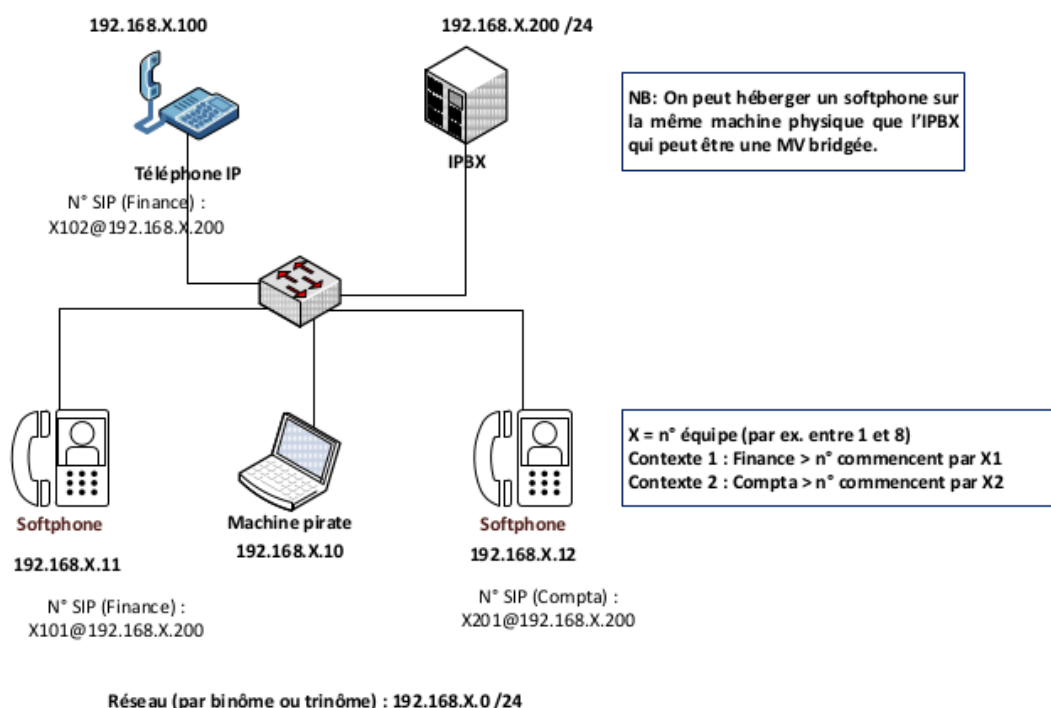


Mise en place et sécurisation d'une infrastructure de téléphonie IP avec Asterisk

Activité 5 – Contre-mesures avec chiffrement des échanges

La plate-forme de test à mettre en place est la suivante :



Adressage et numérotation

CONTEXTES	RÉSEAU IP	N° DE TÉLÉPHONE sur 4 chiffres	N° DE MESSAGERIE	SERVEUR ASTERISK
Finance	192.168.X.0/24	Commencent par X1 Exemple 1101, 1102 etc. pour l'équipe n°1	X199	192.168.X.200/24
Compta		Commencent par X2 . Exemple : 1201, 1202, etc. pour l'équipe n° 1	X299	

Le plan d'adressage et de numérotation ci-dessus illustre deux contextes (finance et compta) qui veulent communiquer au sein d'un même site (un seul serveur Asterisk). Dans la numérotation mise en place, X représente un numéro de groupe de travail d'étudiants (équipe) pouvant aller de 1 à 8. Les captures d'écrans réalisées sont associées à l'équipe n°1.

Par exemple, 1101 représente le numéro du premier téléphone de l'équipe 1 appartenant au contexte *finance*. 1202 représente le numéro d'un deuxième téléphone de l'équipe 1 associé au contexte *compta*.

