Réf : 2007/II3/18E Sessionde septembre2008

Université de la Manouba

École Nationale des Sciences de L'Informatique

RAPPORT
de Mémoire deFin D'Études

Présenté en vue de l'obtention du titre d'INGÉNIEUR EN INFORMATIQUE

Par
Bilel MOHAMED

Sujet:

Prototypage d'un IDS/IPS pour la sécurité des réseaux et services VoIP

Resp onsable : Mr. Patrick BATTISTELLO
Sup erviseur: Pr. Ab delfatteh BELGHITH
Encadrants: Mr. PatrickBATTISTELLO
Mr. Stéphane TUFFIN
Organisme: FRANCE TELECOMR&D
Adresse: 2 AvenuedePièrre Marzin,Lannion22300 FRANCE
Tel: (+33) 029605 1111 Fax: (+33)02 960511 11

Signatures des encadrants

Mr. Patrick BATTISTELLO
Resp onsable de stage et ingénieur à France Télécom

Pr.Ab delfatteh BELGHITH
Sup erviseur de stage et professeur à l'ENSI

Dédicace

Je dédie ce travail

À mon pays, la Tunisie

Àmon père Mohamed

Àma mère Khamissa

À mes soeurs Assia, Takoua, Amira et Manar

À mes amis Marwen, Amin, Wafa ...

Àmes enseignants

Àceux qui m'ont supportés

Je dédie ce travail. .. Bilel

Remerciements

C'est avec plaisir que nous réservonsces quelques lignes ensigne de gratitude et de profonde reconnais sance à tous ceux qui, de prés ou de loin, ont contribué à l'aboutissement de ce travai l.

Nous tenons tout d'abord àremercier Monsieur Patrick BATTISTELLO, responsable de notre stage, pour sa disponibilité, ses critiques et ses conseils judicieux qu'il n'a cessé de nous prodi guer tout au cours de ce projet.

Nous remercions Monsieur Abdelfatteh BELGHITH, Professeur à l'ENSI et enseignant responsable de notre st age, pour la conance qu'il nous a accordée et pour son encadrement.

Nous remercions particulièrement Monsieur Marc CLAQ UIN et Monsieur Stéphane TUFFIN, qui n'ont ménagé aucun eort pournousencadrer d'aussi bonne grâce tout en prodi guant leurs précieux conseils.

Que tout les membres de l'équipe CORE M2V de France Télécom R&D trouvent ici l'expression de nos gratitudes pour leur sympathie et pour avoir facilité mon intégration au seinde l'équipe.

Nous tenons à exprimer l'honneur que nous font les membres du jury pour avoir accepté de nous prêt er leur attention et d'évaluer notre travail.

Merci aux personnes anonymes qui consacrent leur temps pour mettre sur Internet des documents contribuant àla diusion des connaissances.

Merci

Table des matières

Liste des gures

Intro duction générale

De nos jours, la voix sur IP occup e une place privilégiée dans le monde des télécommunications. L'avantage inc ontesté de cette technologie est sa p ossibilité d'intégrer la voix et les donnéessur une même infrastructure Internet déjà existante. Grâce à cette technolog ie,les coûts des communi cations interurbainesont chutéde manière considérable ce qui laisse p enser qu'el lea encore de beaux jours devant elle. Or, avec l'augmentation du nombre des clients et du niveau d'interconnexion entre op érateurs,il est prévisible que les réseaux VoIP[1] soient soumis dans un futur pro che à des actes ou tentatives de vandalisme te ls que: accès gratuit ou usurpation d'identi té, envoi de messages p olluants, tentatives de mise hors service de terminaux tiers ou d'équip ements réseau dans un but de dégradation de l'image de marque de l'op érateur. La mise en place d'une p olitique de sécurité autour de ces systèmes est doncprimordiale.
Outrela mise enplace de pare-feux etde systèmes d'authenticationde plus en plus sécurisés,il est nécessaire,p our compléte r cette p olitique de sécurité, d'avoir des outils de surveillance pour auditer le système d'information et détecter d'éventuelles intrusions: ce que nous app elons intrusion signie pénétration des systèmes d'information mais aussi tentatives des utilisateurs d'accéder à de plus hauts privilèges que ce ux qui leur sont attribués, ou tentativesdesadministrateurs d'abuserde leurs privilèges.

Dans ce même contexte se situe le prése nt travail, dont le but est de prototyp er un système de détection/prévention d'intrusion évolué destiné à la VoIP, basé sur les vulnérabilités du proto cole de signalisation SIP[2].

Ce rapp ort comprend six chapitres: dans le premier chapitre, nous présentons le cadre de notre pro jet, le deuxième chapitre concerne le protocole d'initiation de session SIP où on décrira de manière brève ce proto cole et la signilisation des app els.

[1] Voice over Internet Proto col
[2] Session Initiation Proto col

Le troisième chapi tre est consacré aux systè mes de détection/prévention d'intrusion. Dans ce chapitre, nous donnons un p etit ap erçu sur les principe de fonctionnement de cessystèmesde sécurité.
Le quatrième chapitre est consacré à l'analyse et la sp écication fonctionnelle du pro cédé.Nous allons prése nter les diérents b esoins du systèmeet détailler les diérents diagrammes qui nous permetteront de mieux comprendre lanalité de ce travail.
Dans le cinquième chapitre nous présentons la conception de l'application, lesprincipales classes et tablesdela bases de données qui constituentnotre programme.
Le sixième chapitre est dédié à la réalisation du pro jet, nous allons décrire l'environnement de travail, nous donnons égal ement des captures d'écran de l'execution de programme, nous exp osons les tests réalisés, et enn nous décrivons le chronogramme de réalisation du pro jet ainsi que les app orts de stage.
Nous nirons ce rapp ort par une conclusion générale, des commentaires et suggestions sur cetravail, labibliographie etlapartie annexes.

Chapitre1

Présentation du pro jet

Intro duction

Nous présentons dans ce chapitre le cadre de notre pro jet : nous décrivons brièvement la problématique de travail demandé ainsi que les principaux ob jec tifs.Par la suite, nous intro duisons une présentation de l'organisme d'accueil.

1.1 Cadre du projet

Au cours de la formation d'ingénieurs à l'Ecole Nationale des Sciences de l'Informatique, les élèves ingénieurs sont amenés à eectuer un Pro jet de Fin d'Etude. C'est dans ce cadre que nous avons réalisé ce travail, danslebut de l'obtention du diplôme d'ingénieur en informatique. Ce pro jet s'est déroulé au sein de France Téléc om R&D site de Lannion,durant la pério de du 31 Mars au 29 Août 2008

1.2 Problématique

Les équip ements IDS/IPS actuels incorp orent un nombre limité de fonctions pour la VoIP et restent relativement permissifs face à des attaques avérées.De plus, ces systèmes sont peu évolutifsç'est-à-dire qu'ils appliquent systématiquement les mêmes contrôl es à chaque paquet, avec des notions de contexte assez rudimentaires, et peu de sp écicités VoIP.

1.3 Ob jectifs

L'ob je ctifdu stage est de prototyp er un IDS/IPS évolué p our la VoIP, c'est-à-dire capable d'analyser nement des paquets potentiellement malicieux, sanscompromettresa résistance à la charge. De plus, ce t IDS/IPS doit tenir compte des contextes relatifs aux entités sup ervisées et être évolutif, c'est-à-dire pouvoir recevoir de nouvelles règles de détection. Le travail de prototypage s'appuiera sur une sp écication FTR&D décrivant les fonctionnalités debase del'IDS/IPS. Les étap es à réaliser dans le stage sont la dénition de l'architecture logicielle du système, des comp osants élémentaires de l'IDS/IPS, et la réalisation d'une maquette pour prouver la validité du concept.

1.4 Présentationde l'entreprise

France Télécom, qui emploieprès de191.000 salariéset compte quelques 159 millions de clients dansle monde, est la principale entreprise française de télécommunications.Elle dévelopg e trois grandes familles de services commercialisés sous la marque Orange : des services de téléphonie xe, des services de téléphonie mobile et desservicesde communicationd'entreprise,via Orange Business Services.
Bien que France Télécom soitnée ociellementle 1er janvier 1991, son histoire remonte à plus de deux siècles. C'est en 1792 que le premier ré se au de communication français, le réseau de télégraphie optique de Chapp e, a vu le jour. Avec l'invention du Télégraphe électrique et du téléphone, un ministère des Postes et Télégraphes est nalement créé en 1878. Il annexe les services du Téléphone et le ministèredesPTdevientcelui des PTT en 1923. En 1941, une Direction Général e des Télécommunications ou DGT est créée au sein de ce ministère.En 1988, la DGT se sé pare des PTT et prend le nom de "France Télécom". Il faut toutef ois attendre le 1er janvier 1991 p our que France Télécomdevienne unexploitant autonome dedroitpublic.
En 1997, l' entreprise ouvre son capital et est cotée sur les marchés b oursiers de Paris et New York.
En 2000, elle fait l'acquisition de l'op érateur mobile britannique Orange, au prix de 40 milliards d' euros, p our en faire une liale nommée Orange SA. Elle constitue alors le deuxième réseau mobile europ éen.De nombreusesautres acquisitions de so ciétés luip ermettent de devenir le quatrièm e plus grand op érateur mondial.
En septembre 2004,l'Etat français cède une partiede ses actions et France Télécom de vient une entreprise privée.

En 2006, la plupart des activités du group e passent sous la marque et le logo Orange. C'est le ca s des services Internet, de Télévision et de téléphonie mobile ai nsi que des se rvices numériques.
Aujourd'hui, France Télécom continue d'é largir ses activités p our orir une gammecomplètede prestations dans l'audiovisuel et lemultimédia, ainsi que de nouveaux pro duits et services : vente de contenus (musique, cinéma, télé-chargement),E commerc e et publicité en ligne,domotique et téléassistance aux malades.
Le group e compte 49 millions de clients en téléphonie xe, 12 millions en Internet ha ut débit et 9 8 millions de clients en téléphonie et multimédia mobiles.

Conclusion

Ainsi, nous avons présenté le cadre de notre pro jetDans la suite, nous nous intéresserons à l'etude théorique présentant les diérentes appro ches relatives à l'application.

Chapitre2

Le Proto cole SIP

Intro duction

De nombreuses applicati ons de l'Internet demandent la création et la gestion d'une session,oùune sessionestconsidérée comme unéchangede données entre une asso ciation de participants : les usagers p euvent se déplacer entre les points d'extrémité, ils peuvent être désignés par plusieurs noms, et ils p euvent communiquer sur plusieurs supp orts diérents.De nombre ux proto coles ont été rédigés qui p ortent diverses formes de données de session multimédia en temps réel. Le Proto cole SIP travaille de concert avec des protocoles en permettant aux points de terminaison Internet (app elés agents utilisateurs) de se découvrir et de se mettre d'accord sur une caractéri sation d'unesession qu'ilsaimeraient partager.

2.1 Informations sur le protocole SIP

SIP a été normalisé par le group e de travail WG MMUSIC[1] de l' IETF[2]. La première version est sortie en 1997, et une seconde version ma jeure a été prop osée en mars 1999(RFC 2543). Cettedernièrea elle-mêmeététélargement revue, complétéeet corrigée en Juin 2002(RFC 3261).Des compléments au proto cole ont été dénis dans des nombreux RFC, en particulier les RFC 3262 et 3265.
SIP est au sens propre un proto cole de signalisation hors bande pour l'établissement, le maintien, la mo dication, la gestion et la fermeture de sessions interactives entre utilisateurs pour la téléphonie et la vidéo conférence, et plus

[1] Work Group Multiparty Multimedia Session Control
[2] Internet Engineering Task Force
[3] Request For Comment

généralement p our toutes les co mmunications multimédias.
Le proto cole n'assure pas le transport des données utiles, mais a pour fonction d'établir la liaison entre les interlo cuteurs. Autrement dit, il ne véhicule pas la voix, ni la vidéo, maisassure toutsimplement la signalisation. Il se situe au niveau de la couche applicative du mo dèle de référence OSI et fonctionne selon une archite cture clie nt-serveur, le client émettant des requêtes et le serveur exécutant en rép onse les actions sollicitées par le client.
SIP fournit des fonctions annexes évoluées, comme la redirection d'app el, la modication des parammètres asso ciés à la session en cours ou l'invo cation de services. Enfait, SIPne fournit pas l'implémentation desservices, mais propose des primitives génériques p ermettant de les utiliser. De cette m ani ère, l'implémentation des service s est laissée libre, et seul le moyen d'accéder au service est fournit [Oua08].

2.1.1 Capacités du protocole SIP

SIP a les capacités sui vantes:

- Lo calise l'extrimité cible: SIP supp orte la résolution d'adresses et la redirection d'app els.
- Détermine les capacités mé dia de l'extrémité cible: SIP détermine le niveau de service communle plus basentre les deux extrémités au travers de SDP[4]. Les conférences sont établies en utilisant le s capacités média qui peuvent être supp ortées par les deux extrémités.
- Détermine la disp onibilité de l'extrémité : si un app el ne p eut pas ab outir car l'extrémité cible est indisp onible, SIP détermine si l'e xtré mité app elée est déjà connectée avec un app el en cours ou ne rép ond pas après le nombre de sonneries paramétré.
- Etablit une session entre les extrémités origine et cible : si l'app el p eut ab outir, SIP établit une session entre les extrémités. SIP supp orte également les mo dications en cours de communication, telles que l'addition d'une autre extrémité à la conférence, le changement de ca rac téristiques de média ou de co dec.
- Gère le transfert et la n de communication : SIP supp orte le transfert d'app els d'une extrémité vers une autre. Pendant le transfert d'app els, SIP établit une session entre le transféré et la nouvelle extrémité (sp éciée parlapartie transférante) et terminela session entre le transféré et la partietransférante. Alan del'échange SIP ferme lessessions entre toutes le s parties.

[4] Session Description Proto col

2.1.2 Composants SIP

Les extrémités dans une session sont app elées agents utilisateurs.Un agent utilisateur peut avoir un des rôles suivants:

- UAC[5] :une applicationclientequi initieunerequête SIP.
- UAS[6] : une application serveur qui contacte l'utilisateur quand une requête SI P est reçue et qui retourne une rép onse à la demande de l'utilisateur.

Typiquement, une extrémité SIP est capable de fonctionner dans les mo des UAC et UAS, mais fonctionne dans l'un ou l'autre mo de par transaction. Que l'extrémité fonctionne comme un UAC ou un UAS dép end de l'agent utilisateur qui ainitié la requête. D'un point de vue architectural, les composants physiques d'un réseau SIP p euvent être groupés en deux catégories: Clients (extrémités) et Serveurs.

Clients SIP

- Téléphones: peuvent agircommeUACouUAS,ilexiste deux sortesde téléphones: des téléphones physique s IP et des softphones (PCs avec des fonctions téléphone installées).
- Passerelles : fournissent le contrôle d'app el. Les passerelles fournissent plusieurs services,le plus commun étant une fonction de traduction entre les extrémités de conférence SIP et d'autres typ es de terminaux. Cette fonction comprend la traduction des formats de transmission et des pro cédures de communication. En plus, la passerelle traduit entre co decs audio et vidéo,réalise l'établissement d'app elet la lib ération de communications du côté LAN et du côté réseau à commutation de circuits.

Serveurs SIP

- Serveur proxy : reçoit les requêtes SIP d' un client et les achemine vers l'autre client. De manière basique, les serveurs proxy reçoivent des messages SIP et les acheminent vers le pro chain serveur SIP dans le réseau. Les serveurs proxy peuvent fournir des fonctions telles que l'authentication, l'autorisation, le contrôle d'accès ré seau, le routage, la retransmission able de requêteset lasécurité.
- Serveurde redirection : fournit au clientl'information surle ou lespro-chains sauts qu'un message doit atteindre et ensuite le client contacte

[5]User Agent Client
[6]User Agent Server

le serveur du pro chain saut ou l'UAS directement.
- Serveurregistrar: traite les requêtes des UACs pour l'enregistrement de leur lo calisation courante. Les serveurs d'enregistrement sont très souvent lo calisés avec le serveur de redirection ou le serveur proxy.

2.2 Lesmessages SIP

Les messages SIP sont décrits dans laRFC 822,qui dénitla syntaxeà la fois des requêtes et des rép onses. On y trouve une très forte inuences des autres proto coles de l'IETF, principalement HTTP[7] et SMTP[8]. Le format des requêtes et des rép onses est en eet similaire à celui utilisées dans le proto cole HTTP, et les ent-têtes s'apparentent à celles utilisées dans le proto cole SMTP. On y trouve parailleurle conceptd'URL [9][Oua08].
Les messages SIP sont co dés en utilisant la syntaxe de message HTTP/1.1 (RFC 2068). Qu'il soit une requête, ou une rép onse à une requête, un message SIP doit resp ecter le format illustré à la qure 2.1. La première partie est

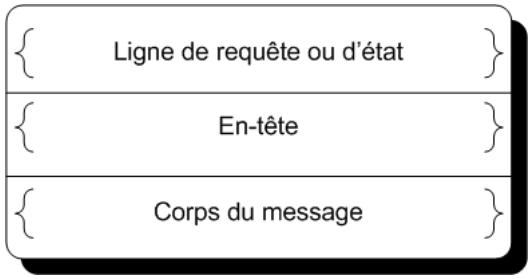

Fig. 2.1 Format gé nérique d'un message SIP

soit uneligne de requête, s'il s'agit d'une requête, soit une ligne d'état, s'il s'agit d'une ré p onseLa seconde parti e rassemble les en-têtes du message. Enn vient le corp du message.

