

## Voice-over-IP Risk Analysis

Enno Rey, CISSP/ISSAP, CISA  
erey@ernw.de



## ISO/IEC GUIDE 73:2002

“Combination of the **probability** of an **event** and its **consequence**“

**where**

Probability = extent to which an **event** is likely to occur

Event = occurrence of a particular set of circumstances

Consequence = outcome of an **event**



## ISO/IEC GUIDE 73:2002

“systematic use of information to identify **sources** and to estimate the **risk**“

Source: item or activity having a potential for a **consequence**

- Risk analysis provides a basis for **risk evaluation, risk treatment** and **risk acceptance**.
- Information can include historical data, theoretical analysis, informed opinions, and the concerns of **stakeholders**.



# Security Objectives VoIP

- **Availability**
- **Confidentiality**
- **Privacy**
- **Integrity (?)**
  - - of calls/transported data
  - - of billing data/arrival time of voice mails/state of communication participants/etc.
- **Compliance with regulations (Privacy protection, Lawful interception, 911 calls, other)**
  
- **Prevention/avoidance of**
  - identity spoofing
  - - of caller/callee (both may lead to social engineering attacks)
  - => billing fraud
  - => other fraud (telephone banking)
  
  - covert channels (*Skype*)



# VoIP – Threats (“Sources”)

- Threats on protocol level
- Threats on connection level
- Threats on gateway level
- Threats on endpoint level
  
