeur MAC qui lui correspond à l'aide d'une clé secrète qu'il partage avec le domaine source. Comme la clé n'est connue que par le domaine source et le domaine du transit, la validation de la valeur du MAC permet de démontrer que le paquet est bien originaire du domaine source.

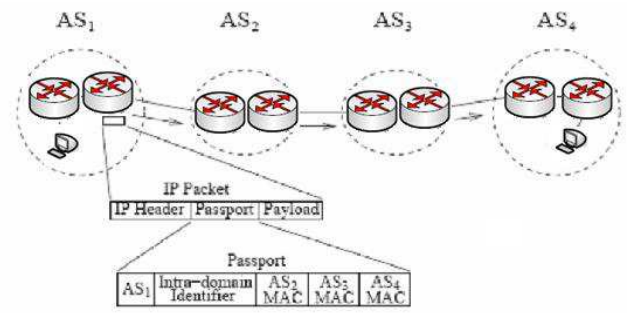


Figure 43:Illustration de la méthode «Packet Passport »

La figure 42 illustre le contenu d'un paquet construit par le routeur de bordure du domaine AS_1. Ce paquet inclut le « passeport » contenant le numéro de AS1 ainsi que les valeurs de AS_2 MAC, AS_3 MAC, AS_4 MAC qui vont permettre respectivement aux routeurs de transit de AS_2, AS_3, AS_4 de vérifier que le paquet provient bien de AS_1.

- **Evaluation** : L'avantage de ce concept est que les paquets falsifiés sont éliminés car même si les routeurs de bordure d'un domaine sont compromis, ils ne peuvent falsifier les passeports de tous les autres domaines. Toutefois, ce protocole est complexe à mettre en œuvre vu qu'il implique le partage de clés secrètes entre domaines. De plus, ce protocole peut générer de faux positifs surtout lorsque le routage n'est pas stable.
- **Méthodes basées sur la collaboration entre les domaines de l'émetteur et du destinataire :**

Les mécanismes de protection contre l'usurpation d'identité basés sur la collaboration entre les domaines de l'émetteur et du destinataire sont comme suit :

- **La méthode basée sur la valeur du TTL[32] :**

[32] Le TTL est une donnée placée au niveau de l'en-tête du paquet IP qui indique le nombre de routeurs maximal de transit.

- **Description**: Le filtrage « Hop-count » [37] a été conçu sur la base de l'observation que la plupart des paquets IP usurpés arrivent aux victimes avec des valeurs de sauts non compatibles avec celles des paquets légitimes. Ce mécanisme construit une table de correspondance nommée IP2HC (IP To hop-count) qui associe un nombre de sauts à une adresse IP donnée. Il regroupe les préfixes des adresses en se basant sur le nombre de sauts afin de réduire un espace optimisé de stockage. Les valeurs des nombres de sauts sont mises à jour pour tenir compte des changements pouvant survenir au niveau du réseau.
- **Evaluation**: L'avantage de ce mécanisme est qu'il est simple à mettre en œuvre. Les inconvénients sont que la valeur du TTL est facile à falsifier et qu'il peut générer de faux positifs surtout lorsque le routage n'est pas stable.

▪ **La méthode « Spoof Prevention Mechanism » (SPM)**

- **Description**: Dans l'architecture de SPM [2], une clé numérique est calculée pour marquer le trafic entre un système autonome source et un système autonome destination. La clé est rajoutée à chaque paquet quittant le domaine source et allant vers le domaine destination. L'authenticité des paquets est vérifiée par des routeurs du domaine destination, et les clés sont supprimées des paquets après cette phase. Un routeur doit effectuer entre autres les opérations suivantes afin d'être en mode SPM:

1) Marquer les paquets sortants avec la clé appropriée.

2) Vérifier l'authenticité de la clé des paquets entrants.

La distribution de la clé peut être réalisée par la conception d'un protocole dédié à la distribution.

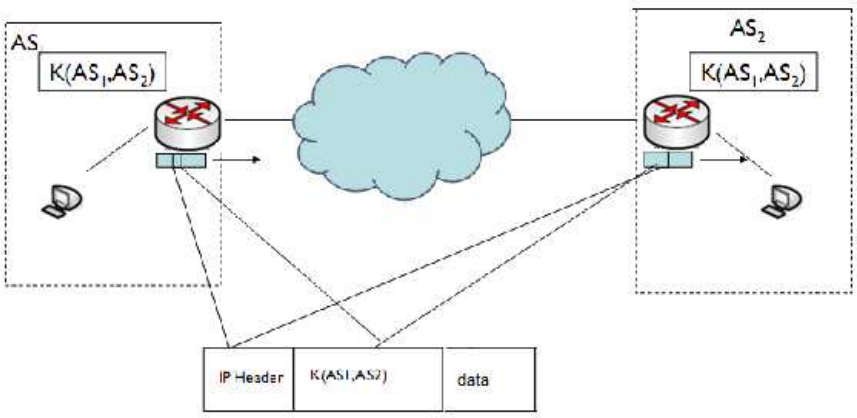


Figure 44: Illustration de la méthode SPM

La figure 43 décrit le paquet construit par le routeur de bordure du domaine AS_1 contenant l'entête IP, la clé partagée entre les domaines AS_1 et AS_2 ainsi que les données.

- **Evaluation** : Les avantages de cette architecture est qu'elle peut être déployée de manière incrémentale et qu'elle présente des incitations à son déploiement comme par exemple la simplicité de sa mise en oeuvre. L'inconvénient de cette architecture est que les concepteurs du SPM supposent que les domaines de transit sont de confiance et que les attaquants ont seulement accès aux équipements de bordure et ne vont donc pas user de la clé partagée entre le domaine source et le domaine destination pour de mauvais escients.

▪ **La méthode APPA (Automatic Peer-to-Peer Anti-spoofing):**

- **Description**: APPA [63] est une méthode de prévention de l'usurpation d'identité basée sur l'utilisation de signature. APPA opère sur deux niveaux: au niveau d'un système autonome et au niveau de la communication entre les systèmes autonomes. Au niveau d'un système autonome, une clé à usage unique est insérée dans chaque paquet sortant et vérifiée par le routeur du système autonome source. Au niveau de la communica-

tion entre les systèmes autonomes, le routeur de bordure du domaine source génère périodiquement une clé changeante qui est insérée dans le paquet sortant et que le routeur de bordure du domaine destination vérifie et supprime. Les clés sont mises à jour automatiquement grâce à une machine à état qui se synchronise automatiquement entre les deux routeurs. En effet, à chaque état correspond une clé et la transition entre les états enduit donc le changement des clés. Cette transition d'état est réalisée au de l'émetteur lors de l'envoi d'un paquet et au niveau du récepteur lors la réception du paquet.

- **Evaluation**: Les avantages de la méthode APPA sont que les équipements de bordure ne peuvent pas usurper les adresses de leur système autonome, que le coût d'exécution et de gestion est très faible et que le déploiement de cette méthode peut être incrémentale. L'inconvénient de cette méthode est la difficulté à mettre à jour automatiquement les clés.

- Méthodes basées sur la génération de paquets de contrôle et de surveillance:

▪ **Le mécanisme « Active Internet Trafic Filtering » (AITF)**

- **Description**: Le mécanisme « Active Internet Traffic Filtering (AITF) » [42] est destiné à empêcher le déni de service distribué (DDoS). Quand une victime identifie un flux indésirable, elle envoie une requête de filtrage à sa passerelle. Le flux indésirable est alors temporairement bloqué par la passerelle de la victime. Ensuite, la passerelle de la victime déclenche un accord de non transmission de certains paquets avec le routeur en bordure de l'AS situé près de la source d'attaque (désigné par passerelle d'attaque). Ensuite, la passerelle de la victime retire son filtre temporaire. La passerelle de la victime peut relayer la demande de filtrage à un routeur proche de la passerelle d'at-

taque si la passerelle d'attaque ne coopère pas. L'escalade peut se poursuivre d'une manière récursive jusqu'à ce qu'un routeur sur le chemin de l'attaque réponde et qu'un accord de non transmission de certains paquets est assuré. Si aucun routeur ne répond, le trafic de l'attaque est bloqué localement par la passerelle de la victime.

- **Evaluation**: L'avantage de cette méthode est qu'elle incite les routeurs proches de la source de l'attaque à bloquer son trafic. L'inconvénient est qu'elle peut générer des faux positifs.

▪ **ITrace**

- **Description**: Dans le mécanisme « ICMP Traceback » (ITrace) [55], un nouveau type de message ICMP est défini pour véhiculer l'information sur les itinéraires qu'un paquet IP a pris. Dans ce schéma, un message ITrace est généré quand un paquet IP passe par un routeur et est envoyé de manière aléatoire, avec une probabilité égale, à la destination ou à l'origine des paquets IP. Afin de réduire le trafic supplémentaire, ce message est généré avec une faible probabilité d'environ 1 / 20000.

- **Evaluation**: Ce mécanisme présente des avantages et des inconvénients. L'avantage de ce mécanisme est qu'il est facile à mettre en œuvre. L'inconvénient est que les messages ITrace sont générés aléatoirement ce qui restreint la capacité de ce mécanisme à détecter des paquets usurpés.

▪ **La méthode "Hash-based IP Traceback"**

- **Description**: La méthode « Hash-based IP Traceback » [6] génère des rapports d'audit pour le trafic dans le réseau. Il peut alors remonter à l'origine d'un paquet IP émis dans un passé récent.

- **Evaluation** : Cette technique peut générer des faux positifs.

- Méthodes basées sur le contrôle de l'accès au réseau

Les mécanismes de protection contre l'usurpation d'identité basés sur le contrôle de l'accès au réseau sont comme suit :

- **Filtrage en Entrée/Sortie :**

- **Description** : Le filtrage en entrée est une politique de «bon voisinage» qui repose sur la coopération mutuelle entre les FSI et ce pour leur bénéfice mutuel. Les meilleures pratiques actuelles pour le filtrage en entrée sont documentées par l'IETF dans le BCP 38 [53], qui est actuellement défini par la RFC 2827. BCP 38 recommande que les fournisseurs en amont filtrent les paquets IP provenant de leurs clients, et éliminent tous les paquets ayant une adresse source non appropriée. Le filtrage en sortie consiste en la surveillance et éventuellement, la restriction des flux d'informations allant d'un FSI à un autre.

- **Evaluation** : L'inconvénient de ce mécanisme est qu'il n'est pas approprié dans le cadre d'un réseau ayant plusieurs connexions à différents FSI (multihomed). En effet, un paquet ayant une adresse IP source d'un FSI 1 peut sortir par le réseau du FSI 2. De ce fait, il ne devrait pas être filtré.

