Département de formation doctorale en informatique **École doctorale IAEM Lorraine**
UFR STMIA

Monitorage et Détection d'Intrusion dans les Réseaux Voix sur IP

RÉSUMÉ DE THÈSE

présentée et soutenue publiquement le 31 Mars 2009

pour l'obtention du

Doctorat de l'université Henri Poincaré – Nancy 1

(spécialité informatique)

par

Mohamed Nassar

Composition du jury

Rapporteurs :	Georg CARLE Ludovic MÉ
Examinateurs :	François CHARPILLET Olivier FESTOR Radu STATE

Laboratoire Lorrain de Recherche en Informatique et ses Applications — UMR 7503

Mis en page avec la classe thloria.

Remerciements

Je tiens tout d'abord à remercier mon directeur de thèse M. Olivier Festor qui m'a donné la chance de travailler sur un sujet d'actualité, d'importance et d'ouverture scientifique remarquables. Je remercie également mon co-directeur de thèse M. Radu State avec qui j'ai eu la chance et le plaisir de travailler durant ces trois années et demi. Leurs conseils aux niveaux scientifiques et personnels ont toujours été clairs et m'ont permis d'aboutir à la production de ce travail. Je les remercie aussi pour leur disponibilité et les discussions régulières que nous avons eues. Merci pour m'avoir montré mes faiblesses et aussi pour m'avoir félicité à chaque fois que je complète une certaine étape avec succès

Je remercie M. George Karl et M. Ludovic Mé pour avoir accepté de rapporter ma thèse et pour les efforts que leur a demandés ce travail. Leurs critiques étaient constructives et leurs indications m'étaient utiles.

Je présente mes vifs remerciements pour M. François Charpillet qui m'a fait l'honneur de présider le jury et pour le temps qu'il a passé à la lecture de ce document.

J'exprime mes sincères remerciements aux membres de l'équipe MADYNES pour l'ambiance conviviale qu'ils ont fait régner dans l'équipe. Je remercie mes collègues aux bureaux des doctorants (certains ont déjà terminé leurs doctorats) : Humberto Abdelnur, Mohamed Salah Bouassida, Rémi Badonnel, Thibault Cholez, Vincent Cridlig, Guillaume Doyen, Jérome François, Abdelkader Lahmadi, Tom Leclerc, Cristian Popi, Julien Siebert et Gérard Wagner pour leur vraie amitié, pour leur écoute et pour leur soutien dans les moments difficiles. Sans eux, ces années passées n'auraient pas été aussi agréables. Je tiens à remercier Humberto Abdelnur, Balamurugan Karpagavinayagam, Nataraj Mocherla et Cristi Stefan qui ont travaillé en parallèle sur d'autres aspects de la sécurité VoIP. Leurs résultats et les discussions que nous avons eues m'étaient très utiles et constructives. Je remercie également Frédéric Beck et Abdelkader Lahmadi pour leur aide au niveau technique et leurs recommendations avisées. Je remercie Mohamed Bouali et Anca Ghitescu qui ont marqué leur passage à MADYNES par un humour et une convivialité remarquables.

Je suis reconnaissant à Charbel Rahhal pour sa lecture attentive du manuscrit et pour les remarques qu'il m'a données.

Je pense aussi à mes amis avec qui j'ai eu des moments de complicité durant cette période passée à Nancy (dans l'ordre alphabétique) : Mohamed Ali Ahmad, Ali Attar, Toufik El Khatib, George Habib, Jamil Houhou, Rimond Hamia, Nazih Ouwayed, Samer Merhi, Ali Nassour, Jamal Saboune et Rami Saad. J'en oublie sûrement. Qu'ils m'excusent.

Je remercie tout de même M. et Mme. Kassem, M. et Mme. Masri pour m'avoir considéré comme un membre de leurs familles et pour toute leur générosité et courtoisie.

Mes remerciements vont également à Mlle. Hania Rida pour son optimisme et ses encouragements qui ont été d'un réconfort essentiel durant la rédaction de ce manuscrit.

Enfin, je veux exprimer toute ma gratitude à mes parents et à ma famille qui m'ont soutenu et encouragé depuis toujours et sans eux je ne serais pas parvenu à accomplir ce travail.

Je dédie cette thèse
à ma mère Hayat
et mon père Khodor

Table des matières

Chapitre 3
Évaluation

Table des figures

Introduction Générale

La Voix sur IP (VoIP) est une technologie très attirante. Sa définition dépasse la transmission de la voix par les réseaux de commutation des paquets pour englober d'autres applications multimédia et pour garantir de la dynamité, de la mobilité et du caractère innovant de ces applications. Elle est de plus en plus employée par les entreprises et les particuliers à cause de sa grande flexibilité et son avantage financier par rapport à la téléphonie traditionnelle (RTC). L'ensemble des produits VoIP n'est pas seulement constitué par des équipements utilisateurs mais également des processeurs/gestionnaires des appels, des passerelles vers d'autres réseaux téléphoniques, des serveurs et serveurs mandataires (Proxys), des pare-feux dynamiques spécifiques, un ensemble de protocoles standards et propriétaires. VoIP hérite des problèmes de sécurité adjacents aux réseaux IP auxquelles s'ajoutent des problèmes spécifiques. Les attaquants peuvent exploiter les différentes vulnérabilités dans les protocoles et les architectures VoIP. Les protocoles de signalisation comme SIP (Session Initiation Protocol [37]) et H.323 [13] et les protocoles de transport des médias comme RTP et RTCP [39] peuvent tous être la cible d'un ensemble d' attaques, comme l'écoute illicite des conversations, le déni de service, l'usage frauduleux et le SPIT (Spam over Internet Telephony). Les considérations de sécurité et les remèdes pour les problèmes de la VoIP ont été au cœur d'une large discussion dans les communautés industrielles, académiques et gouvernementales. Les mécanismes de sécurité sont fortement limités par les caractéristiques liées à la VoIP comme la qualité de service, la translation des adresses réseaux (NAT), et l'établissement des appels à travers les pare-feux. Les politiques de sécurité conventionnelles comme TLS [6], IPsec [17] et S/MIME [32] utilisées dans les réseaux de données sont fortement recommandées mais ne peuvent pas être intégrées pratiquement dans des déploiements à grande échelle, ouverts et dynamiques comme ceux imposés par la VoIP. Certains de leurs inconvénients sont l'augmentation de latence, l'incompatibilité avec les NATs, et leur dépendance vis-à-vis d'une infrastructure de distribution de clés. Une deuxième ligne de défense s'avère essentielle. Des systèmes d'alerte précoce, des mécanismes de monitorage et de détection d'intrusion jouent un rôle indispensable dans la protection, l'atténuation et la prévention des agressions. Des travaux importants dans le domaine de la détection d'intrusion ont déjà été menés par l'industrie et la recherche universitaire. Ces travaux se sont principalement intéressés aux couches de routage, transport et application alors que les approches spécifiques à la VoIP sont encore dans leur phase initiale. Notre contribution est motivée par la prise en compte des solutions conceptuelles existantes pour les adapter au domaine spécifique de la VoIP. Notre travail se focalise sur la conception, l'implantation et la validation de nouveaux modèles et architectures effectuant de la défense préventive, du monitorage et de la détection

d'intrusion dans les réseaux VoIP. Ce manuscrit est composé par trois chapitres organisés comme suit : Le premier chapitre établit un état de l'art dans le domaine de la sécurité VoIP. Nous donnons une introduction générale aussi brève que possible sur les protocoles dédiés à la VoIP : la signalisation, le transfert des médias et le passage à travers les NATs. Nous nous concentrons essentiellement sur le protocole SIP, celui-ci étant le sujet principal de notre étude. Ensuite, nous présentons -via un panorama des menaces possibles- la problématique de notre thèse. Enfin, nous présentons les travaux principaux dans le domaine, nous discutons les différentes approches proposées et nous positionnons notre contribution à leur égard. Dans le deuxième chapitre, nous illustrons nos contributions composées de trois approches : en premier lieu, nous proposons un système de monitorage du trafic de la signalisation VoIP. Notre système est basé sur des algorithmes d'apprentissage. Nous proposons deux techniques pour constituer le cœur de notre système : les machines à vecteurs support (SVM) et les réseaux Bayésiens. Comme un système d'alerte précoce, nous proposons un pot de miel spécifique que nous décrivons la conception et l'implantation. Nous détaillons un mécanisme d'inférence qui sert à classifier les messages reçus par le pot. Enfin, nous proposons une solution distribuée multi-niveaux de détection d'intrusion en utilisant deux sources des événements : l'une basé hôte, la seconde basée réseau ainsi qu'un moteur de corrélation des événements couche application. Nous montrons comment des approches complémentaires peuvent, lorsqu'elles sont utilisées conjointement, fournir une défense profonde dans les architectures VoIP. Dans le troisième chapitre, nous enchaînons avec l'évaluation de nos contributions. En premier lieu, nous présentons notre outil : le VoIP bot, qui est un agent SIP/RTP contrôlé et configuré par IRC pour lancer (ou recevoir) des attaques. Cet outil ouvre la discussion sur l'apparition de maliciels VoIP dans le futur proche. Ensuite, nous validons notre approche de monitorage en utilisant un mixage de trafic réel et des attaques générées localement dans un banc d'essai. Nous performons des expérimentations exhaustives pour configurer et ajuster nos paramètres de monitorage et comparer les deux techniques proposées (les SVM et les réseaux Bayésiens) en termes de performance en classification et en détection d'anomalie. Enfin, nous présentons un prototype d'un corrélateur des événements basé-réseau qui peut être intégré dans un proxy SIP. Nous montrons la capacité de notre prototype à détecter un ensemble de signatures d'attaques de signalisation. Les résultats de notre évaluation sont prometteurs dans deux directions : vers un déploiement temps-réel de notre schéma de monitorage, et vers une protection efficace basée-signature à l'aide de notre plateforme de corrélation d'événements. Notre pot de miel va être incorporé dans un laboratoire haute-sécurité. Avec l'émergence de SPIT attendue comme une menace majeure dans l'Internet de futur, nous estimons que notre pot de miel va démontrer une originalité et une importance certaine dans les prochaines années.

1

État de l'art

Sommaire

1.1 Introduction

Plusieurs normes et protocoles sont impliqués dans la livraison de la voix sur IP et des services multimédias sur Internet. Les couches Internet de lien physique, de routage et de transport assurent des services différents pour soutenir trois catégories de protocoles dans la couche application :

- Les protocoles de signalisation : SIP (Session Initiation Protocol), H.323 (une famille de protocole pour la communication multimédia dans les réseaux à commutation de paquets) et MGCP (Media Gateway Control Protocol) ;
- Les protocoles de média : RTP (Real-Time Transport Protocol) ;
- Les protocoles utilitaires : DNS (Domain Name Service), DHCP (Dynamic Host Configuration Protocol), TFTP (Trivial File Transfer Protocol) ;

Toutefois, la signalisation a une valeur particulière dans toute architecture de téléphonie ; elle sert à mettre en place, router, commuter et facturer les appels. De même pour la téléphonie sur Internet, la signalisation est l'outil clé pour créer des services et applications innovants. SIP est reconnu comme le protocole de-facto de signalisation d'aujourd'hui et il est prévu de l'être pour le futur. Nous introduisons les notions de base de ce protocole

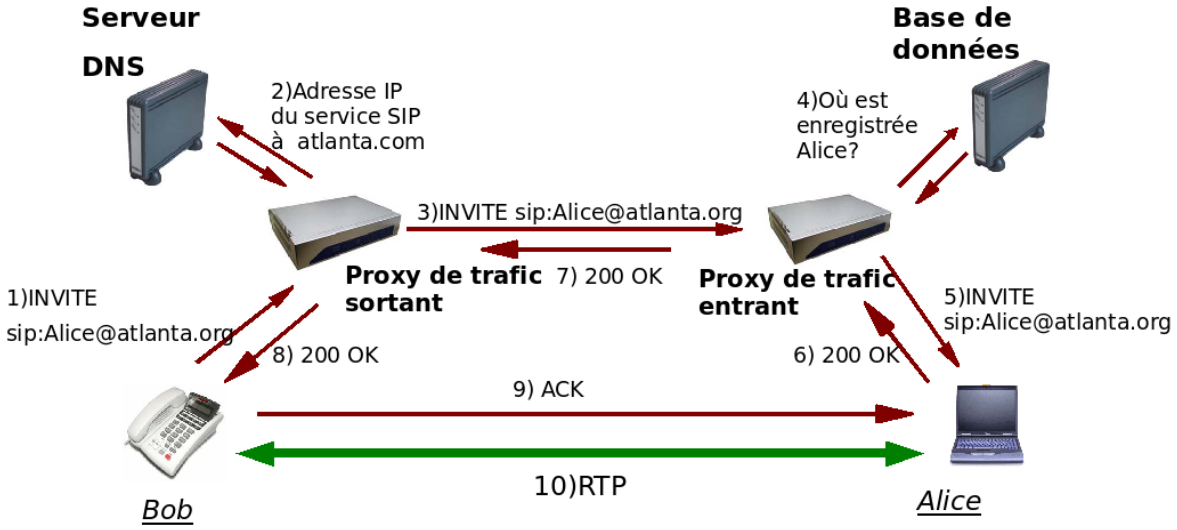

FIG. 1.1 – Le trapèze SIP

dans Section 1.2. Nous étudions les menaces qui entourent la VoIP dans Section 1.3. L'état de l'art sur la détection et la prévention de ces menaces suit dans Section 1.4.

