Sécurité des systèmes VoIP

Ou comment tester ses équipements...

Nicolas Bareil
nicolas.bareil@eads.net

EADS Corporate Research Center
SSI Department
Suresnes, FRANCE

18 Janvier 2007
GITSIS

Banc de torture

Montage d'un banc d'essai

- Un Cisco Callmanager 4.x,
- Deux téléphones Cisco (7960 et 7970) ;

$\Longrightarrow$ Étude de type « **blackbox** »

Boîte noire

- Configuration inconnue ;
- Version des firmwares inconnue ;
- Protocole peu connu ;
- Aucun manuel fourni.

EADS CCR

Plan

EADS CCR

Plan

EADS CCR

Matériel présent

Avec un peu d'intuition et de curiosité :

- Processeur MIPS (???) ;
- L'espace de stockage ne dépasse pas les 4 Mo ;
- Ports switch et PC bridgés par défaut.

Configuration réseau : VLAN

VLAN & CDP

Récupération des informations sur les VLAN disponibles (voix ou données) via le protocole propriétaire Cisco.

En abuser, ça craint

Les annonces CDP ne sont pas authentifiées.
Sur un réseau n'utilisant pas les VLAN, que se passe-t-il si on annonce un faux VLAN ?
$\Longrightarrow$ Création d'un réseau virtuel ?

Configuration réseau : IP

Simplement

Récupération de l'adresse IP via une requête DHCP.
L'option 150 identifie l'adresse IP du serveur TFTP (le Call Manager en fait).

Si aucune réponse DHCP, réutilisation de la dernière configuration utilisée.

Chargement de la configuration

Téléchargement de fichier

Les fichiers sont téléchargés par TFTP au démarrage uniquement.

Plusieurs types de fichiers :

Extension	Description
`.tlv`	certificate trust list
`.loads`	universal application loader
`.sbn`	secure universal application loader
`.cnf`	configuration
`.bin`	firmware non signé
`.sb2`	firmware signé
`.jar`	Java

EADS CCR

Rogue TFTP server

Gros fichier toi même !

L'envoi d'un gros fichier entraine une fuite mémoire dans le padding des trames Ethernet. Overflow ? Mémoire non initialisée ?

```
>>> a.nzpadding()
0022 Ether / IP / UDP 10.0.1.11:49946 > 10.0.0.1:33572 / Raw / Padding
---> 4C 53 45 50 30 30 31 34  41 38 39 32 34 44          LSEP0014A8924D
...
0536 Ether / IP / TCP 10.0.1.11:50099 > 10.0.0.1:skinny S / Padding
--->   46 2E                                               F.
0549 Ether / IP / TCP 10.0.1.11:50103 > 10.0.0.1:skinny S / Padding
--->   34 44                                               4D
0560 Ether / IP / TCP 10.0.1.11:50108 > 10.0.0.1:skinny S / Padding
--->   46 2E                                               F.
```

Fichier de configuration

Le Call Manager, un serveur TFTP particulier

Composition du nom de fichier : `SEP.<adresse mac>.cnf.xml`
Les configurations ne sont pas stockées mais générées à la volée !

- Fichier XML ;
- Logique inversée : $0 \Rightarrow \textit{vrai}, 1 \Rightarrow \textit{faux}$;
- Aucune signature cryptographique présente.