2.2.1 Les requêtes

Comme indiqué précédement, une requête est comp osée de trois parties: une ligne derequête, un champs d'entêtedu message et le corps.
La partie dénissant la ligne de requête se comp ose des trois champs suivants illustrés à la gure 2.2:

[7] Hyp erText Transfer Proto col
[8] Simple Mail Transfer Proto col
[9] Uniform Resource Lo cator

- Métho de : qui indique l'action sollicitée.
- URI[10] : qui précise la de stination de la requête.
- Version : qui sp écie le numéro de la version du protocole SIP utlisée.

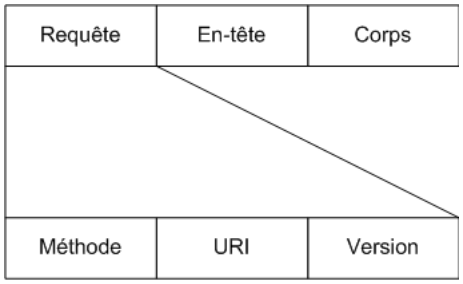

Fig. 2.2 Formatd'une requêteSIP

SIP n'utilise que six métho des fondamentales p our formuler ses requêtes, ces métho des sont détaillées dans la RFC 3261. À ces méthodes fondamentales, ont été a joutées des métho des supplémentaires, destinées à diverses améliorations, qui ne sont pas forcément implémentées par tous le s terminaux contrairement au six requêtes fondamentales, décrites ci-dessous, quidoivent être supp ortées par tous les terminaux et serveurs sollicités.

- Métho de INVITE : p ermet d'initier une communication en invitant un corresp ondant à y particip er.
- Métho de ACK: corresp ond à un aquittement de l'appelant,elle peut être utilisée suite à l'acceptation d'un app el par l'app elé ou bien à la suite d'une réponse de lo calisation fournie par un serveur de redirection après la détermination de la position de l'app elé.
- Métho de OPTIONS: permet d'interroger un serveur SIP, ycompris l'entité UAS surdiérentes informations.
  Avec cette métho de,il est possible d'obtenir des informations sur un serveur relativement aux typ es de média supportés (audio, vidéo, données),aux co decs supportés,aux méthodes supp ortées et aux options d'app els,si le serveur ena diusé. Le serveur qui reçoit cetterequête rép ond par son état et ses capacités.
- Métho de BYE: p ermet de lib érer une communicationCette requête p eut être émise indiérement par l'app elant ou par l'app elé. Elle n'attend pas d'acquittement, puisqu'une terminaison d'app el p eut être décidée unilatéra lement.
- Métho de CANCEL : annule une requête dont la rép onse n'est pas encore parvenueau demandeur.

[10] Uniform Resource Ident ier

Elle ne permet pas d'interrompre une session, mais indique que la réponse n'est plus attendue et qu'il n'est donc pas nécessaire de traiter la requête.

- Métho de REGISTER : permet d'enregistrer son adresse IP auprès d'un serveur d'enregistrement. Elle permet donc d'assurer le service de localisation. L'information enregistrée corresp ond à une entrée dans la base sp éciant la corresp ondance d'une adresse SIP avec une adresse IP ; cette entrée a une durée de vie limitée. Passé ce délai, le serveur de localisation la supprime de sa base de données. Pério diquement, chaque terminal doit rafraî chir cette entrée p our la conserver en base ou, s'il est mobile, la mo dier la cas échéant [Oua08].

2.2.2 Les réponses

Quelle que soit la métho de utilisée dans une requête, le réce pte ur nal doit y apporter au moins une réponse en retour, ne serait-ce qu'une rép onse temp oraire p our informer l'émetteur que sa requête est prise en compte et en train d'être traitée et qu'elle sera suivie d'une rép onse nale dès que possible. Les rép onses SIP doivent resp ecter le format illustré à la gure 2.3. Les ré-

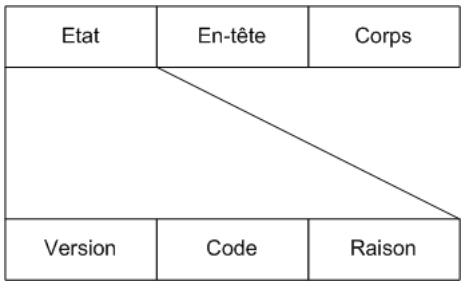

Fig. 2.3 Format d'une rép onse SIP

ponses aux requêtes SIP débutent par une ligne d'état (Status-Line), laquelle comp orte les trois champs suivants:

- Version : c'est la version du proto cole SIP utilisée.
- Co de d'état : co de numérique à trois chires sp éciant la rép onse donnée à la requête.
- Raison: message textuel expliquant brièvement le co de d'état de la rép onse [Oua08].

2.3 Fonctionnement du protocole SIP

SIP est un proto cole simple, basé sur l'ASCII[11], qui utilise des requêtes et des rép onses pour établir des communications parmi les divers comp osants d'un réseau et optionnellement établir une conférenc e entre deux ou plusieurs extrémités. Les utilisateurs d'un réseau SIP sont identiés par une adresse SIP unique. Une adresse SIP est similaire à une adresse e-mail dont le format est : sip :userI D@dom aine.com. Le userID p eut être soit un nom d'utilisateur soit une adresse E164[12].
Les util isateurs s'enregistrent avec un serveur d'enregistrement en utilisant leur adresse SIP aectée. Le serveur d'enregistrement fournit cette information au serveur de lo calisation sur requête.
Quand un utilisateur initie un app el, une requête SIP est transmise vers un serveur SIP (soit un se rveur proxy, soit un serveur de redirection). La requête comprend l'adresse de l'app elant (dans le champ From de l'en-tête) et l'adresse de la partie app elée (dans le champ To de l'en-tête).
Au cours du temps, un utilisate ur SIP p eut se déplacer d'un système d'extrémité à un autre. La lo calisation d'un utilisateur p eut être enregistrée dynamiquement avec un serveur SIP. Le serveur de lo calisation peut utiliser un ou plusieurs proto coles (LDAP[13], Finger[14],. ..) p our localiser l'utilisateur.
Comme l'utilisateur peut être connecté sur plusieurs stations et que le serveur de lo calisation peut avoir quelques fois des informations imprécises, celui-ci p eut retourner plusieurs adresses p our l'utilisateur.
Si la requête vient au travers d'un serveur proxy, ce dernier essaie chacune des adresses retournées jusqu'à ce qu'il lo calise l'utilisateur. Si la requête vient d'un serveur de redirection, il achemine toutes les adresses vers l'app elant dans le champ Contact del'en-tête du message invitation response.

2.3.1 SIP avec un serveur proxy

L'agent utilisateur de l'app elant transmet un requête INVITE au serveur proxy, ce dernier détermine le chemi n et achemine la requête vers la partie app elée.
La partie app elée répond au serveur proxy qui, à son tour, achemine la rép onse vers l'appelant.
Le serveur proxy achemine les acquittements des deux parties. Une session

[11] American Standard Co de for Information Interchange
[12] Un numéro de téléphone avec une chaîne de ch ires décimaux
[13] Lightweight Directory Access Proto col
[14] Application that allows you to have information ab out a logged user

est ensuite établie entre les parties app elante et app elée.RTP[15] est util isé p our la communication entre les parties appelante et appelée.

2.3.2 SIPavec un serveur deredirection

L'agent utilisateur de l'app elant transmet une requête INVITE au serveur de redire ction, ce dernier contacte le serveur de lo calisation p our déterminer le chemin vers la partie app elée et ensuite il renvoie l'information vers l'app elant. L'app elant acquitte la réception de l'information et transmet la requête à l'équip ement indiqué dans l'information de redirection (qui peut être la partie app elée ou un autre serveur qui achemine la requête).
Une fois que la requête atteint la partie app elée, celle -ciémet une rép onse et l'appelant acquitte cette rép onse. RTP est utilisé p our la communication entre les parties app elante et app elée.

Conclusion

Le proto cole SIP, dé ni de manière totalementintégrée dans l'environnement de l'internet, devrait bénécier de tous les dévelopg ements éectués dans ce cadre en matière d'applications et de proto coles.SIP couvre ainsi toutesles applications multimédia H323[16] mais avec une appro che plus homogène. Ànoter aussiqueSIP a été retenudansl'industrie du câble comme protocole préféré de téléphonie en mo de paquet pour les services vo caux destinés au grandpublic

[15] Real-time Transfer Proto col
[16] is an ITU standard multimedia conferencing proto col

Chapitre3

Les systèmes IDS/IPS

Intro duction

An de détecter les attaques que peut subir un système, il est nécessaire d'avoir un logiciel sp écialisé dont le rôle serait de surveiller les données qui transitentsur ce système, et qui serait capable de réagir si des données semblent susp ectes. Plus communément appelé IDS[1]/IPS[2], les systèmes de détection/prévention d'intrusions conviennent parfaitement pour réaliser cette tâche.

3.1 Systèmede détectiond'intrusions

Un IDS est un mécanisme écoutant le trac sur leréseau, de manière furtive. Cela a p our but de rep érer les activités et évènements anormaux, susp ects,. ..
Cela permet ainsi d'avoir une action de prévention sur les diérents risques d'intrusion.
Un IDS aquatrefonctions: l'analyse, la journalisation,la gestionet l'action:

- Analyse : analyse des journaux pour identier des motifs dans la masse de données recueillie par l'IDS. Il y a deux métho des d'analyse: une baséesur les signatures d'attaques,et l'autre surla détectiond'anomalies.
- Journalisation: Enregistrement des évènements dans un chier (un chier log). Exemples d'évènements : arrivée d'un paquet, tentati ve de connexion.

[1] Intrusion Detection System
[2] Intrusion Pr evention System

- Gestion: les IDS doivent êtres gérés de manière continuells doivent êtres congurés, vériés. .. On peut assimiler un IDS à une caméra de sécurité : ça détècte les intrusions, mais est inutile si il n'y a personne derrière cette caméra.
- Action : alerter le p ersonnel, ou transme ttre une commande, quand une situationdangereuse est détectée.

3.1.1 Les diérents types d'IDS

Il existe deux sortes d'ID S:

- Les NIDS[3], ils assurent la sécurité au niveau du réseau.
- Les HIDS[4], ils assurent la sécurité au niveau des hôtes.

NIDS

Un NID S est eectif sur un maté riel précis, et est capable de contrôler tous les paquets qui circulent à un e ndroi t précis du réseauIl utilise des cartes réseau en mo de espion, ceci garantit un fonctionnement furtif qui lui p ermet d'analyser tout les paquets passant par le lien en question.
-Points forts : les NIDS voient tous les paquets qui passent par un point précis du réseau.C'est la plupart du temps le meilleur diagnostic possible des attaques.
-Points faibles : suivant l'endroit où se trouvent les NID S sur le réseau, certains cas de gure intro duisent des angles morts où ils ne peuvent pas voir les paquets.
Les NIDS ne peuvent pas lire les données chirées. Il p euvent uniquem ent scanner les parties non chirées d'un paquet ; cela fournit donc des informations limitée s.

HIDS

Le HIDS réside sur un hôte sp écique, et est utilisé en tant qu'agent. Il analyse les informations particulières dans les chie rs de log p our détecter toute activité d'intrusion. Il capture les paquets réseauxentrant/sortant de l'hôte sur lequel il setrouve,etalerte lorsquenécessaire.
-Points forts: Les HIDS sont eectifs même si l'ordinateur en question est situé dans un angle mort. Uniquement les données relatives à l'ordinateur surlequel setrouvele HIDS sontanalysées, cequisimplie.
-Points faibles : Une vision restrei nte de ce qui se passe sur le réseau.

[3] Network Intrusion Detection System
[4] Host Intrus ion Detection System

Les HIDS peuvent être victimes d'attaques (mo dication et eacement de chiers) emp êchant leur fonctionnement.

3.1.2 Fonctionnementdes IDS

Les métho des de détection des IDS

Les systèmes de détection d' intrusions se divisent en deux catégories:

1. Signatures:
   Les intrus p ossèdent des signatures, tout comme les virus, qui p euvent êtres détectés par certains logiciels. La pro cédure consiste à trouver les paquets de données contenant des signatures connues comme anormales et dangereuses.Basé sur un ensemble de signatures et de règle s,le système de détection peut trouver et loguer les activités susp ectes et pro duire des alertes.Cep endant les IDS nécessitent des mises à jour de leur base de signatures p our pouvoir détecter les nouveaux typ es d'attaques.
2. Anomalies:
   Les IDS basés sur la détection d'anomalies consistent à comparer les schémas d'évènements en cours pris dans leur ensemble aux schémas d'évènements habituels pris dans leur ensemble.Cela permet d'analyser b eaucoup de choses comme par exemple des uti lisateurs accédant à des chierssystèmes, des mo dications de chiers inhabituelles, de nombreux échecs de connexion,. ..Cette métho de permet d'identier des attaques inhabituelles.Mais il est dicile de distinguer ce qui est normal de ce qui ne l'est pas, car les schémasd'activités varient très largement.

Où placer un IDS dansle réseau

la gure 3.1indique les emplacementspossibles d'unIDS dansle réseau:

- Lo calisation 1 : à l'entrée du rewall externe, relié à internet. C'est le meilleur endroi t p our analyser les attaques externes contre le réseau.
- Lo calisation 2: dans la zone des serveurs,une zone sensible pour le reseauet donc à surveiller.
- Lo calisation 3: sur chaque segment réseauIl se concentre sur les attaques ayant passé le rewall et s'étant intro duites sur ce segment réseau.
- Lo calisation 4: sur un sous réseau, comme p our la lo cation 3,viseà proteger un sous réseau particulier.

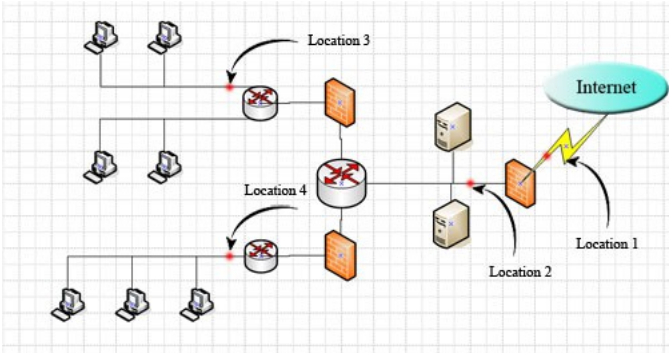

Fig. 3.1 EmplacementdesIDS

Les diérentes actions des IDS

Les IDS p euvent déclencher diérents typ es d'alarmes et proposent des disp ositifs d'analyse interactifs pour aider l'administrateur à identier des motifs dans les journaux. Il existe plusieurs métho des pour signaler les intrusions.Les principalessont les suivantes:

- Envoid'unemail auxutilisateursconcernés
- Journalisation(log)de l'attaque. En quelque sorte une sauvega rde des circonstances et détail s de l'attaque, comme les adresse IP et le protocole utilisé.
- Alerte visuellede l'attaque,un messages'ache signalantà l'utilisateur l'attaque.
- Sauvegarde des paquets suspects ; les paquets jugés suspects sont capturés et sto ckés.

Bon nombre d'IDS exécutent des actions limitées suivant certains typ es d'évènements, sans intervention humaine. Cep endant,les actions automatisées sont à limiter carlaplupart des schémas indiquent seulement des activité susp ectes, et non des actions très certainement malveillantes.

3.2 Systèmede prévention d'intrusions

Un IPS est un disp ositif aussi bien matériel que logiciel, qui permet de détecter des attaques, connues et inconnues, et de les emp êcher d'être réussies.
L'IPS fait partie du réseau ; il est placé en ligne et examine tous les paquets qui entrent et sortent. Il surveille ce trac et intervient par limitation ou supression du trac qu'il juge dangereux. Il réalise un ensembl e d'analyses sur chaquepaquet et sur les motifs du réseau, en visualisant chaque transfert

dans le contexte qui précède etsuit.

3.2.1 Les diérents types d'IPS

Il existe deux typ es d'IPS:

- Les NIPS[5], un logiciel ou un matériel dédié qui est connecté directem ent à un segment du réseau et qui protège le s systèmes de ce segment.
- les HIPS[6], un programme système installé directement sur l'ordinateur àsurveiller.

