

12. téma

Bezpečnost IP telefonie

Obsah

1. Taxonomie slabin a útoků
2. Řešení Cisco
3. Útoků na IP telefonii v LAN

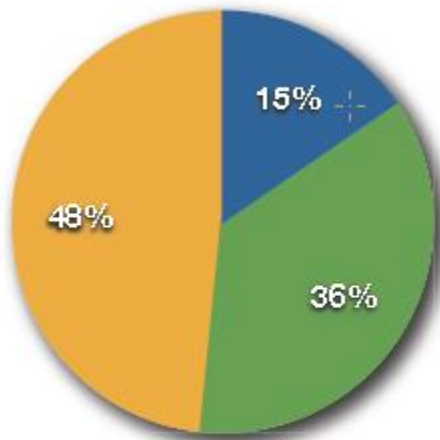
1. Taxonomie slabín a útoků

Jak to vlastně je

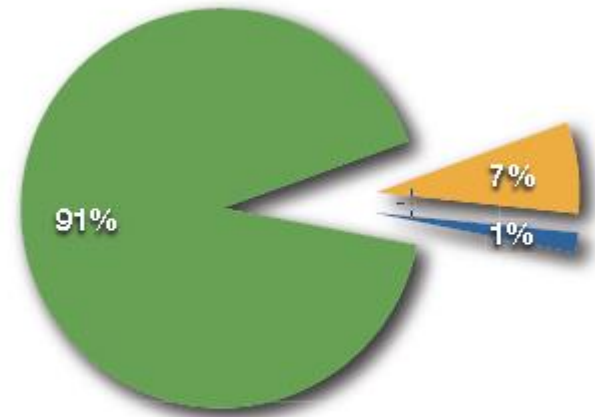
- Voice/VoIP systémy jsou zranitelné:
 - platformy, sítě, protokoly, aplikace – vše je zranitelné
 - k dispozici je množství nástrojů
 - výrobci posilují bezpečnost svých produktů
 - ale během jejich vývoje bezpečnost není hlavní kritérium
- Naštěstí to není tak strašné, protože
 - IP telefonie je převážně používána uvnitř kampusů
 - omezené stimuly pro útoky
 - Přístup do veřejných sítí je stále založen na tradičních truncích
 - Hlavní zdroj útoků jsou aplikace
- SIP trunking a UC mohou hrozby navyšovat (TDoS, harrasment, vishing...)

Kategorie útoků

(<https://gforge.inria.fr/docman/view.php/1766/6771/d1.1-full.pdf>)

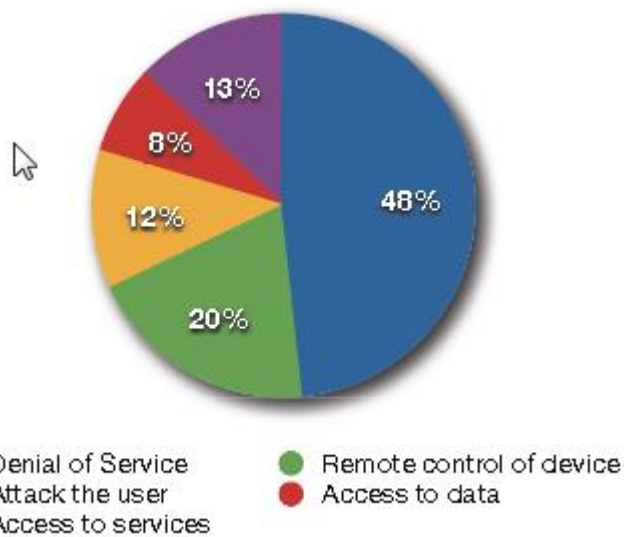


● Confidentiality ● Integrity ● Availability

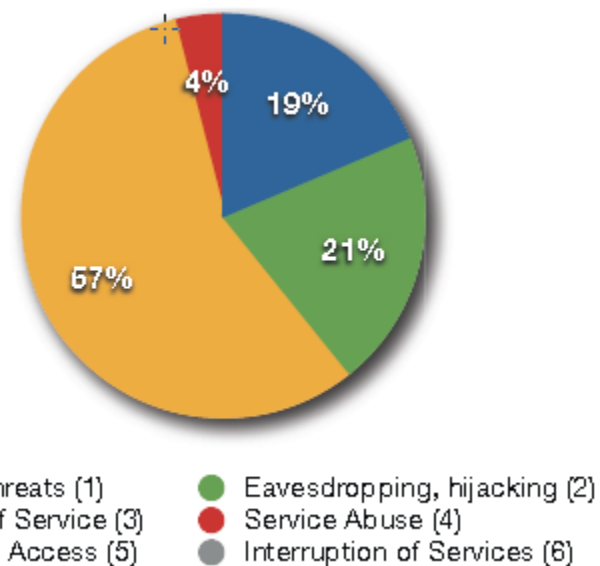


● Protocol ● Implementation ● Configuration

Slabiny měřené podle odlišných metodik



Taxonomie zdroje z předchozího slajdu



Taxonomie VoIPSA

Jaké porty můžeme skenovat?

- SIP používá UDP/TCP ports 5060 and 5061
- H.323 devices use multiple ports, including TCP 1720, UDP 1719
 - H.245 – dynamická TCP
 - H.225.0 – Q.931 – Call Setup – TCP 1720 a RAS – UDP 1719
 - Audio Call Control – TCP 1731
 - RTCP – a RTP dynamické UDP
- SCCP telefony (Cisco) používají porty UDP/TCP 2000-2001
- Unistim (Nortel) používají UDP/TCP 5000
- MGCP zařízení používají UDP 2427

Flooding (záplava, zahlcení)

- Slabá místa
 - redukovaný hardware
 - neautentizované a neautorizované funkce
- Útok
 - záplava pakety (SIP INVITE, OPTIONS...)
 - falešné pakety RTP
 - záplava běžných paketů (TCP SYN, ICMP...)
- Účinek
 - degradace QoS
 - výpadek zařízení
- Nástroje
 - Scapy, InviteFlood, IAXFlood, UDPFlood, RTPFlood, Sivas
- Opatření
 - ochrana zařízení jádra sítě před externími útoky
 - omezení provozu VoIP ve vybraných místech sítě

Flood Amplification (zesílení záplavy)

- Slabá místa
 - protokoly poskytující funkčnost bez autentizace
 - protokoly bez navazování spojení (UDP)
- Útok
 - použití zdrojové adresy paketu oběti
 - v rámci dané funkčnosti poskytování více dat než je třeba
- Účinek
 - zesilování záplav
- Nástroje
 - Scapy, NetSamhain, Nemesis
- Opatření
 - použití spojově orientovaných přenosů
 - autentizace zpráv
 - omezení provozu VoIP ve vybraných místech sítě

Fuzzing

(z Fuzz – US , polda, chlupatý)

- Slabá místa
 - nezralé či slabé implementace protokolového zásobníku
- Útok
 - posílání znetvořených zpráv na vstup zařízení
- Účinek
 - výpadek koncových zařízení, někdy i jádra sítě
 - efektivní metoda pro identifikaci softwarových chyb
- Nástroje
 - Sulley Fuzzer, ohrwurm (RTP)
 - PROTOS Suite (SIP, HTTP, SNMP)
 - NastySIP, Protos suite, Asteroid, Fuzzy Packet...
- Opatření
 - používat odolná a otestovaná zařízení

Termín byl poprvé použit v roce 1988 prof. Millerem z University of Wisconsin

Call Teardown

(násilné přerušení spojení)

- Slabá místa
 - většina realizací protokolů používá nešifrované přenosy
 - pakety jsou nešifrované
 - lze monitorovat signalizační kanály
- Útok
 - vkládání zpráv pro rozpojení: BYE (SIP), HANGUP (IAX)
- Účinek
 - rozpojení
- Nástroje
 - SIP: Teardown, sip-kill, sip-proxykill
 - IAX: IAXHangup
- Opatření
 - šifrování přenosů hlasu
 - autentizace signalizace