- Remote control of hosts / covert channels

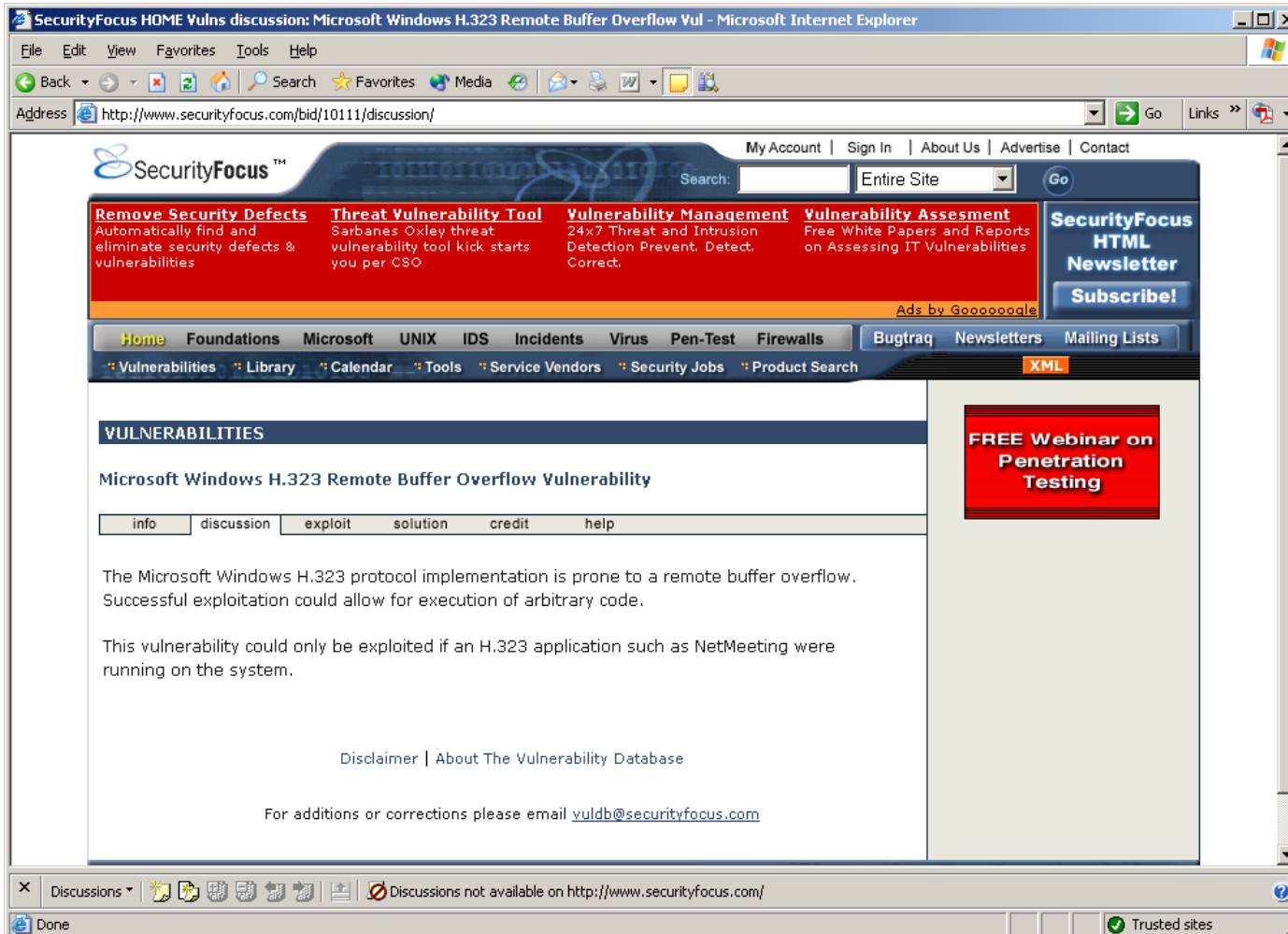


# Threats on protocol level

- **TP1: Poorly designed protocols may lead to breach of conf/int/avail**
- **TP2: Bad implementations suffering from buffer overflows etc.**
- **TP3: Protocol complexity may lead to bad firewall configuration**



# Example: Bad implementation with buffer overflow



SecurityFocus HOME Vulns discussion: Microsoft Windows H.323 Remote Buffer Overflow Vul - Microsoft Internet Explorer

Address: <http://www.securityfocus.com/bid/10111/discussion/>

SecurityFocus™

Remove Security Defects: Automatically find and eliminate security defects & vulnerabilities

Threat Vulnerability Tool: Sarbanes Oxley threat vulnerability tool kick starts you per CSO

Vulnerability Management: 24x7 Threat and Intrusion Detection Prevent, Detect, Correct.

Vulnerability Assessment: Free White Papers and Reports on Assessing IT Vulnerabilities

SecurityFocus HTML Newsletter  
Subscribe!

Home Foundations Microsoft UNIX IDS Incidents Virus Pen-Test Firewalls Bugtraq Newsletters Mailing Lists XML

Vulnerabilities Library Calendar Tools Service Vendors Security Jobs Product Search

**VULNERABILITIES**

Microsoft Windows H.323 Remote Buffer Overflow Vulnerability

info discussion exploit solution credit help

The Microsoft Windows H.323 protocol implementation is prone to a remote buffer overflow. Successful exploitation could allow for execution of arbitrary code.

This vulnerability could only be exploited if an H.323 application such as NetMeeting were running on the system.

Disclaimer | About The Vulnerability Database

For additions or corrections please email [vuldb@securityfocus.com](mailto:vuldb@securityfocus.com)

Discussions not available on <http://www.securityfocus.com/>

# Threats on connection level

- **TC1: Eavesdropping / Call Monitoring (Breach of confidentiality)**
- **TC2: Data Corruption / Modification (Breach of integrity)**
- **Denial-of-Service (Loss of availability)**  
**TC3: - by attack**  
**TC4: - by misconfig. (e.g. insufficient resources/prioritization)**



# Threats on gateway level

- **Note: term “gateway“ applies to any central component like gateways, gatekeepers, call managers (CM), session border controllers (SBC), SIP proxies/registrars/redirectors etc.**
- **TG1: System compromise**
  - ⇒ Eavesdropping
  - ⇒ Call redirection
  - ⇒ Billing fraud
- **Denial-of-Service** (Loss of availability)
  - TG2: - by attack**
  - TG3: - by misconfiguration**



# Threats on endpoint level

- **TE1: System compromise**
  - ⇒ Eavesdropping
  - ⇒ Call redirection
  - ⇒ Billing fraud
- **TE2: Denial-of-Service** (Loss of availability)  
- by attack
- **TE3: VoIP endpoint as attack vector for malware spread**  
(applies particularly to softphones)
- **TE4: Covert channels**