P00307010200.loads : Signature cryptographique ?

```
0100 0201 0102 0002  0194 0300 5B04 0027   ............[..'
434E 3D73 6F6D 6553  6967 6E65 723B 4F55   CN=someSigner;OU
3D73 6F6D 654F 7267  556E 6974 3B4F 3D73   =someOrgUnit;O=s
6F6D 654F 7267 0005  0008 1234 5678 90AB   omeOrg.....4Vx..
CDEF 0600 2343 4E3D  736F 6D65 4341 3B4F   ....#CN=someCA;O
553D 736F 6D65 4F72  6755 6E69 743B 4F3D   U=someOrgUnit;O=
736F 6D65 4F72 6700  0700 0F08 0001 0109   someOrg.........
0008 0A00 0100 0B00  0102 0C01 0041 4314   .............AC.
E106 1D84 F20E 0B2A  C4B7 F49B FF0D CCCC   .......*........
0F7C F714 B818 24AE  4B3B 049F 75F8 D32B   .|....$.K;..u..+
BDAB 8AC0 7E5E EDFE  9D01 162F 8F65 1877   ....~^...../.e.w
F092 FC14 A186 37AB  5388 B6AC 27FC 3702   ......7.S...'.7.
8955 0F89 26DD 3FCF  72C2 3FE3 327F CB1D   .U..&.?.r.?.2...
54BF E577 6DE4 03F8  8BB2 2393 3A21 F2B6   T..wm.....#.:!..
F07C 9321 0C3B 7382  08C8 B4DE 6AD7 BA4F   .|.!.;s.....j..O
CE7A 8B4F 4FAB 8F7E  E283 8699 05A9 C24D   .z.OO..~.......M
3B3B 0E05 34C4 9074  9F5B 2482 8322 A084   ;;..4..t.[$.."..
CC76 71CD C2E2 3619  1906 EC98 5FC6 63FC   .vq...6....._.c.
6E74 A693 3E29 5E07  2E9B D3D0 9E44 6C79   nt..>)^......Dly
81D5 A272 C8B0 44D3  6718 9D7E 081F 81FC   ...r..D.g..~....
88A6 2BE3 92FB AC19  4A30 AAC8 27BC 71B7   ..+.....J0..'.q.
5A55 8D29 5B87 F44B  EC6B 8C84 3217 012A   ZU.)[..K.k..2..*
BA84 377C 717B F6F0  F42E 12BD 55C8 3C3B   ..7|q{......U.<;
E931 F33D EB80 E734  8E35 A93B E30E 0013   .1.=...4.5.;....
5030 3033 3037 3031  3032 3030 2E6C 6F61   P00307010200.loa
6473 000D 5030 3033  3037 3031 3032 3030   ds..P00307010200
2E73 626E 0D0A 5030  3033 3037 3031 3032   .sbn..P003070102
3030 2E73 6232 0D0A  4C41 5F56 4552 5349   00.sb2..LA_VERSI
4F4E 3D50 4153 3330  3730 380D 0A          ON=PAS30708..
```

Constatations

- Téléchargé à chaque fois ;
- Ressemble à un certificat ;
- Contient des noms de fichier.

Dissection de ces octets

```
\x01\x00                                    ## début de section ?
  \x02\x01\x01
\x02\x00                                    ## début de section ?
  \x02\x01\x94
\x03\x00                                    ## début de section ?
  \x5b
\x04\x00                                    ## début de section ?
  \x5c
  \x27                                      ## longueur : 39 octets
  CN=someSigner;OU=someOrgUnit;O=someOrg\x00    ## Certificat Autorité
\x05\x00                                    ## début de section ?
  \x08                                      ## longueur : 8 octets
  \x12\x34\x56\x78\x90\xab\xcd\xef          ## 123456789abcdef Pour l'endianess ?
\x06\x00                                    ## début de section ?
  \x23                                      ## longueur : 35 octets
  CN=someCA;OU=someOrgUnit;O=someOrg\x00    ## Certificat racine
\x07\x00                                    ## début de section ?
  \x0f
\x08\x00                                    ## début de section ?
  \x01\x01\t\x00
  \x08\n\x00\x01\x00
  \x0b                                      ## longueur : 11 octets
\x00\x01\x02\x0c\x01\x00
AC\x14\xe1\x06\x1d\x84\xf2\x0e\x0b*\xc4\xb7\xf4\x9b\xff\r
\xcc\xcc\x0f|\xf7\x14\xb8\x18$\xaeK;\x04\x9fu\xf8\xd3\xbd\xab\x8a\xc0~^\xed\xf
e\x9d\x01\x16/\x8fe\x18w\xf0\x92\xfc\x14\xa1\x867\xabS\x88\xb6\xac\'\xfc7\x02\x8
9U\x0f\x89&\xdd?\xcfr\xc2?\xe32\x7f\xcb\x1dT\xbf\xe5wm\xe4\x03\xf8\x8b\xb2#\x93:
!\xf2\xb6\xf0|\x93!\x0c;s\x82\x08\xc8\xb4\xdej\xd7\xba0\xcez\x8bOO\xab\x8f~\xe2
\x83\x86\x99\x05\xa9\xc2M;;\x0e\x054\xc4\x90t\x9f\[$\x82\x83"\xa0\x84\xccvq\xcd\xc
2\xe26\x19\x19\x06\xec\x98_\xc6c\xfcnt\xa6\x93>^\x07.\x9b\xd3\xd0\x9eDly\x81\xd
5\xa2r\xc8\xb0D\xd3g\x18\x9d~\x08\x1f\x81\xfc\x88\xa6\xe3\x92\xfb\xac\x19J0\xaa
\xc8\'\xbcq\xb7ZU\x8d\[\x87\xf4K\xeck\x8c\x842\x17\x01*\xba\x847|q{\xf6\xf0\xf4.x12\xbd\x55\xc8
\x3c\x3b\xe91\xf3\x3d\xeb\x80\xe74\x8e5\xa9\x3b\xe3\x0e\x00 ## MD5? 3C3BE931F33DEB80E7348E35A93BE30E
\x13                                    ## longueur : 19 octets
P00307010200.loads\x00\r                ## nom de fichier avec octet nul
P00307010200.sbn\r\n                    ## nom de fichier
P00307010200.sb2\r\n                    ## nom de fichier
LA_VERSION=PAS30708\r\n                 ## version du loader
```