Pomocí SCAPY hledám základ pro BYE

```
>>> sip[7].show() ###[ Ethernet ]###
dst= 00:0e:08:dd:1a:bd src= 00:01:02:1a:8d:ab type= 0x800 ###[ IP ]###
version= 4L ihl= 5L tos= 0x0 len= 764 id= 0 flags= DF frag= 0L ttl= 54 proto= udp
chksum= 0x880e src= 86.64.162.35 dst= 192.168.0.215 options= ' ' ###[ UDP ]###
sport= 5060 dport= 5060 len= 744 chksum= 0xbcdc ###[ Raw ]###
load= 'SIP/2.0 200 OK\r\nVia: SIP/2.0/UDP 192.168 . 0 . 215 : 5060;b
ranch=z9hG4bK-82 6b4f7;rport=50 60\r\nRecord-Route: <sip:8 160.216.1.3;ftag=
e3bfc272 9667 92 8fo0;lr=on>\r\nFrom: "unob" <sip: jarda@unob.cz>;tag=e3 bfc272
9667 92 8fo0\r\nTo: <sip:50 0@unob.cz>;tag=as48e6f2f4\r\nCall-ID: 92 3cae6e-
7b8136c3@192.168.0.215\r\nCSeq: 102 INVITE\r\nUser-Agent: UNOB.CZ\r\nAllow:
INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY\r\nContact:
<sip:500086.160.216.3:50 8 0>\r\nContent-Type: application/sdp\r\nContent-
Length: 240\r\n\r\nv=0\r\no=root 9126 9126 IN IP4 86 . 64.162.35\
\r\ns=session\r\nnc=IN IP4 86.64.162.35\r\nnt=0 0\r\nnm=audio 19064 RTP/AVP 0
97 101\r\nna=rtpmap:0 PCMU/8000\r\nna=rtpmap:97 iLBC/8000\r\nna=rtpmap:101
telephone-event/8000\r\nna=fmtp:101 0-16\r\nna=silenceSupp:off - - - -\r\n' >>>
bye=sip[7] >>> raw=bye.getlayer(Raw)
>>> raw.load="BYE sip: ferda@unob.cz SIP/2.0" + raw.load[14:] >>>
packet=IP(src="86.64.162.35", dst="192.168.0.215") / UDP(sport=5060, dport=5060)
/ raw >>> send(packet)
```

Directory Enumeration (inventarizace adresáře)

- Slabá místa
 - neautorizované funkčnosti
 - protokol odpovídá jinak na platná a neplatná usernames
 - nezašifrované přenosy
- Útok
 - aktivní: speciální zprávy
 - pasivní: odchyt zpráv registračního procesu
- Účinek
 - prozrazení jmen uživatelů
- Nástroje
 - SIPCcrack, enumIAX, SIPSCAN, NeWT Security Scanner, Retina Network Security Scanner, SAINT
- Opatření
 - šifrování signalizace
 - protokoly nesmí jinak odpovídat na platná a jinak na neplatná usernames

Skenovací nástroje – NeWT Security Scanner

The screenshot displays the Tenable NeWT Security Scanner interface. The title bar reads "Tenable NeWT Security Scanner". The main header includes the Tenable NeWT logo and the text "Tenable NeWT Security Scanner". A notification banner in the top right corner asks "Are your checks up to date?" and prompts the user to "Register NeWT or purchase a direct feed of the latest security checks".

The interface features a left-hand navigation menu with the following items:

- Tenable NeWT
- Welcome
- New Scan Task
- View Reports
- Configure NeWT
- Other Options
 - Address Book
 - Manage Plugins
 - Update Plugins
- See Also
 - NeWT Help
 - About NeWT

The main content area shows a progress bar indicating "Scan in progress, 44 of 254 host(s) done." with a progress indicator at 19%.

Below the progress bar is a table with the following data:

| Host being scanned | Progress | Open Ports | Notes | Warnings | Holes |
|--------------------|----------|------------|-------|----------|-------|
| 192.168.1.1 | 5% | 3 | 4 | 0 | 0 |
| 192.168.1.22 | 1% | 3 | 4 | 0 | 0 |
| 192.168.1.24 | 97% | 3(99%) | 4 | 0 | 5 |
| 192.168.1.27 | 72% | 4 | 8 | 0 | 0 |
| 192.168.1.53 | 97% | 7 | 9 | 0 | 1 |
| 192.168.1.23 | 97% | 0 | 0 | 0 | 0 |
| 192.168.1.21 | 95% | 5 | 10 | 0 | 0 |
| 192.168.1.25 | 6% | 3(94%) | 4 | 0 | 0 |
| 192.168.1.54 | 95% | 3 | 3 | 0 | 0 |
| 192.168.1.51 | 96% | 5 | 13 | 0 | 0 |

At the bottom of the interface, there are two control buttons: "Pause" and "Stop".

Copyright © 2003-2005 Tenable Network Security, All rights reserved.

Skenovací nástroje – Tenable NeWT Security Report

Tenable NeWT Security Report - Microsoft Internet Explorer

file:///C:/Documents%20and%20Settings/Me/Tenable/NeWT/reports/html/20060222133029.xml.view_by_host.xml.htm#192.168.1.27

192.168.1.27 [Return to top]

- smtp (25/tcp)**
 - Port is open
Plugin ID : [11219](#)
- http (80/tcp)**
 - Port is open
Plugin ID : [11219](#)
 - A web server is running on this port
Plugin ID : [10330](#)
 - The remote web server type is :
Polycom SoundPoint IP Telephone HTTPd
Plugin ID : [10107](#)
- pop3 (110/tcp)**
 - Port is open
Plugin ID : [11219](#)
- sip (5060/tcp)**
 - Port is open
Plugin ID : [11219](#)
- general/tcp**
 - Synopsis :
It is possible to determine the exact time set on the remote host.
 - Description :
The remote host answers to an ICMP timestamp request. This allows an attacker to know the date which is set on your machine.
This may help him to defeat all your time based authentication protocols.
 - Solution :** filter out the ICMP timestamp requests (13), and the outgoing ICMP timestamp replies (14).
 - Risk factor :**
None / CVSS Base Score : 0
(A:V/R/AC:L/Au:NR/C:N/A:N/I:N/B:N)
CVE : CVE-1999-0524
 - Plugin ID : [10114](#)
 - The remote host is running Polycom SoundPoint IP Phone
Plugin ID : [11936](#)
 - Here is the route recorded between 192.168.1.120 and 192.168.1.27 :
192.168.1.27.
Plugin ID : [12264](#)

192.168.1.51 [Return to top]

smtp (25/tcp) Port is open

Skenovací nástroje – Retina Network Security Scanner

The screenshot displays the Retina Network Security Scanner interface. The title bar indicates it is an evaluation version with 15 days remaining. The main window is divided into several sections:

- Left Sidebar:** Contains navigation menus for "Audit Tasks" (Start Scan, Modify Address Groups, Modify Port Groups, Modify Audit Groups, Manage Credentials), "Other Places" (Discover, Remediate, Reports, Options), and "Help and Support" (Help Topics, eEye Website, Technical Support, About Retina).
- Top Panel:** Shows the current address (192.168.1.120) and scan template (Complete Scan). Below this are tabs for "Discover", "Audit", "Remediate", and "Report".
- Actions Panel:** Includes "Targets" (Advanced, 192.168.1.27), "Output Type" (File), "Filename" (test), and "Job Name" (test). Buttons for "Scan" and "Schedule" are present.
- Scan Jobs Table:** A table listing scan jobs with columns for Job Name, Status, Start Time, End Time, and Data Source. The last job is highlighted as completed.
- Scanned IPs:** A list of scanned IP addresses, with 192.168.001.027 selected.
- IP Details Panel:** Provides detailed information for the selected IP, including:
 - Ping Response:** Host Responded, Average Ping Response (8 ms), Time To Live (64), Traceroute (192.168.1.27).
 - Audits:** IP Services (ICMP Timestamp Request).
 - Machine:** Domain Name (unknown), OS Detected (Cisco 11151/Arrowpoint 150 load balancer, Neoware (was HDS) NetOS V. 2.0.1, HP ENTRIA C3230A), Closed TCP Ports (65532), Filtered TCP Ports (1), Open TCP Ports (2), Closed UDP Ports (1409), Open or Filtered UDP Ports (64126).
 - Ports:** TCP: 80 (WWW/HTTP - World Wide Web HTTP (Hyper Text Transfer Protocol)), TCP: 5060 (Unknown Port).
 - Processes:** (Empty list).
- IP Services: ICMP Timestamp Request:** Description: ICMP Timestamp request is allowed from arbitrary hosts. Admin Rights Required: No. Risk Level: Low. How To Fix: For information on how to protect against this vulnerability, upgrade to the full version of Retina. CVE: CVE-1999-0524.

At the bottom left, the status "Scan complete" is displayed.

Skenovací nástroje – SAINT

SAINT Data Collection - Mozilla

File Edit View Go Bookmarks Tools Window Help

Back Forward Reload Stop <http://domain2:32775/5277c8c9b6c60ee44e6581c1887831e//root/saint-6.0> Search Print

Home Bookmarks Red Hat, Inc. Red Hat Network Support Shop Products Training

SAINT® Examine. Expose. Exploit.

SAINT data collection

Data collection in progress...