1.2 SIP

SIP est le principal candidat pour devenir la norme de signalisation dans l'Internet du futur. Particulièrement, il a les points forts suivants :

- SIP est professionnellement développé par l'IETF (Internet Engineering Task Force) pour passer à l'échelle de l'Internet et utiliser ses normes et ses capacités (DNS, support des URLs, supporté par le sans-fil) ;
- SIP est un protocole en mode texte héritant du patrimoine d'HTTP et d'SMTP, ce qui facilite sa programmation, son acceptation et sa compréhension ;
- SIP a des capacités de présence et de messagerie instantanée ce qui présente un potentiel pour inventer des nouvelles applications ;
- SIP est soutenu par l'industrie ; il a été adopté par les opérateurs de téléphonie mobile pour leur troisième génération des réseaux et services (3GPP) ;

En fondamental, SIP permet à deux parties communicantes d'établir, de modifier et de terminer un appel téléphonique. SIP est basé-transaction ; chaque transaction est composée par une requête et une réponse. Son schéma d'adressage est basé sur l'URI (Uniform Resource Identifier), par exemple *sip :user@host :port ;parameters*. SIP définit de nombreux éléments architecturaux tels que l'agent, le proxy (serveur mandataire), le serveur de redirection, le serveur d'enregistrement et d'emplacement. Un exemple de base d'un scénario d'appel est représenté dans Figure 1.1. Voici un exemple de message SIP :

```
INVITE sip:1000@192.168.1.10 SIP/2.0
Max-Forwards: 10
Via: SIP/2.0/UDP 192.168.1.2:5060;branch=z9hG4bK1248BB87
```

```
CSeq: 7599 INVITE
To: <sip:1000@192.168.1.10>
Content-Type: application/sdp
From: <sip:bob@192.168.1.2>;tag=2AC98585
Call-ID: 580112446@192.168.1.2
Subject: Direct Call
Content-Length: 256
User-Agent: kphone/4.2
Contact: <sip:bob@192.168.1.2:5060;transport=udp>
P-hint: outbound
<corps SDP pas affiché>
```

C'est une requête SIP dont La première ligne contient l'URI appelé et la méthode (INVITE). Les lignes suivantes sont des entêtes SIP ayant une forme générale *tête :valeur;paramètre= valeur*. Les entêtes *From* et *To* permettent d'identifier l'expéditeur et le destinataire. L'entête *Contact* indique l'adresse à laquelle l'expéditeur souhaite recevoir la réponse. L'entête *User-Agent* contient la marque du dispositif utilisé. Les entête *Via* sont utiles pour le routage. Dans notre exemple, l'entête Via indique le protocole de transport (UDP), l'IP et le port du dispositif à l'origine du message. Le paramètre *Branch* dans *Via* identifie la transaction en cours. Un dialogue entre deux entités est composé d'une ou plusieurs transactions et est identifié par l'entête *Call-ID*. À cause de certains cas -par exemple si le message est fourchu vers des destinations différentes- deux paramètres servent à identifier un dialogue en addition au Call-ID : un tag dans le From est ajouté par l'appelant et un tag dans le To est ajouté par l'appelé. Les transactions peuvent être classées comme transaction-client (de la part de l'expéditeur de la requête) et transaction-serveur (de la part de la destinataire de la requête). Ils sont classés aussi comme des transactions INVITE (où des réponses intermédiaires -aussi appelées informationnelles- peuvent précéder la réponse finale) et des transactions non-INVITE (Les autres requêtes les plus importants sont REGISTER, CANCEL, BYE, ACK, OPTIONS et NOTIFY). Seules les requêtes INVITE sont acquittées. Une requête ACK est utilisée pour l'acquittement d'une transaction INVITE. Si la réponse finale à l'INVITE est une réponse 200 OK (succès) alors l'ACK est considéré comme une nouvelle transaction.

1.3 Les menaces de la VoIP

Cette nouvelle génération des services offre des réductions de coût et une grande flexibilité aussi bien pour les utilisateurs que pour les entreprises. Néanmoins, cette génération apporte des grandes considérations de sécurité. La VoIP hérite des défauts de sécurité de l'Internet et ajoute des nouvelles menaces spécifiques. À force de partager la même infrastructure avec les réseaux de données, les possibilités d'écoute illicite sont réelles. Les mises à jour des logiciels de la VoIP peuvent être malicieusement modifiées par défaut d'une bonne vérification d'intégrité. L'identification et la classification de ces risques constituent la première étape dans tout projet de sécurité. En comptant la cible d'une attaque comme un premier critère de classification, nous avons classé les attaques spécifiques à la VoIP

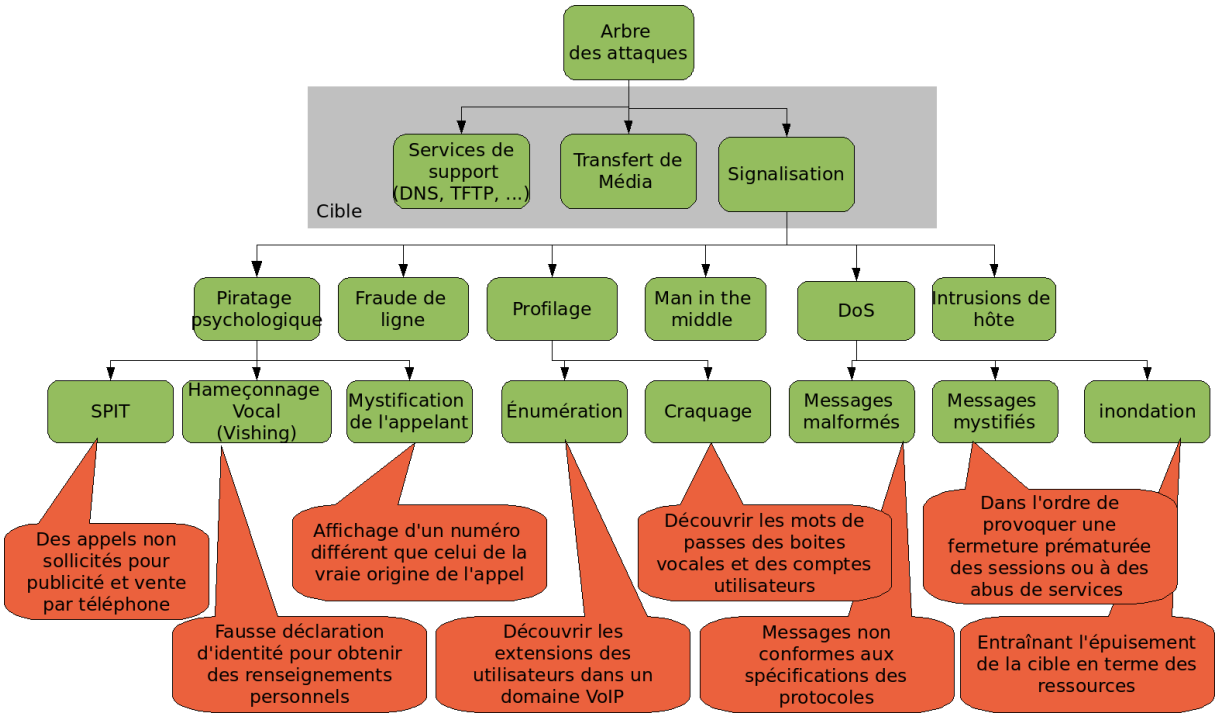

FIG. 1.2 – Les attaques spécifiques à la VoIP

dans l'arbre de Figure 1.2. Nous nous focalisons sur les attaques déni de service (DoS) et SPIT.

1.3.1 DoS

Les attaques de déni de service peuvent être effectuées en utilisant des méthodologies différentes. Les vulnérabilités des logiciels et intergiciels des applications VoIP sont la cible des exploits à distance comme le bordement de tampon et les messages non conformes syntaxiquement ou sémantiquement (SIP respecte une certaine grammaire ABNF). Les dégâts éventuels peuvent être le crash du système, l'exécution de code à distance ou l'accès non autorisé à des ressources. D'autres attaques ont lieu contre la procédure d'établissement d'appel SIP en utilisant des messages usurpés. Par exemple, Alice appelle Bob en envoyant un INVITE. Trudy envoie un CANCEL à Bob en se faisant passer pour Alice ce que lui empêche de recevoir l'appel. Si chaque fois qu' Alice tente de passer un appel, Trudy envoie un CANCEL à la destination alors Alice sera en déni de service. Dans un scénario similaire, Trudy pourrait envoyer un BYE pour mettre fin à une session après son initiation. Des réponses usurpées telles que 4xx (erreur client), 5xx (erreur de serveur) ou 6xx (erreur globale) peuvent être utilisées en se faisant passer pour un serveur et convaincre un utilisateur que le service est actuellement en panne ou en le dirigeant vers une autre destination. Les attaques d'innondation (Flooding) visent les éléments de signalisation (proxy, passerelle, PBX) dans l'objectif de les planter ou de réduire leur disponibilité, la qualité de service et leur fiabilité. Elles peuvent être classées suivant leur stratégie et leur destination. Du point de vue stratégie, Certaines attaques sont dites mé-

moire parce qu'elles atteignent la mémoire de la cible alors que d'autres sont dites CPU. Les attaques mémoire submergent le serveur par des requêtes qui nécessitent être gardées pour un certain temps en mémoire en attente de l'évaluation de certains paramètres réseaux (ex. DNS). Les attaques CPU visent le mécanisme d'authentification au serveur en utilisant des nonces valides [22]. Du point de vue destination -comme il est proposé par les auteurs de [9]- ces attaques peuvent être divisées comme suit :

- Innondation d'INVITE avec une URI valide dans le domaine cible : L'attaque est dirigée vers un destinataire enregistré à travers un proxy cible. Le téléphone destinataire est rapidement surchargé par le grand nombre d'appels et n'est plus en mesure d'y mettre fin. Si le proxy est stateful (il tient compte de la machine d'état de chaque transaction servie), il subira une allocation de mémoire pour une durée longue et arrivera à saturation.
- Inondation d'INVITE avec une URI inexistante dans le domaine cible : Si l'attaquant ne connaît pas une URI valide servie par la cible et qu'il dirige son attaque vers une URI invalide, le proxy cible répond par une réponse d'erreur de type "404 User not found". En conséquence, le proxy est surchargé par des opérations inutiles et risque de rejeter des requêtes légitimes.
- Inondation d'INVITE avec une adresse IP invalide comme domaine de destinataire : L'attaque est dirigée vers une destination avec une fausse adresse IP dans la partie domaine de l'URI. La cible va essayer de router les messages vers cette destination tout en gardant en mémoire un grand nombre de transactions.
- Inondation d'INVITE avec un nom de domaine invalide comme domaine de destinataire : L'attaque est dirigée vers une destination avec un mauvais nom de domaine (qui ne peut pas être résolu) dans la partie domaine de l'URI. La cible va essayer de traduire ce nom en une adresse IP en émettant plusieurs requêtes DNS (A, AAAA, SRV, NAPTR) ce qui provoque un temps d'attente pour servir chaque message. Ce temps d'attente permet d'accumuler les requêtes dans la mémoire de la cible. Nous illustrons l'effet de cette attaque sur un serveur de type OpenSER dans Figure 1.3. Le serveur ralentit et à un certain moment arrête totalement de répondre aux requêtes arrivantes. Dans nos expériences, le serveur est bloqué après 20 secondes d'une attaque à un taux faible (1 INVITE/s).
- Inondation d'INVITE avec une destination valable dans un autre domaine : L'attaque est dirigée vers un URI situé dans un autre domaine que celui du domaine cible. Le proxy cible transmet les appels des requêtes vers le proxy de l'autre domaine qui les transmet à son tour vers le téléphone destination. Ce dernier tombe rapidement hors service alors que les transactions en attente vont submerger la mémoire des deux proxys.
- Inondation d'INVITE avec une destination invalide dans un autre domaine : L'attaque est dirigée vers un URI situé dans un autre domaine que celui du domaine cible. Le proxy cible va transmettre les requêtes vers le proxy entrant de l'autre domaine en attendant les réponses. Comme la destination n'existe pas, des réponses d'erreur seront envoyées. Cette attaque vise plusieurs proxys en même temps et des événements de cascade peuvent se produire.

