

SÉCURITÉ VOIP



Sécurité de l'application

- ▣ Firewall hard. (SBC Session Border Controller)
- ▣ Firewall software sur la machine
- ▣ Mot de passe fort ou authentification forte
- ▣ Protéger le sip contre le relaying
- ▣ Désactiver les protocole non utilisé
- ▣ Activation des log et CDR (call detail record)



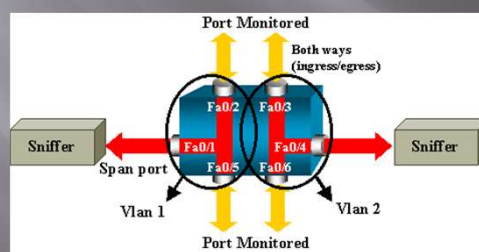
Sécurité de l'authentification

- ▣ Exemple d'insécurité au niveau de l'authentification.

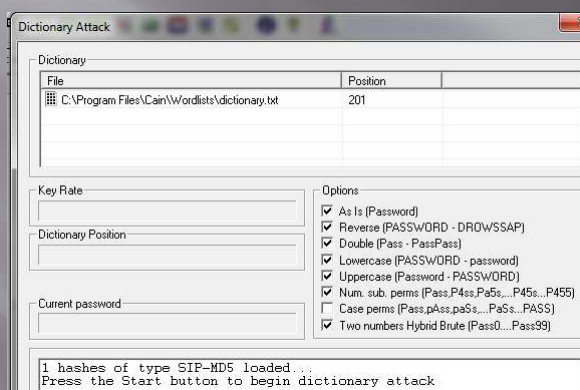
Démonstration

Sniff du réseau

- ▣ Collecter les informations entre le téléphone (UA) et le registrar à l'aide d'un port mirroring
- ▣ Création d'un dump de l'échange



Utilisation d'un dictionnaire



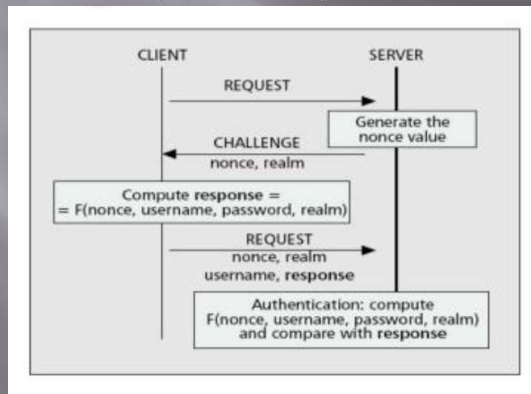
Crack à l'aide du dictionnaire

Traceroute CCDU Wireless Query							
Realm	User Name	Password	URI	Nonce	Response	Method	Type
asterisk	100	Test1235	sip:192.168.234...	1716F334	f5dae359674f6...	REGISTER	MD5

Authentication SIP

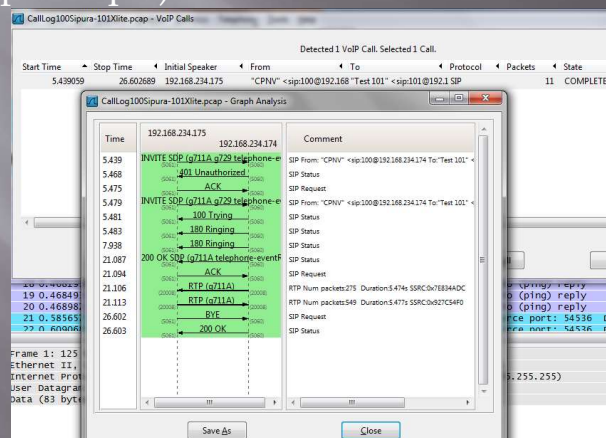
$$HA1 = MD5(A1) = MD5(\text{username} : \text{realm} : \text{password})$$

$$HA2 = MD5(A2) = MD5(\text{method} : \text{digestURI})$$

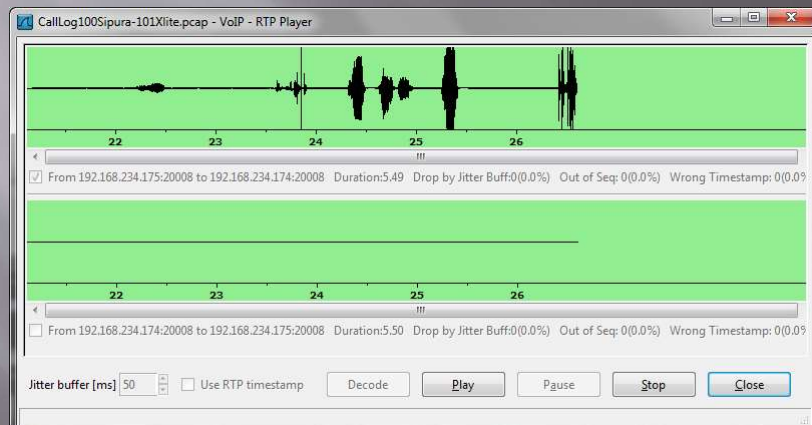
$$\text{response} = MD5(HA1 : \text{nonce} : HA2)$$