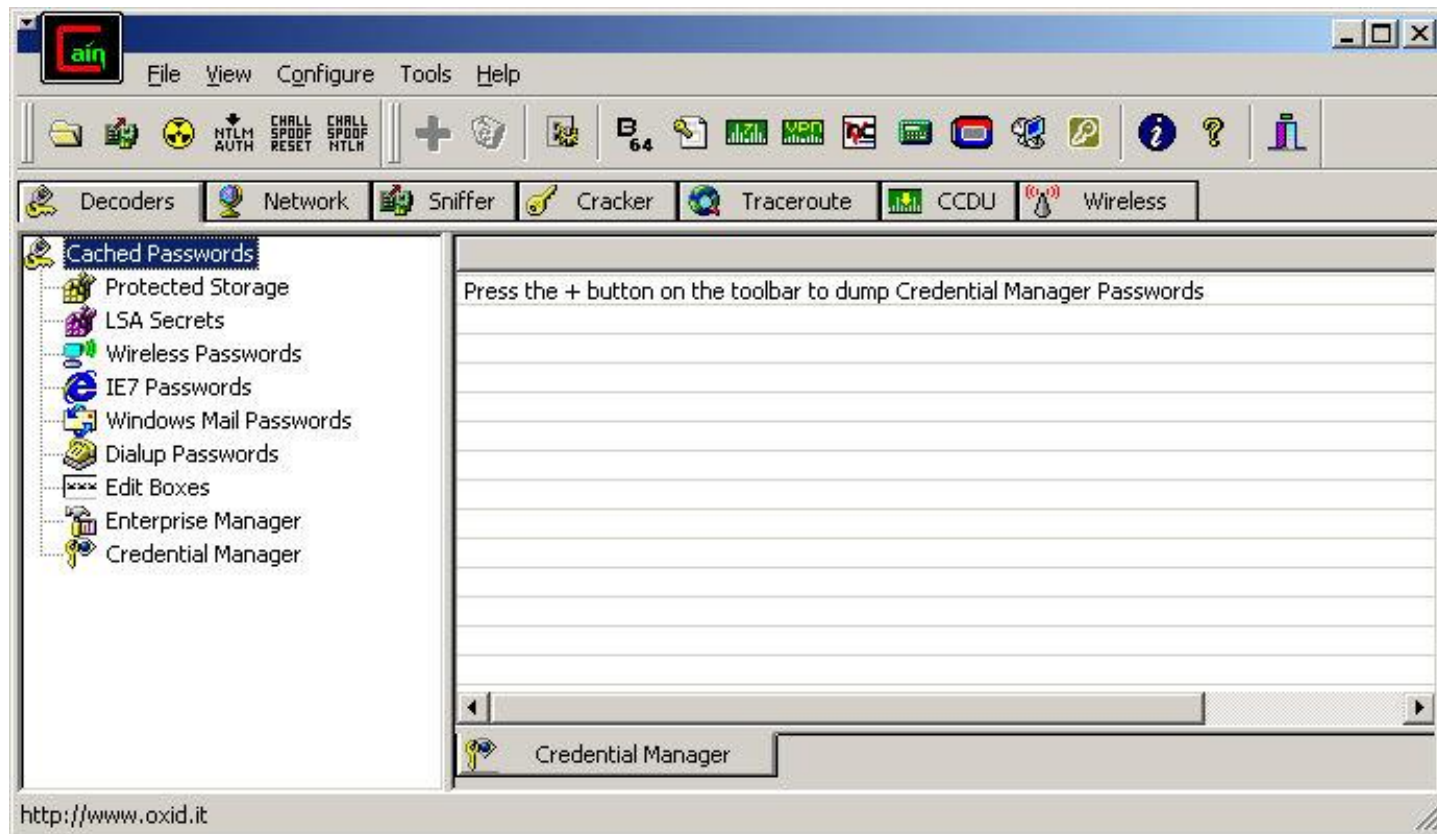
Maximum concurrent probes = 10

- Running fping -f hosts_to_fping (maximum 120 seconds)
- Running dns.saint 192.168.1.27 (maximum 45 seconds)
- Running ostype.saint 192.168.1.27 (maximum 120 seconds)
- Running tcpscan.saint
10008,10202,10203,12754,13701,13722,14247,15104,16660,20031,20432,21700,25702,27374,27665,32766,33270,33567,33568,36010,36794,41080,41523,428192.168.1.27 (maximum 1250 seconds)
- Running rpc.saint 192.168.1.27 (maximum 45 seconds)
- Running ddos.saint 192.168.1.27 (maximum 45 seconds)
- Running adore.saint 192.168.1.27 (maximum 45 seconds)
- Running udpscan.saint
1-19,53,67-69,111,123,137-139,161-162,177,1434,1812,1900,3401,5060,5135,5632,7777,8999,9900,17185,20-52,54-66,70-110,112-122,124-136,140-160,163-18192.168.1.27 (maximum 120 seconds)
- Processing data
- Processing data
- Running oracle.saint -u "" 5060:TCP 192.168.1.27 (maximum 45 seconds)
- Running proxy.saint http-connect http 192.168.1.27 (maximum 45 seconds)
- Running sybase.saint -u sa 5060:TCP 192.168.1.27 (maximum 45 seconds)
- Running http.saint -u "" -x 0 /cgi-bin/ http 192.168.1.27 (maximum 360 seconds)
- Running http.saint -u "" -x 0 / http 192.168.1.27 (maximum 360 seconds)
- Running http.saint -u "" -x 0 /scripts/ http 192.168.1.27 (maximum 360 seconds)
- Running tcp_reset.saint 5060:TCP 192.168.1.27 (maximum 45 seconds)

Transferring data from domain2...

Cain Abel: Sniffer, Password cracker

http://www.oxid.it/ca_um/



G711 uLaw, G771 aLaw, ADPCM, DVI4, LPC, GSM610, Microsoft GSM, L16, G729, Speex, iLB and my understanding is that it is

Caller-ID Name Disclosure (získání jména volajícího)

- Slabá místa

- přístup k Caller-ID

- Útok

- falešná identifikace volajícího

- Účinek

- prozrazení jména volajícího

- Nástroje

- www.fakecaller.com, www.iax.cc, www.spoofcard.com

- Opatření

- kontrola, jaké jméno je s číslem asociováno

Configuration Disclosure: Device (odhalení zařízení)

- Slabá místa

- říditelné rozhraní hardphonů
- debugging

Útok

- port 80, SNMP, debugger

Účinek

- zjištění

- Nástroje

- tcpkill

- Opatření

- raději obnovu relace než reboot

Configuration Disclosure: Infrastructure (odhalení infrastruktury)

- Slabá místa

- většina hardphonů používá pro bootování FTP nebo TFTP
- FTP není bezpečný a TFTP je na tom ještě hůře

Útok

- rekonstrukce konfigurace

Účinek

- odhalení citlivé informace (jméno uživatele, heslo, služby, server, brána, registrační server)

- Nástroje

- Wireshark, TFTP-Bruteforce, dedukce...

- Opatření

- nepoužívat TFTP, FTP je lepší, ale ne zase tak o tolik 😊
- nepoužívat defaultní jména souborů

Web Management Interface XSS

- Slabá místa

- zařízení nechrání web s jeho slabinami
- lze si zobrazit jeho logy

Útok

- vložený XSS kód

Účinek

- vykonání kódu Cross-Side-Scripting

Nástroje

- jakýkoliv zařízení VoIP s uživatelsky konfigurovatelným zobrazováním polí

- Opatření

- pokud není potřebné, je třeba webové rozhraní vypnout

A řada dalších...