- **CGA based Source Address Authorization and Authentication (CSA) :**

- **Description :** Dans le cadre du mécanisme « CSA » [80], un hôte génère un identifiant auto-certifié, et le routeur d'accès lie cet identifiant avec l'adresse de l'hôte. Un secret partagé appelé « signature seed » est également échangé entre l'hôte et le routeur d'accès. Quand l'hôte veut envoyer des paquets, il rajoute au paquet une chaîne de bits générés à partir de la « signature seed ». Le routeur d'accès peut ainsi vérifier si la signature est correcte ou pas.

- **Evaluation :** L'inconvénient de ce mécanisme est que le routeur de bordure doit avoir un secret partagé avec chaque client.

- **Les mécanismes Ethane et «TCG's Trusted Network Connect (TNC) » :**

Les mécanismes Ethane [82] et «TCG's Trusted Network Connect (TNC) » [83] ont des approches similaires pour gérer l'accès au réseau, c'est pour cela que nous avons décidé de regrouper leurs descriptions dans la même section.

Éthane contrôle le réseau en imposant la nécessité d'une permission explicite pour toute communication entre hôtes.

Ce contrôle est réalisé à travers ces deux composantes principales :

- Contrôleur central: le contrôleur central contient la stratégie globale du réseau qui détermine la destination de tous les paquets. Quand un paquet arrive au contrôleur, il décide si le flux représenté par ce paquet devrait être autorisé ou pas. Le contrôleur connaît la topologie globale du réseau et réalise un calcul d'itinéraire pour les flux autorisés. Elle accorde l'accès en permettant explicitement les flux au sein des commutateurs réseau qui existent tout au long du parcours choisi. Le contrôleur peut être répliqué pour les besoins en redondance et en performances.

- Un ensemble de commutateurs ETHANE: Composés simplement d'un tableau de flux et d'un canal sécurisé avec le contrôleur, les commutateurs transmettent simplement les paquets sous la direction du contrôleur. Quand un paquet arrive et qui n'est pas dans le tableau des flux, ils transmettent le paquet au contrôleur, ainsi que des informations concernant le port par lequel le paquet est arrivé. Quand un paquet arrive et que le flux correspond est présent dans le tableau des flux, il est transmis conformément à la directive du contrôleur. Selon la conception d'ETHANE, il est permis de rajouter les commutateurs ETHANE graduellement, et le réseau devient plus facile à gérer avec chaque commutateur supplémentaire.

L'architecture TNC définit trois entités de base:

- Le demandeur d'accès
- Le point de décision
- Le « point de vérification/contrôle de la politique »

Le demandeur d'accès est l'entité qui tente d'accéder au réseau. Le point de décision est l'entité qui décide si l'accès devrait être accordé ou pas en se basant sur les politiques du réseau et le « point de vérification/contrôle de la politique » est l'entité qui met en œuvre la décision d'accorder soit l'accès au réseau complet, soit un accès limité ou soit pas d'accès du tout.

- **Discussion :**

Ces trois mécanismes sont plus ou moins simples à mettre en œuvre. Cependant, il ne protège les paquets qu'au niveau de l'accès.

3.4.3 Présentation de DNSSEC

Le Domain Name System (DNS) est un service permettant d'établir une correspondance entre une adresse IP et un nom de domaine grâce à sa base de données répartie contenant des enregistrements, appelés RR (Resource Records). La conception du service DNS n'a pas pris en compte les aspects relatifs à la sécurité et les extensions « Domain Name System Security Extensions » (DNSSEC) [84] ont été proposés pour protéger le DNS, tout en conservant la compatibilité ascendante. DNSSEC offre les services suivants :

- sécurisation des transactions DNS ;
- sécurisation des informations contenues dans les messages DNS par le biais de l'authentification de leur origine ainsi que par la garantie de leur intégrité durant le transport ;

- stockage et distribution des clés nécessaires au bon fonctionnement des deux premiers services cités ci-dessus.

Notons que les extensions DNSEC adressent les menaces recensées dans la RFC 3833. Ainsi, DNSSEC a été conçu pour protéger les résolveurs DNS (clients DNS) des données DNS forgées, telle que celles créées par des attaques de type « empoisonnement de cache DNS »[33]. Toutes les réponses dans DNSSEC sont signées numériquement. En vérifiant la signature numérique, un résolveur DNS est en mesure de vérifier si l'information est identique (correcte et complète) à l'information sur le serveur d'autorité DNS. DNSSEC permet donc d'assurer l'intégrité des données.

DNSSEC ne prévoit pas la confidentialité des données et de ce fait, toutes les réponses DNSSEC sont authentifiés, mais non chiffrées. Les RFC 4033, 4034, et 4035 décrivent en détail le protocole DNSSEC.

Les extensions DNSSEC est basé sur deux niveaux de sécurisation :

- Niveau 1 (local): la signature des enregistrements d'une zone est réalisée par une (des) clé(s) propre(s) à la zone.

- Niveau 2 : Ce niveau tire parti de la structure arborescente du DNS. Ainsi, la connaissance des clés de la racine permettra d'accéder à n'importe quelle zone de manière sécurisée en parcourant les chaînes de confiance.

DNSSEC utilise la cryptographie à clé publique pour la signature numérique des réponses aux requêtes DNS. Pour se faire, plusieurs nouveaux types enregistrement DNS ont été créés [85]: RRSIG, DNSKEY, DS, et NSEC. Lorsque les extensions DNSSEC sont utilisées, chaque réponse à une requête DNS contient un

[33] L'empoisonnement de cache DNS est une technique consistant en l'envoi au serveur DNS de requêtes paraissant valides mais qui sont en réalité falsifiées.

enregistrement DNS RRSIG, outre le type d'enregistrement DNS qui a été demandée. L'enregistrement DNS RRSIG est une signature numérique de l'enregistrement DNS de réponse. La signature numérique peut être vérifiée en utilisant la clé publique correspondante se trouvant dans un record DNSKEY.

Grâce à ces enregistrements figurant dans la réponse, le résolveur DNS du client peut déterminer si la réponse reçue est correcte, si le serveur de noms faisant autorité pour le domaine interrogé ne supporte pas le protocole DNSSEC, ou s'il y a eu une erreur. L'enregistrement DNSKEY est obtenue via une chaîne d'authentification, à commencer par une clé publique connue pour être une bonne ancre de confiance. Cette clé publique peut alors être utilisée pour vérifier un enregistrement DS. Un enregistrement DS dans un domaine parent (zone DNS) peut ensuite être utilisé pour vérifier un enregistrement DNSKEY dans un sous-domaine, qui peut alors contenir d'autres records DS pour vérifier les sous-domaines supplémentaires.

- La procédure de recherche:

La procédure de recherche diffère selon qu'il s'agit de serveurs de noms récursifs, tels que ceux de nombreux FSI, ou d'un résolveur stub, tels que ceux inclus par défaut dans les systèmes d'exploitation grand public des terminaux des utilisateurs.

Prenons l'exemple d'un résolveur récursif : soit un serveur de noms d'un FSI donné qui veut obtenir les adresses IP (enregistrement et / ou enregistrements AAAA) du domaine « www.domaine.com ».

1. Le processus commence quand un résolveur met le bit de flag "DO"[34] (DNSsec OK) dans une requête DNS.

[34] Le flag DO positionné indique le support DNSsec

2. Le résolveur procède à la vérification de la réponse DNS dès sa réception. Idéalement, le résolveur commence par la vérification des records DS et DNSKEY au niveau du DNS racine. Puis il utilise les enregistrements DS pour le domaine de premier niveau « com » trouvé à la racine pour vérifier les records DNSKEY de la zonen «com». De là, il cherche un record DS pour le sous-domaine « domaine.com » dans la zone « com », et si cet enregistrement existe, il utilise l'enregistrement DS pour vérifier un enregistrement DNSKEY se trouvant dans la zone « domaine.com ». Enfin, il vérifie l'enregistrement RRSIG[35] se trouvant dans la réponse pour les enregistrements A de « www. domaine.com ».

Il existe plusieurs exceptions à l'exemple ci-dessus. D'abord, si « domaine.com » ne supporte pas le protocole DNSSEC, il n'y aura pas de record RRSIG dans la réponse et il n'y aura pas un record DS pour « domaine.com » dans la zone «com». Si l'enregistrement DS existe pour « domaine.com », mais qu'il n'existe aucune trace RRSIG dans la réponse, il est possible qu'une attaque de type « homme de milieu » soit en cours.

- Les chaînes d'authentification:

Une chaîne d'authentification est une série de records DS et DNSKEY, en commençant par un point d'ancrage de confiance sur le serveur de noms faisant autorité pour le domaine en question. Une réponse à une requête DNS ne peut pas être correctement authentifiée sans une chaîne d'authentification complète. Pour être en mesure de prouver qu'une réponse DNS est correcte, le résolveur doit au moins connaître une clé ou un enregistrement DS qui soit correct à partir de sources autres que le DNS. Ces sources sont par exemple des points d'ancrage de confiance et sont généralement obtenus los de l'installation du système d'exploi-

35 Les enregistrements RRSIG comportent des signatures numériques qui ont été créés en signant l'enregistrement d'une ressource associée à un nom de domaine en utilisant un DNSKEY

tation ou par une autre source de confiance. Lorsque les extensions DNSSEC ont été conçues à l'origine, on pensait que le point d'ancrage de confiance serait au niveau de la racine DNS. Comme la racine n'a pas encore été signée en 2009 mais en juillet 2010, d'autres points d'ancrage de confiance ont été mis en place comme alternatives à la racine du DNS.

- La gestion des clés:

DNSSEC implique l'usage de différentes clés comme suit:

- Les clés Key Signing Keys (KSK) sont utilisées pour signer les enregistrements DNSKEY. Elles sont stockées au niveau des TLD.
- Les clés de signature de zones (ZSK) sont utilisées pour signer d'autres types d'enregistrements comme les enregistrements RRSIG. Les ZSKs peuvent être changés plus facilement et plus souvent tant qu'ils restent sous le contrôle d'une seule zone DNS. Par conséquent, les ZSKs peuvent être plus courtes que KSKs mais offre le même niveau de protection, tout en réduisant la taille des enregistrements RRSIG et DNSKEY.
- Quand un KSK est créé, l'enregistrement DS doit être transférée et publié à la zone parent. Les enregistrements DS utilisent un condensé du KSK au lieu de la clé complète afin de maintenir la petite taille des records. Ceci est utile pour les zones telles que le domaine com, qui sont très grandes.
- Un système de mise jour des clés est nécessaire afin de permettre le remplacement des clés.