Vous disposez de la documentation suivante :

- **document 1** : présentation du chiffrement ;
- **document 2** : installation de Blink ;
- **document 3** : configuration TLS du serveur Asterisk ;
- **document 4** : configuration des comptes TLS sur les softphones Blink ;
- **document 5** : premier appel et captures de trames.
- **Document 6** : configuration TLS des téléphones IP CISCO SPA 303.
- **Document 7** : autres contre-mesures.

Travail à faire

À l'aide du dossier documentaire fourni, vous devez réaliser l'ensemble des travaux. Vous prendrez soin de rédiger une documentation au fur et à mesure de votre avancement. Lors de chaque étape, vous devez indiquer les commandes utilisées vous permettant de tester vos configurations. Vos captures d'écran ne devront prendre en compte que la zone d'affichage nécessaire à vos démonstrations.

Travail à faire 1 : préparation des machines et installation de Blink

Dans cette première partie, vous devez commencer par installer et configurer le softphone Blink sur deux machines. L'adressage IP doit être cohérent avec la maquette fournie.

Q1.1. Créer deux clones d'une machine de type Ubuntu ou Lubuntu Desktop 16.04 Xenial. Vérifier leur connexion à internet. Si vous ne disposez pas de ce type de machine, l'image ISO se trouve sur le site d'Ubuntu : <https://www.ubuntu.com/download/desktop>

Q1.2. A l'aide du dossier documentaire fourni, installer le logiciel Blink sur ces deux machines.

Q1.3. Configurer l'adressage IP sur ces deux machines en suivant les indications du tableau suivant :

	ADRESSAGE IP
SOFTPHONE 1	192.168.X.11/24
SOFTPHONE 2	192.168.X.12/24

Pour le moment, ne pas configurer de comptes sur ces softphones.

Travail à faire 2 : configuration du serveur Asterisk

Dans cette deuxième partie, vous devez configurer votre serveur Asterisk pour mettre en place le chiffrement avec TLS. Les comptes concernés sont décrits dans le tableau suivant :

	CONTEXTE	COMPTE	NUMÉRO
SOFTPHONE 1	FINANCE	Utilisateur1	X101
SOFTPHONE 2	COMPTA	Utilisateur2	X201

→ Modification du fichier `users.conf`

Q2.1. Commencer par modifier le fichier `users.conf`, sur le serveur Asterisk, afin de disposer des deux comptes présents dans le tableau ci-dessus.

Q2.2. Toujours sur le fichier `users.conf`, configurer ces comptes pour qu'ils supportent le chiffrement. Pour cela, ajouter les lignes **transport = tls** et **encryption = yes**.

→ Création des certificats

Q2.3. A l'aide du dossier documentaire, créer sur votre serveur les certificats nécessaires (CA, serveur, et pour les deux softphones).

Q2.4. Installer le paquet **srtp-utils** sur votre serveur. Recharger la configuration d'Asterisk, puis vérifier que le module **res_srtp.so** est chargé à l'aide de la commande **module show like srtp** dans la console Asterisk.

→ Modification du fichier `sip.conf`

Q2.5. Modifier le fichier **sip.conf** afin de configurer le chiffrement avec TLS sur le serveur. Pour cela, considérer l'exemple de configuration fourni dans le dossier documentaire. Recharger la configuration d'Asterisk afin de prendre en compte les modifications effectuées.

Travail à faire 3 : configuration des comptes TLS sur les softphones Blink

Q3.1. A l'aide du dossier documentaire, configurer les deux comptes Blink associés aux deux utilisateurs présents dans le fichier **users.conf**. Ces comptes doivent permettre le chiffrement du flux de signalisation et du transport de la voix. Vérifier leur enregistrement sur le serveur à l'aide de la commande de console **sip show peers**. Toujours sur la console Asterisk, attendre l'affichage du message confirmant l'acceptation des certificats (SSL CERTIFICATE OK).

Remarque : pour transférer les certificats du serveur vers la machine associée au softphone, vous pouvez utiliser la commande **scp** ou un partage entre machines virtuelles.