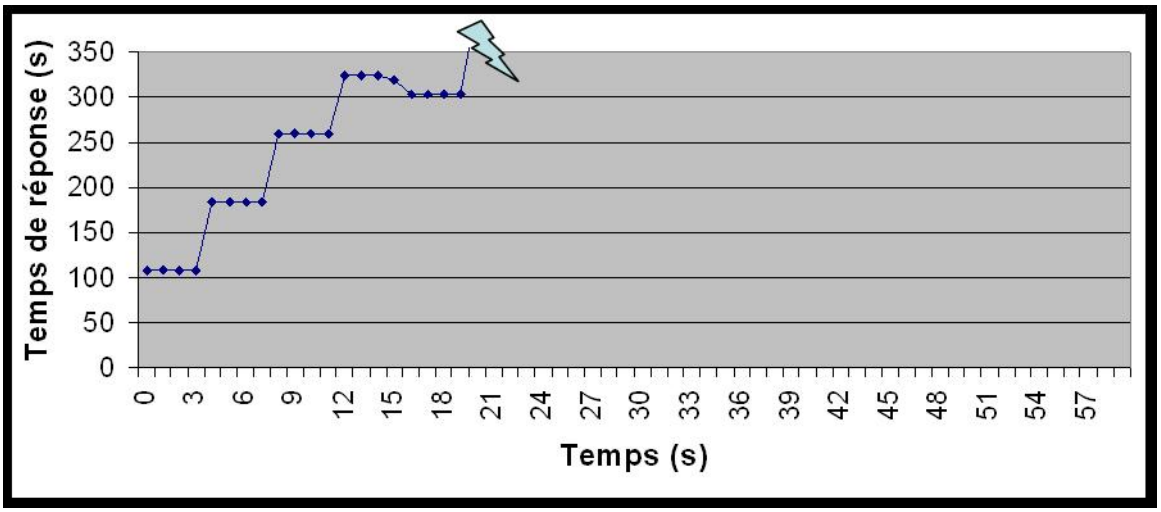

FIG. 1.3 – Réponse d'Openser à une inondation d'INVITEs avec un domaine/destination invalide

1.3.2 SPIT

Le piratage social allant des appels non sollicités qui vont ennuyer et perturber les utilisateurs (SPIT), jusqu'aux tentations de vol des informations personnelles (Vishing) constitue une vraie menace à la VoIP. Ces attaques sont difficilement définies parce que le terme "non sollicité" est étroitement lié aux préférences de chaque utilisateur. SPIT (SPAM over Internet Telephony), semblable au SPAM qui envahit les boîtes de messages électroniques, est un bon marché pour les annonceurs en raison de la quasi-gratuité de la téléphonie sur Internet (Il est actuellement estimé que les appels VoIP sont trois fois moins chers que les appels RTC de nombreux opérateurs). Le SPIT va être utilisé pour diriger les clients vers un service ou essayer de leur vendre des produits. Une variante subtile du SPIT est le Vishing (Voice Phishing). Dans un schéma de Phishing, l'attaquant tente de se faire passer pour un tiers digne de confiance et envoie un e-mail à la victime pour la diriger, à partir d'un lien web comme leurre, vers une page web semblant être la page d'accueil de sa banque. Ensuite, on demande à la victime de remplir des formulaires qui révèlent des informations privées sensibles (données bancaires). Dans le cas de VoIP, on demande à la victime de composer un certain numéro de sélection directe à l'arrivée (DID). Ensuite on la dirige vers un système de réponse vocale interactif (IVR) semblant d'être digne de confiance et en tirer des données personnelles, ou on la dirige pour composer des numéros surtaxés pour en tirer un profit. La plupart de ces attaques vont être produites automatiquement par des machines (bot-nets) programmées à cet égard. Les transactions de SPIT et Vishing sont correctes du point de vue technique ce qui rend leur détection plus difficile. Ce n'est pas possible de distinguer à partir du message INVITE, dans le cas de SIP, s'il s'agit d'une opération illicite ou non. Le problème est plus compliqué parce qu'on ne peut pas connaître le contenu d'un appel avant que le téléphone ne sonne vraiment et que l'on réponde ce qui engendre la perturbation. Pour cette raison, les techniques utilisées avec succès contre le SPAM comme le filtrage de texte ne sont pas réutilisables dans le domaine VoIP. Même si une transaction est identifiée comme non sollicitée, les

poursuites juridiques sont fortement dépendantes des lois dans le pays de l'appelant. La transmission de l'identité de l'appelant est un service de téléphonie traditionnel qui permet à l'équipement privé d'abonné (CPE) de l'appelé de recevoir un numéro d'appel tel qu'il est fourni par l'appelant. L'enregistrement automatique des numéros (ANI) est un système utilisé par les entreprises de télécommunications pour identifier le numéro de l'appelant. Traditionnellement, le spoofing de numéro d'appel ou de l'ANI était un processus compliqué qui demandait l'accès aux PBX et locaux de l'opérateur. Avec la VoIP, il est devenu plus facile de falsifier l'identité de l'appelant (L'entête *From* dans le cas de SIP). Le spoofing de Caller-ID favorise l'usurpation d'identité et nuit aux systèmes de vérification humains ou automatisés comme par exemple les boîtes vocales.

1.4 Travaux liés

La VoIP est exposée à des vulnérabilités de sécurité dont l'ampleur n'est pas mesurée à ce moment. Une taxonomie importante de la sécurité et du respect de la vie privée dans le contexte de la VoIP est publiée récemment par VoIPSA [47]. Un certain nombre de livres sont consacrés à l' étude de ces aspects en partant des perspectives différentes : du point de vue hacking [9] et du point de vue des précautions [33]. Ainsi, des précautions sérieuses doivent être mises en place par les utilisateurs et les entreprises souhaitant installer VoIP. En addition à celles concernant les réseaux de données, les meilleurs pratiques de sécurité sont : désigner une architecture appropriée à la VoIP en la séparant du réseau de données ; utiliser des mécanismes d'authentification et de cryptage ; résoudre les problèmes liés au NAT, pare-feu et qualité de service ; utiliser IPsec ou SSH pour toute gestion et audition à distance ; de préférence éviter les téléphones logiciels (soft-phone) ; garder les systèmes à jour en téléchargeant les patches et les mises à jour tout en vérifiant leur intégrité ; et finalement donner une importance particulière aux systèmes d'appel en urgence [20, 48, 33]. Les auteurs de [10] analysent les mécanismes de sécurité dans les protocoles VoIP et marquent certaines de leurs faiblesses. Plusieurs composants de sécurité ne peuvent pas être directement utilisés pour protéger la VoIP : les pares-feu doivent permettre l'ouverture et la fermeture dynamique de ports suivant les demandes de transfert de média ; les NAT compliquent l'établissement des appels s'ils ne sont pas accompagnés des procédures de dépassement comme le STUN ou le TURN ; le cryptage cause une expansion de volume des paquets, des délais de délivrance et de la complexité de distribution des clefs. Des nouveaux mécanismes de détection d'intrusion sont indispensables. La détection d'intrusion dans les réseaux VoIP constitue un défi important pour les raisons suivantes (dont certaines ont été soulignées par [49]) :

- Les systèmes VoIP sont distribués (Agents, proxys, PBX). Le monitorage d'un seul point d'entrée est insuffisant surtout si nous voulons surveiller des activités malicieuses internes au réseau et pas seulement des attaques externes ;
- Les systèmes VoIP utilisent des protocoles différents pour la signalisation, le transfert de media, la configuration et la gestion ;
- Les systèmes VoIP sont hétérogènes et typiquement situés sous des administrations autonomes et indépendantes.
- Les systèmes VoIP sont la cible d'un grand ensemble d' attaques dans un environ-

nement où les pirates ont déjà une grande expérience
- Un compromis existe entre sécurité et isolation : nous devons être joignables sans être perturbés par les appels SPIT.
- On doit respecter des exigences strictes en terme de vérification : Certaines attaques DoS sont accomplies à l'aide d'un seul message, d'autres sont accomplies à l'aide d'une inondation à faible intensité.

Dans la suite nous exposons les travaux récents dans le domaine de la détection d'intrusion VoIP en portant une attention particulière à la détection de DoS, de SPIT et sur le monitorage de trafic.

1.4.1 Travaux généraux

Niccolini et. al. [26] suggèrent l'utilisation d'un système de détection et de prévention basé-réseau au point d'entrée d'un réseau VoIP. Ils proposent un processus à deux étapes : la première est basé-connaissance (signature) et la deuxième est basé-modèle de comportement (anomalie). En se basant sur le système Snort[1], les auteurs implantent une unité de prétraitement logique des messages SIP composé par plusieurs modules : vérification et analyse de syntaxe, vérification des entêtes, et vérification de l'état à partir d'un ensemble de messages. Une évaluation de performance de ce prototype est réalisé à l'aide de générateur de trafic BRUTE [3]. Le système SCIDIVE [49] déploie deux méthodes de détection des signatures : détection basé-état à partir des messages d'un seul protocole et détection croisée de messages à partir de protocoles différents. Le système utilise un moteur de règles (matching). Le système est démontré pour détecter des classes différentes d'intrusion allant de l'usurpation d'identité jusqu'au déni de service, les attaques des flux média, et la fermeture prématurée des sessions. Sengar et. al. [41] proposent un système basé sur l'interaction entre les machines d'état SIP et RTP pour détecter la violation de certaines spécifications de sécurité. De façon similaire, Ding et al. [7] proposent des réseaux de Petri colorés hiérarchiques et temporisés (timed HCPN) pour détecter le même ensemble des attaques. Une approche de détection d'intrusion basé-spécification est encore appliquée pour les protocoles H.323 [43]. Les approches précédentes sont testées sur un ensemble limité des attaques et ne montrent pas de réelle capacité de passage à l'échelle. Par exemple, dans [26], le système fonctionne bien pour une charge de 850 messages/s ce qui est n'est pas acceptable pour des liens à grande vitesse. Une architecture plus prometteuse est nommée "VoIP Defender" et est spécialement dédiée à des trafics de grand volume. Cette architecture -basée sur un schéma de répartition des charges- est générique parce qu'elle construit un cadre pour des algorithmes de détection sans les définir. Les auteurs définissent les caractéristiques générales d'un point de protection qui protège un point de provision de service. Ces caractéristiques sont : la transparence, la vitesse, le passage à l'échelle, l'indépendance et l'extensibilité. D'autres travaux se concentrent sur la protection de signalisation intégrée lors du passage de VoIP à la RTC et vice versa [40] ainsi que sur les systèmes d'empreinte des équipements VoIP [50].

[1] `www.snort.org`

1.4.2 Travaux sur le DoS

Deux approches portent sur la détection des messages malformés : [11] propose un cadre de détection basé-signature et [35] propose un cadre de détection basé-anomalie. Les auteurs du premier argumentent que les messages malformés peuvent être efficacement décrits en utilisant des structures spécifiques connues sous le nom de "signatures". Ils utilisent des signatures composées de deux parties en se basant sur des expressions régulières du langage Perl : la première partie vérifie si le message est conforme aux spécifications du protocole comme décrit par le RFC 3261 [37] alors que la deuxième partie définit des règles de vérification additionnelles contre des attaques comme l'injection SQL. Les auteurs du deuxième proposent un système d'apprentissage automatique qui est capable de détecter des anomalies nouvelles. Le système transforme un message SIP en un vecteur d'attributs dans un espace multidimensionnel. Une anomalie est détectée comme une déviation d'un modèle de normalité. Les auteurs proposent des attributs de type Tokens ou les N-grams et définissent deux modèles de détection : le premier est global basé sur la plus petite sphère englobante alors que le deuxième est local basé sur les K-plus proches voisins. Le système s'adapte aux changements dans le réseau en s'entrainant automatiquement avec le temps. Il est protégé contre les manipulations malicieuses comme l'empoisonnement de trafic. D'autres travaux portent sur la détection d'inondation [34, 5, 8, 51].

1.4.3 Travaux sur le SPIT

Le principe clef dans l'identification de SPIT est l'identité de l'appelant. Les communications basées-consentement (l'appelant demande d'abord de s'ajouter à la liste des contacts de l'appelé) sont perturbantes lorsque les utilisateurs commencent à recevoir beaucoup de requêtes de consentement. Les listes blanc/noir ne résolvent pas le problème quand certains appelants apparaissent pour la première fois ou quand l'attaquant inonde la liste noire avec des identités inconnues. Les émetteurs de SPAM peuvent découvrir une identité appartenant à la liste blanche et l'usurper. En résultat, des assertions fortes de cryptographie sont nécessaires pour authentifier les appelants en particulier dans un contexte inter-domaines. Le groupe IETF SIPPING suggère la définition de deux nouveaux entêtes SIP [29] : Identity pour communiquer un certificat d'une identité et Identity-Info pour communiquer l'autorité qui a signé ce certificat. Dans une autre approche, les domaines VoIP peuvent construire des cercles de confiance en utilisant des connexions TLS. Ces approches sont très utiles dans une relation proxy à proxy mais malheureusement ne passent pas à l'échelle d'un environnement ouvert et dynamique tel qu'est l'Internet. Un algorithme de liste grise progressive multi-niveaux (nommé PMG) est proposé dans [42]. L'algorithme est basé uniquement sur le nombre des appels alors que les leçons de SPAM nous montrent l'importance d'utiliser plusieurs mesures de détection. Quittek et. al. [31] appliquent des tests de Turing du côté de l'appelant et comparent leurs résultats à des patrons de communication humaine. Pour passer ces tests, des ressources sont demandées du côté des attaquants ce qui réduit leur efficacité. Les auteurs valident leur approche en implantant un prototype dans leur système modulaire VoIP SEAL [38]. VoIP SEAL utilise deux étapes de détection : la première analyse l'appel avant de le transférer à l'appelé et la deuxième interagit avec l'appelé ou l'appelant pour raffiner la

détection. Comme la deuxième étape peut être inconvenante, un système de notation est utilisé dans la première étape pour déterminer le degré de soupçon. Une autre approche utilise une défense socio-technique [18]. Les auteurs décrivent un filtre adaptatif multi-étapes basé sur la présence (lieu, temps, état d'esprit), la confiance et la réputation. Ils décrivent une boucle fermée de contrôle entre les différentes étapes et un formalisme pour l'analyse de confiance et de réputation dédié à la VoIP. Cette méthode formelle est basée sur le comportement intuitif humain pour accepter ou rejeter un appel en se basant sur ses relations directes et indirectes avec l'appelant. Une approche similaire appelé " CallRank " [1] est proposée en parallèle : elle est basée sur la durée de l'appel, les réseaux sociaux et la réputation globale. Elle propose l'ajout des crédits de chaque appel au message INVITE ainsi que les notes de réputation données par les proxys. Ces approches exigent une infrastructure de distribution des clefs ce qui peut compliquer leur déploiement à grande échelle.

1.4.4 Monitorage de trafic

Le profilage et le monitorage de trafic sont impératifs aux fournisseurs de services pour protéger leurs infrastructures et leurs applications. À notre connaissance, le seul travail qui porte sur le profilage de trafic de signalisation VoIP et sur ses applications est publié dans [16]. Les auteurs proposent une méthodologie générale pour le profilage de trafic SIP à plusieurs niveaux : niveau hôte, niveau serveur (d'enregistrement ou proxy) et niveau individuel utilisateur. Des traces de trafic fournies par un environnement de production VoIP sont caractérisées suivant la méthodologie proposée. Les auteurs ont développé un algorithme de détection d'anomalie basé-entropie et ont montré son efficacité dans deux applications directes : diagnostique des problèmes et protection de sécurité. Parmi les résultats obtenus, l'approche proposée est capable de détecter une attaque SPIT à petit volume (10 appels concurrents) générée par une seule source seulement quand l'activité utilisateur de cette source est impliquée dans la détection. Ceci n'est pas applicable dans des scénarios du monde réel où plusieurs sources participent à l'attaque parce que le monitorage de toutes les sources possibles ne passe pas à l'échelle et le système de monitorage lui-même peut être une cible d'attaque. Nous suggérons qu'un profilage de trafic plus orienté vers la sécurité devrait être discuté ce que nous considérons dans nos contributions.