Chargement du firmware

Extrait de strings P00307010200.sb2

« The Moving Finger writes ; and, having writ,
Moves on : nor all thy Piety nor Wit
Shall lure it back to cancel half a Line,
Nor all thy Tears wash out a Word of it. »

— *Omar Khayyam*

Désassemblage impossible

- Processeur inconnu ;
- Format de fichier inconnu : ni ELF, ni PE, etc ;
- Où est le point d'entrée du fichier ?
- Problème de légalité.

Scan des téléphones : TCP

Ports TCP

```
Interesting ports on CCM:
Not shown: 1678 closed ports
PORT    STATE SERVICE
80/tcp open  tcpwrapped

Device type: VoIP phone
Running: Cisco embedded
OS details: Cisco IP Phone 7970G
```

Protocoles

```
Interesting protocols on phoneA:
Not shown: 252 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open|filtered tcp
17       filtered      udp
```

Maigre résultat mais. . .

Beaucoup d'informations utiles sur le téléphone via l'interface Web.

Bien protégé

Une fois la connexion TCP vers le Call Manager établie, on est bloqué.

Jute pour rire...

nmap Call Manager

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS webserver 5.0
102/tcp  open  iso-tsap?
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  ssl/http      Microsoft IIS webserver 5.0
445/tcp  open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
1433/tcp open  ms-sql-s?
1720/tcp open  tcpwrapped
2000/tcp open  callbook?
2001/tcp open  dc?
2002/tcp open  globe?
3389/tcp open  microsoft-rdp Microsoft Terminal Service
8009/tcp open  ajp13?
```

Non !

On ne tire pas sur les ambulances !

Jute pour rire...

nmap Call Manager

```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS webserver 5.0
102/tcp  open  iso-tsap?
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn
443/tcp  open  ssl/http      Microsoft IIS webserver 5.0
445/tcp  open  microsoft-ds  Microsoft Windows 2000 microsoft-ds
1433/tcp open  ms-sql-s?
1720/tcp open  tcpwrapped
2000/tcp open  callbook?
2001/tcp open  dc?
2002/tcp open  globe?
3389/tcp open  microsoft-rdp Microsoft Terminal Service
8009/tcp open  ajp13?
```

Non !

On ne tire pas sur les ambulances !

Cisco Discovery Protocol

cédépé. nom composé masculin. protocole de découverte réseau

Protocole fermé, propriétaire, utilisé uniquement par les équipements Cisco.

Espoir ?

Implémentation d'un add-on CDP pour [scapy] :

- Fuzzing possible ;
- Injection de fausses annonces ;
- Debugging du réseau plus aisé.

scapy+cdp+skinny

```
>>> sniffed[2].show()
###[ Cisco Discovery Protocol version 2 ]###
    vers= 1
    ttl= 180
    cksum= 0xf960
    \|###[ Device ID ]###
     |  type= Device ID
     |  len= 25
     |  val= 'ccm.papanoel.fr'
     |###[ Addresses ]###
     |  type= Addresses
     |  len= 17
     |  naddr= 1L
     |  \|###[ CDP Addresses ]###
     |   |  ptype= NLPID
     |   |  plen= 0x1
     |   |  proto= IP
     |   |  addrlen= 4
     |   |  ipaddr= 10.0.0.1
     |###[ Software Version ]###
     |  type= Software Version
     |  len= 33
     |  val= 'Cisco Discovery Protocol v4.0'
     |###[ Platform ]###
     |  type= Platform
     |  len= 18
     |  val= 'Win2000 Server'
     -------------------
```

Fuzzing