# Vulnerabilities

- **Vulnerabilities on protocol level**
- **Vulnerabilities on connection level**
- **Vulnerabilities on gateway level**
- **Vulnerabilities on endpoint level**

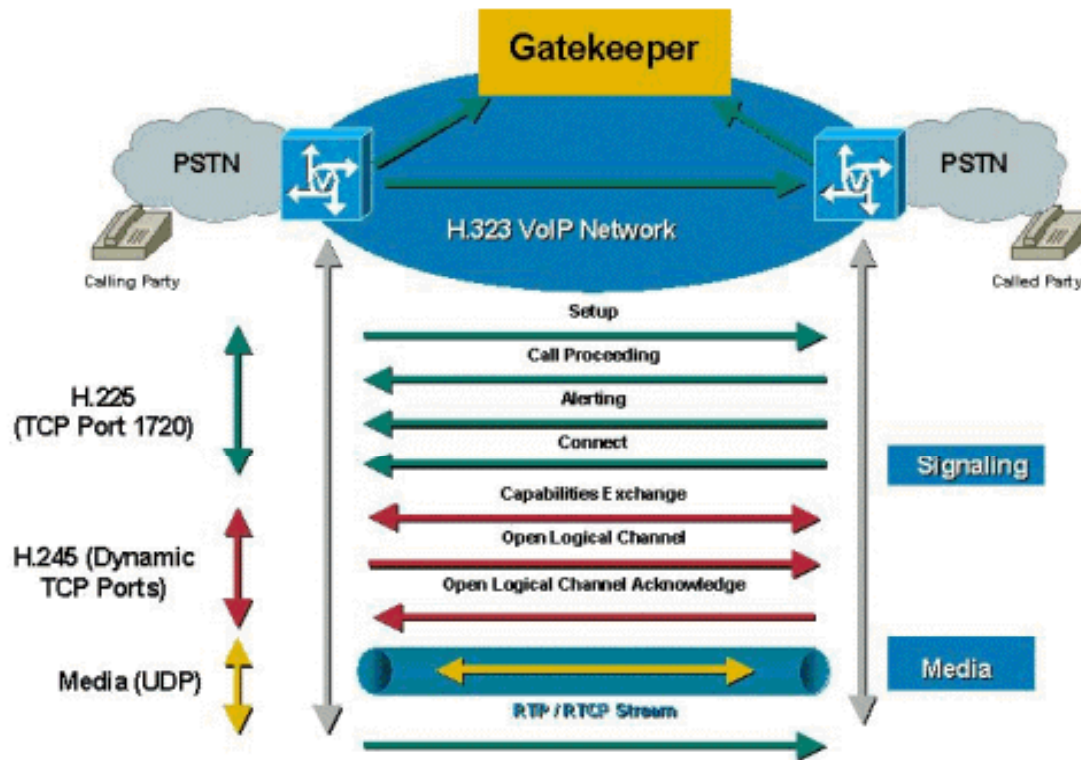


# Vulnerabilities on protocol level

- **Designed without security in mind**
- **Protocols work with highly dynamic port assignments**



# Example: Dynamic port assignments



```

value RasMessage = registrationRequest
{
  requestSeqNum 3923
  protocolIdentifier { 0 0 8 2250 0 2 }
  discoveryComplete FALSE
  callSignalAddress
  {
  }
  rasAddress
  {
    ipAddress
    {
      ip '8DF52B03'H
      port 54338
    }
  }

  terminalType
  {
    mc FALSE
    undefinedNode FALSE
  }
  gatekeeperIdentifier {"Bxl-GK"}
  endpointVendor

```

141.245.43.3:54338  
IP Address:Port embedded in  
H.323 signaling

# Vulnerabilities on connection level

- **Nearly no encryption by default**
- **SRTP not used due to inter-vendor keymgmt incompatibilites**