1.5 Conclusion

La nouvelle révolution dans le monde des télécommunications est menacée par des dangers plus ou moins élevés. Plusieurs travaux ont porté sur la détection d'intrusion, la protection contre le SPIT et le DoS et le monitorage de trafic. Ces systèmes ne vont pas mûrir avant d'entrer en contact réel avec les attaques. En même temps, les chercheurs ont intérêt à préparer leurs plateformes pour toujours devancer les pirates. Nous focalisons nos travaux sur les pièces manquantes dans le puzzle de la sécurité VoIP. Nos contributions sont présentées dans le chapitre suivant.

2

Contributions

Sommaire

2.1 Introduction

Nous travaillons sur trois axes différents :

- Nous assistons le monitorage de trafic SIP à des fins de sécurité. En particulier, nous incorporons des techniques d'intelligence artificielle pour la classification et la détection d'anomalie de trafic. Deux approches sont particulièrement étudiées : les réseaux Bayésiens et les machines à vecteurs support.
- Nous compensons l'absence des systèmes d'avertissement par la création de pots de miel et des réseaux des pots de miel. Nous proposons un "honeyphone" individuel suivi par un honeynet simulant tout un réseau VoIP en coopération avec le département recherche de NEC.
- Comme chaque solution déjà citée résout une seule partie du problème, couvre un sous ensemble des attaques et est placée dans des endroits différents dans le domaine VoIP, nous travaillons sur l'interconnexion de plusieurs dispositifs de sécurité par le fil de la corrélation des événements et de corrélation des alertes dans le but de posséder une perspective globale. La corrélation des événements permet de détecter des signatures distribuées de certaines attaques ce que nous prétendons nécessaire dans une application distribuée comme la VoIP. La corrélation des alertes nous laisse découvrir les plans et les stratégies des attaquants et reconstruire leur chaîne des actions.

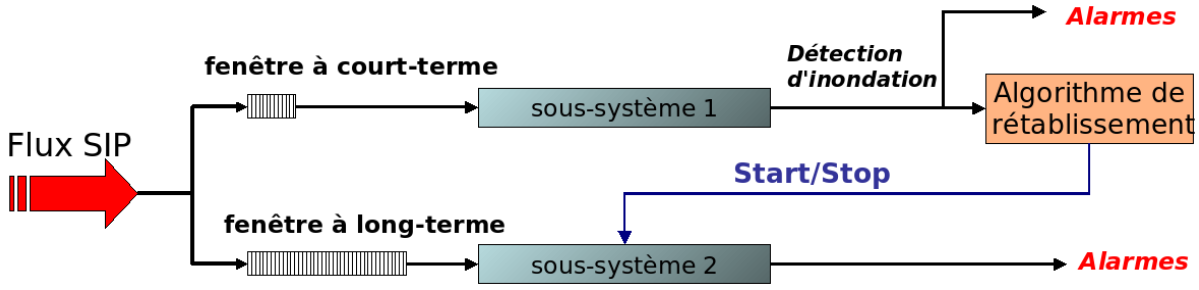

FIG. 2.1 – Système de monitorage long-terme/court-terme de trafic SIP

2.2 Monitorage de trafic SIP

Notre système de monitorage est illustré dans Figure 2.1. Il est composé par deux Sous-systèmes principaux travaillant en parallèle (par embranchement des messages reçus).

- Un moniteur à court-terme : travaillant comme une armure contre les attaques d'inondation. Il est responsable de protéger l'intégrité du système : une surcharge de trafic doit être détectée rapidement pour empêcher l'attaque de surprendre le système. Il contrôle une réponse de prévention et bloque l'alimentation du deuxième sous-système après le déclenchement d'une alarme. Les algorithmes de rétablissement sont hors de la portée de notre étude pour le moment mais ceux référencés par [34] peuvent être adoptés.
- Un moniteur à long-terme : agit comme un classificateur de trafic et un détecteur d'anomalie visant à détecter des attaques plus intelligentes et plus cachées.

Chaque sous-système est composé d'une série de composants comme l'indique Figure 2.2 :

- Une file de taille prédéfinie où on accumule des messages SIP. Comme il était proposé par l'un des travaux pionniers sur la conception des IDS [15], deux types de fenêtre peuvent être utilisés :
  - chronologique : nous accumulons les messages SIP pour une période de temps prédéfinie (ex. une seconde pour le sous-système à court-terme et 10 secondes pour le système à long-terme) ;
  - nombre : nous accumulons un nombre prédéfini de messages SIP (ex. 10 messages pour le sous-système à court-terme et 100 messages pour le sous-système à long-terme).
- Un analyseur : une fois la file remplie, l'analyseur en extrait un ensemble des attributs/statistiques prédéfinies ;
- Un moteur de classification : qui juge un vecteur comme appartenant à une certaine classe de trafic ou représentant une certaine anomalie et émet un événement si nécessaire. Ce moteur est basé sur une phase d'apprentissage durant laquelle il était nourri avec des couples de la forme (vecteur, Id. Classe).
- Un corrélateur des événements (ou décideur) : qui filtre et corrèle les événements pour déclencher une alarme et une réponse de prévention si nécessaire. Une alarme est générée pour un groupe d'événements s'ils déclenchent une règle parmi les règles de corrélation (ex. si le nombre des événements de type i dépasse un certain seuil dans une période de temps t). La motivation derrière ce corrélateur est de réduire

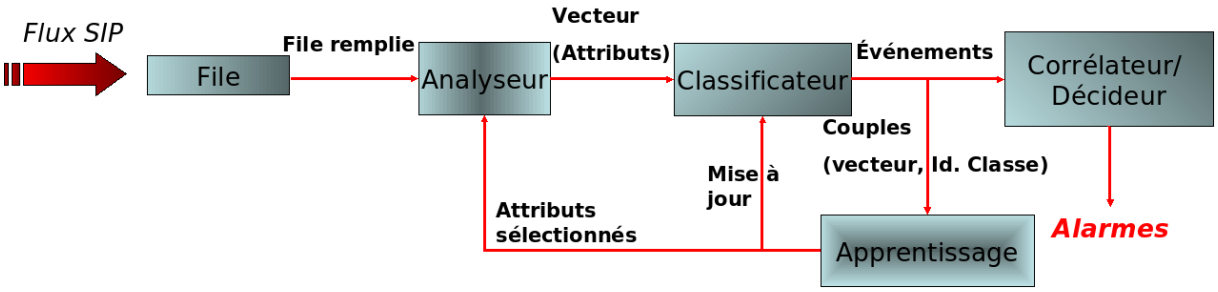

FIG. 2.2 – Sous-système basé sur une machine d'apprentissage

le nombre de fausses alarmes au minimum. Comme Figure 2.3 le montre, les faux positifs du système sont distribués et par conséquence ne sont pas corrélées ensemble et ne conduisent pas à une alarme, tandis que les vrais positifs provenant d'une vraie attaque se produisent dans une petite période et conduisent à une vraie alarme. Les attaques cachées (stealthy) sont caractérisées par des événements périodiques qui peuvent être corrélés par des règles spécifiques.

Le processus d'apprentissage peut être initialisé avec des traces labélisées. Si des traces "normales" sont uniquement disponibles, alors le système est boosté avec un algorithme de détection d'anomalie qui découvre des nouvelles attaques et les ajoute au schéma de classification. S'il n'y en a pas du tout des traces labélisées, alors des algorithmes d'apprentissage non supervisés sont employés. La détection d'anomalie et l' apprentissage non supervisé peuvent continuer à monitorer le trafic dans la phase opérationnelle en parallèle au classificateur dans le but de détecter des nouvelles classes d'attaque. Le réapprentissage de système est possible en temps réel en lui permettant d'actualiser son modèle de prédiction à partir du trafic en cours. Ainsi, notre système doit être immunisé contre les attaques d'empoisonnement et de manipulation (où les attaquants essayent de tromper le modèle de prédiction de la machine d'apprentissage). Plusieurs techniques peuvent être mise en place à cet égard comme la randomisation (apprentissage avec des portions de trafic choisies par hasard),et la vérification (le nouveau modèle de prédiction ne doit pas être très différent de l'ancien). Le pas du système t_{pas} est le temps qu'il prend pour prendre une décision à propos d'un seul créneau de trafic tout en négligeant la phase de corrélation . Ce temps est composé par deux valeurs :

- Le temps d'analyse ($t_{analyse}$) : est le temps consommé par l'analyseur pour extraire les attributs,
- Le temps de la machine ($t_{machine}$) : est le temps consommé par la machine d'apprentissage pour prédire la classe de ce créneau.

$$t_{pas} = t_{analyse} + t_{machine}$$

Le système achève un pas de temps réel si t_{pas} est plus petit que la taille de la fenêtre S divisée par le taux d'arrivée des messages λ dans le cas d'une fenêtre à compte :

$$t_{pas} < \frac{S}{\lambda}$$

Et si t_{pas} est plus petit que la durée de la fenêtre D dans le cas d'une fenêtre chronologique.

$$t_{pas} < D$$

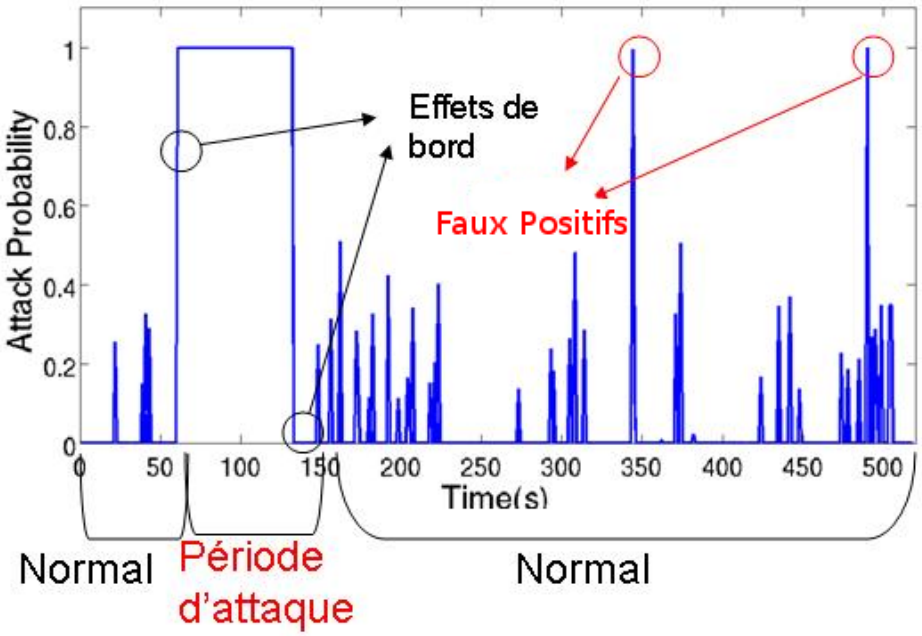

FIG. 2.3 – Détection d'intrusion à temps réel

Nos expérimentations montrent que le temps machine est relativement inférieur au temps d'analyse. Le nombre et la complexité des attributs sélectionnés sont un critère très important pour une analyse en ligne. Par exemple, des attributs en relation avec des dialogues SIP sont plus coûteux que des attributs en relation avec des transactions. Maintenir des listes de dialogues et des transactions exige des algorithmes optimisés pour leur parcours et est coûteux en termes de mémoire. Notre architecture proposée est modulaire et permet d'expérimenter avec des techniques différentes d'intelligence artificielle allant des modèles statistiques et de théorie de l'information (basé-entropie) jusqu'à la reconnaissance des patrons. Après une discussion élaborée de plusieurs approches dans l'état de l'art de la détection d'intrusion et autres domaines, nous avons choisi deux techniques récentes et importantes pour nos expérimentations avec : les réseaux Bayésiens (Bayesian Networks (BN)) [28, 25, 44, 19, 2] et les machines à vecteurs support (SVM) [45, 46, 12, 36, 23, 21].

2.2.1 Modèle Bayésien pour le monitorage de trafic SIP

Les modèles Bayésiens sont des graphes où les nœuds représentent une certaine connaissance et les relations entre les nœuds sont causales. Nous avons défini notre modèle en étudiant les relations cause-effet dans un ensemble d'attaques SIP (craquage, énumération, SPIT, DoS, traverse de pare-feu). Le modèle est illustré dans Figure 2.4.