- odchyt zprávk na médiu
- falešná komunikace (RTPInsetSound, RTPMixSound, RTPInject)
- změna komunikace (SteganRTP atd.)
-

IP phone reboot

- Slabá místa

- SCCP běží na TCP, který je citlivý na reset, telefon pak dělá plný reboot

Útok

- vložení paketu RST do signalizačního kanálu

Účinek

- služba je během rebootu nedostupná
- telefon rebootuje i po záplatě od Cisco

- Nástroje

- tcpkill

- Opatření

- raději obnovu relace než reboot

2. Řešení Cisco

Vývoj Cisco Unified CallManagera

- 1998, akvizice mladé společnosti Selsius Systems
- 2000 verze 3.0
- 2001 verze 3.1
- 2004 verze 4.0 a 4.1
- 2006 verze 4.2 (Unified) a 5.0
- 2007 verze 4.3 (Windows) a 5.0 (Linux)
- 2007 verzi 6.0 (Linux)
- 2008 verze 7.0
- 2010 verze 8.0.1

Šifrování hlasu od verze 4.0, od verze 5.0 i konfigurační soubory

| Parameter Name | Parameter Value | Suggested Value |
|---|---------------------------------|---------------------------------|
| Synchronization Between Auto Device Profile and Phone Configuration * | True | True |
| Max Number of Device Level Traces * | 12 | 12 |
| DSCP for Phone-based Services * | default DSCP (000000) | default DSCP (000000) |
| DSCP for Phone Configuration * | CS3(precedence 3) DSCP (011000) | CS3(precedence 3) DSCP (011000) |
| DSCP for Cisco CallManager to Device Interface * | CS3(precedence 3) DSCP (011000) | CS3(precedence 3) DSCP (011000) |
| Connection Monitor Duration * | 120 | 120 |
| Auto Registration Phone Protocol * | SCCP | SCCP |
| BLE For Cell Lists * | Disabled | Disabled |
| TETP Encrypted Configuration * | True | False |

šifrovaný konfigurační soubor

Kvalitní algoritmus: AEC-128-CBC

Autentizací proti hrozbám

- modifikace signalizace mezi telefonem a CCM
- útoky typu MITM
- útoky na identitu zařízení a serverů

Kvalitní algoritmus: HMAC-SHA-1

- podpis obrazů firmware od CCM 3.3(3)
- podpis konfiguračních souborů od CCM 4.0

Certifikáty

- nesmazatelné tovární certifikáty telefonů
- lokálně významné certifikáty
- certifikáty telefonů jako proxy funkce – vytváří seznamy CTL
- certifikát HTTPS zajišťující autentizaci mezi IIS a prohlížečem klienta
- sebou podepisovaný certifikát CCM; součást identifikace serveru
- certifikát bezpečného řešení náhrady výpadku spojení mezi telefonem a CCM

Kvalitní algoritmus pro podpis: RSA

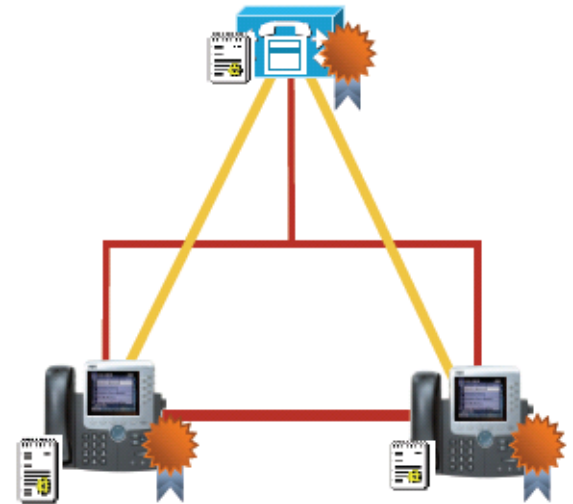
Použité kryptografické algoritmy

TLS (Transport Layer Security) mezi CCM a IP telefony:

- RSA pro podpisy
- HMAC-SHA-1 pro autentizaci
- AES-128-CBC pro šifrování

SRTP (Secure RTP) mezi IP telefony:

- HMAC-SHA-1 pro autentizaci
- AES-128-CM pro šifrování



Co není zapotřebí – je třeba vypnout

- vypnutí nastavení přístupu
- vypnutí nastavení PC Portu
- vypnutí přístupu k PC Voice VLAN
- vypnutí nastavení gratuitous ARP
 - falešné ARP odpovědi, generuje je např. ettercap či dsniff
- vypnutí webového přístupu


Zodolnění sítě pro hlasovou službu

- Oddělení hlasových a datových VLAN a nastavení ACL pro každou VLAN
- Ochrana jednotlivých portů povolením MAC adres před tzv. IP a MAC spoofingem
- Ochrana před P2P provozem a hrami pomocí tzv. scavenger-class provozu (mapuje se do DSCP CS1)
- Ochrana před útokem MITM neautorizovanými DHCP odpověďmi (DHCP Snooping)
- Ochrana před útokem MITM falešnými ARP odpověďmi

Zodolnění IP telefonu

Podepsané konfigurační soubory a firmware, vypnutí všeho zbytného

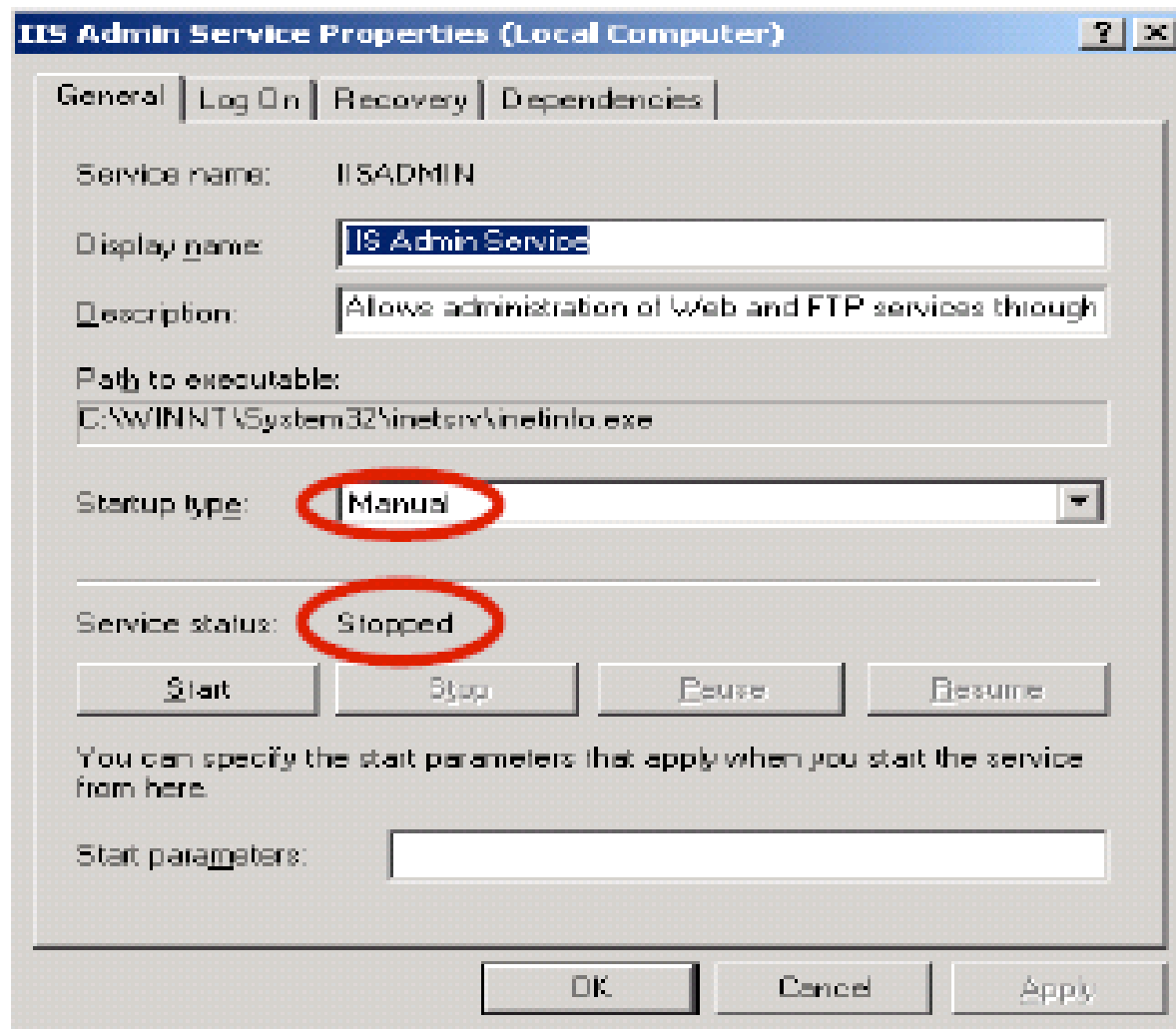
| Secure Shell Information | |
|--------------------------|----------------------|
| Secure Shell User | <input type="text"/> |
| Secure Shell Password | <input type="text"/> |

| Product Specific Configuration  | |
|--|------------|
| <input checked="" type="checkbox"/> Disable Speakerphone | |
| <input checked="" type="checkbox"/> Disable Speakerphone and Headset | |
| PC Port * | Disabled |
| Settings Access * | Restricted |
| Gratuitous ARP * | Disabled |
| PC Voice VLAN Access * | Disabled |
| Web Access * | Disabled |
| Span to PC Port * | Disabled |
| Logging Display * | Disabled |

Red arrows on the left point to the following rows in the Product Specific Configuration table:


- Disable Speakerphone
- Disable Speakerphone and Headset
- PC Port *
- Gratuitous ARP *
- Web Access *
- Span to PC Port *

Windows: 80 % útoků vede přes IIS (verze 4.3)