Q3.2. Vérifier que le mode de transport des comptes configurés est TLS à l'aide de la commande de console **sip show tcp**.

Travail à faire 4 : premiers appels et capture de trames

Q4.1. Installer le logiciel wireshark sur la machine associée au softphone de l'utilisateur 1.

Q4.2. Tester un appel entre les deux softphones et capturer les trames de signalisation associées aux échanges à l'aide du filtre wireshark **tcp.port == 5061**.

Travail à faire 5 : positionnement MITM (Man In The Middle)

Dans cette partie, vous devez configurer la machine pirate afin de tenter la capture d'un message déposé sur une boîte vocale.

Q5.1. Démarrer la machine pirate d'adresse IP 192.168.1.10 puis lancer Wireshark sans configurer de filtre.

Q5.2. Relever les caches ARP du softphone de l'utilisateur 1 (192.168.X.11) et du serveur (192.168.1.200).

Q5.3. Configurer un empoisonnement de cache ARP entre le softphone de l'utilisateur 1 (192.168.X.11) et le serveur (192.168.X.200).

Q5.4. Vérifier le succès de l'empoisonnement en relevant à nouveau le contenu des caches ARP.

Q5.5. Utiliser le softphone de l'utilisateur 1 (192.168.X.11) afin de déposer un message sur la boîte vocale de l'utilisateur 2.

Q5.6. Sur le Wireshark de la machine pirate, constater l'échec de la capture du message vocal.

Travail à faire 6 : configuration TLS des téléphones IP CISCO SPA 303

Pour les étudiants plus rapides.

Q6.1. A l'aide du dossier documentaire, configurer deux téléphones CISCO d'adresse IP 192.168.X.100 et 192.168.X.101 en les associant aux comptes non chiffrés des utilisateurs 1 et 2.

Q6.2. Tester une écoute clandestine et capturer les trames associées à l'échange entre les deux téléphones. Tester le dépôt d'un message vocal puis l'écouter, sur la machine pirate, à l'aide du lecteur RTP de wireshark.

Q6.3. Modifier la configuration des comptes du serveur et des téléphones IP en activant les options associées au chiffrement.

Q6.4. Tenter une nouvelle écoute clandestine.

Dossier documentaire

Document 1 – Présentation du chiffrement

L'écoute des messages est rendue possible par le positionnement MITM et l'utilisation de comptes non chiffrés. Le chiffrement n'évitera pas l'empoisonnement ARP mais rendra impossible l'écoute des messages. Deux éléments sont à considérer :

- -le chiffrement du flux associé à la signalisation. Il s'agit des messages échangés dans le cadre du protocole SIP, c'est à dire l'authentification du client et la préparation de l'appel.
- -le chiffrement du transport de la voix. Il s'agit de la voix transportée par le protocole RTP.

La configuration du chiffrement des échanges nécessite de créer des certificats sur le serveur et de préparer les téléphones pour des échanges à travers le protocole TLS.



Attention, l'utilisation d'un softphone pour le chiffrement nécessite de vérifier qu'il est compatible avec la configuration TLS. Le logiciel Blink est un bon candidat en la matière.

Document 2 - Installation de Blink

L'installation de Blink sur des machines Ubuntu ou Lubuntu 16.04 Xenial nécessite d'enrichir le fichier `/etc/apt/sources.list`. Tout d'abord, il faut télécharger la clé de signature associée au projet :

```
#wget http://download.ag-projects.com/agp-debian-gpg.key
```

Puis, il faut ajouter la clé :

```
#apt-key add agp-debian-gpg.key
```

Ensuite, il faut ajouter les deux lignes suivantes à la fin du fichier des dépôts `/etc/apt/sources.list`

```
deb http://ag-projects.com/ubuntu xenial main
deb-src http://ag-projects.com/ubuntu xenial main
```

Enfin, il faut mettre à jour les dépôts pour prendre en compte les ajouts effectués. L'installation de Blink est alors possible.

```
#apt-get update
```

```
#apt-get install blink
```

Document 3 - Configuration TLS du serveur Asterisk

Il faut créer des certificats signés par notre autorité de certification. Le paquet `openssl` permet l'utilisation des commandes permettant de créer ces fichiers.