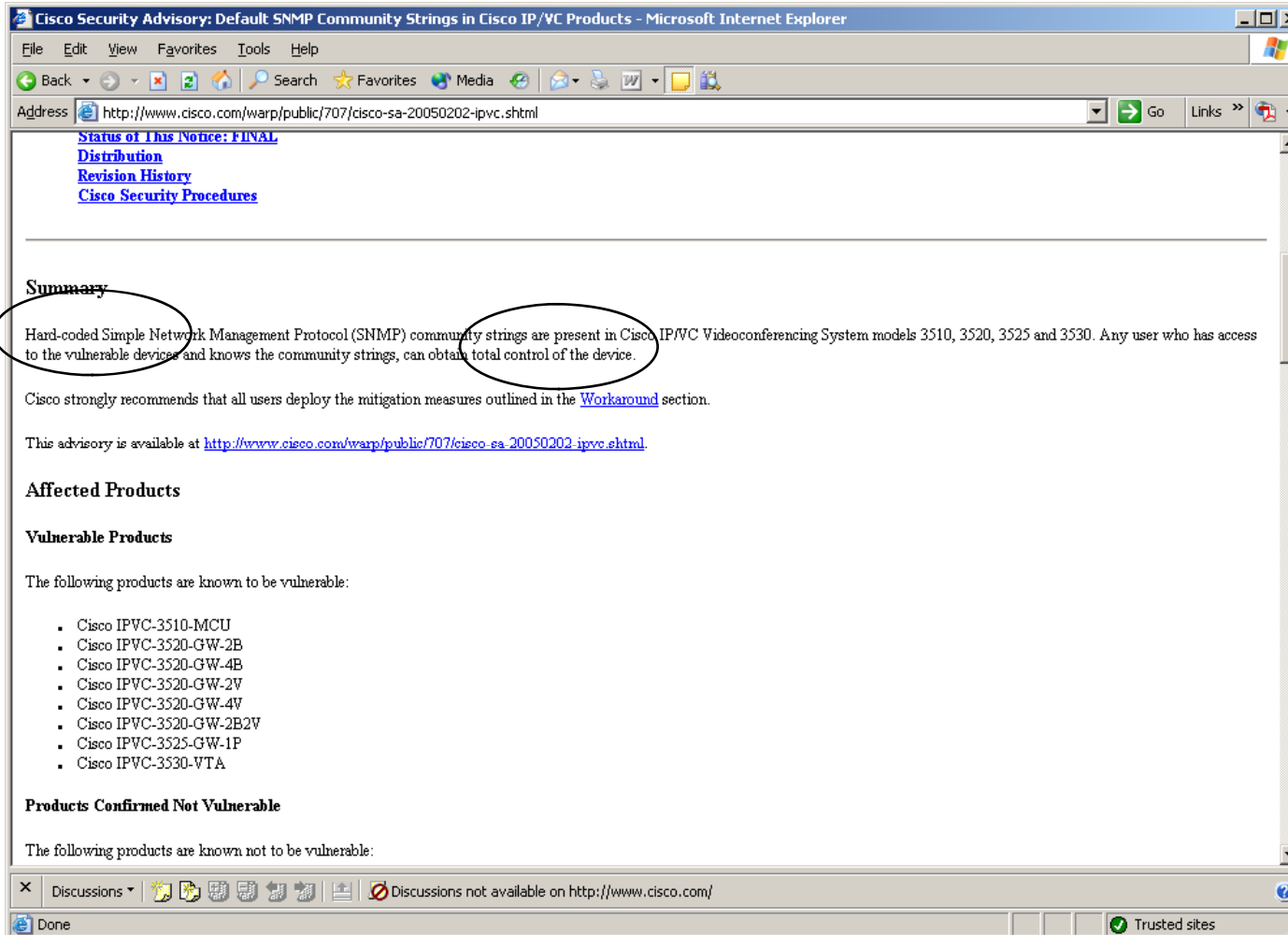


# Vulnerabilities on gateway level

- **Designed/assembled/configured without security in mind**
- **Unsecure default configurations**
- ***Segregation of duties* principle may be violated**



# Example: Components with “teething problems“



Cisco Security Advisory: Default SNMP Community Strings in Cisco IP/VC Products - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvcs.html> Go Links >>

[Status of This Notice: FINAL](#)  
[Distribution](#)  
[Revision History](#)  
[Cisco Security Procedures](#)

---

**Summary**

Hard-coded Simple Network Management Protocol (SNMP) community strings are present in Cisco IP/VC Videoconferencing System models 3510, 3520, 3525 and 3530. Any user who has access to the vulnerable devices and knows the community strings, can obtain total control of the device.