Problém web přístupu k IP telefonu

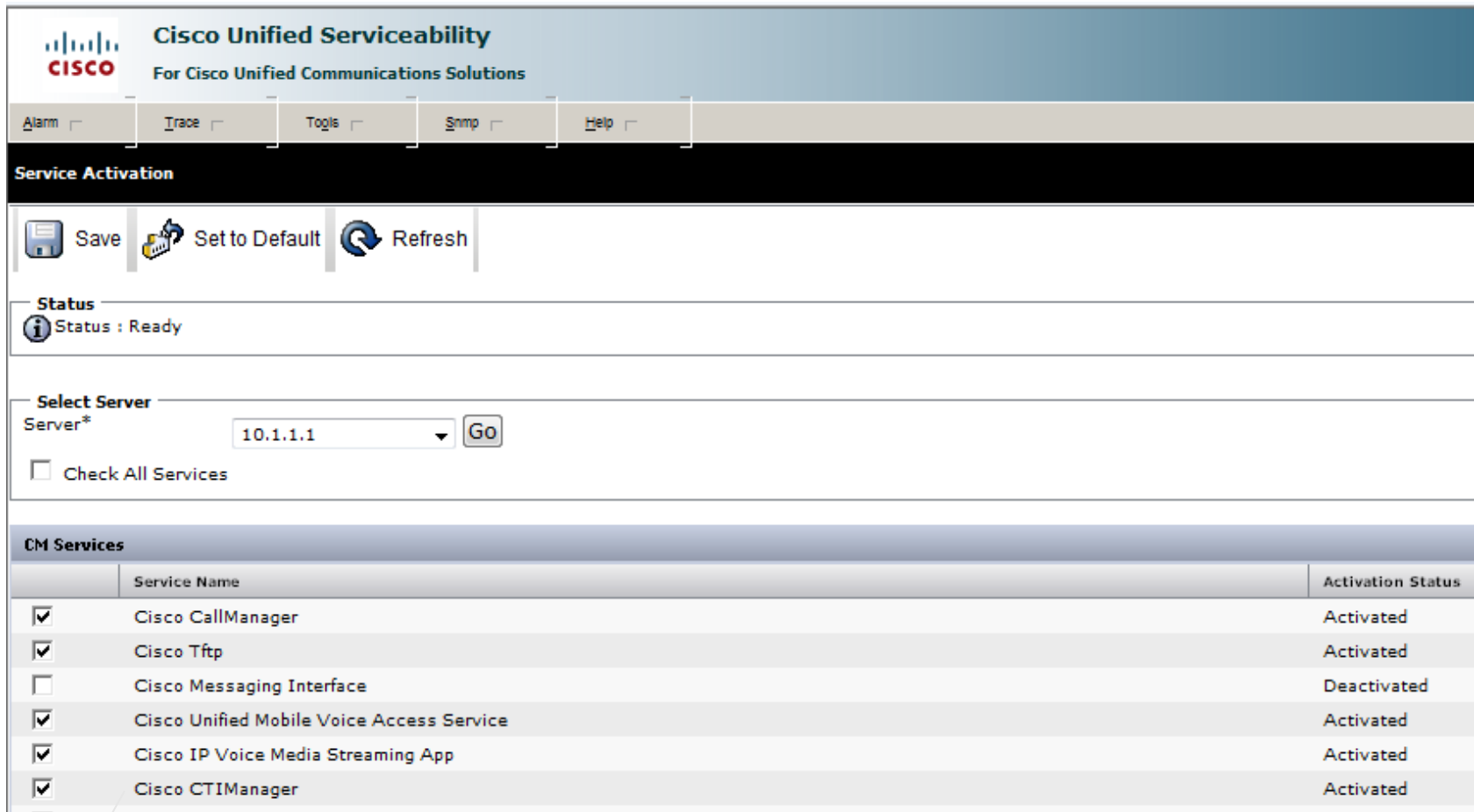
Mnoho cenných informací a vypnout to jen tak nejde (ztráta aplikací na bázi XML)

|  | | Network Configuration | |
|---|----------------|--|--|
| | | Cisco Systems, Inc. IP Phone CP-7960 (SEP003094C25E70) | |
| Device Information | DHCP Server | 10.27.15.1 | |
| Network Configuration | BOOTP Server | No | |
| Network Statistics | MAC Address | 003094C25E70 | |
| Ethernet | Host Name | SEP003094C25E70 | |
| Port 1 (Network) | Domain Name | | |
| Port 2 (Access) | IP Address | 10.27.15.27 | |
| Port 3 (Phone) | Subnet Mask | 255.255.255.0 | |
| Device Logs | TFTP Server 1 | 10.27.11.12 | |
| Debug Display | Default Router | 10.27.15.1 | |
| Stack Statistics | 1 | | |

Řešení:

ACL umožňující komunikaci mezi IP telefonem a serverem pouze přes port 80.

Aktivace potřebných služeb (verze 5.0)



The screenshot shows the Cisco Unified Serviceability web interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified Serviceability For Cisco Unified Communications Solutions". Below this are menu items: Alarm, Trace, Tools, Snmp, and Help. The main content area is titled "Service Activation" and includes buttons for Save, Set to Default, and Refresh. A "Status" section shows "Status : Ready". The "Select Server" section has a dropdown menu set to "10.1.1.1" and a "Go" button, with a "Check All Services" checkbox below it. The "CM Services" section contains a table with the following data:

| | Service Name | Activation Status |
|-------------------------------------|---|-------------------|
| <input checked="" type="checkbox"/> | Cisco CallManager | Activated |
| <input checked="" type="checkbox"/> | Cisco Tftp | Activated |
| <input type="checkbox"/> | Cisco Messaging Interface | Deactivated |
| <input checked="" type="checkbox"/> | Cisco Unified Mobile Voice Access Service | Activated |
| <input checked="" type="checkbox"/> | Cisco IP Voice Media Streaming App | Activated |
| <input checked="" type="checkbox"/> | Cisco CTIManager | Activated |

Komunikace s aplikacemi přes CTI, TAPI, JTAPI – šifrovaná a autentizovaná za pomoci certifikátu

Nové bezpečnostní vlastnosti Call Manageru 5.0 (r. 2006)

- TLS pro autentizaci a šifrování přenosu s SIP telefony
- SRTP pro komunikaci mezi SIP telefony a s bránou MGCP
- IPSec pro tunelování k branám s IOSem
- SSL pro dotazy na adresář LDAP
- HTTPS rozhraní místo HTTP; možnost generovat a rušit certifikáty
- hostující firewall
- Automaticky instalovaný Cisco Security Agent
- rychlé resety hesla (rychlý – bez obtěžování admina, bezpečný – bez přerušení služeb)
- bezpečnostní profily telefonu s protokolem SIP, SCCP či trunkem
- příjem datumu a času od NTP serveru a jejich další výdej
- rozdělení uživatelů do základní a pokročilé skupiny
- různé administrátorské účty zaručující pružnost řízení přístupu
- vypnutí po třiceti minutách pasivity

Klíčové nové či vylepšené bezpečnostní vlastnosti verze 7.1(2)

- auditní logy
- H.235
(např. MIKEY pro klíčový management SRTP)
- 802.1x EAP-FAST/TLS (RFC 4851)
místo EAP-MD5 (RFC 3847)
- Trusted Relay Point

Auditní logy



Cisco Unified CM Administration For Cisco Unified Communications Solutions

System ▾ Call Routing ▾ Media Resources ▾ Voice Mail ▾ Device ▾ Application ▾ User Management ▾

Role Configuration

Copy Add New

Role Information

Application* Cisco Call Manager Serviceability
Name*
Description

Resource Access Information

| Resource | Privilege | |
|------------------------------|--|--|
| | <input type="checkbox"/> read | <input type="checkbox"/> update |
| Alarm Configuration web page | <input type="checkbox"/> read | <input type="checkbox"/> update |
| Alarm Definition web page | <input type="checkbox"/> read | <input type="checkbox"/> update |
| Audit Configuration | <input checked="" type="checkbox"/> read | <input checked="" type="checkbox"/> update |
| Audit Trace | <input checked="" type="checkbox"/> read | <input checked="" type="checkbox"/> update |
| CDR Management | <input type="checkbox"/> read | <input type="checkbox"/> update |

novinka
pro
externisty

H.235

(CUCM se dá nastavit jako pass-through)

Gateway Configuration

Save  Delete  Copy  Reset  Apply Config  Add New

| | |
|--------------------------|------------|
| Location* | Hub_None |
| AAR Group | < None > |
| Tunneled Protocol* | None |
| QSIG Variant* | No Changes |
| ASN.1 ROSE OID Encoding* | No Changes |
| Use Trusted Relay Point* | Default |
| Signaling Port* | 1720 |