2.2.2 Modèle SVM pour le monitorage de trafic SIP

Les SVM ne permettent pas une représentation des connaissances ou des relations causales comme les modèles Bayésiens. Ainsi , nous utilisons une stratégie différente pour

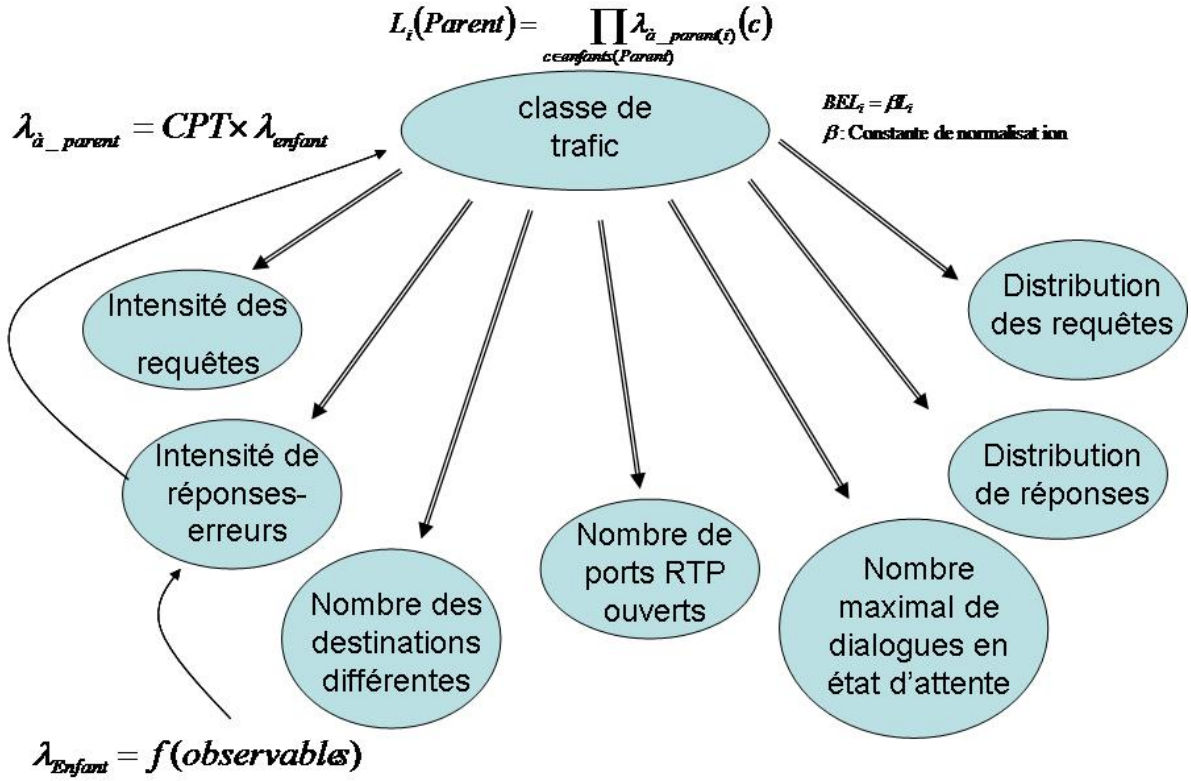

FIG. 2.4 – Modèle Bayésien naïf pour le monitorage de trafic SIP

construire un modèle SVM : Nous définissons un grand ensemble des attributs caractérisant le trafic SIP, puis nous appliquons des algorithmes de sélection pour en extraire les plus représentatifs (discriminatifs). Les attributs sélectionnés sont très dépendants de l'environnement supervisé et du schéma de classification (le trafic normal et les classes d'attaques) qu'on souhaite établir ce qui donne à notre approche un grand potentiel de généralisation. L'ensemble général des attributs est énuméré dans Tableau 2.1 (pour une fenêtre à compte).

2.3 Pot de miel VoIP

Un pot de miel est défini comme un environnement isolé où des vulnérabilités sont introduites délibérément dans le but d'y observer des attaques et des intrusions [30, 14]. Pot de miel (honeypot) et réseaux de pots de miel (honeynet) sont une stratégie de défense préventive : un système d'alarme anticipée pour déclarer des nouveaux types des attaques, et un support pour enregistrer et analyser les activités intrusives. Nous proposons un pot de miel individuel spécifique à la VoIP. Tout simplement, notre "honeyphone" joue le rôle d'un téléphone qui s'enregistre sur un proxy entrant et déclare un certain nombre d'URIs. Comme ces URIs n'appartiennent pas à des services et individus existants, ils ne doivent jamais être appelés par des humains mais par des robots de SPIT et des pirates. L'environnement de travail d'un tel pot est illustré à Figure 2.5 où un scénario de

TAB. 2.1 – Liste des attributs

Numéro	Nom	Description
Groupe 1 - Statistiques générales		
1	Durée	La durée de créneau
2	NbReq	# de requêtes / # total de messages
3	NbResp	# de réponses / # total de messages
4	NbSdp	# de messages portant SDP / # total de messages
5	AvInterReq	Moyenne d'inter arrivée de requêtes
6	AvInterResp	Moyenne d'inter arrivée réponses
7	AvInterSdp	Moyenne d'inter arrivée des messages portant SDP
Groupe 2 - Statistiques basées Call-ID		
8	NbSess	# de Call-IDs différents
9	AvDuration	Moyenne de durée d'un Call-ID
10	NbSenders	# d'émetteurs différents/ # total de Call-IDs
11	NbReceivers	# de récepteurs différents/ # total de Call-IDs
12	AvMsg	moyenne de # de messages par Call-ID
Groupe 3 - La distribution d'état final des dialogues		
13	NbNOTACALL	# de NOTACALL/ # total de Call-IDs
14	NbCALLSET	# de CALLSET/ # total de Call-IDs
15	NbCANCELED	# de CANCELED/ # total de Call-IDs
16	NbREJECTED	# de REJECTED/ # total de Call-IDs
17	NbINCALL	# de INCALL/ # total de Call-IDs
18	NbCOMPLETED	# de COMPLETED/ # total de Call-IDs
19	NbRESIDUE	# de RESIDUE/ # total de Call-IDs
Group 4 - Distribution des requêtes		
20	NbInv	# de INVITE /# total de requêtes
21	NbReg	# de REGISTER/# total de requêtes
22	NbBye	# de BYE/ # total de requêtes
23	NbAck	# de ACK/# total de requêtes
24	NbCan	# de CANCEL/ # total de requêtes
25	NbOpt	# de OPTIONS / # total de requêtes
26	Nb Ref	# de REFER/ # total de requêtes
27	NbSub	# de SUBSCRIBE/ # total de requêtes
28	NbNot	# de NOTIFY/ # total de requêtes
29	NbMes	# de MESSAGE/ # total de requêtes
30	NbInf	# de INFO/ # total de requêtes
31	NbPra	# de PRACK/ # total de requêtes
32	NbUpd	# de UPDATE/# total de requêtes
Groupe 5 - Distribution des réponses		
33	Nb1xx	# de réponses informationnelles (1xx) / # total de réponses
34	Nb2xx	# de réponses succès (2xx)/ # total de réponses
35	Nb3xx	# de réponses de redirection (3xx)/ # total de réponses
36	Nb4xx	# de réponses d'erreur client(4xx) / # total de réponses
37	Nb5xx	# de réponses d'erreur serveur (5xx)/ # total de réponses
38	Nb6xx	# de réponses d'erreur global (6xx)/ # total de réponses

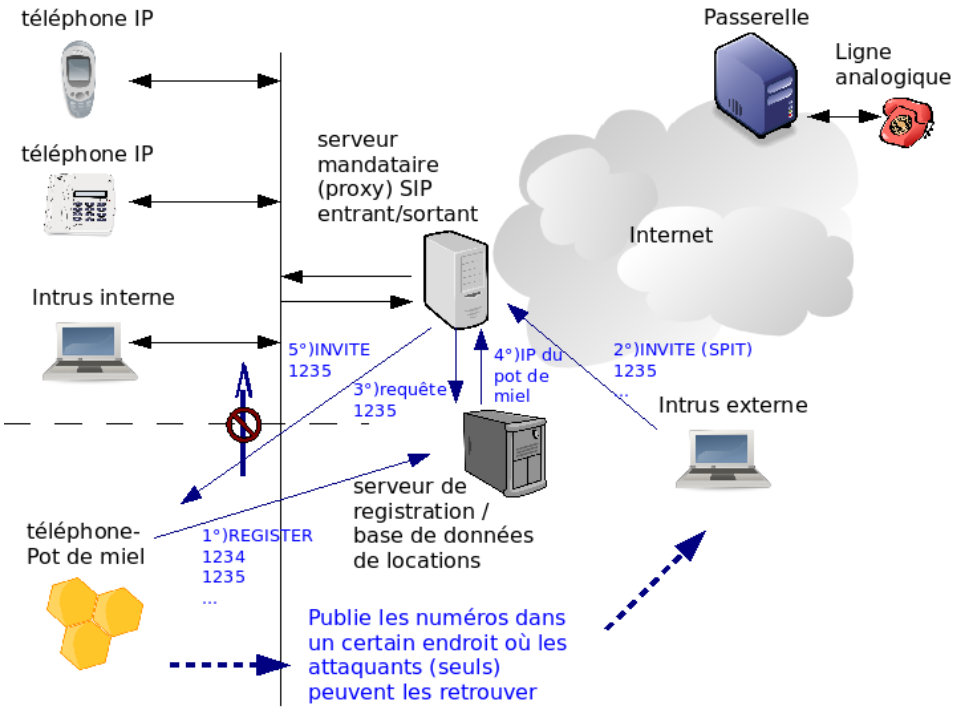

FIG. 2.5 – Environnement d'un pot de miel VoIP

réception d'un appel est représenté. Notre pot de miel est particulièrement efficace pour la détection d'une énumération de réseau VoIP, mitigation de SPIT, collection des signatures d'attaques et d'intrusions. Nous en proposons une architecture intérieure comme illustré dans Figure 2.6. Le "honeyphone" est constitué de cinq composantes principales :

- Un agent : est responsable d'accepter et d'enquêter les appels arrivants. Il est défini par des paramètres réseaux et un profil de comportement qui ajuste sa réponse (passif, actif ou agressif).
- Des piles (stacks) des protocoles VoIP et protocoles de support (SIP, RTP, SDP) : sont responsables de la construction, la transmission et du parsing des messages.
- Une base de donnée profils : permet la configuration du pot de miel dans son environnent (paramètres réseaux, SIP, STUN, URI à déclarer...) pareillement à un agent SIP normal et à préconfigurer sa machine d'états et ses réactions aux événements.
- Des outils de reconnaissance : sont utilisés dans l'investigation et le traçage des messages reçus (exemple : NMAP pour des opérations de balayage (scanning) de réseau, SIPSAK pour des opérations SIP, POF pour des opérations de détection d'empreinte (fingerprinting) ...) .
- Un moteur d'inférence : est capable d'interpréter automatiquement les résultats de la procédure d'investigation en se basant sur un modèle d'intelligence artificielle. Nous avons désigné un modèle Bayésien qui permet de différencier entre un appel correct mais soupçonné (SPIT), un appel par erreur (faute de routage) et un message malformé.
- Une interface graphique : permet à l'administrateur de configurer le pot de miel,

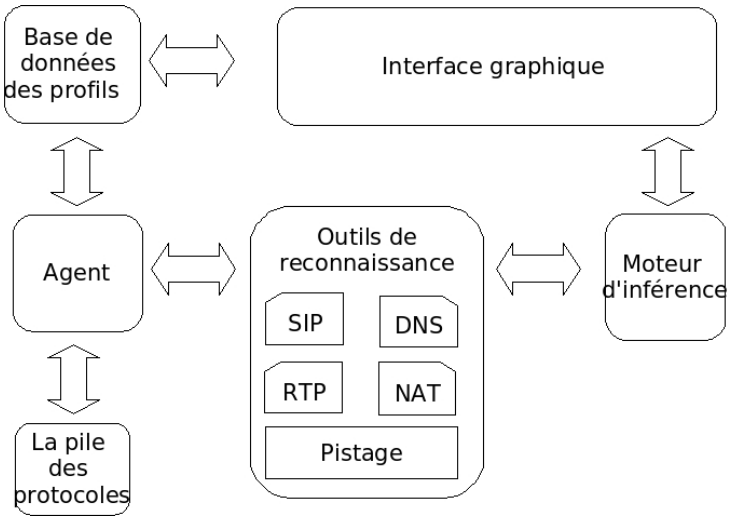

FIG. 2.6 – Architecture d'un pot de miel VoIP

ajouter et modifier des profils et visualiser les résultats.
Un pot de miel individuel a un champ de vue limité et par conséquent ne détecte qu'un sous ensemble des attaques. Pour en augmenter l'importance, nous proposons d'utiliser un réseau de pots de miel qui émule tout un domaine VoIP (utilisateurs, services(ex. : Asterisk PBX) et infrastructure (ex. : SIP router) offrant une valeur plus attirante aux attaquants. L'implantation est toujours en cours dans le cadre du projet européen EMANICS.