```
>>> CDPv2_HDR(str(fuzz(CDPv2_HDR()))).show()
###[ Cisco Discovery Protocol version 2 ]###
  vers= 251
  ttl= 56
  cksum= 0x4c7
>>> send(fuzz(IP(dst='callman...') / CDPv2_HDR())
        , loop=1)
```

Packet of death ?

```
>>> killme=Dot3(dst='01 :00 :0c :cc :cc :cc')
            / LLC() / SNAP() / CDPv2_HDR()
            / CDPMsgPower(power=0xffff)
>>> killme.show()
###[ Cisco Discovery Protocol version 2 ]###
###[ Power ]###
       type= Power
       len= 6
       power= 65535 mW
>>> sendp(killme, iface='eth0')
```

scapy+cdp+skinny

```
>>> sniffed[2].show()
###[ Cisco Discovery Protocol version 2 ]###
    vers= 1
    ttl= 180
    cksum= 0xf960
    \|###[ Device ID ]###
     |  type= Device ID
     |  len= 25
     |  val= 'ccm.papanoel.fr'
     |###[ Addresses ]###
     |  type= Addresses
     |  len= 17
     |  naddr= 1L
     |  \|###[ CDP Addresses ]###
     |   |  ptype= NLPID
     |   |  plen= 0x1
     |   |  proto= IP
     |   |  addrlen= 4
     |   |  ipaddr= 10.0.0.1
     |###[ Software Version ]###
     |  type= Software Version
     |  len= 33
     |  val= 'Cisco Discovery Protocol v4.0'
     |###[ Platform ]###
     |  type= Platform
     |  len= 18
     |  val= 'Win2000 Server'
     -------------------
```

Fuzzing

```
>>> CDPv2_HDR(str(fuzz(CDPv2_HDR()))).show()
###[ Cisco Discovery Protocol version 2 ]###
  vers= 251
  ttl= 56
  cksum= 0x4c7
>>> send(fuzz(IP(dst='callman...') / CDPv2_HDR())
        , loop=1)
```

Packet of death ?

```
>>> killme=Dot3(dst='01 :00 :0c :cc :cc :cc')
            / LLC() / SNAP() / CDPv2_HDR()
            / CDPMsgPower(power=0xffff)
>>> killme.show()
###[ Cisco Discovery Protocol version 2 ]###
###[ Power ]###
       type= Power
       len= 6
       power= 65535 mW
>>> sendp(killme, iface='eth0')
```

scapy+cdp+skinny

```
>>> sniffed[2].show()
###[ Cisco Discovery Protocol version 2 ]###
    vers= 1
    ttl= 180
    cksum= 0xf960
    \|###[ Device ID ]###
     |  type= Device ID
     |  len= 25
     |  val= 'ccm.papanoel.fr'
     |###[ Addresses ]###
     |  type= Addresses
     |  len= 17
     |  naddr= 1L
     |  \|###[ CDP Addresses ]###
     |   |  ptype= NLPID
     |   |  plen= 0x1
     |   |  proto= IP
     |   |  addrlen= 4
     |   |  ipaddr= 10.0.0.1
     |###[ Software Version ]###
     |  type= Software Version
     |  len= 33
     |  val= 'Cisco Discovery Protocol v4.0'
     |###[ Platform ]###
     |  type= Platform
     |  len= 18
     |  val= 'Win2000 Server'
     -------------------
```

Fuzzing

```
>>> CDPv2_HDR(str(fuzz(CDPv2_HDR()))).show()
###[ Cisco Discovery Protocol version 2 ]###
  vers= 251
  ttl= 56
  cksum= 0x4c7
>>> send(fuzz(IP(dst='callman...') / CDPv2_HDR())
        , loop=1)
```

Packet of death ?