Media Termination Point Required

Retry Video Call As Audio

Wait for Far End H.245 Terminal Capability Set

Path Replacement Support

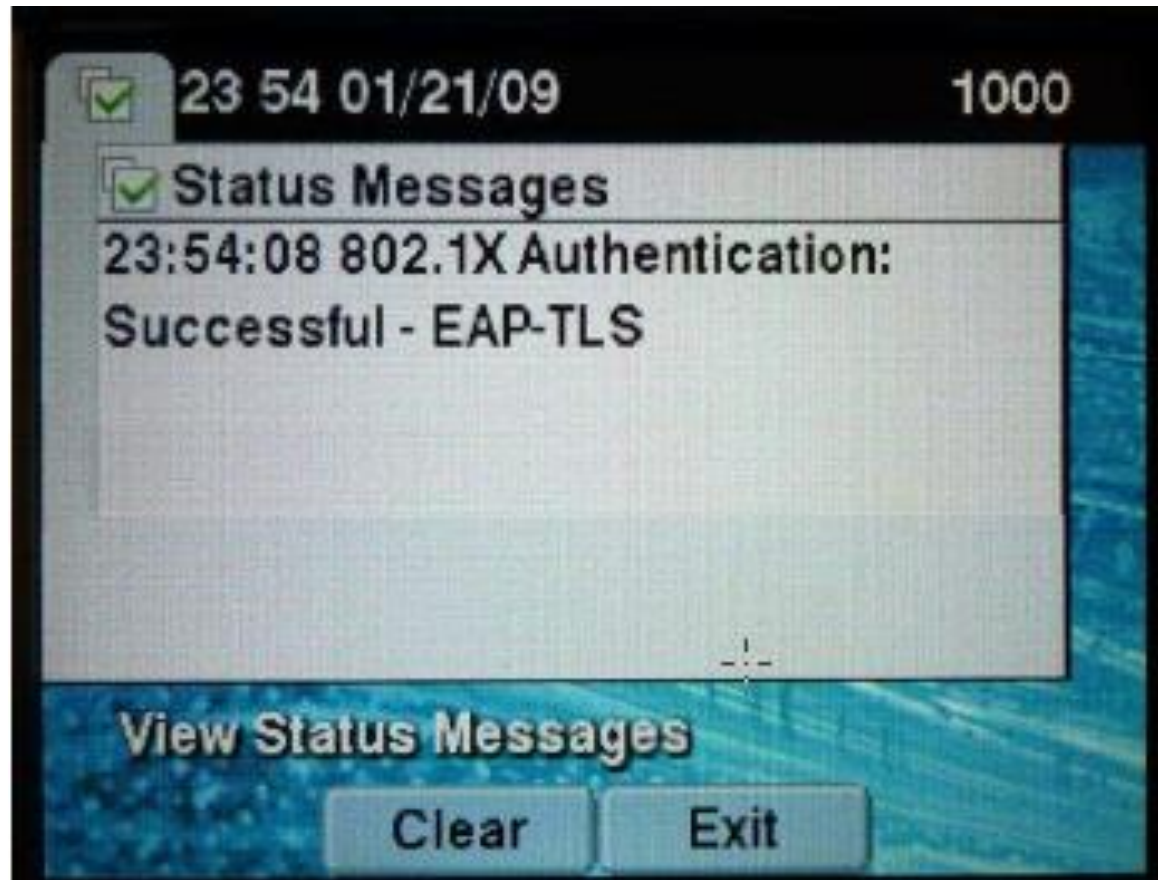
Transmit UTF-8 for Calling Party Name

SRTP Allowed - When this flag is checked, IPsec needs to be configured in the network to provide end to end security information.

H.235 Pass Through Allowed

Multilevel Precedence and Preemption (MLPP) Information


802.1x EAP-FAST/TLS



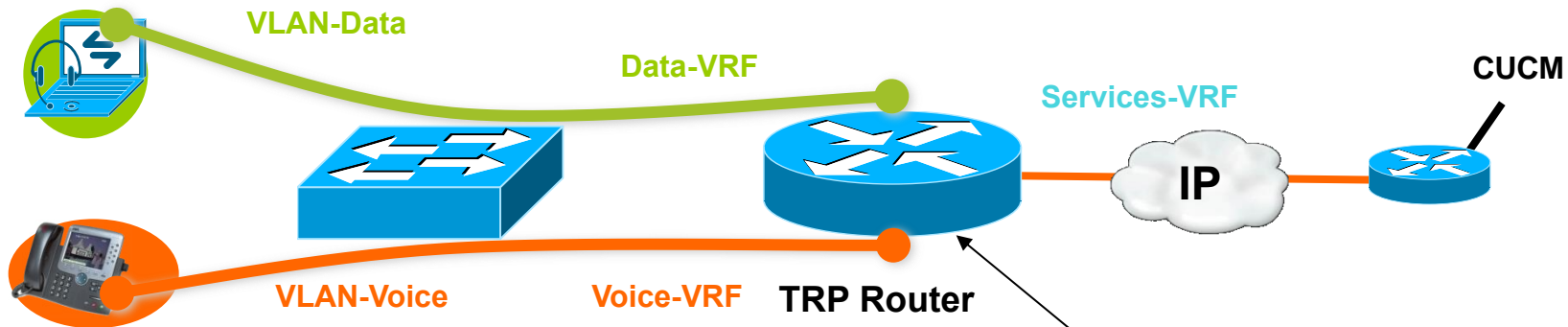
TLS zabezpečuje šifrování, autentizaci a kompresi, autentizace může být i vzájemná, nejen klienta vůči serveru

Trusted Relay Point (trusted VLAN traversal)

| | | |
|---|--|----------------------|
| Location* | siteA | |
| AAR Group | < None > | |
| User Locale | < None > | |
| Network Locale | < None > | |
| Built In Bridge* | Default | |
| Privacy* | Default | |
| Device Mobility Mode* | Default | View |
| | Current Device Mobility Settings | |
| Owner User ID | < None > | |
| Phone Load Name | | |
| Join Across Lines | Default | |
| Use Trusted Relay Point* | On | |
| BLF Audible Alert Setting (Phone Idle)* | Default | |
| BLF Audible Alert Setting (Phone | Default | |



Virtuální směrovače propojují datovou a hlasovou VLAN



```
Data-VRF  
export Data-VRF  
import Services-VRF  
!  
Voice-VRF  
export Voice-VRF  
import Services-VRF  
!  
Services-VRF  
export Service-VRF  
import Data-VRF  
import Voice-VRF
```

Nové či vylepšené bezpečnostní vlastnosti verze 8.0.1

- bezpečnostní monitoring a záznamy
- podpora HTTPS pro telefonní služby
- vylepšení kreditních služeb
- VPN klienti pro IP telefony
- bezpečnost ve výchozím nastavení
(Security by Default)

Bezpečnostní monitoring a záznamy

- příposlechy
- problémy se šifrováním, zvláště u více proudů
- použití Trusted Relay Pointu

Podpora HTTPS

Extension Mobility a to nově i mezi klastry

Service Information

| | |
|---------------------|---|
| Service Name* | EM |
| ASCII Service Name* | EM |
| Service Description | EM |
| Service URL | http://10.89.82.36:8080/emapp/EMAppServlet?device: |
| Secure-Service URL | https://10.89.82.36:8080/emapp/EMAppServlet?device: |
| Service Category* | XML Service ▼ |
| Service Type* | Standard IP Phone Service ▼ |
| Service Vendor | |
| Service Version | |

Enable

Enterprise Subscription

Vylepšení kreditních služeb



VPN klienti pro IP telefony

- tři způsoby

- směrovač – směrovač doma

je ho třeba konfigurovat a spravovat

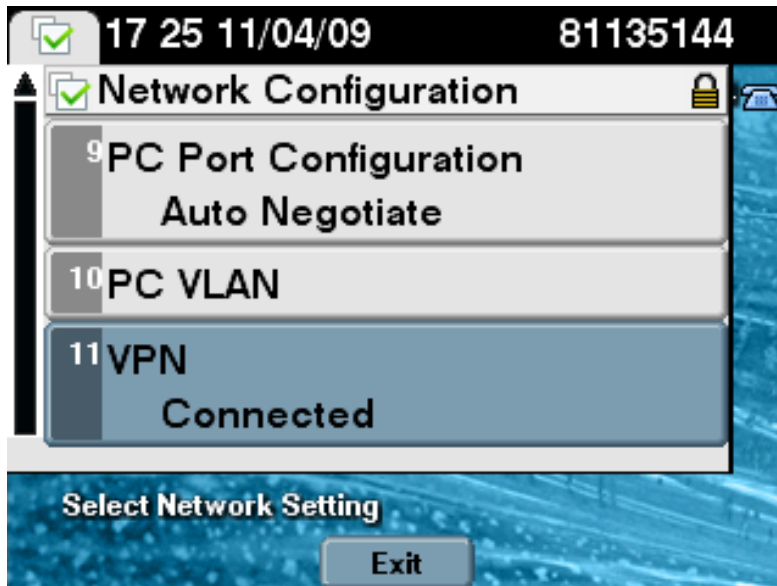
- telefon doma s TLS + SRTP – ASA

phone-proxy – mohou jen telefonovat

- SSL VPN (nové)

mohu volat z domu a užívat si všech služeb bez omezení

Nastavení SSL VPN na telefonu



Nastavení parametrů SSL VPN na CUCM

VPN Parameters



| Parameter Name | Parameter Value | Suggested Value |
|--|-------------------|-------------------|
| Enable Auto Network Detect * | False | False |
| MTU * | 1290 | 1290 |
| Keep Alive * | 60 | 60 |
| Fail to Connect * | 30 | 30 |
| Client Authentication Method * | User And Password | User And Password |
| Enable Password Persistence * | False | False |
| Enable Host ID Check * | True | True |

Security by Default

Oddělení certifikátů pro podepisování/šifrování a podporu HTTPS, pro interní a externí použití atd.