NIPS

Le NIPS combine le s caractéristiques d'un IDS standard avec celles d'un rewall. On le qualieparfois de rewall à insp ection en profondeur (deep insp ection).
Comme avec un rewall, le NIPS a au minimum deux interfacesréseau, une interne et uneexterne. Les paquets arrivent par une des interfa ces et sont passés au moteur de détection. L'IPS fonctionne pour le moment comme un IDS, c'est-à-dire qu'il détermine si oui ou non le paquet est malvei llant. Cependant, en plus de déclencher une alerte dans le cas ou il détecte un paquet susp ect,il rejettera le paquet et marquera cette session "susp ecte".Quand les paquets suivants de cette session arri veront à l'IPS, ils seront jetés.
Les NIPS sont déployés en ligne avec le segmentdu réseau àprotéger. Du coup, toutes les données qui ci rculent entre le segment surveillé et le reste du réseau sont forc ées de passer par le NIPS.
Un NIPS déclenche des alarmes du typ e "telou tel trac a été détecté en train d'essayer d'attaquer ce système et a été blo qué".
Un NIPS ne néc essite pas d'intervention humaine si la sécurité n'est pas primordiale p our l'entre pri se. Dans le cas contraire une intervention humaine est préférable pour surveiller les intervention automatisées du NIPS.Les avantages d'un NIPS:

- Un seul p oint de contrôle p our le trac p eut protéger tout les systèmes situés en aval du disp ositif.
- Le déploiement est facile car unseul disp ositif IPS sut pour des dizaines de systèmes.
- Il protège des autres disp ositifs du réseau car toutes les attaques p euvent aussiêtre dirigéescontredes routeurs,des rewall..

[5] Network Intrusion Prevention System
[6] Host Intrus ion Prevention Sys tem

- il protègedes attaques réseaux: DoS[7], SYN o od [8] etc... Travailler au niveau du réseau p ermet à un NIPS de protéger contre ces attaque s.

HIPS

Le HIPS est un programmerésidantsurunsystèmetel queles serveurs ou les postes de travail.
Le trac qui entre et sort de ce système est insp ecté et les activités au niveau des applications et du système d'exploitation peuvent être surveillées an d'y trouver des signes d'une attaque. Un HIPS peut détecter les attaques visant la machine, et arrêter le pro cessus malveillant avant qu'il ne s'exécute.
Le HIPS nenécessiteplusde servicede journalisationdesévènements (log).
Quand une attaque est détectée,le logi cielblo que l'attaque soit au niveau de l' interface réseau,soit en envoya nt des commandes à l'application ou au système d'exploi tati on, leur disant d'arrêter l'action lancée par l'attaque.
Un HIPS possède une liste prédénie de règles, déniepar le fabriquant et livrée avec le pro duit. Ces règles savent comment un système d'exploitation ou une application doit se "comp orter normalement". Si l'application entame une action susp ecte,une des règles est activée et le pro cessus est tué avant de nuireau système.
D'autres systèmes HIPS emploient la métho de "surveillance". Un agent HIPS tournesur l'ordinateur et seconcentresur lesévénementd'un systèmed'exploitation en observant tous les app els système,les entré es de la base de registre.
Lesavantages d'unHost IPS:

- Protège les systèmes mobiles c ontre une attaque quand il s sont hors du réseau protégé.
- Protège des attaques lo cales,le personnel ayant un accès physique et voulant corrompre certains systèmes à l'aide de disquette ou CD. ..
- Garantieunedernièredéfense contre lesattaquesayantpassé lesautres systèmes de sécurité.
- Lesattaqueslancéesentrelessystèmesdu mêmesegmentréseaune p euvent être contrées qu'avec le HIPS.
- Indép endant de l'architecture réseau

Le HIPS doit resp ecter certaines conditions: il doi t être able, ne doit pas ralentir les p erformances du systèmes, et ne doit pas blo quer le trac légitime.

[7] deny of services
[8] Synchronisation o od

3.2.2 Fonctionnementdes IPS

Les techniques de déte ction

Plusieurs métho des de détection existent:

- L'analyse de proto cole: l'IPS contrôle la norme du proto cole donné et vérie si elle est conforme. De ce fait, la recherche d' une activité d'intrusion est plus précise et donc plusecace.
- Corresp ondance de motifs: le trac est surveillé pour déterminer les signatures des motifs d'attaque connus. Lesystèmeanalysetous les paquets. L'IPS conserve la trace de l'état de connection avec l'éléme nt extérieuretévalue le contexte pluslargedetoutesles transactionséta- blies au cours de la connexion. Cette métho de détecte uniquement les attaques connues,et ce ci uniquement si la liste des si gnature s d'at- taquesest régulièrement actualisée.
- Comp ortementale: basée sur le comp ortement L'IPS tente de cerner les activités anormales en observant le comp ortement du système et des utilisateurs. Si l'IPS constate que l'ac tivité courante s'éloigne trop du comp ortement habituel,il prend ce rtai nes mesures Cette métho dea l'avantage de pouvoir détecter des tentatives malveillantes jusqu'alors inconnues.

Où placer un IPS dans le réseau

la gure 3.2 indique les emplac ement p ossibles d'un IPS dans le réseau:

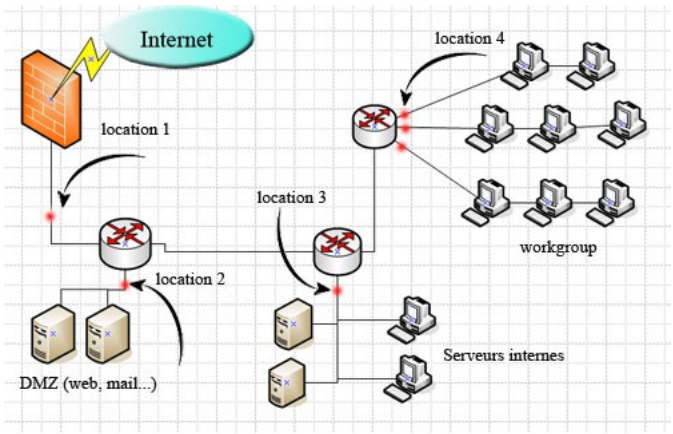

Fig. 3.2 EmplacementdesIPS

- Lo calisation 1: Derrière le rewall de périmètre réseau, assure une sécurité face aux attaques externe s.
- Lo calisation 2 : entre le rewall et les serveurs placé en DMZ[9] comme les serveurs web, email..
- Lo calisation 3: devant les serveurs internes imp ortants, et doncà risques.
- Lo calisation 4 : devant les principaux workgroups d'un service.

3.2.3 Méthodes de mise en place d'un IPS

Il existe cinq métho des pour réaliser un IPS:

les NIDS en ligne

Le NIDS en ligne se trouve entre le système à protégeret le restedu réseau. Toutle trac passe donc par leNIDS en ligne. Il insp ecte chaque paquet, et si l'un d'e ux déclenche une signature, il sera rejeté et logué. Un NIDS en ligne ore les capacités d'un NIDS régulier, avec en pl us la p ossibilité de blo quage d'un rewall.
L'inconvénient de ce système est de n'orir aucune protectio n contre la mauvaiseprogrammationou l'erreurde conguration.

Les rewalls/IDS applicatifs

CesIPS sont misen place surchaque serveurqui doit être protégé. Ils peuvent être congurés p our chaque application. Ils ne font pas attention aux paquets mais surveillent les app els API[10], la gestion de la mémoire, comment l'application, lesystème et l'utilisateur interagissent entre eux.
Lebut estdeprotéger des attaques inconnues.

Les commutateurs de la couche7

Habituellement les commutateur sont des équip ements de couche 2, mais avec l'évolution des réseaux, les commutateurscouche 7sontde plusen plus fréquents.
Ils fonctionnent de la même façon q'un NIDS en ligne basé sur des signatures quand il doit arrêter une attaque. Quand on place un de ces disp ositifs devant les rewalls, il fournit une protection pour tout le réseau. Ils sont également congurables pour la redondance.

[9] DeMilitarized Zone
[10] Application Program Interface

Cep endant comme p our le NIDS en ligne, ils p euvent uniquement arrêter les attaques qu'ils connaissent.

Les commutateurs hybrides

Cettetechnologieest un hybride entre les rewall/IDS applicatifs etle commutateur de couche 7. Ce sont des solutions matérielles que l'on place devant un serveur comme pour le commutateur de couche 7. Maisau lieu d'employer un ensemble de règles d'un NIDS, les commutateurs hybrides emploient une politique semblable aux rewall/IDS applicatifs.

Les applications tromp euses

Cette métho de emploie des techniques tromp euses. Dans un premier temps il observe le trac réseau p our comprendre le trac légitime. Puis quandil voit des tentativesde connexion qui n'existe nt pas sur ce serveur,il envoie une réponse à l'attaquant. La rép onse sera "marquée" avec des données falsiées, de tel sorte que lorsque l' attaqua nt revient et essaie d'exploiter le serveur, l'IPS voit les données"marquées"et arrêtetout le trac venant de l'attaquant.

Conclusion

les équip ements IDS/IPS sont actuellement des produits mûrs et aboutis. Ils continuent d'évoluer p our rép ondre aux exigences technologiques du moment mais orent d'ores et déjàun éventail de fonctionnalitéscapables de satisfaire les b esions de tous les typ es d'utilisateurs. Néanmoins, comme tous les outils techniques ils ont des limites que seule une analyse humaine peut comp enser. Un p eu comme les Firewalls, les IDS/IPS deviennent chaque jour meilleurs grâce à l'exp érience acquise avec le temps mais ils deviennent aussi de plus enplus sensibles aux problèmes de conguration et de paramétrage.

Chapitre4

Analyse et sp écication

Intro duction

La sp écication est une phase cruciale du processus de développement des applications. Dans ce chapitre nous décrivons le pro cédé DCM[1], qui a été élaboré par rapp ort à une problématique de sécurité des applications VoIP, bien que son cadre d'application puisse être beaucoup plus large (exemple : le système p eut également p ermettre de détecter de s terminaux mal congurés).

4.1 Expressiondes besoins

4.1.1 Besoins fonctionnels

1. Déco dage des paquets
   Pour chaque paquet reçu, déco der un ensemble prédéni d'informations, généralementstructuréessous formede champs à l'intérieurdu paquet, ces informations p euvent p orter indiéremment sur les parties routage, transp ort ou applicative contenues dans le paquet.
2. Filtrage
   Cettefonction réalise les actions suivantes:
   - Suppression des paquets malicieux pour éviter les attaques.
   - Comptage des paquets p our connaître le volum e de données d'une source particulière.
   - Marquage des paquets devant subir un traitement sp écique.
3. Détecion d'entité
   Pour chaque paquet reçu, déterminer à partir des éléments d'informa-

[1] Détéction de Comp ortement Malveillant

tion extraits par la fonction de déco dage, quels sont les entités émettrice et destinatrice et récup ère le cas échéant les contextes associés, en particulier les informations de typ e et éventuellement sous-type. Cette fonction pro cède en deux étapes:

- Recherche de corresp ondance.
- Récup ération du contexte asso cié.

4. Priorisation destraitements
   Réguler les temps de traitement en fonction des ressources du système et des autres critères pris en compte par le pro cédé.
5. Analysede conformité
   Il s'agit de la fonction principale du système puisqu'elle est resp onsable de détecter les comp ortements malveillants, en analysant chaque paquet reçu. Par défaut, l'analyse de conformité est eectuée seulement sur les paquetsémisde la zoneC (Customer entities) vers la zoneS (Server entities), puisque les paquets reçus de la zone S sont supp osés non malveillants. De façon symétrique, l'analyse de conformité peut être réalisée également sur les paquets ém is de la zone S vers la zone C. Les traite ments réalisés par la fonction d'analyse de conformité sont basés sur les typ es d'entités source et destination du paquet. Pour toute nouvelle entité du système, ces informations de typ e sont déterminées par la fonction de caractérisation du typ e d'entité[Mem08].
6. Analysedenon conformité
   Cette fonction est appliquée aux pa que ts p our lesquels l'analyse de conformité a donné un ré sultat négatif. Le but de l'analyse de non-conformité estde corréler un ensemblede paquets non-conformes, émis par une entité donnée, an d'en déduire quel type de comp ortement non-conforme est observéPar rapp ort à l'analyse de conformité, qui émet un résultat p our chaque paquet reç u, la fonction d' analyse de non-conformité op ère sur une période plus longue[Mem08].
7. Caractérisation du typ e d'entité
   Déterminer, après réception d'un ensemble de paquetsen provenance d'une entité donnée, àquel typ e appartient cette entité. La caractérisation d'entité s'applique aussi bienaux entités de la zone C qu'à celles de la zone S. A chaque information de typ e est généralement asso ciée une information de sous-typ e. Pour eectuer cette détermination, cette fonction a besoin d'informations de caractérisation qui sont fournies par la fonction d'agrégation d'apprentissage ou qui sontcongurées de façon statique, parexemple sousformede signatures[Mem08].
8. Apprentissage
   Cette fonction collecte des caractéristiques de typ e d'entité, sur la base

des informations contenues dans les paquets qu'elle analyse. Elle op ère entité par entité et les informations collectées dép endent du typ e d'entité considéré. La fonction d'apprentissage s' applique à la fois a ux entités de la zone C et à celles de la zone S. La condition préalable pour quel'apprentissage puisseêtre réalisé surun paquet, est que le paquet aitpassé avec succès l'analyse deconformité[Mem08].

9. Agrégation d'apprentissage
   Cette fonction s'applique en parallèle de la fonction apprentissage dénie ci-dessus. Son but estd'agréger lesinformations apprisesau niveau des entités par type et par sous-typ e d'entité, dès lors qu'un volume susant d' informations est collecté. Après intégration des données, la fonction fournit des informations de caractérisation p our les diérents types et sous-typ es d'entités.
10. Corrélation
    Faire le lien entre les paquets ém is de la zone C vers la zone S et les paquets émis de la zone S vers la zone C (ou inversement)qui leur rép ondent. Cette fonction n'est pas appliquée systématiquement à tous les paquets, mais seulement à ceux p our lesquels la rép onse de l'entité distante est nécessaire au systèmeLafonction de corrélation est invo quée indiéremment et indép endamment par les fonctions d'analyse de conformité, de caractérisation du typ e d'entité, d'apprentissage et d'analyse de non-conformité[Mem08].

Concernant les temps d'exécution, la fonction d'analyse de conform ité est de typ e court-terme car donnant un résultat à l'issue de chaque paquet reçu et analysé. La fonction de corrélation est également de typ e court-terme car dans une transaction, les rép onses suivent généralement de près les requêtes. Les fonctions de caractérisation du typ e d'entité et d'analyse de non-conformité sont de typ e moyen-terme car nécessitant un ensemble de paquets avant de fournir un résultat. Les fonctions d'apprentissage sont de typ e long-terme car nécessitant un grand nombre de données issues d'un ense mble représentatif d'entités.

4.1.2 Besoins nonfonctionnels

1. Eviter de faire du debbug au niveau du co de, en pla çant de s p oints d'arrêt.
2. Eviterd'analyserdes logsdegrande taille.
3. Eviterdedevoirremonter systématiquementauniveaudu paquet.
4. Replacement du système ra pi dement dans une conguration donnée.

5. Pour lesbasesde données:
   - Pouvoir évoluer sans remettre en cause le co de du système.
   - Avoirune structurequifacilite l'interactionavecl'IHM [2].
   - Pouvoir recevoir des informations via les chie rs de conguration.

4.2 Positionnementde DCM dans le réseau

Le système de sup ervision p eut être positionné en dérivation ou en coupure du trac à sup erviser, tel qu'illustré par la gure 4.1.

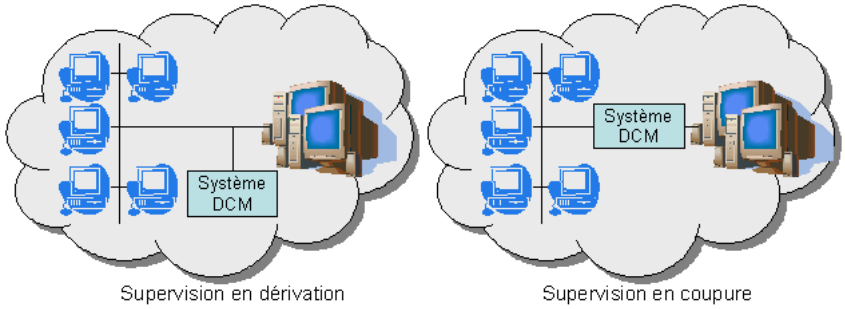

Fig. 4.1 Positionnement réseaudeDCM

Lorsque le système de sup ervision DCM est placé en dérivation, sa fonction principale est la détection du trac susp ect. Les mesures de réaction sont typiquement l'enregistrement des caractéristiques du trac susp ect, la remontée d'alarmes et optionnellement le pilotage d'équip ements de protection réalisant le bl o cage du trac incriminé.
Lorsque le système de sup ervision DCM est placé en coupure,sa fonction principale est la détection et le blo cage du trac susp ect. Les mesures de réaction sont identiques au cas précédent, avec de plus la p ossibilité de blo quer directement le trac susp ect.
Dans lesdeux cas,le systèmeDCM analyse le tracde façonbi directionnelle, c'est-à-dire à la foi s le trac émis par les entités p otentiellement malveillantes vers les serveurs ou le sous-réseau à protéger e t inversement le trac émi s par les serveurs ou le sous-réseau à protége r vers le s entités p otentiellement malveillantes.