```
>>> killme=Dot3(dst='01 :00 :0c :cc :cc :cc')
            / LLC() / SNAP() / CDPv2_HDR()
            / CDPMsgPower(power=0xffff)
>>> killme.show()
###[ Cisco Discovery Protocol version 2 ]###
###[ Power ]###
       type= Power
       len= 6
       power= 65535 mW
>>> sendp(killme, iface='eth0')
```

Plan

EADS CCR

Équipements

Un réseau VoIP est constitué de :

- Téléphones adaptés ;
- Call Manager.

Équipement IP $\Longrightarrow$ Pile IP $\Longrightarrow$ Complexe $\Longrightarrow$ Intéressant !

Équipements

Un réseau VoIP est constitué de :

- Téléphones adaptés ;
- Call Manager.

Équipement IP $\Longrightarrow$ Pile IP $\Longrightarrow$ Complexe $\Longrightarrow$ Intéressant !

Équipements

Un réseau VoIP est constitué de :

- Téléphones adaptés ;
- Call Manager.

Équipement IP $\Longrightarrow$ Pile IP $\Longrightarrow$ Complexe $\Longrightarrow$ Intéressant !

Équipements

Un réseau VoIP est constitué de :

- Téléphones adaptés ;
- Call Manager.

Équipement IP $\Longrightarrow$ Pile IP $\Longrightarrow$ Complexe $\Longrightarrow$ Intéressant !

Pile TCP/IP correcte

Robustesse de la pile TCP/IP

- Génération des ISN : « complétement aléatoire »,
- IP ID incrémentaux,
- Protection anti-DDoS :
- Bonne gestion des numéros de séquence :

Pile TCP/IP correcte

Robustesse de la pile TCP/IP

- Génération des ISN : « complétement aléatoire »,
- IP ID incrémentaux,
- Protection anti-DDoS :
  - Requête/Réponse `ARP`,
  - `SYN` / `SYN+ACK` ;
- Bonne gestion des numéros de séquence :

Pile TCP/IP correcte

Robustesse de la pile TCP/IP

- Génération des ISN : « complétement aléatoire »,
- IP ID incrémentaux,
- Protection anti-DDoS :
- Bonne gestion des numéros de séquence :
  - Détection d'une désynchronisation,
  - Réécriture des données non acquittées ;

Pile TCP/IP correcte

Robustesse de la pile TCP/IP

- Génération des ISN : « complétement aléatoire »,
- IP ID incrémentaux,
- Protection anti-DDoS :
- Bonne gestion des numéros de séquence :

Pile TCP/IP dérivée d'un IOS ?

TCP Hijacking

Avis de tempête

Blind TCP Hijacking non trivial.

$\Longrightarrow$ L'insertion naïve de paquets entraîne un ACK-storm !

The lazy way

Utilisons la possibilité de réécrire des paquets non acquittés !

1. Anticiper la taille du prochain segment,
2. Envoyer le paquet,
3. Réussir à ce qu'il soit traité avant la réception du vrai paquet,
4. Attendre :)

Suite de paquets

Comment anticiper ?

Il y a constamment des suites de paquets :

- Démarrage,
- Keep Alive,
- Décrochage du téléphone,
- Réception d'un appel,
- ...

Applications du TCP Hijacking

Applications possibles :

- Modification des numéros de téléphone composés,