Otázka

Jaký je základní princip ochrany sítě vybavené IP telefony?

Řešení: komplexní ochrana

| | Telefon | Přepínač | Směrovač | Síť | CUCM | Server |
|----------------------|---------|----------|----------|-----|------|--------|
| Odposlech | X | X | X | X | X | X |
| Zahlčení | X | X | X | X | X | X |
| Vložení | X | X | X | X | X | X |
| Útok na aplikace | X | X | X | X | X | X |
| Útok na Soft klienta | X | X | X | X | X | X |
| Krádeže | X | X | X | X | X | X |

3. Útoku na IP telefonii v LAN

Příklady útoků na IP telefonii v sítích Cisco

- Přeplnění tabulky CAM u Cisco sítí
- Útok vygenerováním falešných BPDU
- Útok pomocí odchycené MAC adresy
- Neautorizované DHCP a ARP odpovědi

Tabulka CAM

Jak se s tabulkou CAM (Content-Addressable Memory) pracuje ukazuje následující slajd.

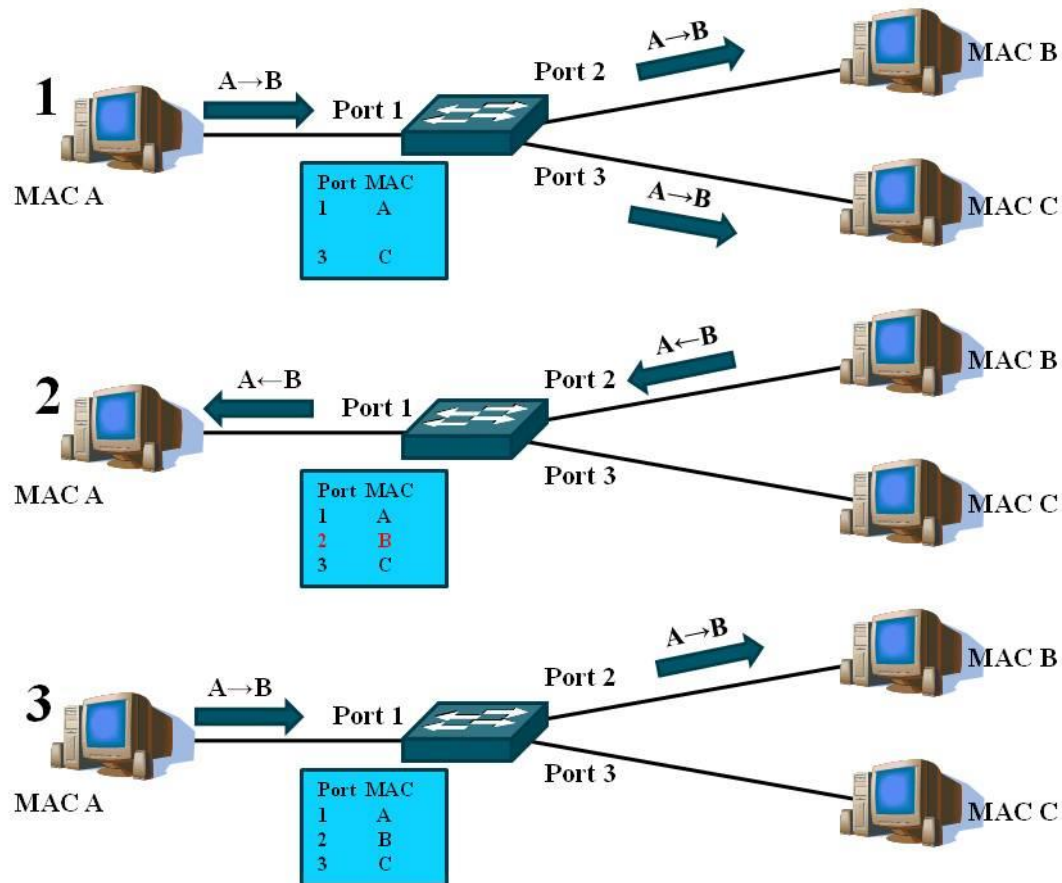
Tabulka CAM registruje MAC adresy přiřazené ke konkrétním portům. PC s MAC adresou A a C jsou registrovány v tabulce CAM, PC s MAC B ne.

Pokud posílá PC A rámeček PC B, je rozeslán všem koncovým stanicím připojeným k přepínači (1).

Pokud ale přijde první rámeček z cílové stanice B, je tato zaznamenána do tabulky CAM (2). Od této doby jsou rámce pro stanici B posílány přímo na ni. Pokud ale začne útočník generovat jeden rámeček za druhým s vymyšlenými MAC adresami odesílatele, je schopen brzy z tabulky CAM vytlačit relevantní údaje a pak se rámce rozhlašují způsobem 1.

Je zřejmé, **že tabulka CAM je nejslabším místem přístupových sítí.**

Přeplnění tabulky CAM u Cisco sítí



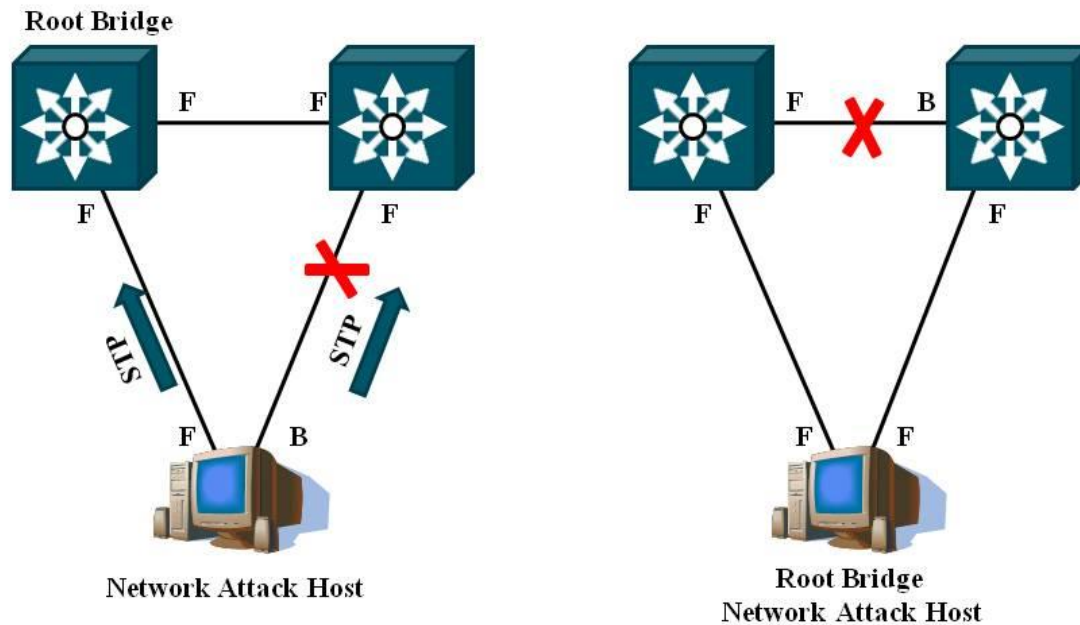
Falešný kořen stromu

Pro volbu falešného kořene stromu (topologicky kostra grafu) stačí vygenerovat rámec BPDU s nejmenší hodnotou priority v síti a tím přinutit ostatní přepínače k tomu, aby zvolily ten, u kterého je připojen útočník, za kořen stromu.