[2] Interface Homme Machine

4.3 Schéma fonctionnel

Le synoptique du pro cédé,lorsque les paquets en prove nance de la zone S sont supp osés non malveillants, est illustré par la Figure4.2.

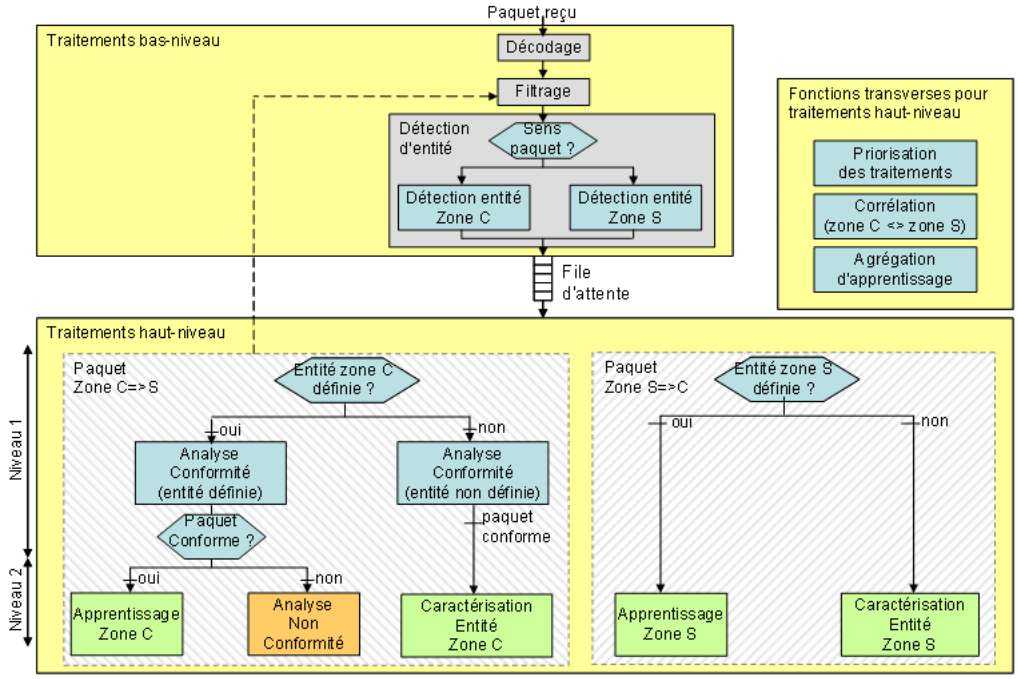

Fig. 4.2 Architecturegénérale

Les paquets reçus corresp ondent aux éléments d'information échangés sur le réseau entre les entités de la zone C et les entités de la zone S, de fa-çon bi-directionnelle, via un systè me de transmission et de routage quiest indép endant du procédé DCM.Pour une application considérée,le système DCM peut être amené à superviser un ou plusieurs proto coles utilisés par cette applic ation.
Optionnellement, les paquets reçus sont pré alablement ltrés par une entité en amont, indép endante du pro cédé, par exemple une entité de typ e pare-feu. Ce premier niveau de ltrage porte typiquement sur les adresses sources ou destination et sur les proto coles supervisés par le système DCM, ceci an de ne pas surchargerle système DCM par des messagesqui ne le concernent pas.

4.4 Etudedes cas d'utilisation

Les cas d'util isation représentent un élément essentiel de la mo délisation orientée ob jet. En eet, ils interviennent très tôt dans la conception. Ils servent à défnir le pro duit à dévelopg er et à le mo déliser.
Dans notre cas, un seul acteur qui est l'administrateur du système peut intervenir, comme pré senté par la gure 4.3, plusieurs fonctionnalités lui

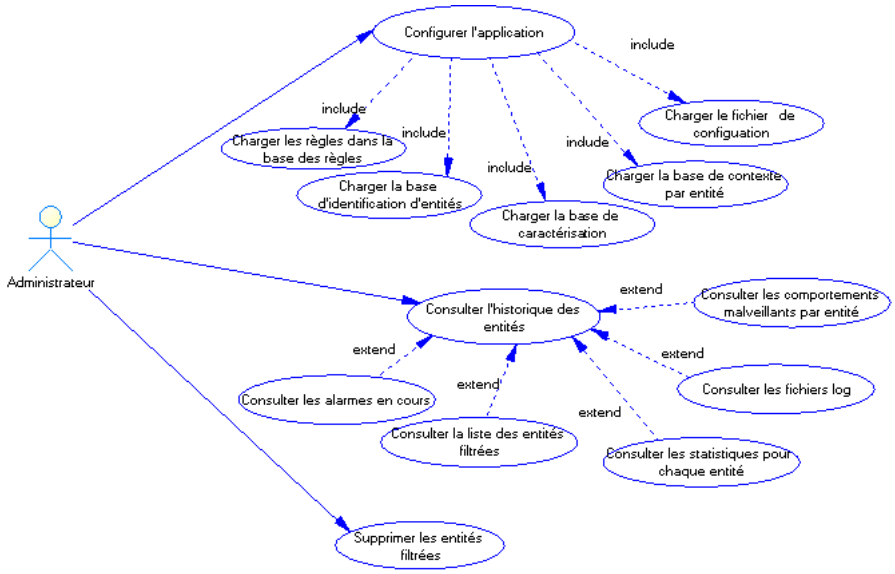

Fig. 4.3 Diagrammedes casd'utilisation

sontaectées ande dénirl'état initial du système. En eet, l'administrateur peut congurer l'application en chargeant des données de conguration initiale dans les bases, ces dernières sont pardéfaut vides, également l'administrateur congurele système à partir des chiers de conguration: il p eut saisir le temps de rafraichissement de l'interface, le nombre de paquets à analyser et les seuil s de détection de non conformité.
En plus, l'adminstrateur a le privil ège de consulter, dans une interface en swing-php ou bie n dans des chiers de journalisation log, l'historique de chaque entité: consulter lesalarmes en cours, la liste des enti tés ltrées et les causes de ltrage, les statistiques pour chaque entité ainsi que les comp ortements malveillants détectés par entité. L'administrateur p eut aussi supprimerles entitésltrées par le système.

Conclusion

Après avoir spécié et analysé les diérents b esoins concernant le pro cédé DCM, nous allons ab order dans le chapitre suivant la conception de notre application.

Chapitre5

Conception

Intro duction

An de réaliser une appl ication qui rép ond aux besoins sp éciés auparavant, une réexion approfondie autour des diérents comp osants de notre travail s'imp ose.Dans ce chapitre, nous décrivons la conception générale, ainsi que la conception détaillée de notre pro jet.

5.1 Conception générale

Notre démarche débute par la compréhensi on du problème, ensuite nous analysons le problème an d'ab outir à une conception adéquate que nous esp érons la plus appropriée p our le dévelopment du prototyp e.

5.1.1 Diagramme dedéploiement

Le premier niveau de conception d'un système est son déploieme nt. C'est p our cette raison que nous désignons cette étap e de la branche technique par leterme conception générique.
Pour le cas de notre systè me, il sera déployé entre les serveurs de la zone S et ceux de la zone C. Le diagrammededéploiement présenté par la gure 5.1 décritles diérentsintervenants dans notresystème.
Notre système réalise lerôle dedeuxsystèmes IDS et IPS présentés: il détecte letrac provenant des entités de la zones S (serveur Proxy, serveur de redirec tion)et C(PC, IPphone, Livebox. ..), l'analyse et blo que le trac malicieux.

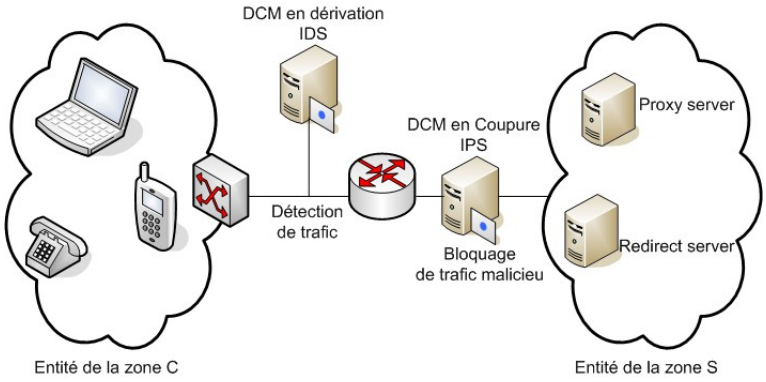

Fig. 5.1 Diagrammede déploiment

5.1.2 Base dedonnées

Pour la réal isation de notre application, nous avons opté p our la solution aveclabase dedonnées.Ce choixest justifé par:

- Lastabilité desdonnéesdans unebasede données.
- Les ressources mémoires et le temps d'exéc uti on des re quêtes sont très minimes par rapp ort aux traitements liés à la mémoire.

Dans un souci de description, les informations manipulées par le système sont organisées en diérentes bases comme indiqué dans la gure5.2 ; cette structurationest purementlogique et n'est pas liée à une implémentation particulière. Du point de vue sémantique, les bases sont divisées en trois typ es:

- Les bases en lecture et écriture : ces bases contiennent des informations qui sont à la fois lues et mo diées par les fonctions de traitement du système,essentiellement les fonctions de traitement haut-niveau,bien que certaines de ces bases soient également lues par des fonctions de traitement bas-niveau.
- Les base s en le cture seule : ces bases contiennent des informations qui sont lues par les fonctions de traiteme nt haut-niveau, mais qui ne sont pas mo diées par ces fonctions. Par contre, ces bases p euvent être con- gurées ou mo diées, via le plan de gestion, par l'administrateur du sys- tème. Cette catégorie de bases est comp osée de la base d'invo cation des diérents typ es de règles.
- Les base s en exécution : ces bases contienne nt des informations qui ont vo cation à être chargées ou app elées par les fonctions de traitement haut-niveau pour exécution. Aussi, ces bases sont par la suite dénom- mées mo dules.Cette catégorie de bases est comp osée des diérents mo dules de règles utilisés par les fonctions de traitement haut-niveau

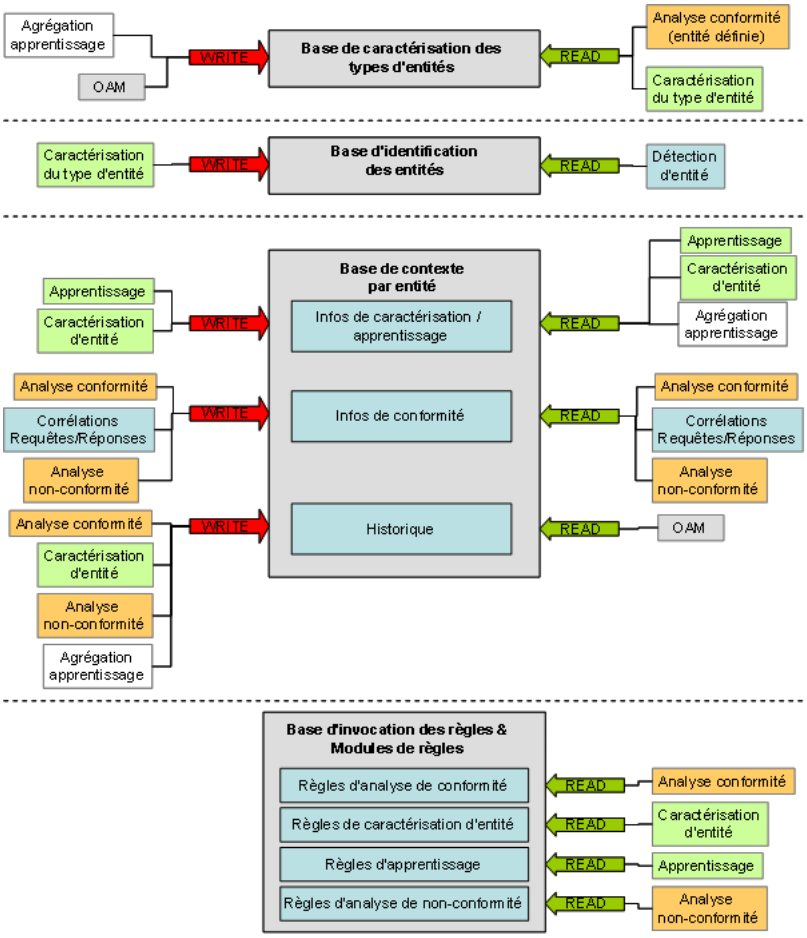

Fig. 5.2 Sché ma de la base de données

du système.

Bases en lecture et écriture

- Base de caractérisation des typ es d'entités:
  Cette base contient des informations descriptives, sur les diérents typ es et sous-typ es d'entités dénis dans le systèmepermettant à la fonction de caractérisation du typ e d'entité de déterminer, à partir des paquets reçus d'une entité donnée, à quel type voire sous-typ e(s) appartient cette entité. Les informations de caractérisation sont également app elées attributs.Par défaut, un sous-typ e hérite de façon récursive des attributs des sous-types ou type supérieur ; réciproquement un attribut déni au niveau du typ e d'entité peut être redéni dans l'un quelconque de ses sous-typ es. Ainsi, la recherche d'un attribut pour un

sous-typ e donnée entraîne de façon récursive la remontée vers le type racine, si l'attribut n'est pas déni p our le sous-typ e recherché. La base de caractérisation des typ es d'entité contient à la fois les attributs décrivant les entités de la zone C et ceux dé crivant les entités de la zone S. Les attributsprésents dans cette base sont lus par la fonctionde caractérisation du typ e d'entité comme indiqué dans la gure 5.2. Ils peuvent être écrits de façon dynamique par la fonction d'agrégation d'apprentissage, ou par l'administrateur du système via le plande gestion, en particulier lors de la phase d'initialisation où certai ns attributs sont congurés par défaut.

- Based'identication desentités:
  Cette base contient les inf ormations p ermettant à la fonction de détection d'e ntité de déterminer, p our chaque paquet reçu, de quelle entité il provient et à quelle entité il est destiné.Les informations contenues dans cette base sont segmentées en deuxparties. La première partie est constituée des informations d'index ; il s'agit d'une clé primaire identiantuneentité dusystème appartenant àla zone C ou à lazone S.La seconde partie est constituée des informations de scriptives de l'entité, c'est-à-dire son identiant qui est unique dans le système, son typ e, le ou les sous-typ es asso ciés et le niveau de conformité de l'entité. Les informations contenues dans cette base p ortent à la fois sur les entités de la zone C et sur celles de la zo ne S. La base d'identication de s entités est lue par la fonc tion de détection d'entité comme montré dans la gure 5.2. Lorsque la fonction de déte ction d'entité détecte une nouvelle entité émettrice, elle écrit dans la base et crée un nouvel identi a nt auquel sont asso ciées les informations d'index IDE correspondant. La base est également écrite par la fonction de caractérisation du typ e d'entité qui met à jour les informations de typ e et sous-type dès lors qu'elle les a déterminé p our une entité précédemment non dénie.
- Base de conte xte par entité:
  Pour un identiant d'entité donné, tel que sto cké dans la base d'identication des entités, cette base contient le contexte corresp ondant, noté IE. Les informations contenues dans la base de contexte par entité sont structuréesen trois parties:
  - Lesinformations deconformité: il s'agit d'informations indiquant le comp ortement observé p our l'entité par les fonctions d'analyse de conformité et d'analyse de non-conformité qui lisent, écriventou mo dient ces informations. Ces informations sont également lues et mo diées par la fonction de corrélation.
  - Lesinformations decaractérisation/apprentissage: il s'agit d'informations décrivant les caractéristiques de l'entité. Ces informations

sont initialement lues et mo diées par la fonction de caractérisation du typ e d'entité, puis par la fonction d'apprentissage.
De plus, elles sont ég alement lues par la fonction d'agrégation d'apprentissage.

- Lesinformations d'historique: il s'agi t d'informations sur le long termequi agrègent les diérentesanomalies oualarmesdétectées par lesfonctions d'analyse de conformité et d'analysede non-conformité.