Le paquet `srtp-utils` permet de configurer le chiffrement du flux associé au transport de la voix.

```
#apt-get install openssl srtp-utils
```

D3.1 - Modification du fichier `users.conf`

Dans le fichier `users.conf`, il faut ajouter les deux lignes suivantes pour chaque utilisateur concerné par le chiffrement.

```
[1101](template)
...
transport = tls
encryption = yes
```

D3.2 - Création des certificats

Par défaut la communication se fait avec le protocole UDP via le port 5060. L'activation de TLS va permettre l'utilisation du port 5061 via le protocole TCP. Plusieurs étapes sont nécessaires pour créer les certificats afin d'obtenir l'exemple d'arborescence figurant dans la capture d'écran ci-dessous.

```
root@asterisk:/etc/asterisk/certificats# ls -R
.:
ca  srv  utilisateur1  utilisateur2

./ca:
ca.crt  ca.key

./srv:
asterisk.pem  key.pem  req-srv.csr  srv.crt

./utilisateur1:
cert-utilisateur1.crt  cert-utilisateur1.pem  key.pem  req-utilisateur1.csr

./utilisateur2:
cert-utilisateur2.crt  cert-utilisateur2..pem  req-utilisateur2.csr
cert-utilisateur2.pem  key.pem
```

→ Création du certificat de l'autorité de certification

Dans le répertoire **ca** :

L'autorité de certification devra signer les certificats générés.

Création de la clé :

```
#openssl genrsa -des3 -out ca.key 4096
```

Une **passphrase** est demandée lors de création du certificat.

Création du certificat :

```
#openssl req -new -x509 -days 365 -key ca.key -out ca.crt
```

→ Création du certificat du serveur Asterisk

Dans le répertoire **srv** :

Création de la clé :

```
#openssl genrsa -out key.pem 1024
```

Création du fichier de demande de certificat :

```
#openssl req -new -key key.pem -out req-srv.csr
```

Création du certificat :

```
openssl x509 -req -days 365 -in req-srv.csr -CA ../ca/ca.crt -CAkey ../ca/ca.key -set_serial 01 -out
srv.crt
```

Les fichiers `.pem` et `.crt` peuvent être mis dans un seul fichier `.pem` qui contiendra ainsi la clé et le certificat.

```
#cat key.pem > asterisk.pem
```

```
#cat srv.crt >> asterisk.pem
```

→ Création des certificats des softphones

Dans le répertoire d'un softphone (**utilisateur 1** par exemple) :

Il faut reproduire les étapes liées à la création du certificat du serveur en l'adaptant pour chaque utilisateur (clé, demande de certificat, certificat).

D3.3 - Modification du fichier `sip.conf`

Dans le fichier `sip.conf`, il faut activer TLS et faire référence au certificat du serveur.

<code>tlscipher = all</code>	<i>;active TLS</i>
<code>tlscertfile = /etc/asterisk/certificats/srv/asterisk.pem</code>	<i>;certificat du serveur</i>
<code>tlscacfile = /etc/asterisk/certificats/ca/ca.crt</code>	<i>;certificat de l'autorité</i>
	<i>;de certification</i>
<code>tlscipher = all</code>	<i>;spécifie quels algorithmes de</i>
	<i>;chiffrement sont utilisés</i>
<code>tlscclientmethod = tlsv1</code>	<i>;version de TLS supportée</i>
<code>...</code>	