3.4.4 Solution proposée

Notre but est de proposer une architecture de sécurité empêchant les attaques d'usurpation d'adresse IP contre les clients des FSIs. Chaque équipement de connexion aux réseaux des FSIs contient son propre de matériel cryptographique

attribué par son FSI. Lors de sa première connexion au réseau du FSI, le client utilise son matériel cryptographique et une nouvelle proposition de version sécurisée du protocole DHCP[36] qu'on nommera S-DHCP sont utilisés afin de récupérer son adresse IP d'un des serveurs S-DHCP. Ensuite, la correspondance entre son adresse IP et sa clé publique est enregistré auprès soit du serveur DNS du FSI soit auprès du serveur DNS hébergeant la zone du FSI. Ceci est réalisé par le biais d'une proposition DNSSEC+ qui consiste en un rajout d'une nouvelle fonctionnalité à un service DNS ainsi que par la définition d'un nouvel enregistrement DNS. Nous avons décidé de nous baser sur DNSSEC car aujourd'hui le processus de déploiement de DNSSEC est massif pour les zones de premier niveau :

- la quasi-totalité des registres TLD[37] auront signé leurs zones d'ici à 2012 ;
- la racine du DNS a été complètement signée en juillet 2010 ;
- d'importants bureaux d'enregistrement accrédités auprès de l'ICANN[38] travaillent aujourd'hui à l'intégration de DNSSEC et permettront prochainement à leurs clients de signer leurs zones ; notons que certains offrent déjà cette possibilité.

Pour protéger les paquets contre l'usurpation d'adresse IP, La clé publique de l'équipement correspondante à l'adresse IP actuelle doit être utilisée pour assurer la protection de l'entête des paquets générés par les clients. Nous proposons une

---

36 DHCP (Dynamic Host Configuration Protocol) désigne un protocole réseau dont le rôle est d'assurer la configuration automatique des paramètres IP d'une station : une adresse IP, un masque de sous-réseau, l'adresse de la passerelle par défaut et les adresses des serveurs de noms DNS.

37 La structuration du système DNS s'appuie sur une structure arborescente dans laquelle sont définis des domaines de niveau supérieurs (appelés TLD, pour Top Level Domains), rattachés à un nœud racine représenté par un point.

38 L'autorité ultime pour l'allocation des adresses

nouvelle version du protocole Internet Key Exchange (IKE)[39] qu'on nommera « Enhanced IKE » (E-IKE) qui générera les clés pour le mode AH (Authentication Header) d'IPSEC[40]. Notre choix s'est porté sur le mode AH d'IPSEC car l'authentification de l'origine du paquet IP suffit à protéger les paquets contre l'usurpation d'adresse IP. Le routeur en périphérie de l'émetteur ainsi que le routeur en périphérie du destinataire vérifient également les paquets au moyen de la clé que leur ont communiqué respectivement l'émetteur et le récepteur de manière sécurisée. Notre architecture se compose de six entités comme suit:

Racine de confiance pour un domaine	Cette entité contient la racine de confiance du FSI. Elle délivre un certificat X509 à chaque équipement.
Les serveurs S-DHCP	Le serveur DHCP a une paire de clé publique et secrète : Kp_dhcp et Ks_dhcp et implémente S-DHCP
Le routeur en périphérie du client	Le routeur en périphérie contient un matériel cryptographique attribué par l'entité de confiance et implémente notre proposition DNSSEC+
L'équipement du client	L'équipement du client contient un matériel cryptographique attribué par l'entité de confiance
Le routeur de périphérie du FSI de la destination	Le routeur de périphérie implémente notre proposition DNSSEC+
Le serveur DNS hébergeant la zone du FSI	Le serveur DNS implémente notre proposition DNSSEC+

Tableau 6: Description des cinq entités de l'architecture proposée

Cette architecture est illustrée par la figure suivante :

39 IKE est un protocole utilisé pour mettre en place le matériel cryptographique au sein des nœuds déroulant le protocole IPsec.

40 IPSEC est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP

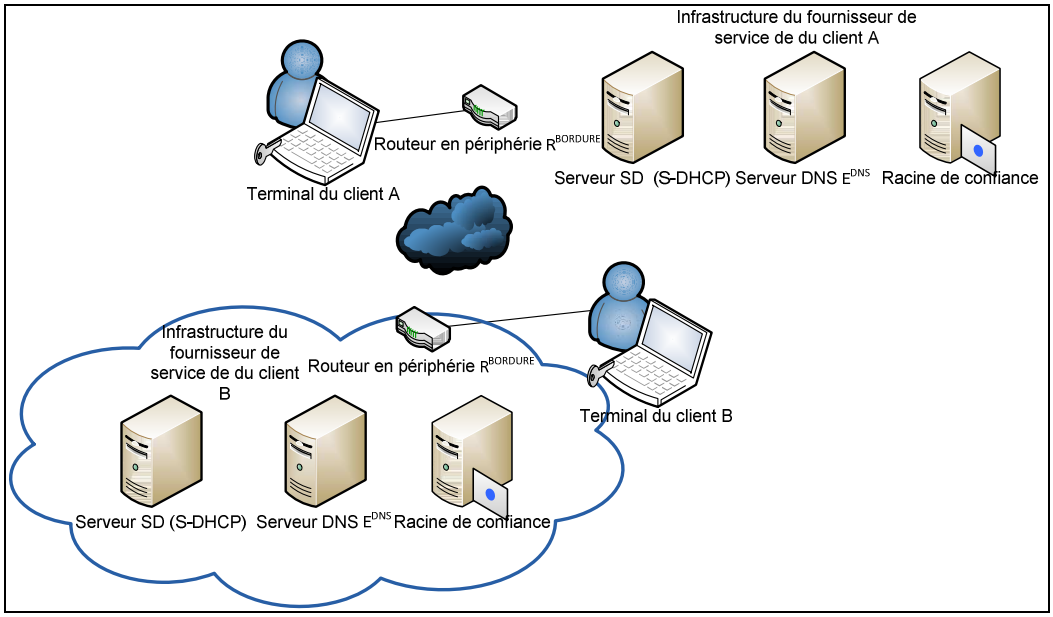


Figure 45: Illustration de notre solution

- <u>Mise en place de la sécurité :</u>

- **Lors de l'acquisition du nouvel équipement :**

Les équipements sont chargés lors de leur installation de:

Paire de clés	Chaque équipement E possède une paire de clés qui est attribué par la racine de confiance du FSI : - une clé publique notée par K^{E}_{PUB} - une clé privée notée par K^{E}_{Priv}
Certificat C^{E}	faisant correspondre l'adresse MAC de l'équipement avec sa clé publique. Le certificat d'un équipement contient donc les champs suivants : - Champ adresse MAC - Champ clé publique K^{E}_{PUB} - Signature de l'entité de confiance E_C. - Clé publique de l'entité de confiance : K^{EC}_{PUB} - L'algorithme de signature

Certificats des serveurs S-DHCP	Le certificat du serveur DHCP SD contient donc les champs suivants : - Champ adresse IP ; - Champ clé publique K^{SD}_{PUB} ; - Signature de l'entité de confiance E_C ; - Clé publique de l'entité de confiance : K^{EC}_{PUB} ; - L'algorithme de signature.
PIN	Le client reçoit le PIN (4 digits) permettant l'accès à son équipement. Il doit changer son PIN lorsqu'il se connecte sur son équipement pour la première fois.

Tableau 7: Paramètres configurés lors de l'acquisition de l'équipement de connexion par un client du FSI

- **Activation du nouvel équipement**

Lors de la réception du nouvel équipement, le FSI donne également sur un support papier le PIN correspondant. Ainsi, lorsque le client se connecte au réseau du FSI depuis chez lui, il utilise ce PIN pour saisir un PIN de son choix puis le client C envoie une requête d'adresse IP au serveur SD qui sélectionne une des adresses disponibles.

$$C\text{-> SD: DHCPDISCOVER } |C^{E}| \, S^{DHCPDISCOVER}$$

Nous avons rajouté pour les besoins de notre solution deux nouveaux champs au message DHCPDISCOVER. Ces deux champs correspondent à la signature du message $S^{DHCPDISCOVER}$ ainsi que le certificat C^{E} de l'équipement du client.

Le serveur SD vérifie le certificat de l'équipement du client à l'aide de la clé publique de l'entité de confiance et si le certificat est valide, il envoie un DHCPOFFER afin de proposer une adresse IP au client C. Ce message DHCP sera signé par la clé privée du serveur DHCP.

$$SD \text{ ->C: DHCPOFFER } | \, S^{DHCPOFFER}$$

Ensuite, le client C envoie un message DHCPREQUEST en diffusion en réponse aux messages DHCPOFFER émis par les serveurs ainsi que sa signature $S^{DHCPREQUEST}$. Ce message indique le serveur SD choisi, la confirmation de l'adresse reçue et éventuellement la durée du bail désirée par le client.

$$C\text{->}SD : DHCPREQUEST|S^{DHCPREQUEST}$$

Le serveur SD retenu envoie un message DHCPACK ainsi que sa signature $S^{DHCPACK}$ en réponse au message DHCPREQUEST du client C. Cette réponse fournit l'ensemble des paramètres de configuration au client.

$$SD\text{ ->}C: DHCPACK\ |S^{DHCPACK}$$

Puis le serveur SD envoie au routeur de bordure l'adresse IP, l'adresse MAC et la clé publique du client. Ceci peut être considéré comme un certificat temporaire au niveau du routeur de bordure $R^{BORDURE}$.

$$SD\text{-> }R^{BORDURE} : [IP|MAC|K^{E}_{PUB}] \_ K^{DHCP}_{PRIV}$$

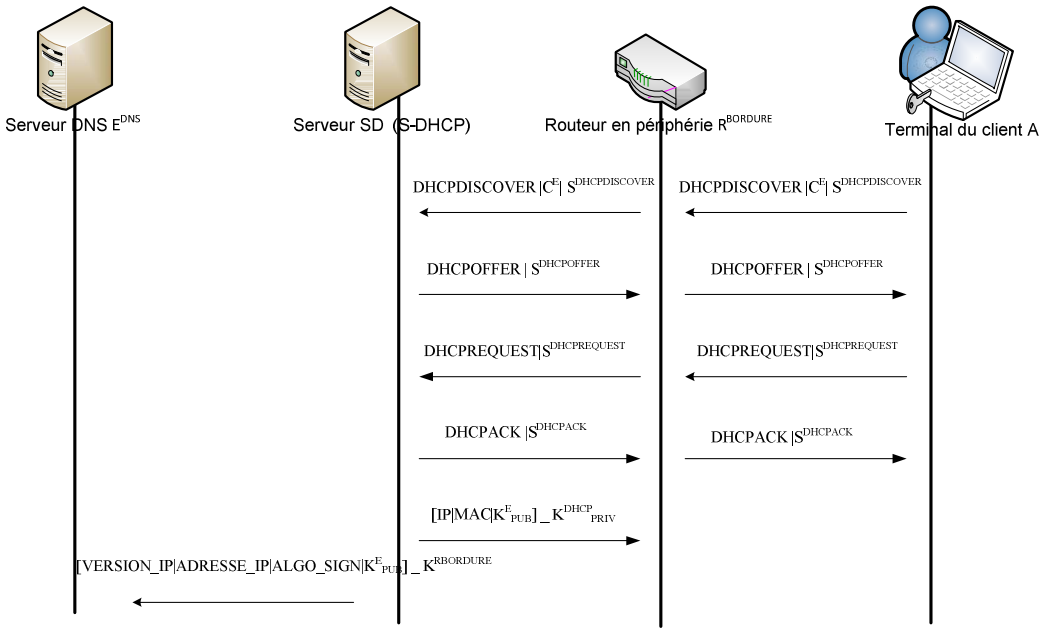


Figure 46: Illustration des messages

- **Publication de la correspondance clé publique/adresse IP :**

Le routeur de bordure envoie la version de l'adresse IP, la correspondance adresse IP/ clé publique ainsi que l'algorithme de signature avec DNSSEC+ au serveur DNS E^{DNS} du FSI.