Base en lecture seule

C'est la base d'invo cation des règles : cette base décrit les fonctions fRAC, fRCE , fAPP et fRANC resp ectivement utilisées par les fonctions d'analyse de conformité, de caractérisation du typ e d'entité, d'apprentissage et d'analyse de non-conformité. La description de ces fonctions est statique,c'est-à-dire qu'elle est congurée à l'initialisation du système par rapp ort à l'application sup ervisée,et qu'ensuite el le ne varie pas,ou peu, lors del'utilisation du système.Pour chaque combinaison possible des paramètres d'entrée des fonctions fRAC, fRCE, fAPP et fRANC la base pointe resp ectivement sur l'ensemble RACi, RCEi, RAPi et RANCi, des règles à invo quer p our cette combinaison. Pour pouvoir être implémenté, il est nécessaire que l'ensemble des combinaisons possibles des paramètres d'entrée de ces fonctions soit discret et borné.

Mo dules des règles

Les règles sont divisées en cinq mo dules selon les fonctions qules invo quent.Chaque mo dule de règles est comp osé d'un ensemble de règles et chaque règle réalise une action ou une véri cation en fonction de paramètres d'entrée propres à la règle. Aprè s exécution, chaque règle re tourne une valeur, ou unensemblede valeurs, vers la fonction app elante.Les sous-mo dules de règles utili sés par le systè me sont:

- Les règles d'analyse de conformité: elles consistentà vérier qu'un paquet est conforme à un certain nombre de règles de séc uri té. Chaque règle retourne un résultat du typ e : OK, NOK ou ND si le résultat de la règle est indéterminé. Ces règles sont classées en deux sous-typ es: les règles critiques et les règles non-critiques. Elles sont invo quées par le mo dule d'analyse de conformité.
- Les règles de caractérisation du typ e d'entité: ellesévaluent laressemblance entre une entité de typ e non déni et les diérents typ es et sous-typ es d'entités dénis dans le système.Pour chaque paquet auquelelles sontappliquées, ces règlescomparent certains paramètres du

paquet aux attributs dénis dans la base de caractérisation des typ es d'entité et font évoluer des indicateurs de vraisemblance pour les différents typ es et sous-types possibles. Ces règles sont invo quées par le module de caractérisation du typ e d'entité.

- Lesrègles d'apprentissage: cesrèglesdénissent lesparamètresà modier parmi les informations de caractérisation asso ciées à l'entité, en fonction des paquets re çus. Ces règles sont invo quées par le mo dule d'apprentissage.
- Les règles d'analyse denon conformité: cesrègles sontappliquées aux paquets détectés non-conformes par la fonction d'analyse de conformi té. Elles visent à déterminer plus nement, quel est le typ e d'attaque ou de vulnérabilité vi sée. Ces règles sont invo quées par le mo dule d'analyse de non-conformité.
- Les règles decorrélation: elles permettentde corréler une requêteà la rép onse correspondante.

5.2 Conception détaillée

Dans cette sec tion, nous essayons de détailler les pri ncipaux tables de la base de donnéesainsi que le s classes principales quiconstituent notre application, nous nirons par décrire les scénarios des cas particulier à l'aide desdiagramme de séquences.

5.2.1 Diagramme entité/association

Lors de la conception de la base de données, notre ob jectif était de concevoir un système homogène. Nous prop osons une conception des tables tout en tenant com pte de l'évolution de notre système dans le futur.
La gure 5.3 représente le mo dèle conceptuel de donnéesde notre basede données du prototyp e DCM.
Conformement à la conception générale présentée dans la première sec ti on dece chapitre, la gure 5.3 présente trois type de tables:

- En lecture seule : ce sont les tables d'invo cation des règles : Règles de conformité, de non conformité, d'apprentissage et de carac té risation.
- Enlecture/ecriture : présentéspar les autres tables, danslesquels nous enregistrons lescontextes, les statistiques et les historiques desentités.
- Invo cation des règles: présentés par les quatre tables de règles, ces tables contiennent les critères d'invo cation et les règles. Suivant les critères cherchés elles renvoie nt les enregistrements des règles correspondantes.

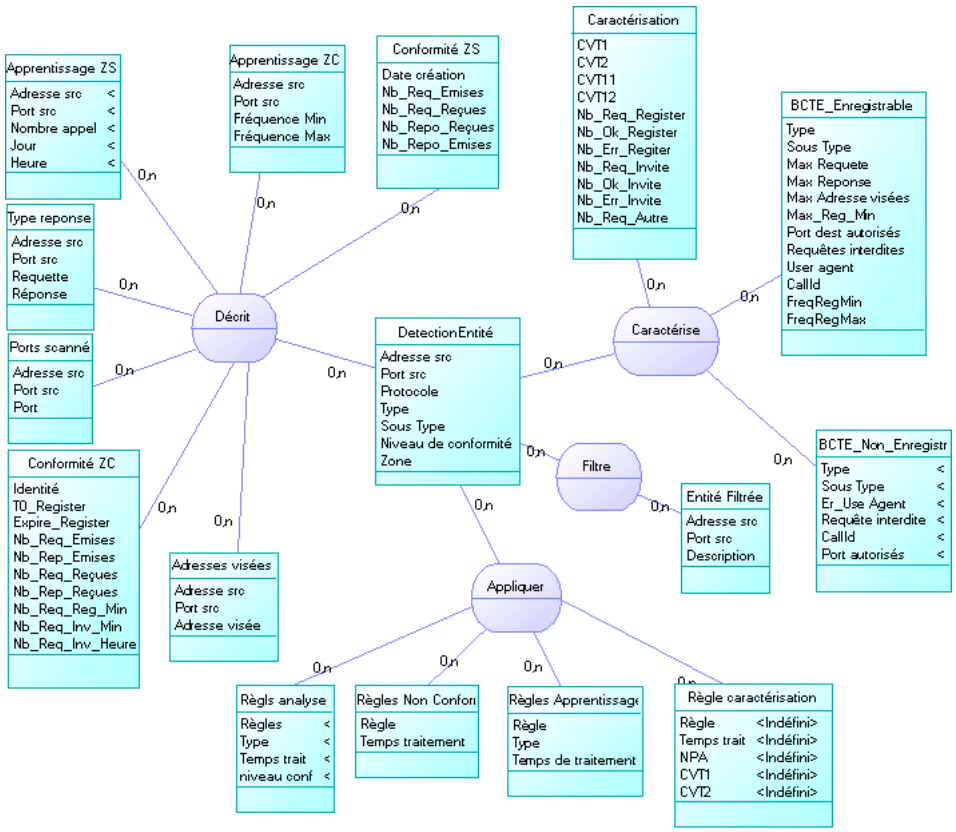

Fig. 5.3 Diagramme entité/asso ciation

5.2.2 Diagramme declasses

La gure 5.4 illustre le diagramme de classes de notre prototype.

Connexion

Se comp ose de l'URL de la baseJe nom d'utilisateur, lemot de passe, une variable Query qui va contenir à chaque fois le co de de la requête et une variable resultat p our sto cker le résultat de cette requête.
Cette classe réalise la connexion à la base de données ; elle est invoquée par toutesles autres classes.

Listening source

Au niveau de cette classe,on p eut sp écier la source de notre analyse: soit un chier PDML [1], soit undossier contenant les chiers à analyser un

[1] Portable Do cument Markup Language

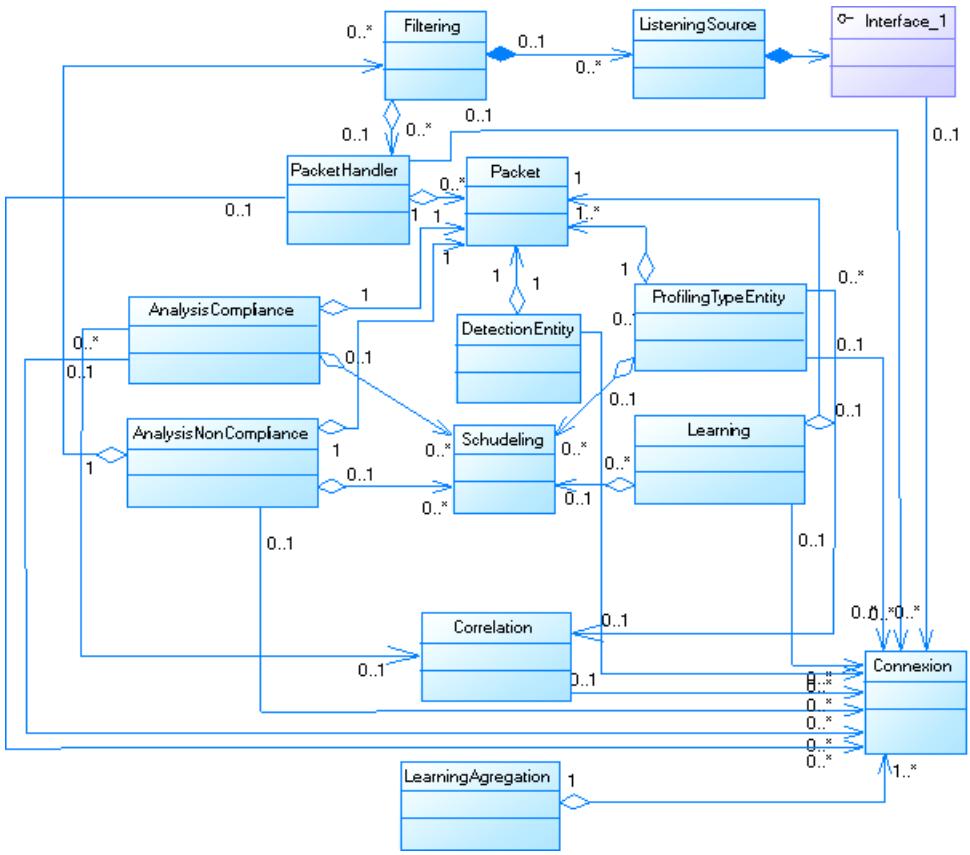

Fig. 5.4 Diagramme de classes

par un. Puis, elle passe la source choisie à la classe PacketHandler pour le commencementdu fonctionnement du système.

PacketHandler

C'est la porte de l'application, elle se comp ose d'un parseur xmlévènementiel, utilisant l'API SAX [2], qui détecte les paquets entrant et ana lyse les champs indiqués.

Packet

Contient tout les champs retournés par la classe PacketHandle r, ces champs sont mo délisés sous forme d'attributs,il sont utilisés par toutes lesautres classes.

[2] Simple API for XML

Scheduling

Cette classe est invo quée à chaque paquet reçu et retourne le temps de traitement approprié p our chaque fonction ha ut niveau du système.

DetectionEntity

A p our but de détecter les typ es des entités émettrices par comparaison des informations de déco dage aux informations enregistrées dans la base de données.

Correlation

Contient les règles de corrélation ; chaque règle est implémentée dans une métho de.Cette classe est invo quée par la classe d'analyse de conformité et la classe de caractérisation du typ e d'entité.

AnalysisCompliance

Contientles règles d'analyse de conformitéainsi que leurs critèresd'invocation, chaque règle est implémentée dans une métho de:

- AnalysisComplianceRule1(DetectionEntity,Packet): Consiste à faire des statisti ques concernant chaque entité et mettre à jour son contexte dans la base.
- AnalysisComplianceRule2(DetectionEntity, Packet): Vériequelesentités envoient vers des ports destination autorisés.
- AnalysisComplianceRule3(DetectionEntity, Packet): Vériequelesentités de zone C n' eectuent pas un balayage réseau,envoi ent vers un nombre limité d'adresse SIP.
- AnalysisComplianceRule4(DetectionEntity, Packet): Vériequelesentités ne dépassent pas lenombre maximum des requêtes INVITE et REGISTER.
- AnalysisComplianceRule5(DetectionEntity, Packet): Vériequ'une entité n'émet pas de requêtes interdites pour son typ e d'entité.
- AnalysisComplianceRule6(DetectionEntity, Packet): Vérieque l'identité revendiquée par l'entité corresp ond bien à l'entité enregistrée.
- AnalysisComplianceRule7(DetectionEntity, Packet): Vérie quele message SIP émis est autorisé p our l'entité émettrice considérée.
- AnalysisComplianceRule8(DetectionEntity,Packet): Pour les entités de typ e enregistrable,et p our les requê te s REGISTER,vérie que la fréquence de rafraîchissement est conforme avec ce qui est attendu pour le typ e/sous-typ e correspondant à l'entité émettrice.

ProlingEntity

Au niveau de cetteclasse, il est implémenté huitrègles de caractérisation du typ e d'entité, qui ont pour but de mettre à jour les compteurs de ressemblance dans la base de contexte par entité an de pouvoir caractériser les entités existantes et déterminer leurs typ es/sous-typ es. Il est implémenté aussi une métho de de détermination de l'ensemble des règles à exécuter selon des contraintes de temps de traitement aecté, compteurs de ressemblance et nombrede paquets analysés.

AnalysisNonCompiance

Nous avons implémenté dans cette classequatre règles d'analysede non conformité ainsi que le critère d'invo cation de ces règles quidép end des résultats des règles d'analyse de conformité

Learning

Détermine les règle s d'apprentissage à exécuteren fo nc tion de temps de traitement aecté et du typ e/sous-typ e d'entité. Il est implémenté aussi quatre rè gles d'apprentissage quiont pour but de mettre à jour les paramètres d'apprentissage des entités dans la base pour les entités de zone S et zone C.

LearningAgregation

Cetteclasse estimplémentée sous forme de thread qui se déclenche de façon p ério dique chaque semaine pour agréger les paramètres mis à jour par la classe d'apprentissage et mettre à jour la base de caractérisation de type d'entité.

Filtering

Cette classe est invo quée par la classe d'analyse de non conformité si cette dernière détecte la présence d'un comp ortement qui menace la sécurité de réseau, elle se charge de ltrer les entités qui manifestent ce comp ortement malveillant.

IHM

La classe IHM modélise l'interface de graphique de notre pro jet, elle est construite à l'aide de la librairie Swing, cette classe se comp ose de plusieurs threads qui accomplissent l'exécution parallèle de plusieurs tâches comme

par exemple l'exécutio n du noyau de l'applica ti on et la consultation de l'historique et desinformationsdes entitéscapturées.

5.2.3 Diagrammes deséquences

Les diagrammes de séquences servent à décrire l'asp ect dynamique des diérents ob jets qui constituent notre système.

Apprentissage d'une entité dénie

La gure 5.6illustre lescénario decaractérisationd'une entité:

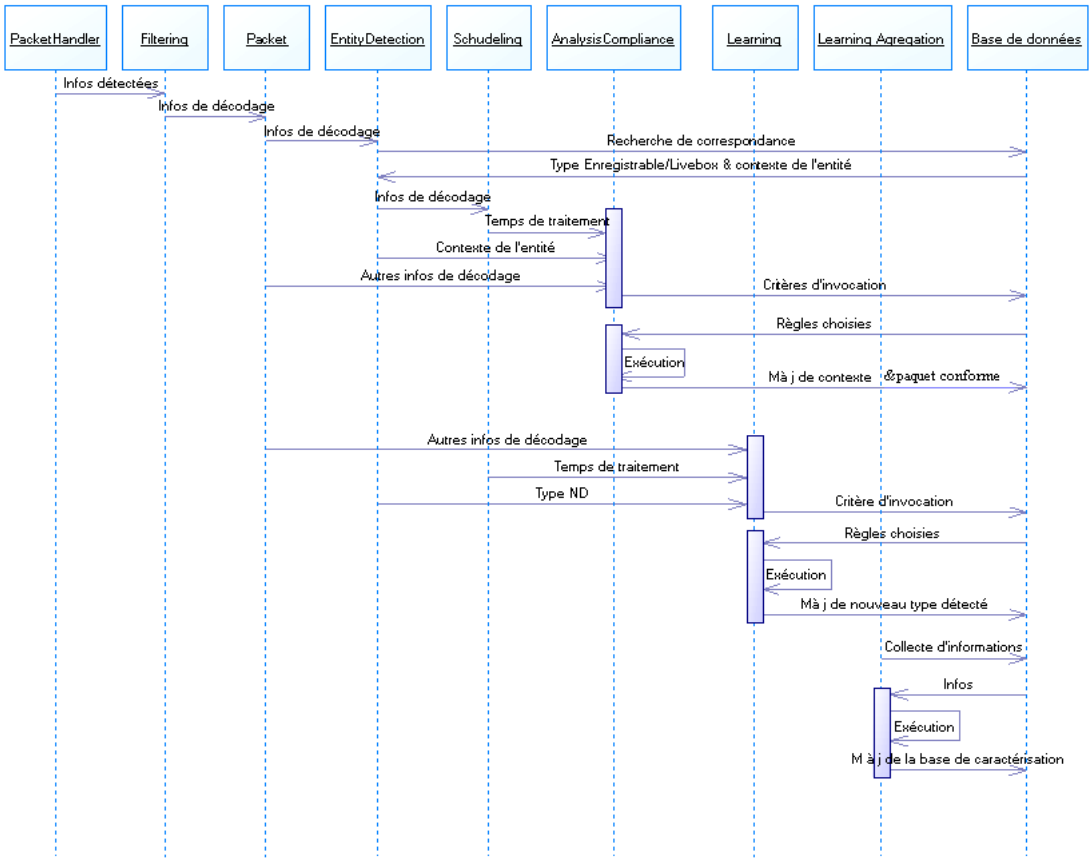

Fig. 5.5 Diagramme de sé quences p our l'apprentissage

La fonction PaketHand ler, en recevant le trac entrant, extrait les informations utiles pour la déterminaison du typ e de l'entité qui a envoyé ce trac, ces informatio ns sont la mises dans l'entité Packet.