Cisco strongly recommends that all users deploy the mitigation measures outlined in the [Workaround](#) section.

This advisory is available at <http://www.cisco.com/warp/public/707/cisco-sa-20050202-ipvcs.html>.

**Affected Products**

**Vulnerable Products**

The following products are known to be vulnerable:

- Cisco IPVC-3510-MCU
- Cisco IPVC-3520-GW-2B
- Cisco IPVC-3520-GW-4B
- Cisco IPVC-3520-GW-2V
- Cisco IPVC-3520-GW-4V
- Cisco IPVC-3520-GW-2B2V
- Cisco IPVC-3525-GW-1P
- Cisco IPVC-3530-VTA

**Products Confirmed Not Vulnerable**

The following products are known not to be vulnerable:

Discussions not available on <http://www.cisco.com/>

Done Trusted sites

# Vulnerabilities on endpoint level

- **Unsecure default configurations**
- **Poorly implemented (see *Shawn Merdinger's* research)**
- **Softphones may be prone to buffer overflows**
- ***Isolation* of softphones' traffic may be difficult**



# Example: Softphones may be prone to buffer overflows



The screenshot shows a web browser displaying the ERNW website. The address bar shows the URL: [http://www.ernw.de/en/eng\\_security\\_advisories.html](http://www.ernw.de/en/eng_security_advisories.html). The page header includes the ERNW logo and the tagline "Wir leben IT-Security". A navigation menu is visible with items: News, Services, References, Team, IT-Security Competence Center, .NET Competence Center, and Contact. The main content area features a green sidebar with links to Publications, Advisories, and Tools. The main article is titled "ERNW Security Advisory 02-2005 Buffer Overflow in SIP Foundry's SipXtapi". The author is Michael Thumann, with contact information: [mthumann\[at\]ernw.de](mailto:mthumann[at]ernw.de) and [www.ernw.de](http://www.ernw.de). The advisory details a critical buffer overflow in the sipXtapi library, which can be exploited to gain control over EIP and execute arbitrary code. It lists affected products: sipXtapi (all versions before 24 of March 2006), PingTel products, and AOL Triton. A search bar is located at the bottom right of the page.

http://www.ernw.de/en/eng\_security\_advisories.html

ERNW - IT-Security Competence Center

We embrace IT-Security. ERNW Wir leben IT-Security

>> Deutsche Version

News Services References Team IT-Security Competence Center .NET Competence Center Contact

>> Publications  
>> Advisories  
>> Tools

**ERNW Security Advisory 02-2005**  
Buffer Overflow in SIP Foundry's SipXtapi

Author:  
Michael Thumann <mthumann[at]ernw.de>  
Homepage: [www.ernw.de](http://www.ernw.de)

1. Summary:  
The sipXtapi library from sip foundry contains a buffer overflow when parsing the CSeq field.  
This flaw can be used by an attacker to gain control over EIP and execute arbitrary code.

2. Severity : Critical

3. Products affected  
- sipXtapi: all version compiled before 24 of march 2006  
- PingTel products  
- AOL Triton

4. Patch Availability:

>> Company >> Legal Notice

Search ERNW:  >> Start Search

# Toolbox of Mitigating Controls

- **Mitigating Controls are taken from/named accordingly to *Common Criteria* to use exact terminology.**
- **Only those relevant to VoIP were chosen.**
- **In the course of the risk analysis itself they will be referenced just by their *class* name. This means some of the controls listed *in this document*, in that class, can/should be implemented to mitigate the respective risk.**