Voici un exemple de configuration :

```
root@asterisk:/etc/asterisk# more sip.conf
[general]

;*****
;Les deux lignes suivantes sont suffisantes
;pour les activités 1 à 4. Pour l'activité 5,
;il faut remplacer transport= udp par transport= tls.
;La ligne transport=udp est donc commentée.
;*****
context=public
;transport = udp

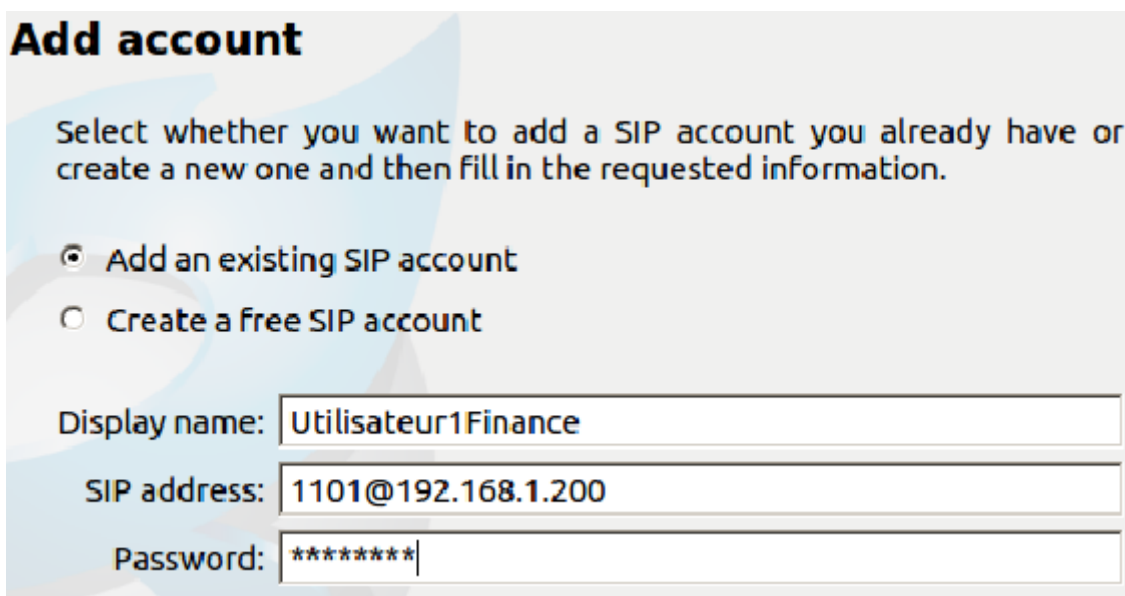
;*****
;lignes à ajouter pour l'activité 5 : chiffrement
;*****
transport = tls
tlscipher=ALL
tlscertfile=/etc/asterisk/certificats/srv/asterisk.pem
tlscacfile=/etc/asterisk/certificats/ca/ca.crt
tlscipher=ALL
tlscclientmethod=tlsv1
tlscdontverifyserver = yes
root@asterisk:/etc/asterisk# _
```

Document 4 - Configuration des comptes TLS sur les softphones Blink

Quelques modifications sont nécessaires par rapport à un compte ne faisant pas appel au chiffrement.

D4.1 - Création d'un compte SIP

Il faut ajouter un compte existant en indiquant le nom, la référence au serveur sous la forme **numéro-téléphone@ip-serveur** et le mot de passe. Pour cela, il faut aller dans **Blink** puis **Accounts** et sur **Manage accounts**.



Add account

Select whether you want to add a SIP account you already have or create a new one and then fill in the requested information.