Les informations extraites sont passées par la suite àla fonction Filtering qui, selon l'entité émettrice, décide s'il est ne céssaire de ltrer le trac correspondant. Puis, les informations de déco dage sont transférées à la fonction EntityDetection qui balaye la base de données pour la recherche du type d'entité et du contexte asso cié. Cette entité détermine que l'entité est dénie de typ e Enregistrable et de sous type Livebox.
Après l'identication de l'entité, les informations de déco dage,le contexte de l'entité et d'autres informations de déco dage sont passées à la fonction deScheduling qui, en fonction de ces entrées, aecte à chaque fonction haut niveau le tempsde traitement approprié.
La fonction AnalysisCompliance , selon son temps de traitement, le contexte de l'entité et d'autres informations de déco dage,détermine les règlesà appliquer, les applique, puis elle met à jour le contexte de l'entité suivant les résultats des règles.
De même p our la fonction Learning, elle récup ère les règles à appliquer en fonction dutemps de traitement qui lui est aecté, le contexte del'entité et d'autres informations de déco dage,applique ces règles et met à jour le contextede l'entité dansla base.
La fonc ti on LearningAgregation,collecte les informations du contexte p our plusieurs entités, eectue des calculs p our agréger le s informations, pui s met à jour la base de caractérisation de typ e d'entité avec ces informations. La gure 5.5 présente le diagramme de sé que nce p our le scénario d'apprentissage des caractéristique s d'une entité dénie.

Caractérisation d'une entité
La gure 5.6présentele diagrammedeséquence pourlescénario decaractérisationd'une entité:

Après reception du trac par PacketHand ler et la construction de l'ob jet Packet contenant toutes les informations nécessaires pour le traitement du paquet, si l'entité de ltrage ne reçoit pa s l'ordre de ltrer le trac provenant de l'entité éme ttrice, le paquetest passé à lafonction de détermination du typ e d'entité qui retourne que l'entité émettrice est non dénie.
La fonction Scheduling aecte à chaque fonctio n haut niveau son temps de traitement.
Aprèsanalyse deconformité lafonction AnalysisComliance retourneque le paquet est conforme.
Dans ce cas on passe à la caractérisation de typ e de cette entité: après avoir invo quer les règles appropriées l'entité Proling détermine le typ e et le sous-typ e de l'entité et met à jour la base de données.

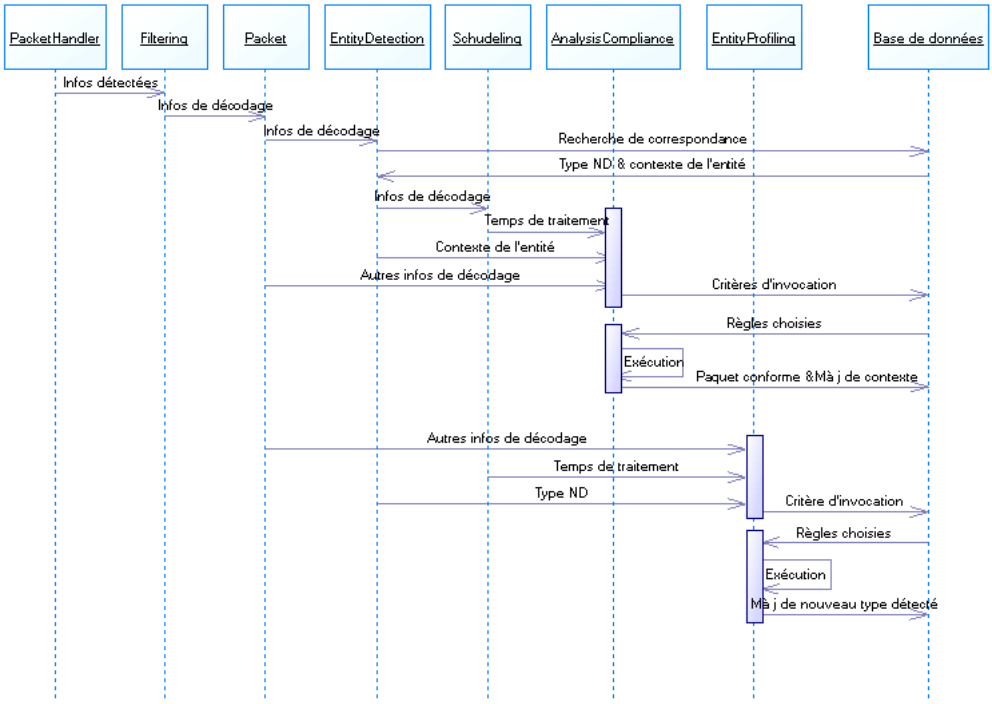

Fig. 5.6 Diagramme de séquence pour la caratérisation d'une entité

Filtrage d'une entité

La gure 5.7 décrit le cas de ltrage d'une entité qui envoie des paquets non conformes:

Les informations sont extraites du paquet par la fonction PacketHand ler.

Lafonction DetectionEntity retournequel'entitéémettriceestnondénie.

Ensuite, la fonctionScheduling aecte le temps de traitement de chaque fonction haut nive au.

L'analyse de conformité ab outit à un résultat négatif ce que signie que le pa quet traité est non conforme et donc qu'il présente un comp ortement mailveillant.

Pour mieux lo caliser ce comp ortement, le paquet est passé à l'analyse de non conformité qui, après avoir invo qué les règles de non conformité appropriées, envoie un ordre à l'entité Filtering p our blo quer le trac provenant de cette entité.

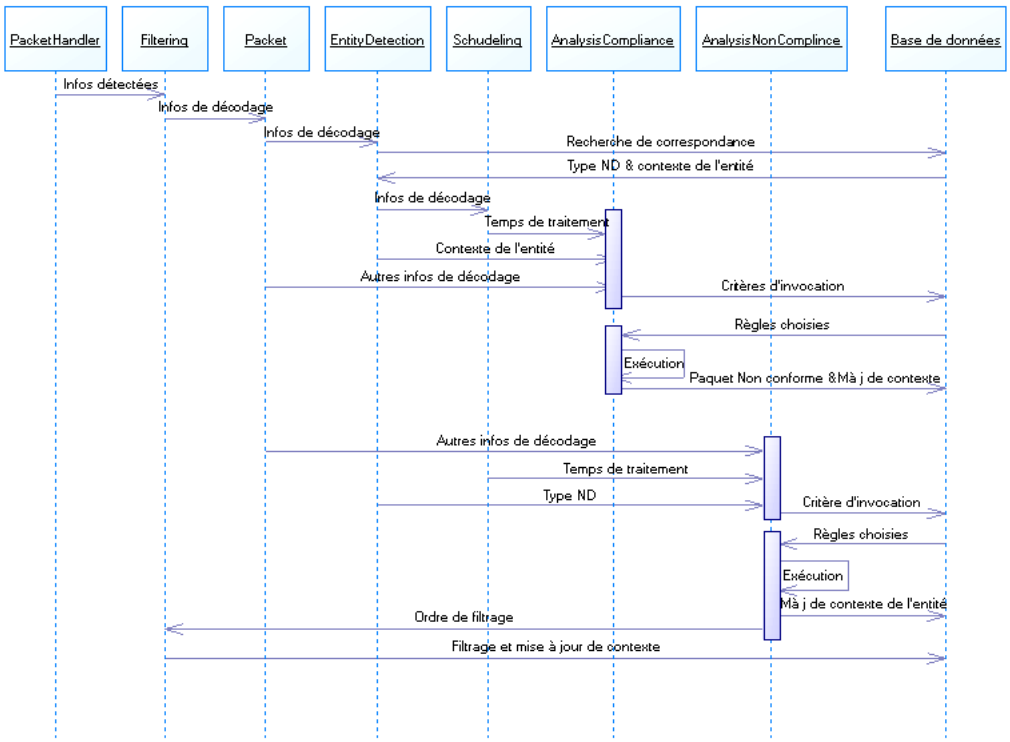

Fig. 5.7 Diagramme de sé quence p our le ltrage d'une e ntité

Conclusion

Après avoir détaillé la conception adopté e p our la réalisation de notre application, nous décrivonsdans le chapitre suivant l'implémentation de ce travail ainsi que les problèmesrencontrés.

Chapitre6

Réalisation

Intro duction

Ce chapitre constitue le dernier volet de ce rapp ort, il a pour but d'exposer letravail réalisé. Ileststructuré comme suit:

- Environnementde travail.
- Tests réalisés.
- Travail réalisé.
- Dicultés renc ontrées.
- Chronogrammede travail.
- App orts du stage.

6.1 Environnementde travail

6.1.1 Environnement matériel

Cette section décrit la plateforme mise en o euvre p our le test du pro cédé DCM, l'architecture organique de cette plateforme est illustrée par la gure 6.1. Elle se comp ose des éléments suivants:

- Proxy Op enSER: remplit les fonctionsdeRegistraret Proxy SIPet route les app els entre les 3 plaques (VoIP1,VoIP2, GSM[1]/RTC [2]) et les terminaux additionnels.
- Terminaux VoIP (ACT P170) p our le trac régulier ponctuel.
- Des softphones pour générer le trac de fond et d'attaque.
- UnPc Dell,Centrino1.74 Ghz,2Go deRAM.

[1] Global System for Mobile

[2] Réseau Téléphonique Commuté

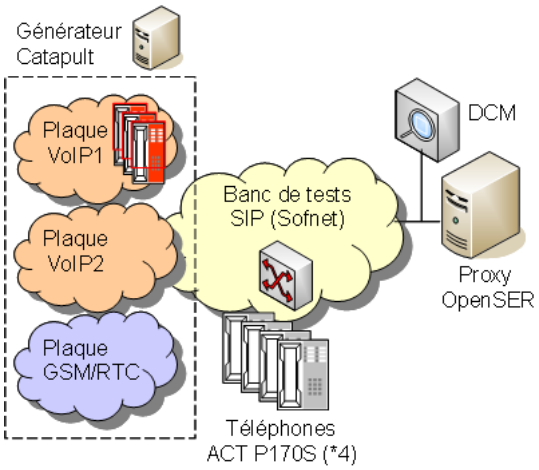

Fig. 6.1 Architecturedela plateforme

6.1.2 Environnement logiciel

- Eclipse SDK 3.2 : p our le développ ement de l'application. C'est un outil de programmation du langage JAVA que nous avons choisi étant donné sa p ortabilité qui s'annonce aujourd'hui comme un facteur ma jeur dans l'évaluation des logiciels. Le nombre de lignes de code développ ées par cet outil au coursde cestageest 10050.
- Mysql: Nousavonschoisicet outilsétantdonné sonarchitecturelogicielle qui le rend extrêmement rapide et facile à personaliser.Les pricipauxavantagesdeMysql sontsarapidité, sarobustesse et safacilité d'administration. Un autre avantage ma jeur de Mysql est sa documentation très complète et bien construite.
- Serveur Apache: pour la réalisation d'interface en PHP représentant desdonnées de labase, suivant la demandede l'administrateur.
- Wireshark: p our la capture des pa quets entrants à travers l'interface réseau et génération les chiers PDML.
- Power AMC : p our la modélisation UML de sp écications et la conception du pro jet.
- SVN : est un système de gestion de version qui assure aussi la sécurité des documents (Sauvegarde régulière de tout le pro jet sur un serveur dédié).
- Doxygen : pour générer la documentation de pro jet en format HTML et format PDF.
- API SAX: basée surdes déclencheurs(évènements/actions)qui se déclenchent sur c ertaines bal ises, cette API est adaptée aux applications qui extraient de l'information d'un do cument. Nous avons utilisé cette

SAX pour le parsing des chier PDML contenant le trac entrant.

- API log4j[3] : pour générer les journaux (.log) de l'application, ses journaux décrivent le comp ortement du pro cédé.Pour mieux classer les informations dans les chiers *. log, cinq niveaux de journalisation sont utilisés:
  - DEBUG:description dufonctionnementnormal desdonnées.
  - INFO : un évènement nonmalveillantest survenu surlesystème (par exemple la détection d'unenouvelle entité,l'agrégation des informations et lamise à jourlesbases) sera loggué auniveauINFO.
  - WARN:toutlesmessages générésparlesrèglesd'analyse deconformité qui ont donné des résultats négatifs sontloggés auniveau WARN.
  - ERROR: tout les messages générés par les fonctions d'anal yse de non conformité sontlogguésau niveau ERROR.
  - FATAL: lorsqu'uneentité est ltrée, l'information corresp ondante est logguée au niveauFATAL.

6.2 Tests Réalisés

Deux typ es de trac de test sont générés sur la plateforme présenté par la gure 6.1:

- Letracde fond: enregistrementdesterminauxVoIPdesplaques1 et 2 et émission/réception d'app els entre les plaques 1 et 2 et GSM/RTC.
- Le trac unitaire : trac généré depui s certains terminaux de la pla que VoIP1 et simulant des termi naux malveillans ou mal congurés, nous avons adopté 5 scripts de test développ ée sur Catapult, chacun entre eux simule un typ e d'attaque:
  - Script 1: terminaux mal congurés qui ne parviennent pas à s'enregistrer du fait de mauvais identiants d'authentication et qui renouvellentrégulièrement leurs requêtes.
  - Script 2: terminaux qui s'enregistrent et essaient d'établir des appels sous des identités usurp ées
  - Script 3: terminaux qui s'enregistrent et font du balayage sur une plagede numérosVoIP via desrequêtes INVITE.
  - Script 4: terminaux qui envoient des re quêtes non autorisées par rapp ort à leurs typ es.
  - Script 5: terminaux qui envoient des requêtes vers des adresse s ou des p orts non autorisés de la zone de s serveurs.

[3] Is a java-based logging ut ility

6.3 Interfaces développées

6.3.1 Interface Supervision

L'administrateur du système sup ervise le procédé à travers cette interface. Cette dernière, développée à l'aide de Swing, comp orte quatre onglets:

Sup ervision

Comme présenté par la gure 6.2, on peut à travers cette interfacesuivre, en temps de réel, l'état de système: le nombre des entités déte ctés¸leurs typ es, leur comp ortements, le nombre de paquets analysés, le taux d'analyse, le temps de traitement, le taux d'utilisation des ressources (pro cesseur et mémoire).

Fig. 6.2 Supervision

Conguration

Cette interface nous p ermet de congurer l'application: vider la base, choisir l'entrée de système, saisir quelques valeurs de seuils utiles pour le fonctionnement et le taux de rafraîchi ssement de l'application.

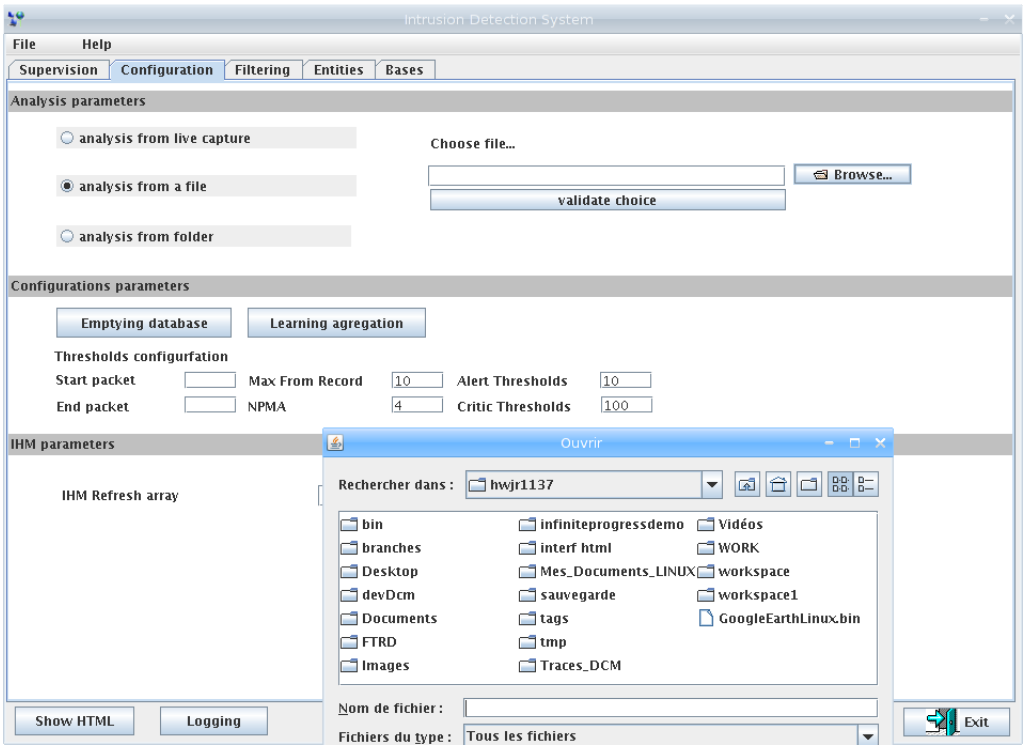

Fig. 6.3 Conguration

Filternig

Cette interface, présentée par lagure 6.4nouspermetde consulterla listedes entitésltréeset desupprimer manuellementce ltrage.