$R^{BORDURE}$ -> E^{DNS}: [VERSION_IP|ADRESSE_IP|ALGO_SIGN|K^{E}_{PUB}] _ $K^{RBORDURE}$

Ces paramètres sont décrits dans le tableau suivant :

Champ	Description	Taille du champ
VERSION_IP	0 si IPv4 et 1 si IPv6	1 bit

Le champ "ADRESSE_IP"	peut accueillir IPv4 et IPv6	128 bits
ALGO_SIGN	HMAC-256	4 bits
$\mathbf{K^{E}_{PUB}}$	Clé RSA	2048 bits

Tableau 8: Description des paramètres utilisés

Dans les zones DNS couvrant les réseaux gérés par le FSI, la correspondance de l'adresse IP vers l'adresse de l'équipement apparait sous forme d'enregistrements PTR.

Nous proposons de nouveaux attributs à l'enregistrement PTR (qu'on renommera « Secure IP ») et correspondant à l'algorithme de signature ainsi la clé publique du client. Ainsi, l'enregistrement « Secure IP » de l'équipement du client ayant une adresse client.domaine.com et ayant une adresse IPv4 courante 11.12.13.14 est comme suit :

14.13.12.11.in-addr.arpa IN PTR client.domaine.fr ALGO_SIGN K^{E}_{PUB}

Notons que l'adresse IP courante de l'équipement du client sera prise en compte dans l'enregistrement PTR grâce au mécanisme de Dymanic DNS et que ce nouveau type d'enregistrements doit être mis sur des serveurs fortement répliqués.

Nous rajoutons également une nouvelle fonctionnalité à la requête « reverse IP » qu'on renommera « Enhanced reverse IP ». Ainsi, cette requête, en plus de retrouver l'adresse de l'équipement à partir d'une IP, permettra de retrouver la clé correspondante.

Phase d'usage:

La clé publique de l'équipement correspondante à son adresse IP actuelle doit être utilisée pour assurer la protection de l'entête des paquets générés par les clients. Nous proposons d'utiliser le mode AH d'IPSEC. Les clés utilisées par IPSEC AH sont générées par notre proposition d'une nouvelle version du proto-

cole IKE qu'on nomme E-IKE. La clé obtenue à l'issue de ce protocole sera envoyé de manière sécurisée par chacune des deux parties de la communication à son routeur de bordure.

Soit A l'émetteur, $R_{bordure1}$ le routeur de bordure du domaine de l'émetteur et CP les préférences en termes d'algorithme. Les messages E-IKE décrits par la figure 47 sont comme suit :

$$A \rightarrow R_{bordure1} : [g^A \bmod p | CP | N_A] | HMAC(g^A \bmod p | CP | N_A , K_A)$$

Le routeur en bordure de l'émetteur $R_{bordure1}$ extrait l'adresse IP et vérifie la signature et relaie le message si c'est ok.

$$R_{bordure1} \rightarrow R_{bordure2} : [g^A \bmod p | CP | N_A] | HMAC(g^A \bmod p | CP | N_A , K_A)$$

Le routeur en périphérie du destinataire $R_{bordure2}$ vérifie la signature grâce à la clé publique qu'il a récupérée en exécutant une requête « Enhanced reverse IP ». Si c'est ok, il relaie le paquet au destinataire.

$$R_{bordure2} \rightarrow [g^A \bmod p | CP | N_A] | HMAC(g^A \bmod p | CP | N_A , K_A)$$

B récupère la clé publique de A du serveur DNS puis spécifie s'il possède un certificat ou si son adresse IP est accessible via DNSSEC+.

$$B \rightarrow A: [g^B \bmod p | CP | [C_B] | N_B] | HMAC(g^B \bmod p | CP | [C_B] | N_B , K_B)$$

A et B calculent alors la clé $K= HMAC (N_A, N_B, CP, g^{AB} \bmod p)$

Ensuite, A et B transmettent leurs clés partagées de manière sécurisée à leurs routeurs de bordure. Ainsi, les paquets seront vérifiés à la sortie et à l'entrée d'un FSI et au niveau des deux parties.

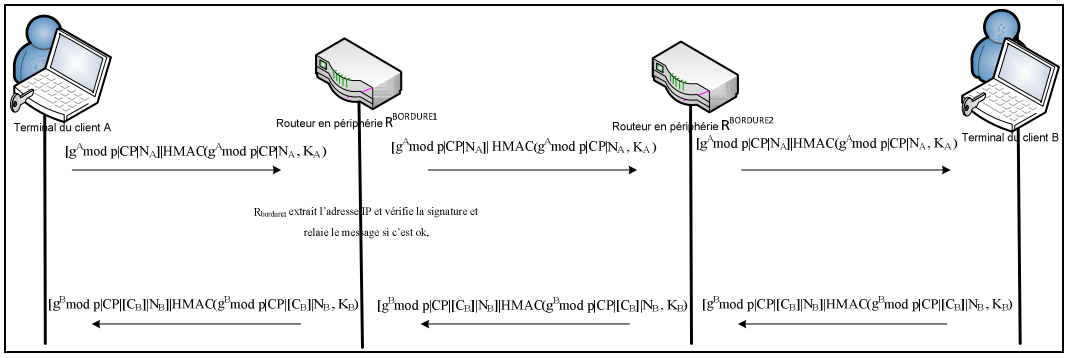


Figure 47: Illustration des messages échangés

Par ailleurs, notons que l'enregistrement « Secure IP » doit être mis à jour au niveau du serveur DNS à chaque changement de correspondance entre adresse IP et clé publique. Notons également que les FSIs peuvent mettre en place tous les mécanismes décrits ci-dessous ou juste implémenter DNSSEC+ au niveau de leurs routeurs de bordure ce qui leur permettra de vérifier les paquets qui arrivent au niveau des leurs domaines en envoyant des requêtes au serveur DNS du FSI de l'émetteur.

3.4.5 Evaluation formelle de la solution

- Description:

Nous proposons d'évaluer dans cette section notre solution. Dans le cadre de cette évaluation, nous allons utiliser le modèle proposé dans [80]. Selon ce modèle, Internet se compose de N FSIs, indexé 1, 2, ..., N. Soit INT = {1,…,N} désignant cet ensemble. Chaque FSI tient à protéger ses clients contre l'usurpation de leurs adresses IP.

Nous voulons déterminer les dommages pouvant être causés aux clients du FSI i à la suite d'attaques effectuées de l'extérieur et de l'intérieur du domaine en fonction des mécanismes de défenses déployés par les différents FSIs.

En particulier, nous nous sommes intéressés à l'évaluation du niveau de dommages causés aux clients du FSI i. Nous allons mener cette évaluation en vertu de:

- Approche de non sécurisation du FSI ;
- Filtrage en entrée/sortie ;
- Notre solution.

Soit $A_{i\to j}^{(k)}$ le taux d'attaques effectuées à partir du FSI i au FSI j où l'adresse de i est falsifié par une adresse du domaine k. Soit $D_{\to i}$ désigne le taux d'attaque total réalisé au domaine i. Les dommages causés aux clients du FSI i ainsi qu'à ses serveurs :

$$D_{\to i} = \sum_{k=1}^{N} \sum_{j=1}^{N} A_{j\to i}^{(k)}$$

$\sum_{k=1}^{N} \sum_{j=1}^{N} A_{j\to i}^{(k)}$ étant l'ensemble des attaques réalisées depuis tous les domaines d'internet en falsifiant une adresse k provenant de n'importe quel domaine internet.

Nous visons à évaluer formellement le niveau des dommages subis sur les serveurs et les utilisateurs du FSI. Pour chacun des mécanismes de défense, nous évaluerons alors la réduction de dommages, mesurée par la réduction du taux DR_i .

Nous nous baserons par la suite sur le ratio DR_i / D_i pour comparer les différentes approches.

- <u>Réduction de dommages :</u>

Dans cette section, nous allons mesurer la réduction de dommages apportés par chacune des méthodes citées ci-dessus.

- **Approche de non sécurisation du FSI:**

En appliquant cette méthode, la réduction des dégâts au niveau de l'ISP i est donnée par:

$$DR(sansapprochedesécurisation) = 0;$$

- **Approche du filtrage en entrée/sortie :**

En appliquant cette méthode, la réduction de dommages au niveau de l'ISP i est donnée par:

$$DR(IEF) \equiv \sum_{j \in IEF} \sum_{k \in INT} A_{j \to i}^{(k)}$$

Avec IEF l'ensemble des FSIs appliquant la méthode du filtrage en entrée/sortie.