- Impossible de modifier les options de sécurité ainsi,
  $\Longrightarrow$ Car modifiées par le fichier de configuration (via TFTP)

Too easy !

L'utilisation de [scapy] et de son add-on Skinny facilite ce type d'interception.

Applications du TCP Hijacking

Applications possibles :

- Modification des numéros de téléphone composés,
- Impossible de modifier les options de sécurité ainsi,
  $\Longrightarrow$ Car modifiées par le fichier de configuration (via TFTP)

Too easy !

L'utilisation de [scapy] et de son add-on Skinny facilite ce type d'interception.

Applications du TCP Hijacking

Applications possibles :

- Modification des numéros de téléphone composés,
- Impossible de modifier les options de sécurité ainsi,
  $\Longrightarrow$ Car modifiées par le fichier de configuration (via TFTP)

Too easy !

L'utilisation de [scapy] et de son add-on Skinny facilite ce type d'interception.

ICMP Redirect

Message ICMP Redirect

Redirection d'un routeur par un autre routeur.

- Support de l'ICMP insuffisant dans [scapy],
- Réimplémentation de l'ICMP,
- Mais les téléphones ne suivent pas les redirections ICMP :-(

ICMP Redirect

Message ICMP Redirect

Redirection d'un routeur par un autre routeur.

- Support de l'ICMP insuffisant dans [scapy],
- Réimplémentation de l'ICMP,
- Mais les téléphones ne suivent pas les redirections ICMP :-(

Modes Gratuitous ARP

Gratuitous ARP

C'est une réponse ARP non désirée afin de mettre à jour les caches.

Les téléphones peuvent autoriser cette fonctionnalité ou non.

- Avec GARP, toutes les attaques ARP sont possibles,
- Sans GARP, rien n'est possible
  - Une fois la première résolution faite, l'entrée du cache est figée

EADS CCR

Modes Gratuitous ARP

Gratuitous ARP

C'est une réponse ARP non désirée afin de mettre à jour les caches.

Les téléphones peuvent autoriser cette fonctionnalité ou non.

- Avec GARP, toutes les attaques ARP sont possibles,
- Sans GARP, rien n'est possible
  - Une fois la première résolution faite, l'entrée du cache est figée

Sauf une fois...

Comportement bonus

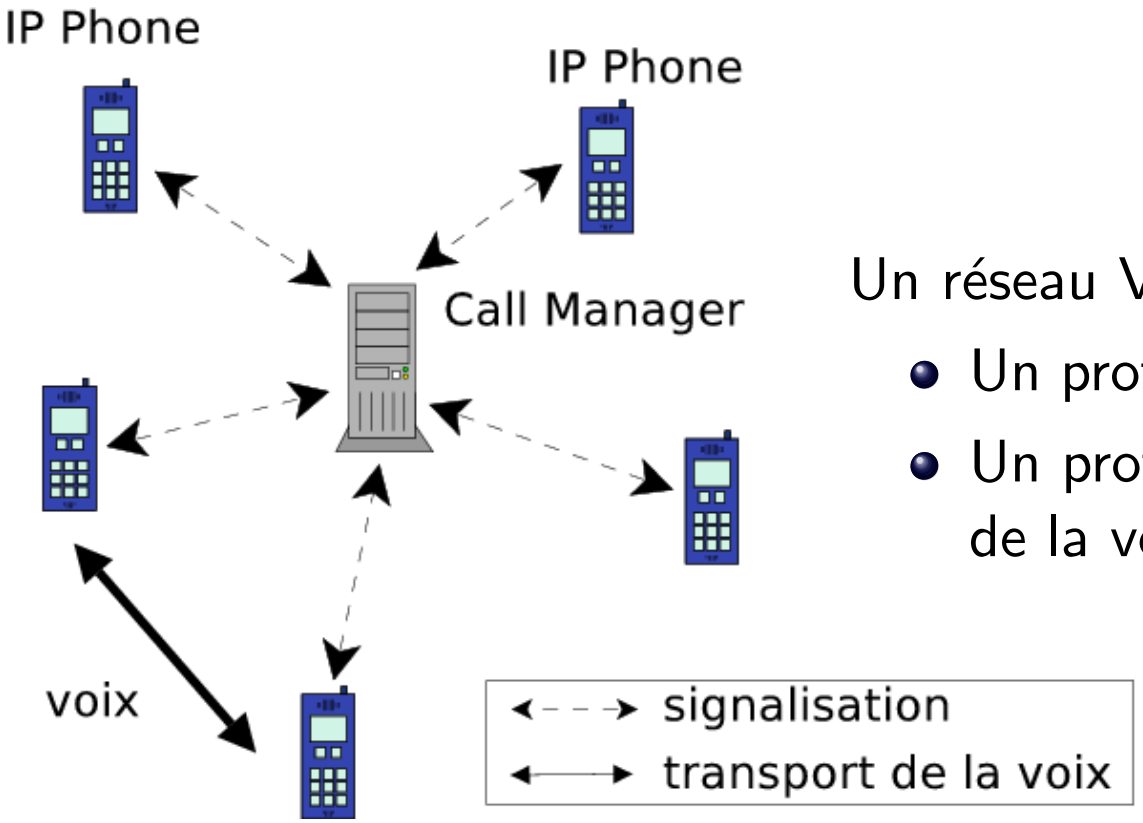
```
>>> from Crypto.Hash import MD5
>>> hash=MD5.new()
>>> def hashoir(x):
...   hash.update(str(x.payload))
...   hex=hash.hexdigest()
...   print x.sprintf("%Ether.src% > %Ether.dst% / {UDP: UDP(%UDP.sport% > %UDP.dport%)}"
...                                                "{TCP: TCP(%TCP.sport% > %TCP.dport%)} MD5=%s" % hex)
...
>>> map(hashoir, sniffedpkt)
00:14:A8:92:4D:3F > 00:0B:CD:AE:FC:27 / UDP(50036 >  tftp) MD5=45733f4ea925a5d4c336287bdd7411c3
00:14:A8:92:4D:3F > 00:0B:AA:BB:CC:DD / UDP(50036 >  tftp) MD5=45733f4ea925a5d4c336287bdd7411c3