2.4 Détection d'intrusion VoIP distribuée

Les architectures VoIP sont difficiles à confronter avec une approche centralisée, un système de détection d'intrusion est de préférence distribué. La signalisation et le média ne suivent pas le même chemin. Un exemple typique de cette séparation est le protocole MGCP où l'agent des appels est responsable pour louer les connexions dans un nombre de passerelles média. Soit un exemple de fraude : Un appelant initie un appel vers le RTC en contactant un agent MGCP. L'agent choisit une passerelle qui a des slots (endpoints) libres et il y loue une connexion média en envoyant une commande CRCX permettant à l'appelant d'y émettre son flux RTP. Ensuite, l'appelant envoie un BYE prétendant qu'il a terminé l'appel vers l'agent. L'agent envoie une commande DLCX à la passerelle pour libérer la connexion. En effet, l'appelant va interrompre la commande DLCX et se fait passer pour la passerelle pour répondre avec un 200 OK disant que la connexion est libérée avec succès (aucun mécanisme d'authentification ni de cryptage ne sont par défaut utilisés avec MGCP). A ce moment, l'appelant fraudeur va continuer à utiliser la connexion sans être facturé. Une telle intrusion ne peut pas être détectée en surveillant l'un ou l'autre de l'agent ou la passerelle mais pas une approche centralisée comme dans Figure 2.7. Pour généraliser cette approche, nous proposons un cadre de corrélation des événements provenant de plusieurs éléments de sécurité ou capteurs (VoIP SEC). Ces capteurs sont des systèmes de détection locale basés hôte ou basé réseau. Un IDS basé hôte peut être installé sur un point d'intérêt comme une passerelle, un agent ou un proxy pour surveiller

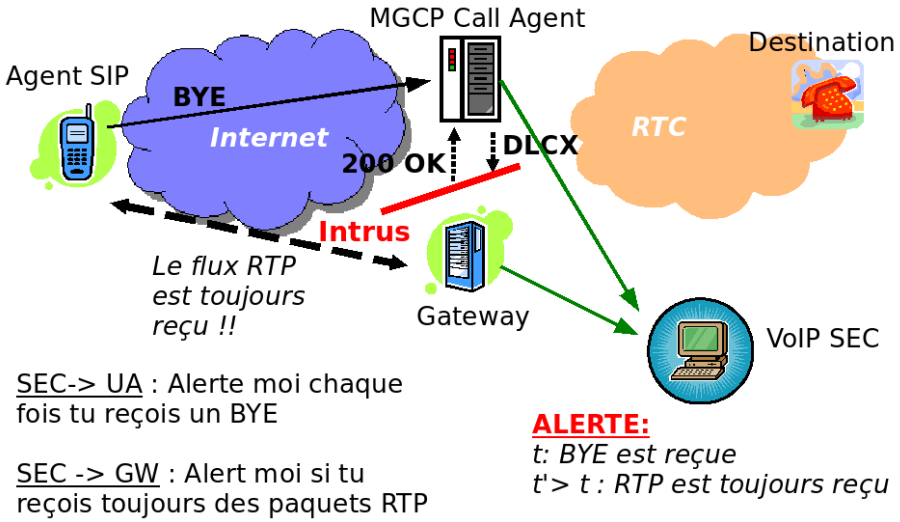

FIG. 2.7 – Une attaque multi-équipements

l'état de système et le comportement des utilisateurs à travers plusieurs sources comme les fichiers de log, les CDRs (Call Detail Record) et les audits. Un IDS basé-réseau peut être installé sur un point d'entrée au réseau pour surveiller le trafic des protocoles comme par exemple le moniteur de trafic déjà proposé. Les capteurs sont gérés et configurés à partir d'une unité centrale de corrélation pour filtrer les événements d'intérêt suivant les priorités et les politiques de cette unité. Un schéma à deux niveaux se forme permettant à l'unité centrale un grand angle de vue et résultant en la détection d'un grand ensemble des attaques distribuées comme illustré dans Figure 2.8. Dans ce cadre, nous proposons

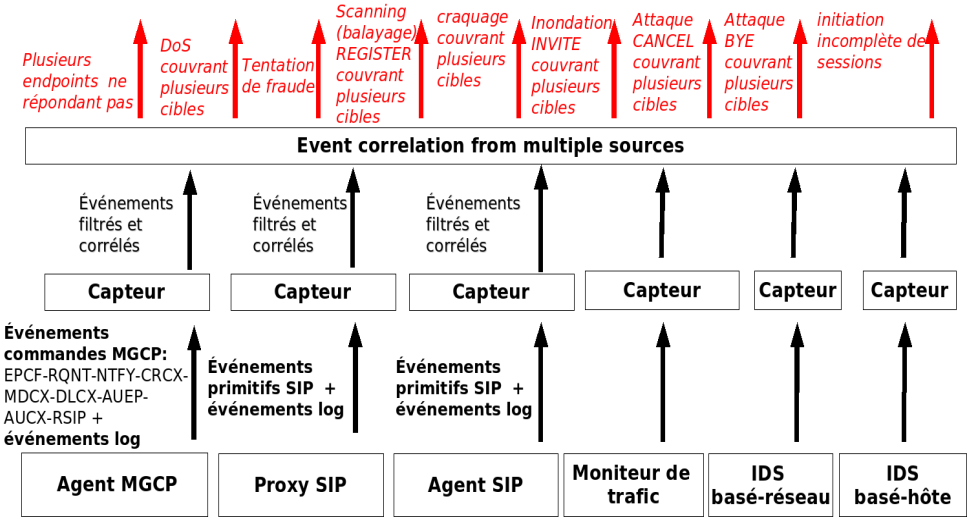

FIG. 2.8 – Corrélation des événements

un IDS basé-réseau et spécifié à SIP pour détecter les signatures des messages malformés. Notre système est dérivé-événement et basé sur des règles d'également des patrons dans une entête de message, un message ou une série des messages. Notre système complémente

des (ou peut constituer un module de vérification dans) des autres travaux comme [26] et [11] mais il introduit une nouvelle notion, celle des attaques à machine d'état (Stateful attacks). Un prototype de ce système est présenté au chapitre suivant basé sur l'outil de corrélation SEC (Simple Event Correlator) et implanté comme un module dans un proxy OpenSER.

2.5 Conclusion

Dans ce chapitre, nous avons discuté les trois contributions majeures de cette thèse : un monitor de trafic SIP basé sur une machine d'apprentissage suivant un modèle de graphes causaux ou un modèle des attributs dans des machines à vecteurs support. Un pot de miel spécifique à SIP pour y entraîner les activités malicieuses dedans à des fins d'analyse et d'investigation. Un cadre de corrélation des événements de sécurité comme une solution globale pour la détection des attaques multi-protocoles, multi-équipements et à machine d'états. Alors que le pot de miel ne peut pas être évalué actuellement tant que les attaques SIP n'ont pas encore envahi l'Internet à un degré remarquable, l'évaluation de nos deux autres solutions est présentée dans le chapitre suivant ainsi que notre outil d'attaque utilisé : le VoIP Bot.

3

Évaluation

Sommaire

3.1 Introduction

Dans ce chapitre, nous évaluons nos solutions de monitorage de trafic SIP, de détection d'intrusion et de corrélation des événements. A cet égard, nous commençons par présenter notre agent SIP programmable appelé VoIP/IRC bot. Ensuite, nous décrivons la série d' expérimentations que nous avons réalisées sur des traces de trafic SIP pour évaluer notre modèle basé sur l'apprentissage et la prédiction. Une comparaison entre les deux modèles proposés en termes de performances a également été effectuée. Enfin, Nous présentons l'implantation d'un système de détection d'intrusion réseau qui détecte les signatures des messages SIP malformés, notamment des signatures distribuées sur plusieurs messages et ceci par l'utilisation des règles de corrélation des événements.

3.2 Une plateforme d'attaque : Les robots VoIP

Pour évaluer des solutions de défense, des attaques du monde réel doivent être mises en œuvre ce qui est difficile actuellement dans le cas de la VoIP. Une plateforme comprenant les stratégies des pirates d'aujourd'hui permet de les émuler. Une telle plateforme doit garantir l'anonymat des attaquants, un grand degré d'efficacité et de passage à l'échelle, et d'échapper aux systèmes de défense traditionnels. Les armées de robots contrôlées à distance (IRC, P2P) comme illustrée dans Figure 3.1 permettent cela. Nous avons implanté une preuve de concept d'un robot attaquant les services VoIP et contrôlé par

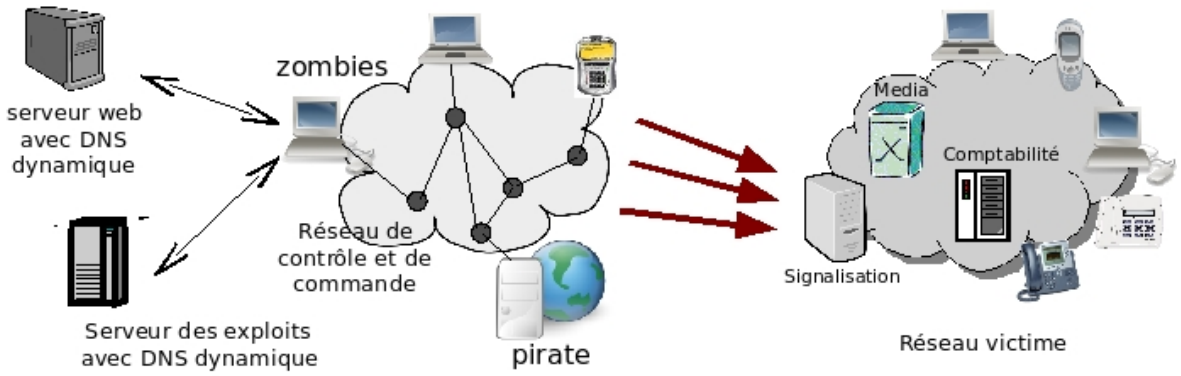

FIG. 3.1 – Une plateforme de robots VoIP

IRC. Le "VoIP Bot" est capable de recevoir ses ordres d'un maître à distance, de trouver plusieurs sortes des données et exploits, et d'effectuer plusieurs attaques en utilisant les protocoles SIP et RTP. Le robot, codé en Java et basé sur les librairies JAIN-SIP, JMF et PIRC BOT ne contient cependant aucune forme de propagation par ver ou virus. Il supporte actuellement les opérations suivantes :

- SPIT : Le robot appelle un URI en argument, et en réponse à un appel passe un fichier audio qu'il retrouve en local (dans la machine compromise) ou à partir d'une URL.
- SCAN : Le robot énumère une liste des utilisateurs qu'il retrouve en local ou à partir d'une URL en utilisant des messages INVITE ou plus discrètement (sans faire sonner les téléphones) des messages OPTIONS.
- CRACK : Le robot essaye de s'authentifier sur un serveur par des messages REGISTER en utilisant une liste de mot de passe qu'il trouve en local ou à partir d'une URL.
- REGISTER : Pour réaliser des fraudes ou des attaques MITM (Man In The Middle) une fois un qu'un mot de passe est craqué.
- DoS : typiquement pour une armée de robots, cette opération permet d'inonder un serveur avec des messages INVITE.
- FingerPrint : Le robot extrait l'empreinte d'un agent VoIP à partir de sa réponse à un message OPTIONS.
- Exploit : Le robot demande un exploit (SIP) spécifique à la cible à partir d'un serveur d'exploit et l'utilise pour réaliser des attaques intelligentes. Un langage de description des signatures des attaques est utilisé entre le robot et le serveur d'exploit.

Cet outil est utilisé dans nos expériences pour générer des attaques et pour émuler des utilisateurs SIP. Il peut être configuré pour émettre et recevoir des appels suivant des profils déterministes ou randomisés.

3.3 Monitorage de trafic SIP : Évaluation des performances

Avec le développement de notre outil d'évaluation, nous disposons de solutions pour évaluer nos approches. Notre système de monitorage de trafic SIP a pour objectif de détecter les manifestations d'attaques dans la signalisation. Nous avons mené des expériences élaborées pour évaluer la précision de la machine d'apprentissage à identifier les attaques et à distinguer entre plusieurs types des attaques. Nous avons comparé entre les deux techniques que nous avons proposées : les réseaux Bayésiens et les machines à vecteurs support. Les données que nous avons utilisées se divisent en deux groupes : des traces de trafic provenant d'un opérateur VoIP du mondé réel que nous avons supposées propres de toute attaque, et des traces d'attaques générées dans un test-bed que nous avons installé en parallèle. Les deux réseaux VoIP (celui du monde réel et celui du banc d'essai) ont la même architecture : les traces sont collectées au niveau d'un proxy (entrée/sortie) OpenSER servant un domaine VoIP. Ainsi, ces traces peuvent être mixées. Nous avons utilisé des traces mixées qui sont des traces "normales" dans lesquelles des traces d'attaque sont injectées. Le test-bed consiste en un serveur OpenSER et trois autres machines : une qui joue le rôle de l'attaquant et est équipée de plusieurs outils de piratage (balayage, inondation, SPIT), et deux autres qui jouent le rôle du réseau victime où 100 agents SIP sont également distribués. Les agents SIP sont des VoIP bots programmés pour s'enregistrer auprès du serveur OpenSER pour recevoir des appels. Nous avons utilisé LibSVM [4] pour réaliser notre modèle de SVM et le Bayes Net Toolbox (BNT) [24] sur Matlab pour implanter notre modèle de réseau Bayésien. Le même schéma de prédiction se répète dans les deux cas : le trafic en entrée est découpé en des petites tranches temporaires. Chaque tranche est analysée pour en évaluer un ensemble d'attributs. Les valeurs des attributs sont entrées sous forme d'un vecteur dans la machine d'apprentissage qui classifie la tranche en question comme suspecte ou non et génère un événement le cas échéant. Nous avons développé notre outil d'analyse en utilisant la libraire Jain SIP [27] sous Java. Les résultats des expériences sur deux types d'attaque (inondation des messages et SPIT) ont permis d'une part d'affiner le réglage des différents paramètres (taille de fenêtre d'analyse, fonction noyau, paramètres de la fonction noyau ...) et ont montré une grande efficacité de détection et des bonnes performances. Cette efficacité doit être soutenue, en cas des attaques furtives, par des règles de corrélation des événements. Nous avons comparé les deux modèles (SVM et BN) en terme de précision de détection : Le modèle Bayésien montre une meilleure capacité pour détecter des variantes de la même attaque (quand elle est entrainée et testée avec deux attaques de même type mais d'intensité différente) et dans la détection d'anomalie en cas où seuls les données "normales" sont disponibles. La SVM montre une meilleure performance lorsque des traces annotées (normale, attaque) sont disponible pour l'entraînement. Les deux machines sont convenables pour un déploiement temps réel. A cette fin, La largeur de la fenêtre d'analyse doit être ajustée en fonction du nombre et de la nature des attributs à évaluer pendant l'analyse. L'étude a aussi montré l'importance d'avoir des algorithmes efficaces de sélection d'attributs. Les attributs sélectionnés sont fortement dépendants de la nature de l'attaque à détecter et du trafic normal de l'arrière-plan.