- **Notre Solution :**

Notons par S l'ensemble des FSI utilisant notre méthode. La réduction des dommages au niveau du FSI i comprend toutes les attaques dont l'adresse usurpée appartient à S et toutes les attaques générées par des attaquants du domaine i visant les clients de ce domaine.

$$DR(Notresolution) = \sum_{j \in INT} \sum_{k \in S} A_{j \to i}^{(k)} + \sum_{j \in S} \sum_{k \in INT - S} A_{j \to i}^{(k)} + \sum_{k \in i} \sum_{j \in i} A_{j \to i}^{(k)}$$

- Application formelle :

Une attaque réalisée depuis un FSI i vers un FSI j en utilisant une adresse k est modélisé comme suit [37] :

$$A_{j \to i}^{(k)} \approx \frac{A}{N} \cdot \frac{1}{ikLn^2 N}$$

Avec A représentant une constante et N représentant le nombre de FSI

Soit T est le nombre de clients du FSI I :

$$D_{\rightarrow i} = \frac{A}{iLnN}(1 + TLnT / NLnN)$$

- **Approche de non sécurisation du FSI:**

$$DR(sansapprochedesécurisation) = 0;$$

donc

$$DR(sansapprochedesécurisation) / D_{\rightarrow i} = 0;$$

- **Approche du filtrage en entrée/sortie :**

$$DR(IEF) = \frac{A}{NLn^2 Ni} KLnN = \frac{AK}{NLn\ Ni}$$

$$DR(IEF) / D_{\rightarrow i} = \left(\frac{AK}{NLnNi}\right) \div \frac{A}{iLnN}(1 + TLnT / NLnN)$$

$$= \frac{KLnN}{NLnN + TLnT} \text{ pour tout i} \in INT$$

- **Notre solution:**

$$DR(Notresolution) = \frac{A}{NLn^2 Ni} \sum_{j \in INT} \sum_{k \in S} \frac{1}{k} + \frac{A}{NLn^2 Ni} \sum_{j \in S} \sum_{k \in INT - S} \frac{1}{k} +$$

$$\frac{A}{NLn^2 N} \sum_{k \in i} \sum_{j \in i} 1 / ik$$

$$DR(Notresolution) = \frac{A}{NLn^2 Ni} \left(NLnK + KLnN - KLnK + TLnT\right)$$

$$DR(Notresolution)_{/} \overset{D_{\to i}}{=} \frac{A}{NLn^2 Ni}\left(NLnK + KLnN - KLnK + TLnT\right) \div$$

$$\frac{A}{iLnN}(1 + TLnT / NLnN) = \left(NLnK + KLnN - KLnK + TLnT\right) \div (NLnN + TLnT)$$

pour tout i∈ *INT*

- Application numérique :

- **Schémas**

La figure suivante décrit la réduction de dommages relative à un FSI en fonction du nombre de FSI déroulant la méthode de filtrage en entrée/sortie. Nous prenons les cas ou T=16000, T=160000 et T=1600000. Notons que le nombre des fournisseurs de services Internet dans le monde est de l'ordre de 15000.

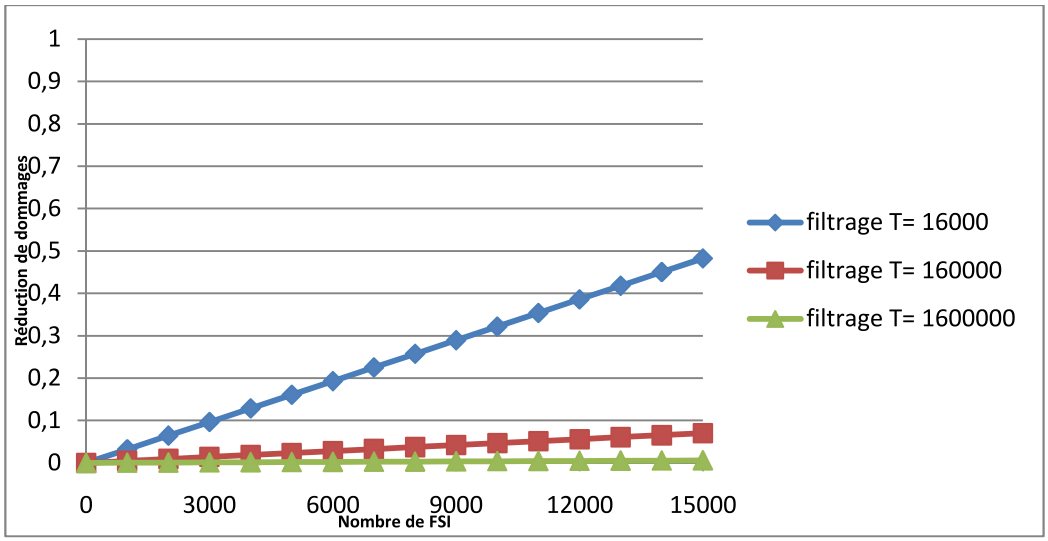


Figure 48: Résultats de l'application numérique de la méthode de filtrage en entrée/sortie

La figure suivante décrit la réduction de dégâts relative à un FSI en fonction du nombre de FSI déroulant notre solution. Nous prenons les cas ou T=16000, T=160000 et T=1600000.

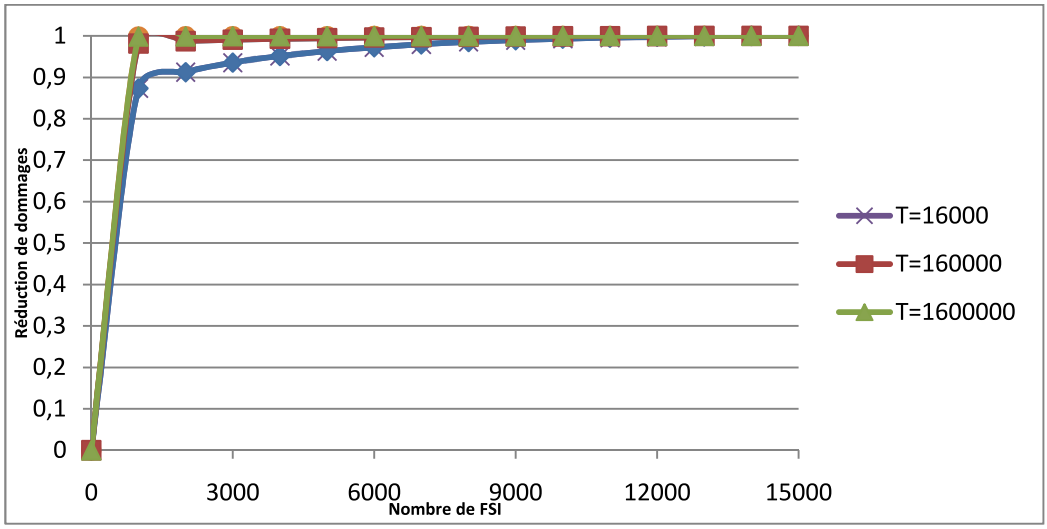


Figure 49: Résultats de l'application numérique de notre solution

La figure suivante regroupe les courbes relatives aux réductions de dégâts en fonction du nombre de FSI déroulant la méthode de filtrage en entrée/sortie et ceux déroulant notre solution.

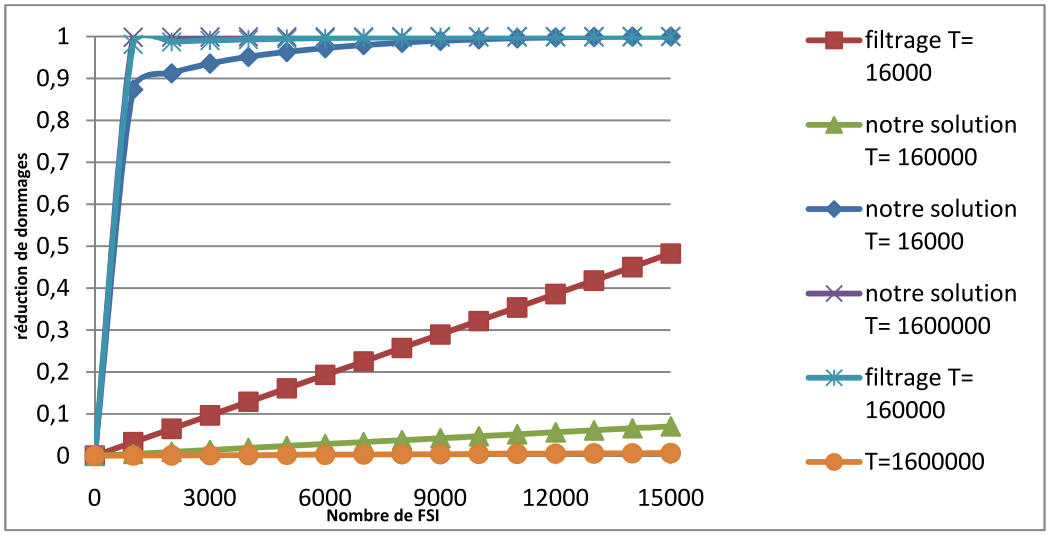


Figure 50: Résultats de l'application numérique

- **Interprétation des résultats:**

Les figures ci-dessus conduisent aux conclusions suivantes :

- Notre solution permet de réaliser une réduction de dommages nettement plus importante que celle de la méthode de filtrage en entrée/sortie.
- Le bénéfice généré par l'adoption de notre solution croit légèrement avec le nombre de ses clients.
- Le bénéfice généré par l'adoption de notre solution croit avec le nombre de fournisseurs qui l'appliquent.

De plus, un fournisseur de services Internet implémentant la méthode de filtrage en entrée/sortie a la même protection contre les attaques externes que ceux qui n'implémentent pas cette méthode contrairement à notre solution.

3.5 Conclusion

Les attaques utilisant la technique d'usurpation d'identité peuvent conduire à l'acheminement des paquets vers des destinataires non légitimes ou conduire au déni de service. Il est donc essentiel de prémunir les infrastructures de routage contre ce type d'attaques. Le routage est effectué à deux niveaux : niveau intra-domaine généralement grâce au protocole OSPF et niveau inter-domaine grâce au protocole BGP. Nous avons donc proposé dans ce chapitre deux mécanismes de protection contre l'usurpation d'identité relatifs respectivement au protocole OSPF et au protocole BGP. Afin de protéger les routeurs BGP contre l'usurpation d'identité, nous proposons dans un premier temps de clustériser les domaines Internet, de sécuriser les liens entre chaque chef de cluster et ses routeurs grâce au paradigme de la cryptographie sans certificats et au concept de « web of trust ». Ensuite, chacun des chefs de cluster forme grâce à ses nœuds un graphe schématisant son cluster dont les nœuds représentent ses routeurs RR et dont les liens représentent les adjacences actuelles entre les RRs. Ensuite, chacun des RR envoie son graphe à autres clusters ce qui permet à chacun d'eux de former le graphe actuel d'Internet. Chaque message BGP UPDATE sera ensuite vé-

rifié à l'aide de ce graphe qui sera mis à jour grâce à des messages de rafraichissement émis par les RRs. Afin de protéger les routeurs OSPF contre l'usurpation d'identité, nous avons préconisé dans le cadre du projet ESTER le stockage de l'identité et du matériel cryptographique dans un coffre-fort électronique qu'est la carte à puce. Les cartes déroulent ensuite un algorithme de dérivation de clés avec les cartes des routeurs voisins ainsi qu'avec celle du routeur désigné. Les clés dérivées entre les cartes à puce servent à signer les messages OSPF et à authentifier au niveau MAC. Les clés dérivées entre les routeurs servent à chiffrer les paquets IP contenant les messages OSPF. Nous avons dans ce document décrit la plateforme du démonstrateur et les scénarios de tests adoptés pour évaluer les performances de notre prototype et les comparer avec ceux du logiciel Quagga sur la base de trois critères : temps requis pour traiter une LSA, temps de convergence, temps de re-calcul d'une table de routage après un changement. Ces temps de augmente peu avec l'introduction du module ESTER. Ainsi, la solution ESTER permet de renforcer la sécurité du protocole OSPF avec un impact raisonnable sur les performances.