Ecoute d'une conversation

- ▣ Problème de confidentialité (Ecoute téléphonique)

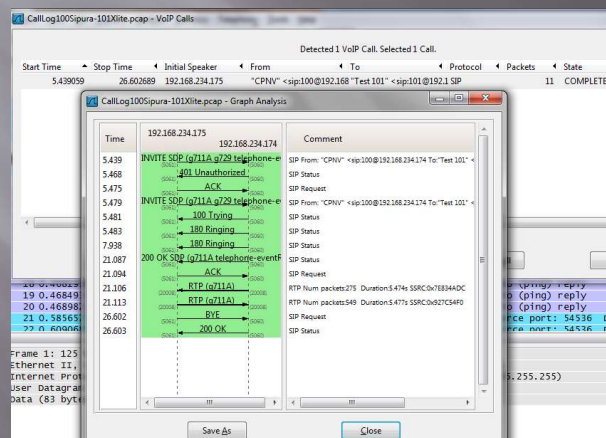


Décodage flux audio



Sécuriser la signalisation

- Sans encryptions de la signalisation.



Sécuriser la signalisation

□ Mise en place de TLS

Call100-101avec TLS.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: ip.src==192.168.234.174 or ip.dst==192.168.234.174

No.	Time	Source	Destination	Protocol	Info
76	2.669582	192.168.234.175	192.168.234.174	TLSv1	Application Data
77	2.670316	192.168.234.174	192.168.234.175	TLSv1	Application Data, Application Data
78	2.684604	192.168.234.175	192.168.234.174	TLSv1	Application Data
79	2.725304	192.168.234.174	192.168.234.175	TCP	sip-tls > ayiya [ACK] Seq=635 Ack=1339 Win=63873 Len=0
80	2.725927	192.168.234.175	192.168.234.174	TLSv1	Application Data
81	2.726202	192.168.234.174	192.168.234.175	TCP	sip-tls > ayiya [ACK] Seq=635 Ack=2360 Win=63873 Len=0
82	2.726858	192.168.234.174	192.168.234.175	TLSv1	Application Data, Application Data
95	2.918428	192.168.234.175	192.168.234.174	TCP	ayiya > sip-tls [ACK] Seq=2360 Ack=1221 Win=16000 Len=0
96	2.925686	192.168.234.174	192.168.234.175	TLSv1	Application Data, Application Data
103	3.118376	192.168.234.175	192.168.234.174	TCP	ayiya > sip-tls [ACK] Seq=2360 Ack=1823 Win=16000 Len=0
104	3.118925	192.168.234.174	192.168.234.175	TLSv1	Application Data, Application Data
109	3.318337	192.168.234.175	192.168.234.174	TCP	ayiya > sip-tls [ACK] Seq=2360 Ack=2425 Win=16000 Len=0
411	13.466822	192.168.234.174	192.168.234.175	UDP	Source port: dnp Destination port: comcontact-http
412	13.466892	192.168.234.175	192.168.234.174	UDP	Source port: dnp Destination port: comcontact-http
413	13.466760	192.168.234.174	192.168.234.175	UDP	Source port: dnp Destination port: comcontact-http
414	13.466812	192.168.234.174	192.168.234.175	UDP	Source port: dnp Destination port: comcontact-http
415	13.466865	192.168.234.174	192.168.234.175	UDP	Source port: dnp Destination port: comcontact-http
416	13.467306	192.168.234.174	192.168.234.175	TLSv1	Application Data, Application Data
417	13.484818	192.168.234.175	192.168.234.174	TLSv1	Application Data
418	13.489514	192.168.234.175	192.168.234.174	UDP	Source port: comcontact-http Destination port: dnp
419	13.499602	192.168.234.175	192.168.234.174	UDP	Source port: comcontact-http Destination port: dnp
420	13.500249	192.168.234.174	192.168.234.175	UDP	Source port: comcontact-http Destination port: dnp

Frame 76: 907 bytes on wire (7256 bits), 907 bytes captured (7256 bits)

Ethernet II, Src: CiscoIn.de:4e:bf (00:0e:08:de:4e:bf), Dst: Vmware.7f:f4:32 (00:0c:29:7f:f4:32)

Internet Protocol, Src: 192.168.234.175 (192.168.234.175), Dst: 192.168.234.174 (192.168.234.174)

Transmission Control Protocol, Src Port: ayiya (5072), Dst Port: sip-tls (5061), Seq: 1, Ack: 1, Len: 853

Secure Socket Layer