- **Class FAU: SECURITY AUDIT**
  - FAU\_GEN "Security audit data generation"**
  - FAU\_STG "Security audit event storage"**
  - FAU\_SAR "Security audit review"**
  - FAU\_SAA "Security audit analysis"**
  
- **CLASS FCO: COMMUNICATION**
  - FCO\_NRO "Non-repudiation of origin"**
  - FCO\_NRR "Non-repudiation of receipt"**



- **Class FCS: CRYPTOGRAPHIC SUPPORT**  
FCS\_CKM "Cryptographic key management"  
FCS\_COP "Cryptographic operation"
- **CLASS FDP: USER DATA PROTECTION**  
FDP\_ACC "Access control policy"  
FDP\_ACF "Access control functions"  
FDP\_DAU "Data authentication"  
FDP\_IFC/FDP\_IFF "Information flow control policy / functions"  
FDP\_SDI "Stored data integrity"  
FDP\_UCT/FDP\_UIT "Inter-TSF user data confidentiality / integrity transfer protection"



- **Class FIA: IDENTIFICATION AND AUTHENTICATION**

- FIA\_AFL "Authentication failures"

- FIA\_UAU "User authentication"

- FIA\_UID "User identification"

- **CLASS FMT: SECURITY MANAGEMENT**

- FMT\_MOF "Management of functions in TSF"

- FMT\_MSA "Management of security attributes"

- FMT\_MTD "Management of TSF data"

- FMT\_REV "Revocation"

- FTM\_SMF "Specification of Management Functions"

- FMT\_SAE "Security attribute expiration"

- FMT\_SMR "Security management roles"



- **Class FPT: PROTECTION OF THE TSF**  
FPT\_RPL "Replay detection"  
FPT\_STM "Time stamps"  
FPT\_TDC "Inter-TSF TSF data consistency"
- **CLASS FRU: RESOURCE UTILISATION**  
FRU\_FLT "Fault tolerance"  
FRU\_PRS "Priority of service"  
FRU\_RSA "Resource allocation"



- **Class FTA: TOE ACCESS**
  - FTA\_MCS "Limitation on multiple concurrent sessions"**
  - FTA\_TAB "TOE access banners"**
  - FTA\_TAH "TOE access history"**
  - FTA\_TSE "TOE session establishment"**
- **CLASS FTP: TRUSTED PATH/CHANNELS**
  - FTP\_ITC "Inter-TSF trusted channel"**



# Risk Analysis

- Protocol level
- Connection level
- Gateway level
- Endpoint level



# RA, Methodology used

- Numbers for likelihood and impact were chosen on a scale from one to five.
- Rating of impact is based on a mixture of several factors (breach of/loss of confidentiality/integrity/availability, violation of regulations).  
The impact rating largely depends on individual/environment/objectives/settings. Your mileage might vary...

## Nevertheless some notes:

- non-compliance nearly always leads to a “5”
  - loss of availability rarely gets a “5”  
(5 only used for “disaster” cases, which are out of scope here)
  - sometimes rating of impact depends on host count/scale concerned
- Assignment of numbers to respective threads is based on “VoIP security common body of knowledge” and author’s experience/research.
  - Here the risk is calculated by simple multiplication (see BS 7799-3, 5.7).



# RA Protocol Level

Source	Likelihood	Rating of & Consequence(s)	Risk	Mitigating Controls
TP1, Poor protocol design	1	5 Breach of con/int, Non-Compliance	5	Class FCS, Class FDP
TP2, Implementat. leading to BO	1	5 Compromise of components	5	Class FAU, Class FDP
TP3, Bad firewall config	3	3 Larger possible attack surface	9	Class FDP, Stateful firewalls/ALGs



# RA Protocol Level, Notes

- Since *Oulu University Secure Programming Group* research [1] on SIP and H.323 their common implementations can be considered less vulnerable.
- Presently most major firewalls are able to cope with SIP, H.323 and RTP without huge problems but still additional proprietary ports (e.g. for connections to CM or SBC) needed frequently.