☒ Add an existing SIP account
☐ Create a free SIP account

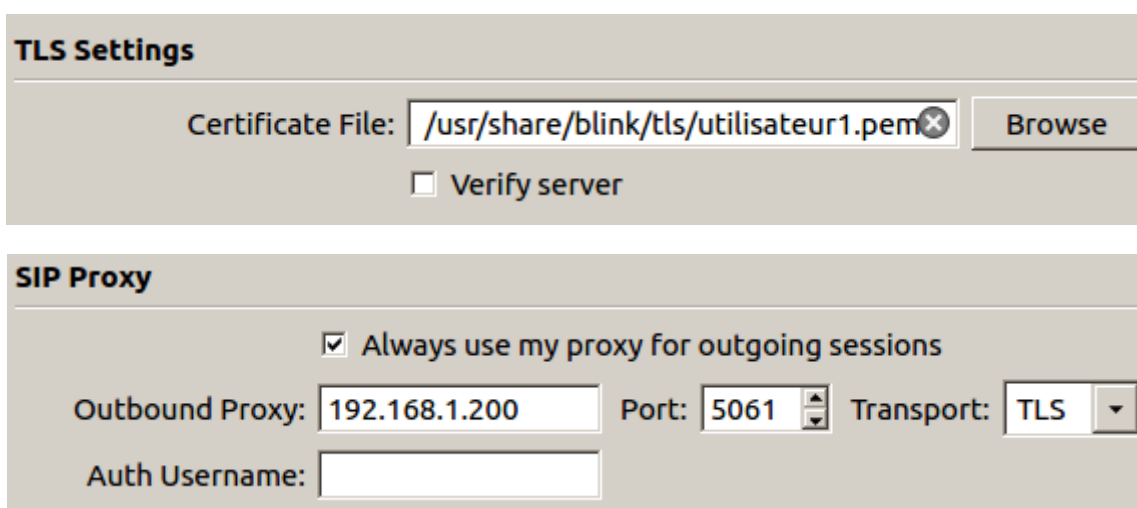
Display name:

SIP address:

Password:

D4.2 - Configuration du chiffrement

Ensuite, il faut indiquer le fichier contenant le certificat de l'utilisateur et positionner le trafic en TLS. Les onglets **Server Settings** et **Advanced** du menu **Account** permettent d'établir ces configurations.



TLS Settings

Certificate File:

☐ Verify server

SIP Proxy

☒ Always use my proxy for outgoing sessions

Outbound Proxy: Port: Transport:

Auth Username:

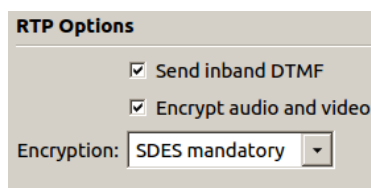
Il faut aussi faire référence au certificat de l'autorité de certification. La configuration se trouve dans le menu **Advanced** du compte SIP.



TLS settings

Certificate Authority:

Pour la configuration du SRTP, il faut activer l'option **SDES mandatory** dans le menu **account/media/rtp options**.



D4.3 - Enregistrement du compte sur le serveur

Lorsque ces configurations sont terminées, la console Asterisk doit tracer l'enregistrement du softphone. Il faut être attentif à la validation du certificat. Le message **SSL certificate OK** doit apparaître. L'enregistrement fait apparaître la référence au logiciel Blink.

```
> Saved useragent "Blink 2.0.0 (Linux)" for peer 1101
> Saved useragent "Blink 2.0.0 (Linux)" for peer 1201
```

D4.4 - Dépannages

- ❖ A la fin de l'étape du paragraphe 4.1, le serveur trace une erreur sur le mode de transport. En effet, nos comptes sont configurés en TLS sur le serveur. Or, la validation de cette première étape positionne un mode de transport par défaut en UDP. Ce n'est qu'à la fin de la configuration en TLS que le message disparaît.

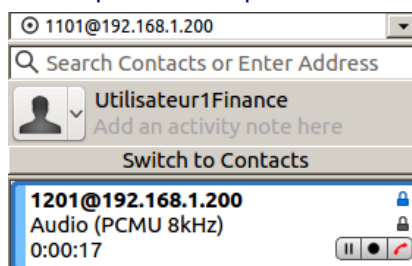
```
[Nov 11 10:45:32] ERROR[1513]: chan_sip.c:16898 register_verify: 'UDP' is not a
valid transport for '1201'. we only use 'TLS'! ending call.
```

- ❖ Dans le fichier **sip.conf**, la ligne **tlsdontverifyserver** permet de ne plus avoir le message d'erreur associé à l'utilisation d'un certificat auto-signé.

```
[Nov 11 11:03:40] ERROR[1876]: tcptls.c:621 handle_tcptls_connection: Certificat
e did not verify: self signed certificate
```

Document 5 - Premier appel et capture de trames

Lors d'un appel, le cadenas bleu indique le chiffrement du flux de signalisation. Le cadenas gris indique le chiffrement du flux RTP. Lorsque la souris passe sur un cadenas, une explication apparaît.