3.4 Détection des signatures des attaques par SEC (Simple Event Correlator)

Simple Event Correlator ou SEC[2] est un outil libre source, indépendant de la plate-forme au dessous et destiné à la corrélation des événements système. Alors qu'il est déjà connu pour sa commodité à des taches de monitorage d'hôtes et des fichiers de logs, nous avons pris l'initiative de l'utiliser dans le monitorage réseau et l'inspection des paquets SIP. Nous présentons une méthode pour surveiller le trafic SIP passant par un routeur OpenSER comme illustré dans Figure 3.2 . Un moteur SEC utilise des règles statiques,

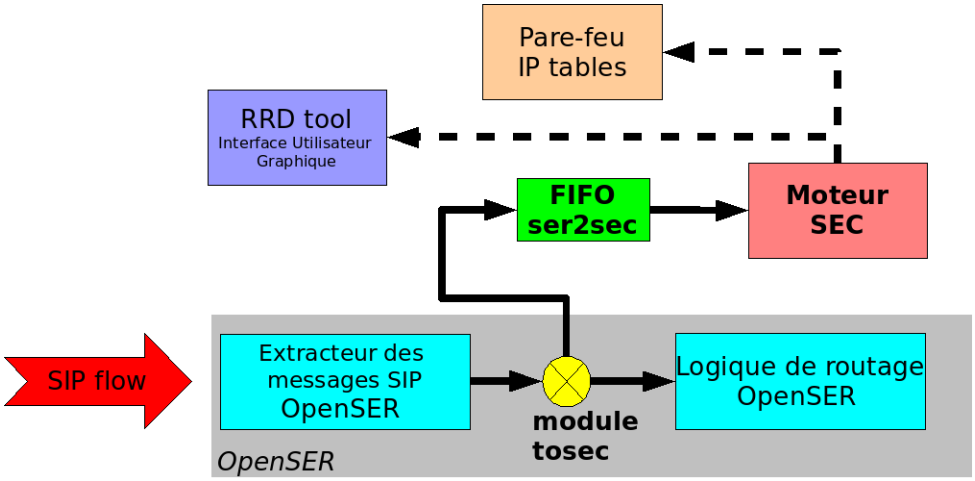

FIG. 3.2 – Diagramme d'un système de détection d'intrusion réseau basé sur SEC et déployé sur OpenSER

accepte des flux de texte (pipes) en entrée et génère des événements en sortie. Il est également capable d'alimenter des fichiers de log et d'exécuter des commandes shell. Chaque règle SEC est constituée par un événement à apparier basé sur une expression régulière PERL, une ou plusieurs listes d'action, et un contexte booléen facultatif qui sert à déclencher la règle lorsqu'il est vrai. Notre moteur SEC est formé par deux composantes en cascade : l'analyseur et le corrélateur. Un module "tosec" est ajouté à OpenSER et sert à dupliquer le message SIP (extrait du paquet arrivant) : un envoyé à la routine de routage OpenSER et l'autre envoyé au moteur SEC. Ce dernier est reçu par l'analyseur qui interprète chacune de ses lignes comme un événement indépendant et l'apparie avec une ou plusieurs expressions régulières. Une règle spéciale détecte la fin du message (une ligne vide) et génère un méta-événement décrivant le message et ses attributs importants vers le corrélateur. A noter que des signatures où une ou plusieurs entêtes sont malformés doivent être détectées au sein du parseur. Le corrélateur est responsable de la détection des signatures qui enjambent plusieurs messages et doit générer des alarmes vers une interface utilisateur graphique (écrite en WXPython[3]). Nous avons utilisé un outil spécial pour mo-

[2] `http://kodu.neti.ee/~risto/sec/`
[3] http ://www.wxpython.org/

déliser le trafic utilisant une base de données Round Robin nommée RRDtool[4]. L'interface de notre outil est affichée à la Figure 3.3. Les alarmes correspondent à une pointe de trafic causé par un afflux de déni de service. L'utilisateur peut solliciter une adresse IP ou un hôte dans l'alarme et l'ajouter à une liste noire. Les éléments de cette liste peuvent être bloqués temporairement ou définitivement en configurant le pare-feu IPtables[5] que nous utilisons. Notre outil constitue un premier prototype de corrélation et il est validé pour

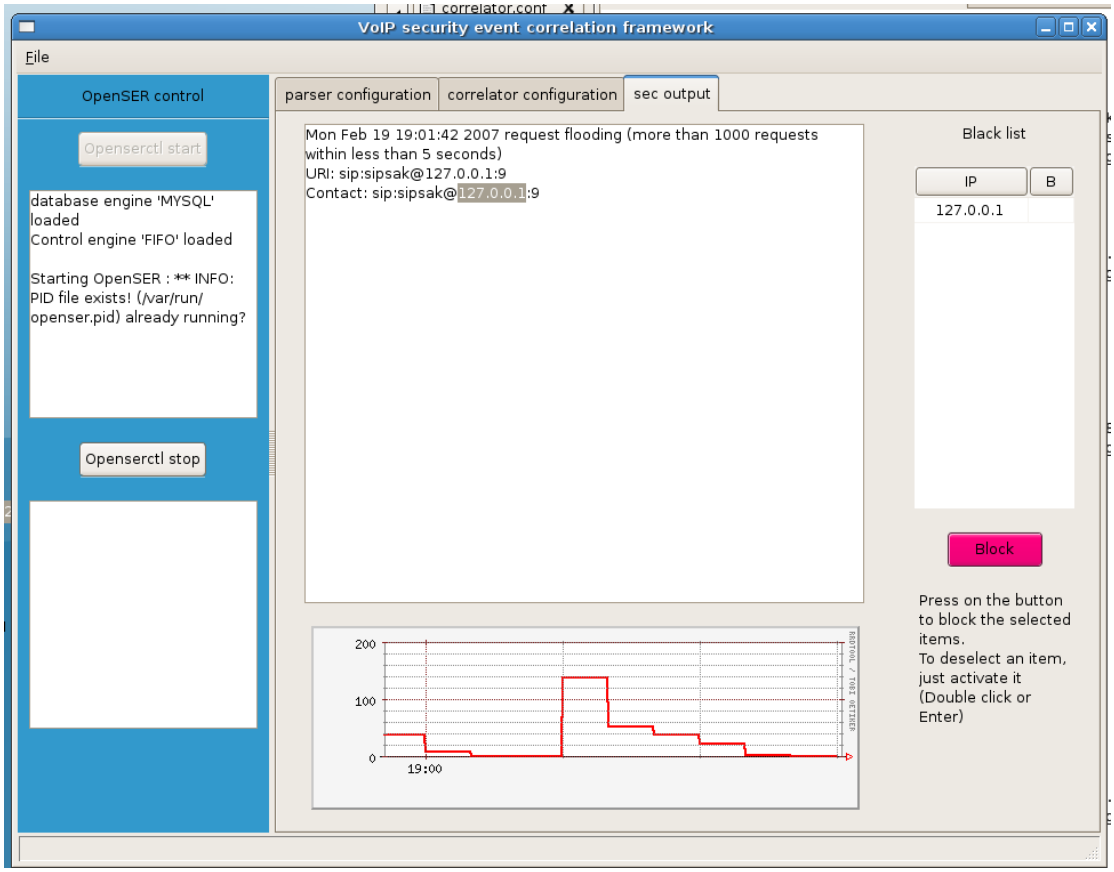

FIG. 3.3 – Détection d'un afflux

détecter plusieurs types des signatures et d'attaques. Cependant, nous avons besoin d'un effort additionnel de développement pour le transformer en un outil commercialisable. La difficulté essentielle liée à l'utilisation de SEC est que les événements internes ne sont pas orientés objet. En d'autres mots ils ne possèdent pas des attributs. En conséquence, nous avons eu recours à des astuces manipulant contextes et règles pour l'adapter à notre but. Ce n'est pas forcement une faiblesse de SEC parce qu'il est initialement conçu comme un outil de gestion système et pas pour la reconnaissance des événements réseaux. D'autre part, SEC remplit les exigences temps-réel imposées par une application comme VoIP. Les règles de corrélation de SEC montrent une grande efficacité pour la corrélation des événements réseau (filtrage des événements, restrictions temporelles). Finalement, nous recommandons d'utiliser les mêmes types de règles que dans SEC mais avec une structure

[4]http ://oss.oetiker.ch/rrdtool
[5]http ://www.netfilter.org/

des événements orientée objet pour construire un outil efficace de filtrage et corrélation SIP.

3.5 Conclusion

Dans ce chapitre, nous avons évalué nos solutions de monitorage et de détection d'intrusion en utilisant notre outil VoIP bot. Le VoIP bot est un agent SIP programmable capable d'exécuter plusieurs types d'attaques ou d'émuler des utilisateurs humains de profils déterministes ou probabilistes. Les expérimentations ont montré une grande efficacité de notre système de monitorage pour détecter les anomalies de signalisation à court (inondation) et à long termes (SPIT) en se basant sur une machine d'apprentissage. Notre prototype de détection des messages malformés constitue la base d'un système de détection d'intrusion basé-réseau. Le modèle de corrélation des événements que nous proposons peut être généralisé pour protéger un domaine VoIP des attaques notamment celles dont la signature enjambe plusieurs entités-réseaux ou plusieurs protocoles.

Conclusion générale

Avec la croissance continue des attaques contre la VoIP, des mécanismes de monitorage et de gestion de sécurité deviennent de plus en plus une nécessité. Dans le cadre de cette problématique, nous avons cherché les pièces manquantes dans les plans de défense actuels. Tout en accentuant la spécificité de l'application visée d'une part, et sa sensibilité financière et confidentielle d'autre part, cette thèse est tout à fait complémentaire aux efforts poursuivies aujourd'hui dans la communauté recherche et dans l'industrie. Dans le premier chapitre, nous avons introduit les protocoles VoIP et souligné leur aspect distribué et hétérogène. Nous avons justifié les besoins de ces protocoles en matière de sécurité par un bref aperçu des menaces les plus pertinentes. Enfin, nous avons présenté les travaux les plus récents portant sur la sécurité et la détection d'intrusion de cette nouvelle technologie. Les contributions sont synthétisées dans le deuxième chapitre. Nous avons proposé des solutions interconnectées qui comblent le manque en matière de monitorage de trafic, de défense préventive et de corrélation des évènements. En effet :

- nous avons proposé un système de monitorage de trafic de signalisation (SIP) se basant sur la théorie de l'apprentissage. L'idée de base est de découper le trafic en de petits morceaux ou créneaux et d'en extraire des valeurs pour des variables statistiques prédéfinies ou attributs. Pour chaque créneau, les valeurs de ces attributs sont regroupées dans un vecteur qui sera donné à la machine d'apprentissage pour le classifier comme normal ou suspects. Des règles de corrélation sont ainsi appliquées pour inférer une conclusion sur le trafic en cours. Nous avons utilisé deux approches différentes : les réseaux Bayésiens et les machine à vecteurs support et nous avons comparé leurs performances.
- Nous avons présenté une approche innovante pour désigner un pot de miel spécifique à la VoIP. Le pot de miel est muni d'une interface applicative qui lui permet de gérer un grand nombre des outils réseau. En plus de recevoir et enregistrer les attaques, le pot de miel est capable de mener une enquête en temps réel sur les messages reçus. Un composant important dans son architecture est un moteur d'inférence qui peut juger si un message reçu est une faute de routage ou énumération, s'il s'agit d'un message malformé lancé pour exploiter une certaine vulnérabilité, ou s'il s'agit d'un appel qui semble être correct mais qui n'est pas digne de confiance. Des évaluations des exemples simulés montrent l'efficacité de notre procédure d'enquête et l'exactitude des décisions prises par le moteur d'inférence.
- Nous avons présenté une approche distribuée à multi-niveaux pour la corrélation des événements de sécurité dans un domaine VoIP. Notre approche est basée sur des systèmes de détection d'intrusion basé-hôte et basé-réseau ainsi que sur les autres

composants de défense (pot de miel, moniteur de trafic).

Dans le troisième chapitre, nous avons évalué nos contributions par des résultats expérimentaux en utilisant notre outil le robot VoIP. Ce robot est un agent basé sur les protocoles SIP/RTP/IRC qui peut être utilisé pour l'évaluation de la sécurité des plates-formes VoIP, et pour l'émulation des utilisateurs (bons ou malicieux). Ce robot ouvre la discussion sur des futurs maliciels et armées de robots utilisant les vulnérabilités Internet pour attaquer la VoIP et vice versa. Nous avons expérimenté notre approche de monitorage à l'aide des traces réseaux d'un fournisseur de service VoIP et des traces d'attaques générées dans notre banc d'essai et inséré dans les traces "normales". Nous avons comparé les performances de deux techniques utilisées (Réseaux Bayésiens et SVM) pour détecter un ensemble des attaques à court-terme et à long-terme. Les résultats ont montré une grande capacité pour un déploiement temps-réel et une grande précision de détection des attaques DoS d'inondation et du SPIT. Les réseaux Bayésiens se montrent plus performants en détectant des variantes d'une même attaque et dans la détection d'anomalies (lorsque seules des données de trafic normal sont disponibles pour apprentissage) alors que les SVM sont plus précises quand des données labélisées comme normal ou attaque sont disponibles pour apprentissage. Finalement, nous avons montré les capacités de SEC comme outil de corrélation pour construire un système de détection d'intrusion VoIP dont nous avons montré la faisabilité en développant un prototype. Plusieurs directions sont intéressantes et importantes pour le futur :

- Dans le système de monitorage : d'autres filtres et algorithmes de sélection peuvent être considérés pour redéfinir et ordonner notre ensemble des attributs. Les règles de corrélation et de filtrage des événements doivent être étudiées profondément dans le but de détecter les attaques et à un niveau plus haut révéler la stratégie des attaquants et d'améliorer la réponse de prévention.
- Les techniques d'apprentissage non supervisé sont attirantes parce qu'elles ne demandent pas une connaissance à priori du trafic et qu'elles peuvent détecter des attaques nouvelles et inconnues auparavant. Ces techniques devront être étudiées dans le contexte du monitorage VoIP.
- Un pot de miel seul a un champ de vue limité et ne peut détecter qu'un ensemble limité des attaques. Un réseau de pots de miel (honeynet) muni d'une grande interactivité peut attirer beaucoup plus d'attaques dans un environnement sécurisé et supervisé en offrant un ensemble riche de services. Un honeynet VoIP devra être conçu et implanté pour émuler tout un réseau VoIP (utilisateurs, infrastructure et services).
- Finalement, notre IDS peut être amélioré en utilisant les mêmes types de règles que SEC mais avec une structure événementielle améliorée. Notre travail sur les signatures d'attaques est un premier pas que nous espérons être suivi par d'autres efforts. Un langage standard pour la description des signatures des attaques (même distribuées) va faciliter l'incorporation de ces signatures dans les pare-feu, ALG et IDS dédiés-VoIP.