Nous avons également été amenés dans ce chapitre à repenser le mécanisme d'octroi des adresses IP chez le FSI. Dans le cadre de notre proposition, chaque équipement de connexion aux réseaux du FSI contient son propre de matériel cryptographique attribué par celui-ci. Ce matériel cryptographique permet d'obtenir une adresse IP de manière sécurisée auprès du serveur DHCP. Ensuite, la correspondance entre son adresse IP et sa clé publique est enregistrée auprès du serveur DNS du FSI en utilisant un nouveau type d'enregistrement et en rajoutant une nouvelle fonctionnalité à la fonction DNS « reverse IP ». La protection des paquets des clients est par la suite assurée avec l'utilisation du mode AH d'IPSEC avec une clé obtenue à partir d'une nouvelle version du protocole IKE qui prend en compte la récupération des certificats auprès des serveurs DNS. Nous avons ensuite comparé notre mécanisme avec l'approche de non sécurisa-

tion du FSI et le filtrage en entrée/sortie. Nous avons ainsi évalué de manière formelle la réduction de dégâts obtenues avec ces trois méthodes et appliqué les formules obtenues au contexte d'Internet. Notre solution permet de réaliser une réduction de dégâts nettement plus importante que celle de la méthode de filtrage en entrée/sortie. De plus, le bénéfice généré par l'adoption de notre solution croit avec le nombre de fournisseurs qui l'appliquent. Par ailleurs, un fournisseur de services Internet implémentant la méthode de filtrage en entrée/sortie a la même protection contre les attaques externes que ceux qui n'implémentent pas cette méthode contrairement à notre solution.

CONCLUSION GENERALE

4 Conclusion générale

Selon le rapport “Arbor Networks” sur la sécurité des infrastructures à travers le monde, les menaces identifiées comme les plus sévères sont relatives aux attaques DDOS utilisant la technique d’usurpation d’identité. Cette technique est également utilisée pour des activités prohibées comme le téléchargement illégal. De ce fait, les fournisseurs de services Internet se doivent de prémunir leurs clients des attaques basées sur la technique d’usurpation d’identité. Dans cette thèse, nous avons adressé la problématique de la protection des réseaux de cœur ainsi que celles des réseaux d’accès aux services Internet contre les attaques basées sur l’usurpation d’identité.

Dans le second chapitre de ce manuscrit, nous avons proposé trois mécanismes de protection contre l’usurpation d’identité qui utilisent différents types de canaux hors bande pour l’attribution de matériel cryptographique permettant la dérivation de clés bilatérales entre les équipements du réseau. Le premier mécanisme est dédié à la connexion d’un équipement personnel depuis un lieu public, le second aux réseaux personnels et le troisième est dédié au cas particulier des réseaux médicaux.

Le mécanisme dédié à la connexion d’un équipement personnel depuis un lieu public consiste en un protocole inter-couche basé sur les principes de la théorie de l’information. Ce protocole fixe la faille de sécurité non abordée dans la littérature qu’est l'attaque d’usurpation d’identité qui survient au début de la communication et protège donc les utilisateurs contre les attaques de type « homme au milieu ». Nous avons proposé que la personne qui désire avoir un accès sécurisé à l'Internet doive être sur un cercle spécifique qu’on a nommé « RED POINT » de telle façon que l'attaquant n'est pas en mesure d'être sur le même cercle au même moment. Le protocole inter-couche proposé se déclinent en trois phases: la phase de vérification de la position de l'utilisateur, la phase d’extraction du secret

partagé de la couche physique et la dernière phase de la dérivation de la clé partagée au niveau de la couche MAC. Nous avons par la suite validé formellement notre solution grâce à l'outil AVISPA et présenté les résultats de son implémentation. L'outil AVISPA a permis de s'assurer est que les objectifs de sécurité après le processus de validation sont atteints et que le protocole est sûr (pas d'attaques recensées). Ces objectifs étant l'authentification forte entre les deux équipements et la confidentialité des nombres aléatoires qu'ils ils ont échangés. De plus, même si l'attaquant a observé plusieurs instances de ce protocole, il reste dans l'incapacité de rejouer ou de falsifier des messages et de compromettre les objectifs de sécurité mentionnés ci-dessus.

Concernant le mécanisme dédié au réseau personnel, les nœuds au sein du réseau se décomposent en nœuds contrôleurs de sites de réseaux personnels (Contrôleurs Locaux de Réseaux Personnels - CLRP) et en nœuds contrôlés. Nous avons préconisé l'utilisation d'un protocole basé sur les canaux hors bande impliquant une intervention minime de l'utilisateur en vue d'attribuer des certificats aux nœuds du réseau personnel. Ces certificats ont permis par la suite de dériver de clés bilatérales entre les équipements du réseau personnel du même site ainsi qu'entre des équipements sur des sites distants. Même si le CLRP joue un rôle important pour la gestion des clés au sein du réseau personnel, il ne peut toutefois pas rajouter/révoquer des équipements sans l'aval de l'utilisateur. De plus, même si le CLRP est volé, il ne peut pas rajouter ou révoquer sans l'approbation de l'utilisateur légitime. Par ailleurs, un équipement ne peut pas usurper l'identité d'un autre car les opérations d'attribution de certificats ainsi que les opérations d'appariement impliquent une intervention minime de l'utilisateur qui est en mesure de reconnaitre l'équipement légitime. Ainsi, les opérations de révocation concernent uniquement la phase de retrait d'un équipement E du RP pour son remplacement par exemple.

Le cas particulier des réseaux médicaux a été présenté au groupe de travail IEEE 802.15.6 qui mène des travaux en vue de la normalisation de réseaux médicaux. Ce mécanisme organise le réseau médical du patient en cluster, est simple à mettre en œuvre et le seul à traiter à notre connaissance à la fois la phase de déploiement ainsi que la phase d'usage des réseaux médicaux. Le protocole proposé exige ainsi peu de participation de la part des utilisateurs et respecte les capacités limitées de calculs de nœuds de capteurs. Durant la phase d'usage, un adversaire ne peut pas ajouter un nœud malveillant sur le corps du patient afin d'envoyer des données erronées car rejoindre le MBAN se fait soit dans la phase de déploiement soit avec l'intervention de l'utilisateur lors de la phase de rajout. De plus, le vol d'un capteur biomédical et sa remise en service avec des données erronées sera détecté par le chef de cluster correspondant puisque les données qu'il envoie ne sont pas chiffrées avec le la clé appropriée. En outre, quand un adversaire vole un capteur qui joue le rôle de chef de cluster, le capteur sera détecté par le serveur personnel comme un capteur corrompu vu que les données qu'il envoie ne seront pas de la forme appropriée car l'attaquant ne possède pas les clés bilatérales des membres du MBAN avec le serveur personnel. De plus, une alerte sera remontée à l'utilisateur en cas de détection d'un nœud corrompu.

Dans le troisième chapitre, nous avons proposé pour les réseaux de cœur des mécanismes de protection contre la technique d'usurpation d'identité pouvant conduire à l'acheminement des données vers des destinataires non légitimes ou au déni de service. Nous avons ainsi proposé trois mécanismes de protection contre l'usurpation d'identité: un dédié au protocole BGP, un second dédié au protocole OSPF et le troisième dédié à la protection contre l'usurpation des adresses IP des clients abonnés à un fournisseur de services Internet. Les travaux relatives aux protocoles de routage OSPF et BGP s'inscrivent dans la cadre du projet ESTER qui vise à démontrer la faisabilité d'une approche basée sur l'intégration de

cartes à puces au sein des nœuds de réseaux agissant ainsi comme un coffre-fort électronique. Afin de protéger les routeurs BGP contre l'usurpation d'identité, nous proposons dans un premier temps de clustériser les domaines Internet, de sécuriser les liens entre chaque chef de cluster et ses routeurs grâce au paradigme de la cryptographie sans certificat et au concept de « web de confiance ». Ensuite, chacun des chefs de cluster forme grâce à ses nœuds un graphe schématisant son cluster dont les nœuds représentent ses routeurs RR et dont les liens représentent les adjacences actuelles entre les RR. Ensuite, chacun des RR envoie son graphe à autres clusters ce qui permet à chacun d'eux de former le graphe actuel d'Internet. Chaque message BGP UPDATE sera ensuite vérifié à l'aide de ce graphe qui sera mis à jour grâce à des messages de rafraichissement émis par les RRs. Notre mécanisme ne requiert ni changements dans les messages BGP, ni d'énormes ressources de calcul au niveau des routeurs. De plus, ce mécanisme assure la validité du chemin et la disponibilité pour le protocole BGP.

Par ailleurs, afin de protéger les routeurs OSPF contre l'usurpation d'identité, nous avons préconisé dans le cadre du projet ESTER le stockage de l'identité et du matériel cryptographique dans un coffre-fort électronique qu'est la carte à puce. Les cartes déroulent ensuite un algorithme de dérivation de clés avec les cartes des routeurs voisins ainsi qu'avec celle du routeur désigné. Les clés dérivées entre les cartes à puce servent à signer les messages OSPF et à authentifier le niveau MAC. Nous avons dans ce document décrit la plateforme du démonstrateur et les scénarios de tests adoptés pour évaluer les performances de notre prototype et les comparer avec ceux du logiciel QUAGGA sur la base de trois critères : temps requis pour traiter une LSA, temps de convergence, temps de recalcul d'une table de routage après un changement. Ces temps de augmente peu avec l'introduction du module ESTER. Ainsi, la solution ESTER permet de renforcer la sécurité du protocole OSPF avec un impact raisonnable sur les performances.

Nous avons également été amenés dans ce chapitre à repenser le mécanisme d'octroi des adresses IP des fournisseurs de services Internet. Dans le cadre de notre proposition, chaque équipement de connexion aux réseaux des fournisseurs de services Internet contient son propre matériel cryptographique attribué par celui-ci. Ce matériel cryptographique permet d'obtenir une adresse IP de manière sécurisée auprès du serveur DHCP. Ensuite, la correspondance entre son adresse IP et sa clé publique est enregistrée auprès du serveur DNS du FSI en utilisant un nouveau type d'enregistrement et en rajoutant une nouvelle fonctionnalité à la fonction DNS « reverse IP ». La protection des paquets des clients est par la suite assurée avec l'utilisation du mode AH d'IPSEC avec une clé obtenue à partir d'une nouvelle version du protocole IKE qui prend en compte la récupération des certificats auprès des serveurs DNS. Nous avons ensuite comparé notre mécanisme avec l'approche de non sécurisation du FSI et le filtrage en entrée/sortie. Nous avons ainsi évalué de manière formelle la réduction de dégâts obtenues avec ces trois méthodes et appliqué les formules obtenues au contexte d'Internet. Notre solution permet de réaliser une réduction de dégâts nettement plus importante que celle de la méthode de filtrage en entrée/sortie. De plus, le bénéfice généré par l'adoption de notre solution croit avec le nombre de fournisseurs qui l'appliquent. Par ailleurs, un fournisseur de services Internet implémentant la méthode de filtrage en entrée/sortie a la même protection contre les attaques externes que ceux qui n'implémentent pas cette méthode contrairement à notre solution.