Concernant le flux de signalisation, une capture avec le filtre **tcp.port == 5061** permet de constater le chiffrement TLS.

Filter: tcp.port == 5061 Expression... Clear Apply Enregistrer

No.	Time	Source	Destination	Protocol	Length	Info
21	11.974387000	192.168.1.11	192.168.1.200	TLSv1.2	1217	Application Data
22	11.974441000	192.168.1.10	192.168.1.11	ICMP	590	Redirect (Redirect for host
23	11.974484000	192.168.1.11	192.168.1.200	TLSv1.2	1217	[TCP Retransmission] Application Data
24	11.975226000	192.168.1.200	192.168.1.11	TLSv1.2	715	Application Data
25	11.975249000	192.168.1.10	192.168.1.200	ICMP	590	Redirect (Redirect for host
26	11.975270000	192.168.1.200	192.168.1.11	TLSv1.2	715	[TCP Retransmission] Application Data
27	11.975389000	192.168.1.11	192.168.1.200	TCP	66	57727->5061 [ACK] Seq=1152 Ack=650 Win=1

▶ Frame 26: 715 bytes on wire (5720 bits), 715 bytes captured (5720 bits) on interface 0

▶ Ethernet II, Src: CadmusCo_08:cb:36 (08:00:27:08:cb:36), Dst: LiteonTe_62:ee:fb (20:16:d8:62:ee:fb)

▶ Internet Protocol Version 4, Src: 192.168.1.200 (192.168.1.200), Dst: 192.168.1.11 (192.168.1.11)

▶ Transmission Control Protocol, Src Port: 5061 (5061), Dst Port: 57727 (57727), Seq: 1, Ack: 1152, Len: 649

▼ Secure Sockets Layer

- ▼ TLSv1.2 Record Layer: Application Data Protocol: sip.tcp
 - Content Type: Application Data (23)
 - Version: TLS 1.2 (0x0303)
 - Length: 644

Document 6 - Configuration TLS des téléphones IP CISCO SPA 303

D6.1 - Configuration TLS des téléphones IP

Pour ce qui est des téléphones CISCO, les étapes suivantes sont nécessaires :

Dans le sous menu *Supplementary Services* du menu *User*, il faut mettre la valeur *yes* à l'option *Secure Call Setting*.

Dans le sous menu *Supplementary Services* du menu *Phone*, il faut mettre la valeur *yes* à l'option *Secure Call Serv*.

Dans le sous menu *SIP Parameters* du menu *SIP*, il faut choisir la valeur *s-descriptor* dans l'option *SRTP method*.

Enfin, dans le sous menu *SIP settings* associé au menu *EXT* de l'utilisateur concerné (EXT1, EXT2 ou EXT3), il faut choisir la valeur *TLS* dans l'option *SIP Transport* afin de chiffrer le flux de signalisation. Le port SIP est alors 5061 au lieu de 5060.

Afin de garantir l'authenticité du flux, il est possible de générer un mini certificat à l'aide d'un utilitaire : <https://www.manualslib.com/manual/423620/Cisco-Spa2102.html?page=73>

Subscriber Information	
Display Name: Utilisateur1Finance	User ID: 1101
Password: *****	Use Auth ID: no
Mini Certificate:	Revised Auth Realm:
SRTP Private Key:	

Cette partie n'est pas couverte dans ce côté labo. Le seul chiffrement du flux garantit sa confidentialité. Dans ce côté labo, vu que les mini certificats ne sont pas utilisés, l'authenticité et donc la non répudiation ne sont pas garantis.