Bibliographie

[1] V. A. Balasubramaniyan, M. Ahamad, and H. Park. CallRank : Combating SPIT using call duration, social networks and global reputation. In *Fourth Conference on Email and Anti-Spam (CEAS2007)*, Mountain View, California USA, 2007.

[2] D. Barbará, N. Wu, and S. Jajodia. Detecting novel network intrusions using Bayes estimators. In *Proceedings of the First SIAM Conference on Data Mining*, April 2001.

[3] N. Bonelli, S. Giordano, G. Procissi, and R. Secchi. BRUTE : A high performance and extensible traffic generator. In *Proceedings of International Symposium on Performance and Extensible Traffic Generator (SPECTS'05)*, PA, USA, July 2005.

[4] C. Chang and C. Lin. *LIBSVM : a library for support vector machines*, 2001. Software available at `http://www.csie.ntu.edu.tw/~cjlin/libsvm`.

[5] E. Y. Chen. Detecting DoS attacks on SIP systems. In *Proceedings of 1st IEEE Workshop on VoIP Management and Security*, pages 53–58, San Diego, CA, USA, apr 2006.

[6] T. Dierks and C. Allen. RFC2246 : The TLS protocol version 1.0, 1999.

[7] Y. Ding and G. Su. Intrusion detection system for signal based SIP attacks through timed HCPN. In *Proceedings of the Second International Conference on Availability, Reliability and Security (ARES'07)*. IEEE Computer Society, 2007.

[8] S. Ehlert, C. Wang, T. Magedanz, and D. Sisalem. Specification-based denial-of-service detection for SIP Voice-over-IP networks. In *The Third International Conference on Internet Monitoring and Protection (ICIMP)*, pages 59–66, Los Alamitos, CA, USA, 2008. IEEE Computer Society.

[9] D. Endler and M. Collier. *Hacking Exposed VoIP : Voice Over IP Security Secrets and Solutions*. McGraw-Hill Professional Publishing, 2007.

[10] D. Geneiatakis, G. Kambourakis, T. Dagiuklas, C. Lambrinoudakis, and S. Gritzalis. SIP security mechanisms : A state-of-the-art review. In *Proceedings of the Fifth International Network Conference (INC 2005)*, pages 147–155, Samos, Greece, July 2005.

[11] D. Geneiatakis, G. Kambourakis, C. Lambrinoudakis, T. Dagiuklas, and S. Gritzalis. A framework for protecting a SIP-based infrastructure against malformed message attacks. *Comput. Netw.*, 51(10) :2580–2593, 2007.

[12] I. Guyon, J. Weston, S. Barnhill, and V. Vapnik. Gene selection for cancer classification using support vector machines. *Mach. Learn.*, 46(1-3) :389–422, 2002.

[13] ITU Recommendation H.323. Packet-based multimedia communications systems, 2000.

[14] The honeynet project. *Know Your Enemy : Learning about Security Threats (2nd Edition)*. Pearson Education, 2004.

[15] H. Javitz and A. Valdes. The SRI IDES statistical anomaly detector. In *Proceedings of the IEEE Computer Society Symposium on Research in Security and Privacy*, pages 316–326. IEEE computer society, May 1991.

[16] H. Kang, Z. Zhang, S. Ranjan, and A. Nucci. SIP-based VoIP traffic behavior profiling and its applications. In *Proceedings of the 3rd annual ACM workshop on Mining network data (MineNet '07)*, pages 39–44, New York, NY, USA, 2007. ACM.

[17] S. Kent and R. Atkinson. RFC2401 : Security architecture for the Internet protocol, 1998.

[18] P. Kolan and R. Dantu. Socio-technical defense against voice spamming. *ACM Trans. Auton. Adapt. Syst.*, 2(1) :Article 2, 2007.

[19] C. Kruegel, D. Mutz, W. Robertson, and F. Valeur. Bayesian event classification for intrusion detection. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC '03)*, page 14, Washington, DC, USA, 2003. IEEE Computer Society.

[20] D. Richard Kuhn, Thomas J. Walsh, and S. Fries. Security considerations for Voice over IP systems. National Institute of Standards and Technology (NIST), Special Publication, 800-58, January 2005.

[21] Kunlun Li and Guifa Teng. Unsupervised SVM based on p-kernels for anomaly detection. In *Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC '06)*, pages 59–62, Washington, DC, USA, 2006. IEEE Computer Society.

[22] M. Luo, T. Peng, and C. Leckie. CPU-based DoS attacks against SIP servers. In *IEEE/IFIP Network Operations and Management Symposium (NOMS 2008)*. IEEE, April 2008.

[23] S. Mukkamala, G. Janoski, and A. Sung. Intrusion detection : Support vector machines and neural networks. *The IEEE Computer Society Student Magazine*, 10(2), 2002.

[24] K. P. Murphy. The Bayes Net Toolbox for MATLAB. *Computing Science and Statistics*, 33 :1–20, 2001.

[25] P. Naïm, P. Wuillemin, P. Leray, O. Pourret, and A. Becker. *Réseaux Bayésiens*. Eyrolles, 2004.

[26] S. Niccolini, R.G. Garroppo, S. Giordano, G. Risi, and S. Ventura. SIP intrusion detection and prevention : recommendations and prototype implementation. In *VoIP Management and Security, 2006. 1st IEEE Workshop on*, pages 47–52, April 2006.

[27] P. O'Doherty and M. Ranganathan. JAIN SIP Tutorial : Serving the developer community. `http://www-x.antd.nist.gov/proj/iptel/tutorial/JAIN-SIP-Tutorialv2.pdf`.

[28] J. Pearl. *Probabilistic Reasoning in Intelligent Systems : Networks of Plausible Inference*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 1988.

[29] J. Peterson and C. Jennings. RFC4774 : Enhancements for authenticated identity management in the Session Initiation Protocol (SIP), 2006.

[30] F. Pouget and M. Dacier. Honeypot-based forensics. In *Asia pacific information technology security conference (AusCERT '04)*, May 2004.

[31] J. Quittek, S. Niccolini, S. Tartarelli, M. Stiemerling, M. Brunner, and T. Ewald. Detecting SPIT calls by checking human communication patterns. In *IEEE International Conference on Communications (ICC 2007)*, Jun 2007.

[32] B. Ramsdell. RFC2633 : S/MIME version 3 message specification, 1999.

[33] J. Ransome and J. Rittinghouse. *Voice over Internet Protocol (VoIP) Security*. Digital Press, Newton, MA, USA, 2004.

[34] B. Reynolds and D. Ghosal. Secure IP telephony using multi-layered protection. In *Proceedings of The 10th Annual Network and Distributed System Security Symposium*, San Diego, CA, USA, feb 2003.

[35] K. Rieck, S. Wahl, P. Laskov, P. Domschitz, and K.-R. Müller. A self-learning system for detection of anomalous SIP messages. In *Principles, Systems and Applications of IP Telecommunications (IPTCOMM), Second International Conference*, Jul 2008.

[36] R. Romano, C. Aragon, and C. Ding. Supernova recognition using support vector machines. In *Proceedings of the 5th International Conference on Machine Learning and Applications (ICMLA '06)*, pages 77–82, Washington, DC, USA, 2006. IEEE Computer Society.

[37] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC3261 : SIP : Session initiation protocol, 2002.

[38] R. Schlegel, S. Niccolini, S. Tartarelli, and M. Brunner. SPam over Internet Telephony (SPIT) prevention framework. In *GLOBECOM*, 2006.

[39] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson. RFC3550 : RTP : A Transport Protocol for Real-time applications, 2003.

[40] H. Sengar, R. Dantu, and D. Wijesekera. Securing VoIP and PSTN from integrated signaling network vulnerabilities. In *1st IEEE workshop on VoIP Management and Security (VoIP MaSe)*, Vancouver, Canada, April 2006.

[41] H. Sengar, D. Wijesekera, H. Wang, and S. Jajodia. VoIP intrusion detection through interacting protocol state machines. In *Proceedings of the 38th IEEE International Conference on Dependable Systems and Networks (DSN'2006)*. IEEE Computer Society, 2006.

[42] D. Shin and C. Shim. Progressive multi gray-leveling : A voice Spam protection algorithm. *IEEE Network*, 20(5) :18–24, Sep/Oct 2006.

[43] P. Truong, D. Nieh, and M. Moh. Specification-based intrusion detection for H.323-based Voice over IP. In *Proccedings of the IEEE International Symposium on Signal Processing and Information Technology*. IEEE Computer Society, 2005.

[44] A. Valdes and K. Skinner. Adaptive, model-based monitoring for cyber attack detection. In *Proceedings of the Third International Workshop on Recent Advances in Intrusion Detection (RAID '00)*, pages 80–92, London, UK, 2000. Springer-Verlag.

[45] V. Vapnik. *The nature of statistical learning theory.* Springer-Verlag New York, Inc., New York, NY, USA, 1995.

[46] V. Vapnik. *Statistical Learning Theory.* John Wiley and Sons, New York, 1998.

[47] VoIPSA. VoIP security and privacy threat taxonomy. Public Realease 1.0, Oct 2005. `http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf`.

[48] T. J. Walsh and R. Kuhn. Challenges in securing Voice over IP. *IEEE Security and Privacy*, 3(3) :44–49, 2005.

[49] Y. Wu, S. Bagchi, S. Garg, N. Singh, and T. K. Tsai. SCIDIVE : A stateful and cross protocol intrusion detection architecture for Voice-over-IP environments. In *International Conference on Dependable Systems and Networks (DSN 2004)*, pages 433–442. IEEE Computer Society, Jun 2004.

[50] H. Yan, K. Sripanidkulchai, H. Zhang, Z.-Y. Shae, and D. Saha. Incorporating active fingerprinting into SPIT prevention systems. In *Third annual security workshop (VSW'06)*. ACM Press, Jun 2006.

[51] G. Zhang, S. Ehlert, T. Magedanz, and D. Sisalem. Denial of service attack and prevention on SIP VoIP infrastructures using DNS flooding. In *Proceedings of the 1st international conference on Principles, systems and applications of IP telecommunications (IPTComm '07)*, pages 57–66, New York, NY, USA, 2007. ACM.

Résumé

La Voix sur IP (VoIP) est devenue un paradigme majeur pour fournir des services de télécommunications flexibles tout en réduisant les coûts opérationnels. Le déploiement à large échelle de la VoIP est soutenu par l'accès haut débit à l'Internet et par la standardisation des protocoles dédiés. Cependant, la VoIP doit également faire face à plusieurs risques comprenant des vulnérabilités héritées de la couche IP auxquelles s'ajoutent des vulnérabilités spécifiques. Notre objectif est de concevoir, implanter et valider de nouveaux modèles et architectures pour assurer une défense préventive, permettre le monitorage et la détection d'intrusion dans les réseaux VoIP. Notre travail combine deux domaines : celui de la sécurité des réseaux et celui de l'intelligence artificielle. Nous renforçons les mécanismes de sécurité existants en apportant des contributions sur trois axes : Une approche basée sur des mécanismes d'apprentissage pour le monitorage de trafic de signalisation VoIP, un pot de miel spécifique, et un modèle de corrélation des événements pour la détection d'intrusion. Pour l'évaluation de nos solutions, nous avons développés des agents VoIP distribués et gérés par une entité centrale. Nous avons développé un outil d'analyse des traces réseaux de la signalisation que nous avons utilisé pour expérimenter avec des traces de monde réel. Enfin, nous avons implanté un prototype de détection d'intrusion basé sur des règles de corrélation des événements.

Mots-clés: Voix sur IP, Session Initiation Protocol (SIP), Corrélation des événements, Détection d'intrusion, Pot de miel, Réseaux Bayésiens, Machines à vecteurs de support (SVM), Réseau zombie.

Abstract

Voice over IP (VoIP) has become a major paradigm for providing flexible telecommunication services and reducing operational costs. The large-scale deployment of VoIP has been leveraged by the high-speed broadband access to the Internet and the standardization of dedicated protocols. However, VoIP faces multiple security issues including vulnerabilities inherited from the IP layer as well as specific ones. Our objective is to design, implement and validate new models and architectures for performing proactive defense, monitoring and intrusion detection in VoIP networks. Our work combines two domains : network security and artificial intelligence. We reinforce existent security mechanisms by working on three axes : a machine learning approach for VoIP signaling traffic monitoring, a VoIP specific honeypot and a security event correlation model for intrusion detection. In order to experiment our solutions, we have developed VoIP agents which are distributed and managed by a central entity. We have developed an analyzer of signaling network traces and we used it to analyze real-world traces. Finally, we have implemented a prototype of a rule-based event-driven intrusion detection system.

Keywords: Voice over IP, Session Initiation Protocol (SIP), Event correlation, Intrusion detection, Honeypot, Bayesian networks, Support vector machines(SVM), Botnet.