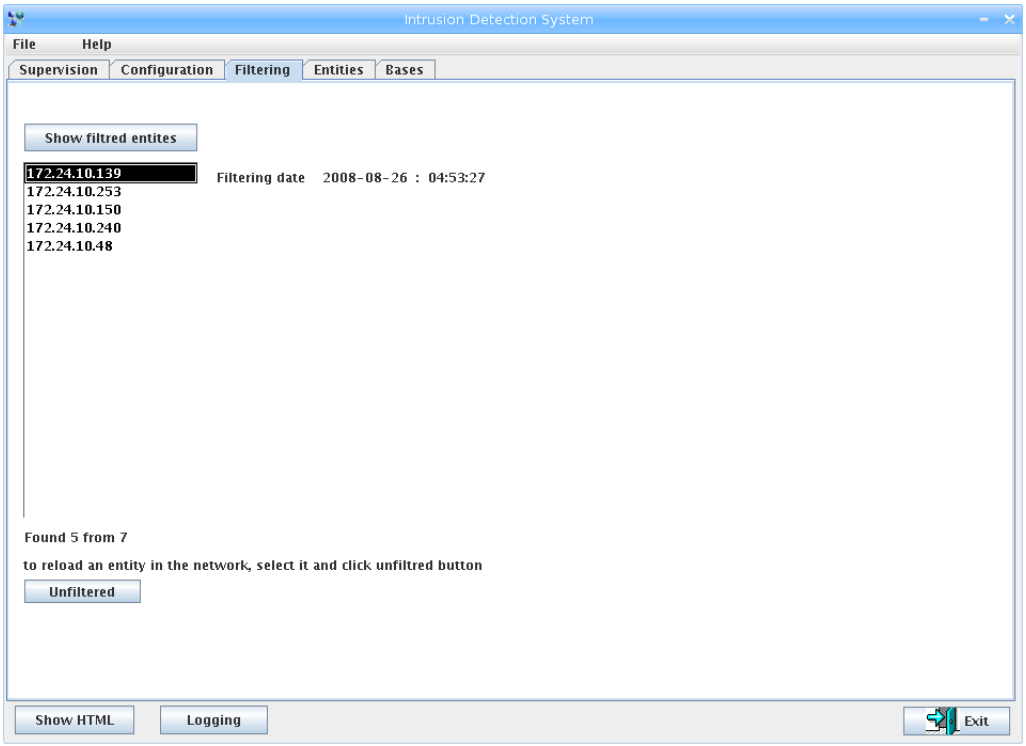

Fig. 6.4 Filtrage

L'administrateur peut aussi supprimer les entités ltrées.

Entities

Au niveau de cette interface, pré sentée par le gure6.5,on peutéectuer des recherche concernant les entités enregistrées dans la base selon les critè res que l'on sélectionne. En cliquant sur l'entité une interface en php s'ouvre pour acher l'historique decetteentité.

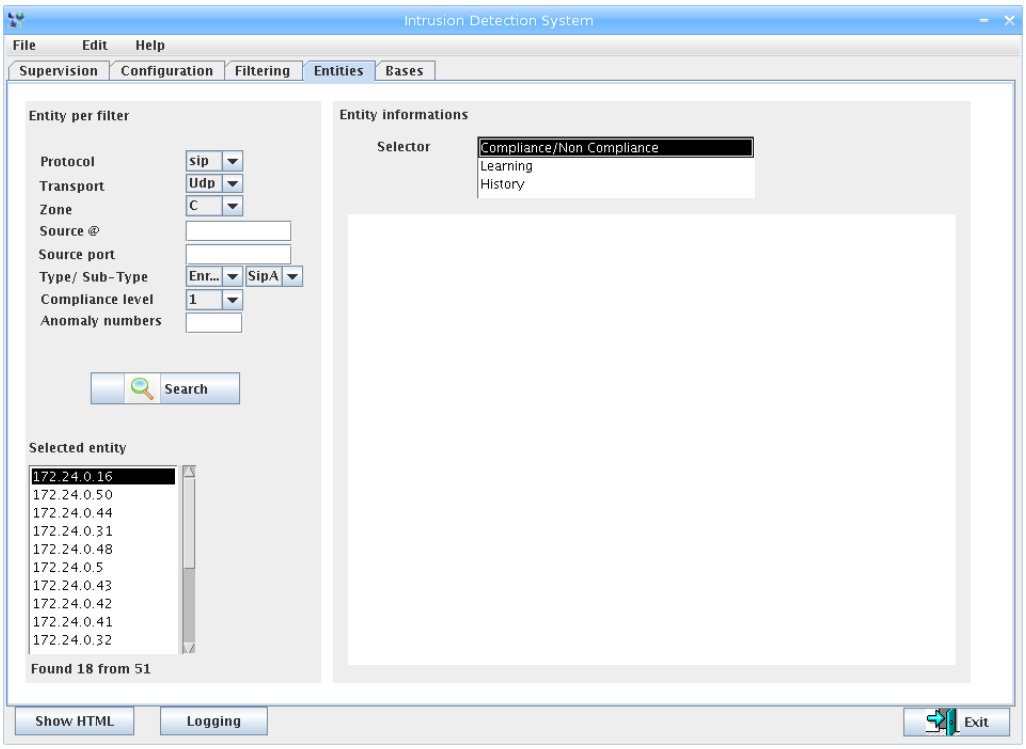

Fig. 6.5 Entities

6.3.2 Interface de suivi

Cette interface permet de consulter l'historique de chaque entité.

Interface PHP Cette interface, développée en php, nous présente l'historique des entités enregistréesdans la base de données,commele montre la gure 6.6 cethistorique est divisé en quatre classes: Détéction, Comp otementsmalveillants,Alertes et Filtrage.

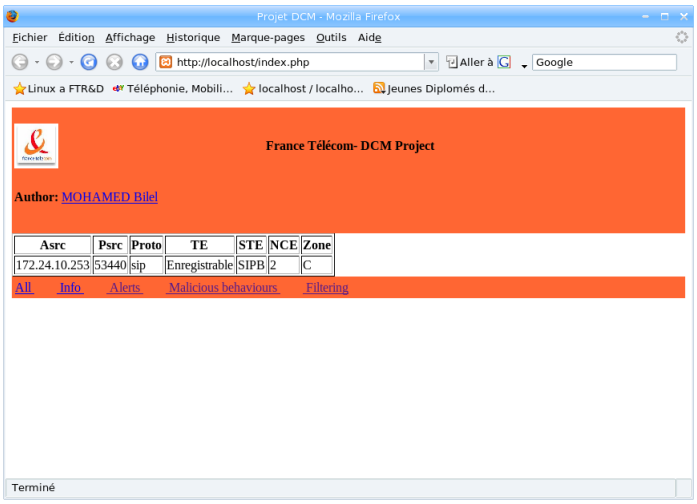

Fig. 6.6 Page d'accueil

Détection Cette interface ache le type, le sous typ e, le niveau de conformité, la zone de l'enti té détectée ainsi que l'heure de détection.

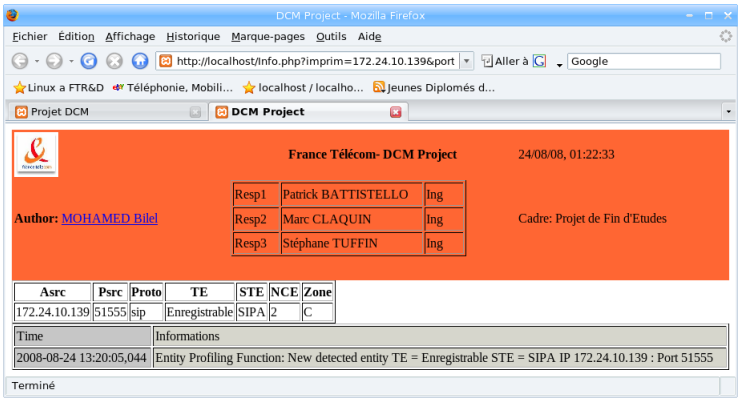

Fig. 6.7 Detectiond'entité

Comp ortements malveillants Achage de l'heure de détec ti on de comp ortement, le numéro du paquet présentant ce comp ortement, ainsi que le typ e de comp ortement malveillant.

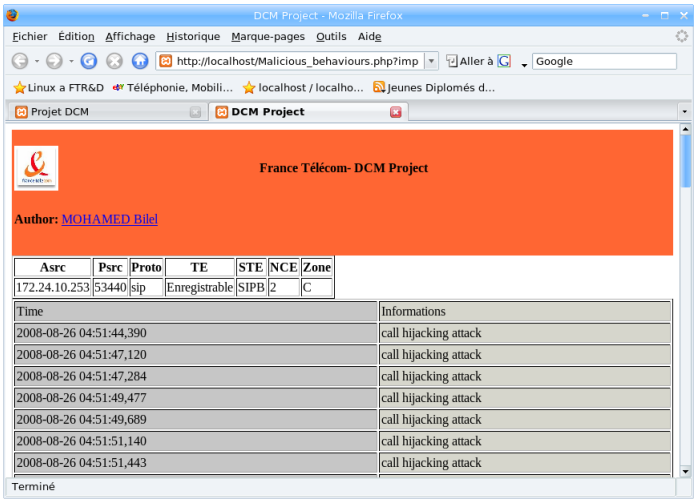

Fig. 6.8 Entité détectée

Alertes Achage de l'heure de détection, du numéro de paquet, et du typ e d'alerte.

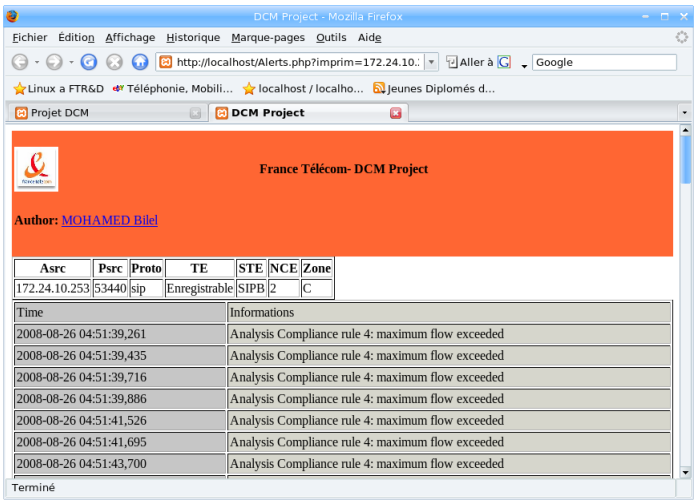

Fig. 6.9 Alerte

Filtrage Achagede l'heuredeltrage, du numéro de paquet qui a causé ce ltrage, ainsi que de larègle de non conformité qui a ltré cette entité.

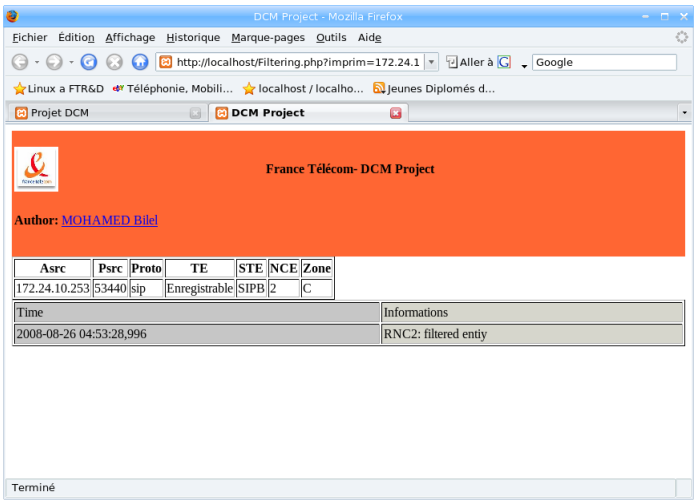

Fig. 6.10 Comportement malveillant

Fichier de journalisation la gure 6.11présentelechierde journalisationdécrivantle fonctionnement de système:

```
08-23 16:59:36,018 DEBUG  - Entity Detection Function: From Zone C : TE = ND : NCE = 1
08-23 16:59:36,018 DEBUG  - Nbr 179 :  Length  :461  IP 172.24.0.14 :  Port 5060 :  Msg type RESPONSE 180
08-23 16:59:36,018 DEBUG  - [172.24.0.14:5060]From sip:33910007918@orange.fr:5060  :  To sip:33910001091@o
08-23 16:59:36,018 DEBUG  - [172.24.0.14:5060]Via SIP/2.0/UDP  172.24.100.12:5060 ;branch=whuWNWmZoQ5cUqRDH
08-23 16:59:36,018 DEBUG  - Scheduling Function: Compliance TT = 3 ; Caracterisation TT = 3 ; Learning TT =
08-23 16:59:36,042 DEBUG  - [172.24.0.14:5060]Analysis compliance Function: Rules selected: 1,2,3,4,5
08-23 16:59:36,042 DEBUG  - [172.24.0.14:5060]Analysis Compliance rule 1: ok
08-23 16:59:36,043 DEBUG  - [172.24.0.14:5060]Analysis Compliance rule 2: ok
08-23 16:59:36,044 DEBUG  - [172.24.0.14:5060]Analysis Compliance rule 3: ok
08-23 16:59:36,044 DEBUG  - [172.24.0.14:5060]Analysis Compliance rule 5: ok
08-23 16:59:36,074 DEBUG  - [172.24.0.14:5060]Entity Profiling Function: Rules Selected: 1,2,3,4,5
08-23 16:59:36,074 DEBUG  - [172.24.0.14:5060]Profiling rule 2: ok
08-23 16:59:36,074 DEBUG  - [172.24.0.14:5060]profiling rule 3: ok
08-23 16:59:36,074 WARN   - profiling rule 4: missing User-Agent field
08-23 16:59:36,075 DEBUG  - [172.24.0.14:5060]profiling rule 5: ok
08-23 16:59:36,098 DEBUG  - ----------------Next packet-----------------
08-23 16:59:36,114 DEBUG  - Entity Detection Function: From Zone C : TE = ND : NCE = 1
08-23 16:59:36,114 DEBUG  - Nbr 180 :  Length  :430  IP 172.24.0.17 :  Port 5060 :  Msg type REQUEST REGIST
08-23 16:59:36,114 DEBUG  - [172.24.0.17:5060]From sip:33910004870@orange.fr:5060  :  To sip:33910004870@o
08-23 16:59:36,114 DEBUG  - [172.24.0.17:5060]Via SIP/2.0/UDP  172.24.0.17:5060 ;branch=ecm4Sl7pKeEFqxPn5qM
3910004870@172.24.0.17:5060
08-23 16:59:36,114 DEBUG  - Scheduling Function: Compliance TT = 3 ; Caracterisation TT = 3 ; Learning TT =
08-23 16:59:36,128 DEBUG  - [172.24.0.17:5060]Analysis compliance Function: Rules selected: 1,2,3,4,5
08-23 16:59:36,128 DEBUG  - [172.24.0.17:5060]Analysis Compliance rule 1: ok
08-23 16:59:36,130 DEBUG  - [172.24.0.17:5060]Analysis Compliance rule 2: ok
```

Fig. 6.11 Fichierdejournalisation

6.4 Dicultés rencontrées

Au cours de réalisation du pro jet, nous avons rencontrés lesdicultés suivantes:

- Nous n'avons pas pu implémenter l'invo cation des règles qu'on va appliquer aux paquets de façon dynamique : en eet, ces règles sont tributaires de plusieurs paramètres dont les plagesde valeurs sont innis, or p our p ouvoir implémenter de façon dynamique, il est nécessai re que l'ensemble des combi naisons p ossibles des paramètres d'entrée soit discret et borné.
- Certaines tâches nécessitent la p ossession des droits ro ot sur l'ordinateur, or ce n'est pas le cas, donc il a fallu que nous implémentions quelques scripts p our nous p ermettre de p ossé der ces droits.
- Dans le rép ertoire de travail "workspace", lors de création d'un projet, Eclipseconstruit automatiquement un dossier intitulé ".metadata" dans lequel il sauvegarde les journaux depuis la construction du pro jet. Après quatre mois de travail, nous avons rencontré un problème de plantage d'Ecl ipse,et la solution était de réi ni ti aliser le dossier ".metadata".

- Lors de l'impléme ntation de l'interface PHP, nous avons rencontré un problème d'intégration java-PHP, et la soluti on était de mettre en place un p ont java/PHP à l'aide des chiers intermédi aires.
- Ayant acquis une b onne connaissance de l'environnement de développ e-ment Eclipse, nous n'avons pas rencontré de problème particulierlors du développ ement du prototyp e, la seule diculté était d'intégrer wi-reshark, SVN et Doxygène avec Eclipse pour avoir un environnement de travail homogène.