00:14:A8:92:4D:3F > 00:0B:CD:AE:FC:27 / TCP(1570 > skinny) MD5=a20675fc6702ae5ebdb1b94dfdc10096
00:14:A8:92:4D:3F > 00:0B:AA:BB:CC:DD / TCP(1570 > skinny) MD5=a20675fc6702ae5ebdb1b94dfdc10096
00:14:A8:92:4D:3F > 00:0B:CD:AE:FC:27 / TCP(1570 > skinny) MD5=ca8f5150150d1090244d9a49d75868e9
00:14:A8:92:4D:3F > 00:0B:AA:BB:CC:DD / TCP(1570 > skinny) MD5=ca8f5150150d1090244d9a49d75868e9
```

Do you ?

Vous ne voyez rien de bizarre ?

Plan

Les protocoles mis en jeux



Un réseau VoIP est géré via :

- Un protocole de signalisation
- Un protocole de transport de la voix

Skinny Client Control Protocol

Skinny :

- Utilise TCP/2000
- Protocole binaire (contrairement à SIP)
- Champs à positions fixes

Skinny : Le Yin ?

Analyse difficile sans spécifications :

- Plus de trois cents types de messages ;
- Champs composés complexes ;
- Beaucoup de champs « réservés » ;

$\Longrightarrow$ Implémentation partielle dans [scapy]

Real Time Protocol : le Yang

RTP : Le Yang

Protocole simple et généraliste standardisé par la RFC 3550.
$\Longrightarrow$ Utilisé par (presque) toutes les solutions VoIP

Les numéros de ports ne sont pas fixes et sont assignés dynamiquement via le protocole de signalisation.

Real Time Protocol : voix

Après les en-têtes. . . la voix !

- La voix n'est pas chiffrée, juste codée ;
- Si on intercepte ces paquets, on peut alors écouter.

État de l'art des logiciels d'écoute téléphonique

- vomit (N. Provos) ;
- voipong (M. Balaban) ;
- cain (M. Montoro).

I'm listening to you !

ilty : I'm listening to you !

- Logiciel Libre,
- Inteface user friendly
- Développé en Python,

Fonctionnalités

- Écouter une conversation en direct,
- Logguer les appels,
- Surveille le protocole de signalisation,

La signalisation

Surveiller le protocole de signalisation permet :

- Reconnaître précisemment les appels :
  - Accès aux informations de l'annuaire,
  - Numéro de téléphone,
  - Extension du numéro de téléphone ;
- Voir les touches composées :
  - Capture du code de messagerie vocale,
  - Numéros de carte bleue ;

Des questions ?

Si on avait eu plus du temps...

Vérification de la solidité du code cryptographique.

Remerciements

Phil, Serpilliere, Sid, Arnaud, news0ft, Kostya, Stf et tout le reste de l'équipe d'EADS CCR DCR/STI/C !

Plus d'information ?

- `nicolas.bareil@eads.net`

Bibliography

P. Biondi, scapy
Interactive packet manipulation program
http://secdev.org/projects/scapy/

N. Bareil, ilty
I'm listening to you
http://chdir.org/~nico/ilty/
SSTIC 2005 — http://actes.sstic.org/SSTIC05/

N. Provos, vomit
http://vomit.xtdnet.nl/

M. Balaban, voipong
http://www.enderunix.org/voipong/

M. Montoro, Cain
http://www.oxid.it/cain.html

EADS CCR