Les attaques utilisant la technique d'usurpation d'identité sont lucratives et peuvent générer beaucoup de revenus de manière illégale avec peu d'investissements. De ce fait, les fournisseurs de services Internet se doivent de mettre en œuvre les mécanismes de protection contre l'usurpation d'identité et de se tenir au courant concernant tous les nouveaux types d'attaques ainsi qu'à adapter les mécanismes existants ou de créer de nouveaux mécanismes.

Les fournisseurs de services Internet doivent également particulièrement veiller à protéger leurs clients contre les attaques d'usurpation d'adresses e-mails qui peuvent servir aux attaques de phishing[41] et à la formation de botnets. De ce fait, nous préconisons de conduire des travaux de recherche permettant la protection contre les attaques d'usurpation d'adresses e-mails. Un axe intéressant serait d'étudier la faisabilité d'une correspondance entre clé publique d'un client et son adresse IP et de se baser sur les serveurs de messagerie des FSI contre racines de confiance.

41 Le « phishing » st une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

Liste des publications

A. Ahmad, A. Biri, H. Afifi, "A Trade-off between Identity-Based and Certificateless Cryptography (TIBC) for Publish/Subscribe systems", in the proceedings of the 20th Personal, Indoor and Mobile Radio Communications Symposium 2009 (PIMRC'09).

A. Ahmad, A. Biri, H. Afifi, "Study of a new physical layer encryption concept", in the proceedings of the Fourth IEEE International Workshop on Wireless and Sensor Networks Security (WSNS'08) held in conjunction with The fifth IEEE International Conference on Mobile Ad-hoc and Sensor Systems, (2008).

A. Biri, A. Ahmad, H. Afifi, “Securing Media Hotspots” , in the proceedings of the 7rd Wireless Telecommunications Symposium, April 24-26 2008, California, USA.

A. Biri, P. Urien, E. Onfroy, H. Afifi, “A Novel Architecture for securing data delivery in Internet”, in proceedings of the 22 rd International conference on Information Networking, January 23-25 2008, Busan, South Korea.

A. Biri and H. Afifi, “A Novel Protocol for Securing Wireless Internet Service Provider's Hotspots” , in proceedings of the 5rd Consumer Communications & Networking Conference, January 10-12, 2008, Las Vegas, USA.

A. Biri, A. Ahmad, H. Afifi, “Securing Medical Body Area Networks” , in proceedings of the second international symposium on medical information and communication technology, December 11-13 2007, Oulu, Finland.

A. Biri, A. Ahmad, H. Afifi, “A zero knowledge cross-layer pairing protocol for Internet Wi-Fi networks” , in proceedings of the 10rd International Symposium on Wireless Personal Multimedia Communications, December 3-6 2007, Jaipur, India.

Références

[1] A. Barbir, S. Murphy, and Y. Yang. Generic Threats to Routing Protocols (Draft). IETF, April 2004.

[2] A. Bremler-Barr, and H. Levy, "Spoofing Prevention Method", INFOCOM 2005.

[3] A. D. Wyner, “The wire-tap channel,” Bell System Technical Journal, 1975. vol. 54 , pp. 1355–1387, no. 8.

[4] A. Juels and M. Wattenberg,, ‘‘A fuzzy commitment scheme’’, in Proc. 6th ACM Conf. Computer and Communications Security, G. Tsudik, Ed., 1999, pp. 28---36.

[5] A. Lo, M. Jacobsson, V. Prasad, and I. G. Niemegeers, "Personal Networks: An Overlay Network of Wireless Personal Area Networks and 3G Networks," presented at the Third Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services, San Jose California, July 2006.

[6] A. Snoeren, C. Partridge, et al. Hash-Based IP Traceback. In Proc. ACM Sigcomm’2001, Aug. 2001.

[7] Adrien Pujol, « Protocole BGP, l’Internet en danger ? [archive] », Crashdump.fr, 29 août 2008

[8] B. Christian and T. Tauber. BGP Security Requirements. IETF, Apr. 2006. Internet Draft: draft-ietf-rpsec-bgpsecrec-06.txt.

[9] Barnes, R. and S. Kent, "An Infrastructure to Support Secure Internet Routing", Internet Draft, draft-ietf-sidr-arch-00.txt, January 2007

[10] Baylis, J, “Error Correcting Codes: A Mathematical Introduction”, Boca Raton, FL: CRC Press, 1998.

[11] Bhukya, W.N.; Suresh Kumar, G.; Atul Negi; "A Study of Effectiveness in Masquerade Detection", TENCON 2006 IEEE Region 10 Conference, Nov 2006

[12] C. E. Shannon, “Communication theory of secrecy systems”, Bell System Technical Journal, Oct.1949. vol. 28, pp. 656–715.

[13] C. Gehrmann, C. Mitchell and K. Nyberg, “Manual Authentication for Wireless Devices,” RSA, Cryptobytes, 7 no.1, pp. 29-37, Spring 2004.

[14] C.C.Y. Poon, S.D. Bao, and Y.T. Zhang, “A novel biometrics method to secure wireless body area sensor networks for telemedicine and mobile healthcare”, IEEE Communication Magazine (special issue on telemedicine), April, 2006.

[15] C. Patrikakis, M. Masikos, and O. Zouraraki, “Distributed Denial of Service Attacks”, The Internet Protocol Journal - Volume 7, Number 4, National Technical University of Athens, Cisco Systems Inc

[16] D. Basin, S. Modersheim, and L. Viganno. “OFMC: A Symbolic Model-Checker for Security Protocols”. International Journal of Information Security, 2004.

[17] D. Boneh and M. Franklin. Identity-Based Encryption from the Weil Pairing. In Advances in Cryptology CRYPTO '2001, pages 213-229, 2001.

[18] D. Eastlake, P. Jones, "US Secure Hash Algorithm 1 (SHA1)", RFC 3174, September 2001

[19] D. J. Malan, M. Welsh and M. Smith, “A Public-Key Infrastructure for Key Distribution in TinyOS Based on Elliptic Curve Cryptography”, In Proc. of The First IEEE International Conference on Sensor and Ad Hoc Communications and Networks (IEEE SECON), Santa Clara, California, October 2004.

[20] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford, "Don't Secure Routing Protocols, Secure Data Delivery," in Proc. ACM SIGCOMM HotNets Workshop, Irvine, CA, Nov. 2006

[21] D. Wendlandt, I. Avramopoulos, D. Andersen, and J. Rexford. Don't secure routing protocols, secure data delivery. http://www.cs.princeton.edu/~jrex/papers/acr.pdf, 2006

[22] D. McPherson, "5th Edition of the Worldwide Infrastructure Security Report", 2010

[23] Draft-ietf-rpsec-ospf-vuln-02.txt : "OSPF Security Vulnerabilities Analysis", june 2006

[24] E. Vetillard, « Combined Attacks and Countermeasures », dans Smart Card Research and Advanced Application, 2010, p. 133–147

[25] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks", In Proceedings of the 7th International Workshop Proceedings, Lecture Notes in Computer Science. Springer-Verlag, 1999.

[26] G. Gross, M. Kaycee, A. Lin, A. Malis, J. Stephens, "PPP Over AAL5", RFC 2364, July 1998

[27] H. Miao, K. Yu, and M. J. Juntti, "Positioning for NLOS Propagation: Algorithm Derivations and Cramer-Rao Bounds," IEEE Trans. Veh. Technol., vol. 56, no. 5, pp. 2568 – 2580, 2007.

[28] IEEE 802.11i Standard specifications http://standards.ieee.org/getieee802/download/802.11i-2004.pdf

[29] Hastings, N.E., McLean, P.A, "TCP/IP usurpation d'identité fundamentals", IEEE Fifteenth Annual International Phoenix Conference, 1996

[30] Hu, Yin-Chun, David McGrew, Adrian Perrig, Brian Weis, and Dan Wendlandt "(R) Evolutionary Bootstrapping of a Global PKI for Secure BGP" In the Workshop on Hot Topics in Networks (HotNets'06), Irvine, CA November 29 - 30, 2006.

[31] I. Avramopoulos and J. Rexford, "Stealth Probing: Efficient Data-Plane Security for IP Routing," in Proc. USENIX Annual Technical Conference, Boston, MA, May-Jun. 2006

[32] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," IEEE Trans. on Information Theory, May 1978, vol. 24, pp. 339–348.

[33] J. Bi, W. Jianping, L. Xing , C. Xiangbin, "An IPv6 Test-Bed Implementation for a Future Source Address Validation Architecture", the 4th EURO-NGI Conference on Next Generation Internet Networks (NGI), Krakow, Poland, 2008.

[34] J. López, and R. Dahab, "An Overview of Elliptic Curve Cryptography'', Technical Report IC-00-10, State University of Campinas, 2000

[35] J. Moy, "OSPF Version 2", RFC 2328, April 1998

[36] Jennifer Rexford and Joan Feigenbaum, "Incrementally-deployable security for interdomain routing," extended abstract, Proc. Cybersecurity Applications and Technologies for Homeland Security, March 2009.

[37] Jin C, Wang H, Shin KG. Hop-count filtering: an effective defense against spoofed ddos traffic. In: Proceedings of ACM conference on Computer and Communications Security; Oct. 2003.

[38] Jun Li, Jelena Mirkovic, Mengqiu Wang, Peter Reiher, and Lixia Zhang, "SAVE: Source Address Validity Enforcement Protocol", INFOCOM 2002.

[39] K. Malasri and L. Wang, "SNAP: an architecture for secure medical sensor networks", Wireless Mesh Networks, 2006, (WiMesh 2006). pp. 160-162.

[40] K. Sriram, D. Montgomery, O. Borchert, O. Kim and Rick Kuhn, “Autonomous System Isolation under BGP Session Attacks with RFD Exploitation”, IEEE JSAC special issue on High-Speed Network Security (2006)

[41] K.Venkatasubramanian and S.K.S.Gupta, ‘‘Security For Pervasive Health Monitoring Sensor Applications’’, in Proc. of 4th International Conference on Intelligent Sensing and Information Processing (ICISIP), Bangalore, India, December 2006.