6.5 Chronogrammede travail

Le stage s'est déroulé sur une pério de de cinq mois en entreprise, précédée d'une phase de do cumentationll a été divisé en plusi eurs tâches comme le montre le graphique 6.12:

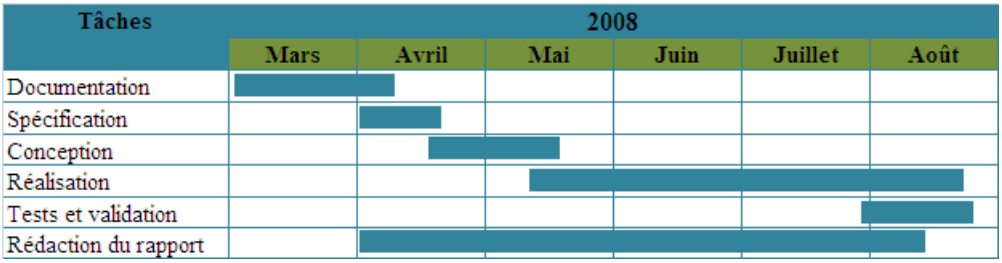

Fig. 6.12 Chronogrammedetravail

À la n du stage, nous avons éectuéunepréseentationau sein deFrance Télé-com R&D , dans laquelle, nous avons présenté notre conception et réalisation tout au longde notre travail.

6.6 Apports du stage

La n de ce chapitre est l'o ccasion d'énumérer les app orts de ce stage:

Point de vue technique

Ce stage fut très riche sur le plan techni que car p our les b esoins de nos missions:

- Nous avons pu découvrir le proto cole SIP et étudier de près sa structure généraleet ses applications.

- Nousnoussommes formésdanslasécuritédes réseaux,enconnaissant des typ es d'attaques et comp ortements malveillants et sachant comment y remé dier.
- Nous avons consolidé les connaissances en programmation ori enté objet, que nous avonsacquises encours,en implémentant un prototype fonctionnelde sécurité de laVoIP.

Une p ério de d'enrichissements

D'un p oint de vue personnel, le bilan de ces cinq mois de stage est largement positif. Cette pério de a été riche en enseignements et illustre particulièrement bien la vie professionnel le.

Grande autonomie pour la gestion du pro jet

Avant tout, il est imp ortant de noter qu'une grande lib erté a été laissée danslagestiondes diérentstravaux. Ainsi,ilfallaitse montrerautonome, organisé et créatif pour mener à bien les diérentes tâches. Il était tout à fait passionnant d'avoir le champ libre p our mettre en place toutes le s structures voulues, notamment la réalisation du prototyp e. Les prop ositions faites ont été discutées et ensuite validées par mon resp onsable. Il a encouragé chacune des initiatives prop osées et a suggéré des améliorations.

L'imp ortance de la communication et du suivi

La communication avec le resp onsable de stage est indisp ensable. Pour cette rai so n, des réunions d'avancement du pro jet ont été eectuées lors de plusieurs réunions accomplies au début du stage; elles ont pour vo cation de présenter le travail accompli durant la p ério de écoulée et de préciser son avancé . L'utilité de ces réunions ne fait aucun doute p our une b onne gestion du pro jet.

Conclusion

Au cours de ce chapitre, nous avons évo qué les asp ects qui sont en relation avec la réali sation et les tests de l'application. Ensuite, nous avons montré des ap erçus d'écran illustrant le résultat d'exécution de l'application et montrantson interface graphique. Puis,nous avons énuméré quelques problèmes rencontrés lors de l'implémentation du prototyp e. Enn, nous avons présenté le chronogramme et résumé les app orts de ce stage.

Conclusion et p ersp ectives

La téléphonie IP a visiblement de grands joursdevant elle, même s'il est évident qu'elle a encore à gagner en maturité. La voix sur IP doit faire face à deux grands problèmes d'actualités: la qualité de service et la sécurité, cette dernière doit, pour résumer, consister en la protection des proto coles Vol P, la protection des systèmes d'exploitation sur lesquels les solutions VoIP sont basées¸laprotection des couches réseauxet laprotection de la bande passante dédiée à la voix sur leréseau.

Dans ce cadre, un prototyp e d'IDS/IPS destiné aux réseaux VoIP a été accompli lors de notre travail. L'IDS/IPS prop osé ici est un système en coupure apte à détecter les comp ortements malveillants basés sur les vulnérabilités du proto cole SIP et de les blo quer si nécessaire.

La simulation des diérentsscénarios de testa prouvéque l'IDS/IPS réalisé peut détecter des diérentes sortes d'attaques, mais il ne serait toutefois pas capable de détecter toutes les attaque s contre un système de la VoIP sans l'implémentation de l'ensemble de toutes les règles d'analyse possibles. Maheureusement,parmanque detemps, cettedernièren'a pas pu êtreréalisée et constituerait une suite intéressante à ce travai l.
Nous ne manquerons pas de souligner que le pro jet reste extensible pour répondre à de nouveaux besoins comme l'a jout de la contrainte des réponses en temps réel.

Enn, cette conclusion est l'o ccasion de faire le bilan de la formation dispensée à l'école.Cette formation ne peut pas être en parfaite adéquation avec chaque stage. Cep endant elle nous a p ermis d'acquérir susamment de connaissances p our ne pas arrive r désarmé ni p our nos stages en entreprise, ni p our notre future vie professionnelle. Les pro jets réalisés en cours donnent une bonne vision du travail en équipe et de ce qu'est un pro jet industriel, avec ses impératifs.

Bibliographie

[Har02] Hardy DANIEL, Gay MALLEUS, Jeanno el MEREUR. Réseaux Internet Téléphonie Multimédia, convergances etcomplémentarités.1ère édition, 2002.

[The06] Pe ter THERMOS. Securing VoIP Networks Threats, Vulnérabilities and Counmeasures. 2006.

[Gon03] CamarilloGONZALO.SIP DEMYSTIDIED.2003.

[Oua08] Laurant OUAKIL, Guy PUJOLE. Téléphonie sur IP. 2è me édition.

[Mem08] PatrickBATTISTELLO,StéphaneTUFFIN.Détection de Comprtements Malveil lants. 2007.

Nétographie

http ://forum.debian-fr.org/viewtopic.php ?f=3&t=11928 : 14/05/2008.
http ://www.interp c.fr/mapage/billaud/index.htm : 14/05/2008.
http ://fr.wikip edia.org/wiki/SystC3A8me_de_gestion_de_versions : 16/05/2008.
http ://www.eteks.com/coursjava/threads.html : 22/05/2008.
http ://www.voip-info.org: 15/06/2008

ANNEXE A :l'API Log4j

Tout au long de la réalisation del'application, nous avons utilisé l' API Log4j pour journaliser la sortie.
Log4j est une API de journalisation très répandue dans le monde Java. Il s'agit d'un système op ensourece extensible qui permet de logger et débugger les applications java. Pour ce pro jet, nous nous sommes appuyé sur la version 1.2.11.

Princip es généraux

Logger

Le Logger est l'entité de base pour eectuer la journalisation, il est mis en o euvre par le biais de la cla sse org.apache.log4j.L ogger. L'obtention d'une instance de Logger se fait en app elant la métho de statique Logger.getLogger. Log4j gère les Loggers de façon hi érarchique, c'est à dire qu'un Logger p eut avoirdesenfants et desparents.

Nivea u de journalisation

L'API Log4j dénit 5 niveaux de logging décrites ci-dessous par gravité décroissante:

- FATAL: utilisé pour journaliser une erreur sérieuse p ouvant menerà l'arrêt de l'application.
- ERROR : utilisé p our journaliser une erreur qui n'emp êche cependant pas l'application de fonctionner.
- WARN: utilisé pour journaliser un avertissement, il peut s'agir par exemple d'une incohérence dans la conguration, l' appl ication p eut continuer àfonctionner mais pasforcément de lafaçon attendue.
- INFO : utili sé p our journaliser des messages informatifs.
- DEBUG : utilisé pour générer des messages utiles au déb ogage.

App enders

Les App enders, représentés par l'interface org.apache.log4j.App ender, sont l'outil utili sé par log4j p our enregistrer les événements de journalisation. Le rôle de l'Appender est de ltrer les messages et de déterminer le mo de de sortie des messagesselon l'implémentation.
Log4j vient avec une série d'App enders qu'il est utile de décrire:

- org.apache.log4j.jdbc.JDBCApp ender:eectue la jo urnali sation ve rs unebase de données.
- org.apache.log4j.lf5.LF5App ender : journalise les événements vers une console basée sur Swing, celle-ci p ermet de trier ou de ltre r les événements.
- org.apache.log4j.varia.NullApp ender : n'eectue aucune journalisation.
- org.apache.log4j.net.SMTPApp ender : envoie un email lorsque certains événements surviennent.
- org.apache.log4j.net.So cketApp ender:envoie lesévénements de journalisationversun serveurde journalisation.
- org.apache.log4j.net.TelnetApp ender:journalise les événe ments vers un so cket auquel on peut se connecter via telnet.
- org.apache.log4j.ConsoleApp endereectuela journalisationvers la console.
- org.apache.log4j.FileApp ender : journalise dans un chier.
- org.apache.log4j.DailyRollingFileApp ender : journalise dans un chier qui tourne régulièrement.
- org.apache.log4j.RollingFileApp ender : journalise dans un chier, celuici est renommélorsqu'il atteint une certaine taille et la journalisation reprend dans un nouveau chier, c'est cet App ender que nous avons utilisé au cours de ce pro jet.

Layouts

Les Layouts dénissent le format du message. On peut par exmple avoir la date, l'heure, le nom de la classequi envoie le message et le niveau de logging au début de chaque message Ils sont utilisés conjointement avec les App enders.
LesLayouts fournis parlog4jsont les suivants:

- org.apache.log4j.SimpleLayout : comme son nom l'indique, ils'agit du Layoutle plus simple, les événem ents journalisés ont le format : Niveau - Message[Retour à la ligne].
- org.apache.log4j.PatternLayo ut:layout le plus exible, le format du message est sp écié par un motif (pattern) comp osé de texte et de

séquences d'échapp ement indiquant les informations à acher.

- org.apache.log4j.XMLLayout: formate lesdonnées de l'événement de journalisation en XML.
- org.apache.log4j.HTMLLayout : les événements sont journalisé s au format HTML.

ANNEXES B: l'API SAX

Fonctionnement de SAX

SAX[4] est une API générale pour la lecture d'un ux XML. Il existe des implémentations de ce tte API dans beaucoup de langages car XML s'est largement imp osé aujourd'hui dans le monde du logiciel p our l'échange d'informations.
Au cours de la réalisation de notre pro jet, nous avons utilisé l'API SAX pour l'analyse de s chiers de sortie de wireshark sous format XML.
Pour comm encer, l'applic ation crée une instance du parseur à partir d'une fabrique de parseurs (javax.xml .parsers.SAXParserFactory).
Ce parseur explore le do cument XML grâce à un lecteur (XMLReader). Ce dernier contient plusieurs gestionnaires(ou handlers). Ce sont ces diérents gestionnaires qui sont chargés du traitement des événements(dans ce pro jet: arrivée d'un nouveau paquet) lors du parsing. Voici les quatre principaux typ es de handlers (interfaces du package org.xml.sax):

- Gestionnaire de Contenu: Le ContentHandler est chargé des évé nements comme le début ou la n du do cument, l'ouverture ou a fermeture de balise souencore la lecture de caractères.
- Gestionnaire d'Erreurs : Le ErrorHandler traite les trois typ es d'erreurs possibles lors du parsing : les erreurs simples, les erreurs fatales et les warnings.
- Gestionnaire de DTD: Le DTDHandler (Do cument Typ e Denition) gère les événements relatifs aux DTD.
- Gestionnaire d'entités externes: L'EntityResolver est chargé de gérer les entités externes, enfournissant une InputSource adéquate.

Gestion les erreur durant le parsing

Au niveau du do cument XML, il existe deux typ es d'erreurs p ossibles:

[4] SIMPLE API for XML

- Le do cument peut être non valide. Dans cecas, le do cument n'ob éit pas à la DTD ou au schéma qu'on lui a imp osé.
- Le do cument p eut être mal formé. Dans ce cas, il y a simplement une erreur par rapp ort au standard XML lui même. Par exemple, des balises mal fermée s ou se chevauchant.

Par contre, au niveau du parseur SAX, il exi ste trois niveaux d'erreurs. Ces trois niveaux d'erreurs sont représentées au niveaudu Gestionnaired'Erreurs (ErrorHandler):

- Erreur fatale: Cette erreur ne p eut être récup érée.C'estle caspar exemple pour un do cument mal formé. Après ce type d'erreur, le parseur SAX arrête son travail.
- Erreur: Cette erreur p eut être récup éréeç'est à dire que le parseur SAX p eut continuer à traiter le reste du do cument XML. Ce genre d'erreur peut se produire lors d'une violation d'une contrainte imp osée par la DTDoule schéma.
- Warning: C'est unsimple avertissement. Après celà, leparseur SAX continue le parsing du do cument.

ANNEXE C :Plan qualité-logiciel

Nous avons intro duit cette partie d'annexe car, malgré la simplicité de son continue, elle a un grand eet pour l'avancement du pro jet et elle est très utile p our gérer le dévelopment des logiciels.
Cette partie décrit les besoins qualité-logiciel du pro jet:
L'anglais doit être utilisé pour tout les noms de chiers, les noms de variables, les commentaires, les commit . .Ceci à un sens dans le but de:

a- Industrialisation de logiciel developpé au cours de pro jet.
b- Vente de logiciel developpé au cours du pro jet
c- L'anglais est la langue de coop ération de la plupart des entreprises de sous-traitance.

Règles générales de dévelopment

Convention de nommage:
Tout lesnoms de variables sont des motscomplets, aucune abréviation n'est acceptée.Si le nom de variable se comp ose de plusieurs mots,la première lettre de chaque mot doit être écrite en Ma jiscule.
Lesnoms desvariablesdoivent être cohérents etcompréhensibles.

- Préxe :Un tabl eau doit commencer par la lettre 't', une énumération par la lettre'e',une variable globaledoit commencerpar"g_"...
- nommage des métho des : Le nom d'une métho de doit contenir un verb e.
- Nommagedesconstantes: Le nom d'une constante doit être écrit en ma jiscul es,i ce nom se comp ose de plusieurs mots,ces mots doivent êtreséparés pardes "_".

Fichier:

- Dénitiondes classes: chaque classe est implémentéedans unseul chier "*.java".
- En-tête d'unchier: chaque chier possède un en-tête comprenant le nom de pro jet ou de sous pro jet si c'est un module a eectuer dans un grand pro jet.

Commentaire:

- Commentaire:Un commentairedoit êtremit entre"/*" et"*/", commenter le co de si nécessaire, et ne pas rép éter des informations p ouvant être comprises par le nom de variables ou de métho de.
- Doxygène : Toutes les déclarations doit être commentées, puis extraites par doxygène, surtout les en-tête des chiers, ils doivent comp orter les descriptions nécessai re s:
  - Description des classes.
  - Commenter toutes les métho des: leurs paramètres, leurs resultats de retours, les exceptions. ..
    Doxygène ne doit généreraucun warning ouerreur lorsdel'extraction de do cument.

Règles générales

- Ne pas utiliser les variables gl obales sauf s'il n'y a pas d'autre choix.
- Toute classe doit comp orter un constructeur.
- Les membresd'une classe doiventêtre déclarés comme private ou protected , si une autre classe a b esoin d'accéder à ces membres, elle le fait à l'aide des métho des set et get.
- Déclarer les attributs d'une cla sse dans l'ordre sui vant:
  - Constantes.
  - Variables statiques.
  - Variables.
  - Construc te ur et destructeur.
  - Métho des.

  Les variables sont déc larées dans l'ordre suivant : protected, private.
- Emplacement desparenthèses: Il existent deux métho des p our l'emplacement des parenthèses,emêmechoixdoit êtreutiliser dans tout le co de:
  - void metho d()
    ```
    {
        Instruction 1;
        . ..
        if(Condition)
         {
            Instruction;
         }
    }
    ```
  - void metho d(){
    ```
        Instruction 1;
        . ..
        if(Condition){
            Instruction;
    ```

```
        }
    }
```

Il faut toujours uti liser les parenthèses même s'il s'agit d'une seule instruction.

- Ne pas utiliser les mac ro si p ossible.
- Toute variable doitêtre déclarée seule dans une ligne, etdoit être initialisée. Les variables doivent être tirées par typ e (int, short, String, . ..).
- Pour les b oucles switch-case,on doit déclarer le cas default, et tout les cas doivent se terminer par break; ou bien par //no break pour mentionner que le break n'est pas été oublie.
- utiliserune seulereturn parfonction.