D6.2 - Capture avec Wireshark

Une capture Wireshark du flux chiffré ne permet pas d'écouter le message vocal. Le filtre utilisé pour voir les messages de signalisation chiffrés peut être **tcp.port == 5061**.

Filter: tcp.port == 5061		Expression...		Clear	Apply	Enregistrer
No.	Time	Source	Destination	Protocol	Length	Info
22	19.307704000	192.168.1.100	192.168.1.200	TCP	66	5078->5061 [ACK] Seq=1 Ack=1 Win=7211 Len=
23	19.307760000	192.168.1.10	192.168.1.200	ICMP	94	Redirect (Redirect for host)
24	19.307817000	192.168.1.100	192.168.1.200	TCP	66	[TCP Dup ACK 22#1] 5078->5061 [ACK] Seq=1
28	19.551386000	192.168.1.100	192.168.1.200	TLSv1	748	Application Data, Application Data
29	19.551428000	192.168.1.100	192.168.1.200	TLSv1	748	[TCP Retransmission] Application Data, A

▶ Frame 28: 748 bytes captured (5984 bits) on interface 0
▶ Ethernet II, Src: Cisco_d3:27:4c (3c:c0:73:d3:27:4c), Dst: CadmusCo_08:cb:36 (08:00:27:08:cb:36)
▶ Internet Protocol version 4, Src: 192.168.1.100 (192.168.1.100), Dst: 192.168.1.200 (192.168.1.200)
▶ Transmission Control Protocol, Src Port: 5078 (5078), Dst Port: 5061 (5061), Seq: 1, Ack: 1, Len: 682
▼ Secure Sockets Layer
▼ TLSv1 Record Layer: Application Data Protocol: sip.tcp
Content Type: Application Data (23)
Version: TLS 1.0 (0x0301)
Length: 32
Encrypted Application Data: 26d6798a0eac22d96b33298f0242244606ab473b5b2020c5...

Document 7 - Autres contre-mesures

D7.1 - Filtrage des adresses MAC

Pour éviter en amont ce type d'attaque, une politique de filtrage des adresses MAC peut être envisagée. L'idée est d'empêcher un utilisateur de connecter son ordinateur portable au réseau. Cette connexion de périphériques non légitimes est souvent le point de départ des attaques associées aux réseaux locaux. Ce filtrage peut être mis en place sur des équipements réseaux comme les commutateurs ou les routeurs dans le cadre d'une politique de sécurisation des ports.

Le filtrage des adresses MAC présente néanmoins l'inconvénient d'alourdir l'administration du réseau. En outre, une adresse MAC peut facilement s'usurper avec l'utilisation de logiciels tel que *macchanger*.

D7.2 - Surveillance du trafic ARP

La création d'entrées statiques dans le cache ARP peut apporter un début de réponse mais ce procédé oblige à figer une configuration. C'est pourquoi des outils existent afin de surveiller les évolutions du cache ARP dans le but de détecter des modifications suspectes.

Le logiciel *arpwatch* assure cette fonction en surveillant l'activité ARP du réseau local.

D7.3 - IDS/IPS

Les systèmes de détection d'intrusion (IDS) sont des dispositifs qui capturent et analysent le trafic à la recherche de trames associées à un trafic malicieux. Un mécanisme d'alerte est alors configuré afin d'avertir l'administrateur. Plusieurs solutions existent. On peut citer l'exemple du logiciel *snort*.

Les systèmes de prévention d'intrusion (IPS) sont des IDS actifs qui peuvent prendre des mesures afin de diminuer les impacts d'une attaque en bloquant des ports par exemple. Le logiciel *snort* est aussi un IPS. Des constructeurs comme CISCO ou JUNIPER sont aussi présents sur ce marché.

L'envoi continu de fausses réponses ARP est considéré comme du trafic malicieux susceptible d'être détecté par un IDS/IPS.