[42] Katerina Argyraki and David R. Cheriton, “Active Internet Traffic Filtering: Real-Time Response to Denial-of-Service Attacks”, USENIX 2005.

[43] Kent, S., Lynn, C., Mikkelson, J., and Seo, K. 2000. Secure Border Gateway Protocol (S-BGP) real world performance and deployment issues. ISOC Symposium on Network and Distributed System Security

[44] L. Lamport. “The temporal logic of actions”. ACM Transactions on Programming Languages and System, May 1994.

[45] Loi n° 2009-669 du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet

[46] M. Bloch, J. Barros, M. R. D. Rodrigues, and Steven W. McLaughlin, “Information-Theoretic Security for Wireless Channels: Theory and Practice. Information Theory and Applications”, Workshop, San Diego, USA, February, 2007.

[47] M. Handley, E. Rescorla,"Internet Denial-of-Service Considerations", RFC 4732, November 2006

[48] McCune, Jonathan M., Adrian Perrig, and Michael K. Reiter. “Seeing-is-Believing: Using Camera Phones for Human-Verifiable Authentiction”, In Proceedings of the IEEE Symposium on Security and Privacy, Oakland, CA, May, 2005.

[49] NIST, Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March, 2006.

[50] N. Ferguson, B. Schneier (2003). Practical Cryptography. John Wiley & Sons.

[51] O. Bonaventure, “Interdomain routing with bgp: Issues and challenges”, IEEE SCVT 2002, Louvain-la-Neuve, Belgium, October 2002.

[52] O. Laurelli, «HADOPI: TMG pourrait injecter votre propre adresse IP sur Emule », http://www.paperblog.fr/3127843/hadopi-tmg-pourrait-injecter-votre-propre-adresse-ip-sur-emule/, 22 avril 2010

[53] P. Ferguson, D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", RFC 2827, May 2000

[54] R. Merkle, “Secure Communications over Insecure Channels”, Communications of the ACM, April 1978, pp. 294-299.

[55] S. Bellovin, Internet Draft: ICMP Traceback Messages. Technical report, Network Working Group, Mar 2000,

[56] S. C. Seo, Hyung-Chan Kim and R. S. Ramakrishna, “A New Security Protocol Based on Elliptic Curve Cryptosystems for Securing Wireless Sensor Networks’’, in Proc. EUC Workshops 2006, pp. 291-301.

[57] S. C. Seo, Hyung-Chan Kim and R. S. Ramakrishna, “A New Security Protocol Based on Elliptic Curve Cryptosystems for Securing Wireless Sensor Networks’’, in Proc. EUC Workshops 2006, pp. 291-301.

[58] S. Cherukuri, K.K. Venkatasubramanian and S.K.S.Gupta, ‘‘BioSec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body’’, in Proc. IEEE Int. Conf. on Parallel Processing Workshops, Oct. 2003, pp. 432 –439

[59] S. Goel, R. Negi, “Secret Communication using Artificial Noise,” in Proceedings VTC Fall ’05, Sept. 2005.

[60] S.D. Bao, L.F. Shen, and Y.T. Zhang, “A Design Proposal of Security Architecture for Medical Body Sensor Networks”, in Proc. International Workshop on Wearable and Implantable Body Sensor Networks (BSN'06) pp. 84-90

[61] Sattam S. Al-Riyami and Kenneth G. Paterson, “Certificateless public key cryptography,” ASIACRYPT,volume 2894 of Lecture Notes in Computer Science, pages 452-473. Springer, 2003.

[62] Schmidt R, Norgall T, Mörsdorf J, Bernhard J, von der Grün T. (2002). "Body Area Network BAN--a key infrastructure element for patient-centered medical applications". Biomed Tech 47 (1): 365–8.

[63] Shen, Y., Bi, J., Wu, J., and Liu, Q, “A Two-Level Source Address Spoofing Prevention based on Automatic Signature and Verification Mechanism”, the 13th IEEE Symposium on Computers and Communications (ISCC), 2008.

[64] The AVISPA project homepage: http://www.avispa-project.org .

[65] The MAGNET BEYOND project Homepage : http://magnet.aau.dk/

[66] The Openssl project Homepage: www.opensssl.org/

[67] The scratchbox project Homepage: http://www.scratchbox.org/

[68] The Wireless USB project Homepage, http://www.usb.org/developers/wusb/

[69] The Xsupplicant project Homepage: www.xsupplicant.org/

[70] Tombak, L.; Safavi-Naini, R., "New Bound for Substitution Attack", proceedings of the 1993 IEEE International Symposium on Information Theory, Jan. 1993

[71] Vlastimil Klima: Tunnels in Hash Functions: MD5 Collisions Within a Minute [archive], Cryptology ePrint Archive Report 2006/105, 18 Mars 2006, revu le 17 Avril 2006.

[72] W.C. Jakes Jr., Microwave Mobile Communications, Wiley, 1974.

[73] Wan, T., Kranakis, E., and van Oorschot, P. C. 2005. Pretty Secure BGP (psBGP). In Proc. Network and Distributed Systems Security 2005. Internet Society (ISOC), San Diego, CA

[74] Website of CLUSIF (Club de la Sécurité de l'Information Français) - « Panorama de la cybercriminalité 2009 » : http://www.clusif.asso.fr/fr/production/ouvrages/pdf/cybercrime2009.pdf

[75] WI-Fi alliance Homepage: http://www.wi-fi.org/

[76] WiFi Alliance. Wi-Fi Protected Setup Specification. Wi-Fi Alliance Document, January 2007.

[77] X. Li, M. Chen and E. P. Ratazzi, “A randomized space-time transmission scheme for secret-key agreement”, the 39th Annual Conference on Information Sciences and Systems (CISS'2005), Johns Hopkins University, Mar. 16-18, 2005.

[78] Xin Liu and Xiaowei Yang, “Efficient and Secure Source Authentication with Packet Passports “,2nd Workshop on Steps to Reducing Unwanted Traffic on the Internet (SRUTI '06), July 2006,

[79] Y. Hu, C., Perrig, A., and Sirbu, M. SPV: Secure Path Vector Routing for Securing BGP. In proceedings of Proceedings of the ACM SIGCOMM 2004 Conference, Sept 2004,

[80] Yao, G., Bi, J., “A CGA Based IP Source Address Authentication Method in IPv6 Access Network”,

[81] Zang Li, Wenyuan Xu, Rob Miller and Wade Trappe, “Securing Wireless Systems via Lower Layer Enforcements,” in Proceedings of the 2006 ACM workshop on Wireless security(WiSe), 2006, pg. 33-42.

[82] Martin Casado, Michael J. Freedman, Justin Pettit, Jianying Luo, Nick McKeown and Scott Shenker, “Ethane: Taking Control of the Enterprise”, SIGCOMM '07 Kyoto, Japan, August 2007.

[83] Trusted Computing Group Homepage: https://www.trustedcomputinggroup.org

[84] Eastlake, D. “Domain Name System Security Extensions”, RFC 2535, 1999

[85] R. Arends, R. Austein, M. Larson, D.Massey, and S. Rose, “Resource Records for the DNS Security Extensions”, July 2004.

ANNEXE: code HLPSL du protocole de dérivation de clés pour l'accès d'un équipement personnel depuis un lieu public

```
role initiator (
A,B : agent, % Initiator and Responder
PKY : symmetric_key,
Hash : hash_func, % Hash Function
G : nat, % Diffie Hellman's public G value
SND,RCV : channel(dy))
played_by A def=
local
State : nat,
X : text, % Initiator's Diffie Hellman Value
Na, Nb, Kab : text, % Initiator's nonce
EGY, K, PK : message
const sec_i_na: protocol_id
init State := 0
transition
0. State = 0 /\ RCV (start)=|>
State':= 2  /\ X':=new()
/\ SND(A.{ exp(g,X')}_ PKY.exp(G,X'))
/\ witness (A,B,auth_part1,Hash(exp(g,X')))
2. State = 2 /\ RCV(EGY'.{Nb'}_Hash(exp(EGY',X))) =|>
State':= 4 /\ Na' := new()
/\ SND({Na'.Nb'}_Hash(Kab,exp(EGY',X)))
/\ witness (A,B,auth_a,Na'.Nb')
4. State = 4 /\ RCV({Na}_Hash(Kab,exp(EGY,X))) =|>
State':= 6 /\ PK':=Hash(Na,Nb,exp(EGY,X))
/\ secret(PK',sec_a_PK,{A,B})
/\ request (A,B,auth_b,Na.Nb)
```

```
end role
role responder (
B,A :agent, % Initiator and Responder
PKY : symmetric_key,
Hash : hash_func, % Hash Function
G :nat, % Diffie Hellman's public G value
SND,RCV : channel(dy))
played_by B def=
local
State :nat,
Y :text, % Responder's Diffie Hellman parameter
Na, Nb, Kab :text, % Responder's nonce
EGX, PK : message
const sec_r_nb : protocol_id
init State := 1
transition
1. State = 1 /\ RCV(A.{ EGX'}_ PKY.EGX')=|>
State':=3 /\ Y':=new()
/\ Nb':=new()
/\ SND (exp(G,Y').{Nb'}_Hash(exp(EGX',Y')))
/\ request (B,A,auth_part1,Hash(EGX'))
3. State = 3 /\ RCV({Na'.Nb}_Hash(exp(EGX,Y)))
=|>
State':=5 /\ SND ({Na'}_Hash(exp(EGX,Y)))
/\ request (B,A,auth_a,Na.Nb)
/\ witness (B,A,auth_b, Na'.Nb)
/\ PK':=Hash(Na',Nb,exp(EGX,Y))
/\ secret(PK',sec_b_PK,{A,B})
end role
role session (
A,B : agent, % Initiator and Responder
OOB : symmetric_key,
```

```
Hash : hash_func, % Hash Function
G :nat ) % Diffie Hellman's public G value
def=
local SA, SB, RA, RB: channel (dy)
composition
initiator(A,B,OOB,Hash,G,SA,RA)
/\ responder(B,A,OOB,Hash,G,SB,RB)
end role
role environment()
def=
const
a,b : agent, % Initiator and Responder
oab, oai, obi : symmetric_key,
hash_ : hash_func, % Hash Function
g : nat, % Diffie Hellman's public G value
auth_part1, auth_a, auth_b: protocol_id
intruder_knowledge = {a,b,oai,obi,hash_,g}
composition
session(a,b,oab,hash_,g)
/\ session(a,i,oai,hash_,g)
/\ session(i,b,obi,hash_,g)
end role
goal
secrecy_of sec_a_PK, sec_b_PK
authentication_on auth_part1
authentication_on auth_a
authentication_on auth_b
end goal
environment()
```