Obrana je jednoduchá – zakázat takové BPDU na jiných portech než k relevantním přepínačům či definovat kořen:

```
S1 (config) #spanning-tree vlan 1-1000 root primary
```

Útok vygenerováním falešných BPDUs

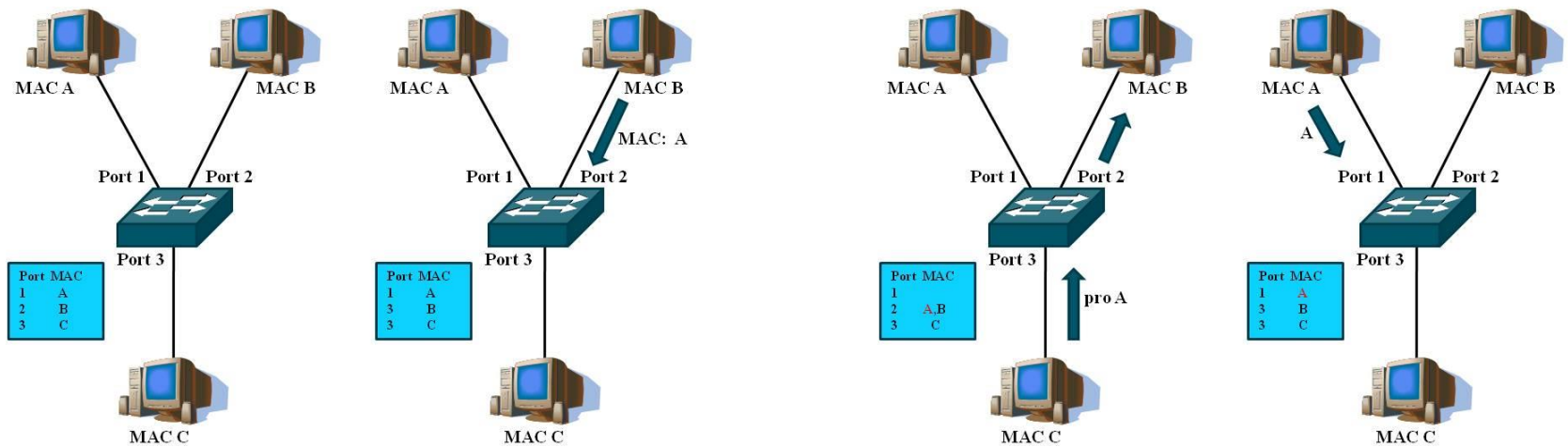


Útok s využitím falešné MAC adresy

- (1) Přepínač má přehled o koncových stanicích.
- (2) PC s MAC B se ohlašuje s falešnou adresou A jako adresou odesilatele.
- (3) Rámce určené pro PC A tečou k PC B.
- (4) Rámec odesílaný uzlem A vše napravuje, možná jen dočasně.

Jak se tomuto útoku bránit? Definovat bezpečnost na portu pomocí příkazu je u rozsáhlejších LAN problematické a tak je vhodnější použití složitějšího prostředku a to VLAN.

Útok pomocí odchycené MAC adresy



DHCP snooping binding

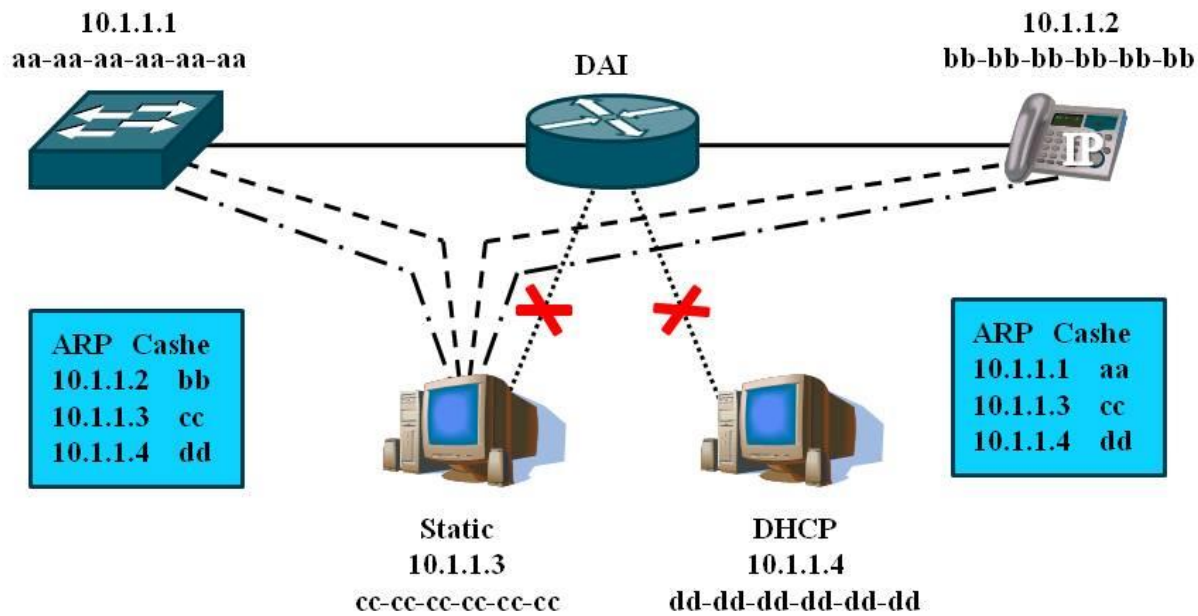
Je třeba zajistit, aby DHCP odpovědi (DHCP Offer, DHCP Ack nebo DHCP Nak) přicházely pouze od relevantního DHCP serveru. To je zajištěno pomocí tzv. **DHCP snooping binding** tabulky obsahující MAC adresu, IP adresu, lease time, binding type, číslo VLAN a specifikace nechráněného rozhraní.

Dynamic ARP Inspection (DAI, také ARP poisoning, ARP Poison Routing) je zase bezpečnostní vlastnost, která má pod dohledem výskyt ARP paketů v síti. DAI umožňuje správci sítě logovat a rušit ARP pakety s neoprávněnou MAC adresou. Cílem je zabránit útoku typu „man-in-the-middle“ (MitM). Útok typu MitM je založen na používání tzv. „nevyžádaných“ ARP paketů zvaných **gratuitous ARP packets**. Jedná o pakety, kterými stanice oznamuje vazbu mezi IP a MAC adresou (ARP Reply), aniž by obdržela požadavek na vyslání takové informace (ARP Request).

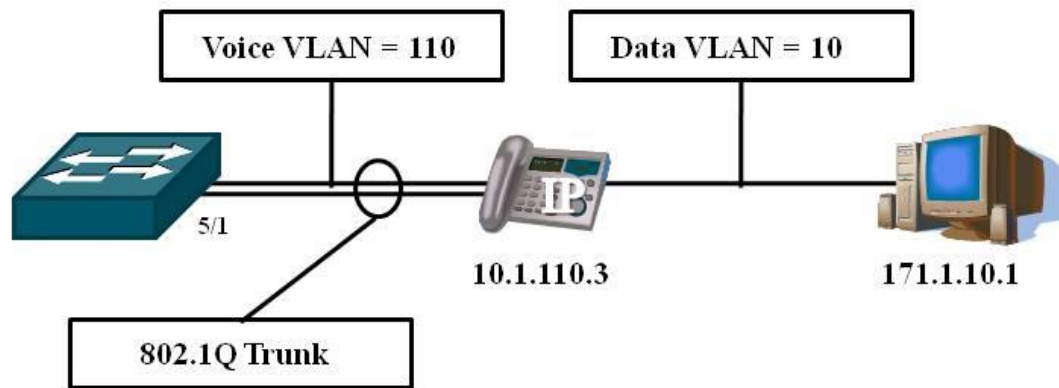
Stanice většinou nevyžádaný ARP paket přijme a informace z něj si zapíše do ARP cache a používá je. Útočník může například pomocí gratuitous ARP podstrčit stanicím svou MAC adresu místo MAC adresy síťové brány. Stanice pak posílají data do jiných podsítí přes počítač útočníka, který je odposlouchává. Obranou je **Dynamic ARP Inspection** (DAI), které využívá tabulku, vybudovanou při DHCP Snoopingu.

Neboli pokud počítač s MAC adresou dd-dd-dd-dd-dd-dd začne posílat falešné DHCP odpovědi, prepínač je nepřijme, protože nejde o důvěryhodný zdroj DHCP informace. Navíc si buduje tabulku DAI, pomocí které kontroluje ARP odpovědi. Pokud útočník z počítače s MAC adresou cc-cc-cc-cc-cc-cc začne posílat ARP odpovědi, nebude mu věřeno.

Neautorizované DHCP a ARP odpovědi



Oddělení hlasových a datových VLAN



Pokyny ke zkoušce



Pozor na <http://www.voiptroubleshooter.com/diagnosis/>