# RA Connection Level

Source	Likelihood	Rating of & Consequence(s)	Risk	Mitigating Controls
TC1, Eavesdrop. / Call Monitor.	2	5 Breach of conf., Non-Compliance	10	Class FCS, Class FDP, NW-Segmentation
TC2, Data Modification	2	5 Breach of conf., Non-Compliance	10	Class FCS, Class FDP, NW-Segmentation
TC3, DoS by attack	3	4 Loss of service	12	Class FRU, NW-Segmentation, SLAs
TC4, DoS due to misconfig	2	4 Loss of service	8	Class FRU, Class FMT, Operational procedur.



# RA Connection Level, Notes

- **Most important tools to eavesdrop VoIP connections include:**  
*vomit*  
*wireshark*  
*cain & abel*  
*oreka*



# RA Gateway Level

Source	Likelihood	Rating of & Consequence(s)	Risk	Mitigating Controls
<b>TG1, System compromise</b>	<b>3</b>	<b>5 Breach of conf., Non-Compliance</b>	<b>15</b>	<b>Class FMT, Class FDP, Hardening &amp; OpSec</b>
<b>TG2, DoS by attack</b>	<b>3</b>	<b>4 Loss of service</b>	<b>12</b>	<b>Class FRU, Class FTA</b>
<b>TG3, DoS due to misconfig</b>	<b>2</b>	<b>4 Loss of service</b>	<b>8</b>	<b>Class FRU, Class FMT, Operational Procedur.</b>



# RA Gateway Level, Notes

- **Special attention should be paid to**
  - **SNMP**
  - **Default passwords (mgmt access, configured users)**
- **Apply usual hardening steps before going productive and (pen-) test!**
- **Bad protocol implementations may have side effects on devices purportedly not running VoIP at all (see for example [3]).**



# RA Endpoint Level

Source	Likelihood	Rating of & Consequence(s)	Risk	Mitigating Controls
TE1, System compromise	2	4 Breach of conf., Non-Compliance	8	Class FMT, Class FDP, Hardening & OpSec
TE2, DoS by attack	1	3 Loss of service	3	Class FRU, Class FRA
TE3, Malwa. spread	3	5 Loss of service, Backdoors	15	Class FRU, Class FMT, Operational Procedur.
TE4, Covert chann.	3	5 Breach of con/int corporate level	15	FAU_SAA (IDS), Desktop OpSec “Do not use Skype!”



# RA Endpoint Level, Notes

- **Special attention should be paid to**
  - **SNMP**
  - **Open Ports/running services (e.g. Telnet)**
- **See presentations and advisories of *Shawn Merdinger*.**
- **(Strong) Authentication is your friend here.**
- **802.1x in the meantime available for some hardphones, check preferred vendor.**
- **Remember trunking/DTP security problems when using Cisco “Voice VLANs“...**
- **Did I already mention? ;-) Do not run *Skype*! Why? See [2] and [4].**



## Questions & Answers



# References

[1] *Oulu University Secure Programming Group*:  
<http://www.ee.oulu.fi/research/ouspg/>

[2] *Hackers call on Skype to spread Trojan*:  
[http://www.theregister.co.uk/2006/12/20/skype\\_trojan/](http://www.theregister.co.uk/2006/12/20/skype_trojan/)

[3] *Cisco Security Advisory: Vulnerabilities in H.323 Message Processing*:  
[http://www.cisco.com/en/US/products/products\\_security\\_advisory09186a00801ea156.shtml](http://www.cisco.com/en/US/products/products_security_advisory09186a00801ea156.shtml)

[4] *Biondi/Desclaux: Silver Needle in the Skype*:  
[http://www.secdev.org/conf/skype\\_BHEU06.handout.pdf](http://www.secdev.org/conf/skype_BHEU06.handout.pdf)

*NIST Special Publication "Security Considerations for Voice Over IP Systems"*:  
<http://csrc.nist.gov/publications/nistpubs/800-58/SP800-58-final.pdf>

*NIST IPTel/VoIP Security Technical Implementation Guide*:  
<http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V2R2.pdf>

*NIST IPTel/VoIP Checklist*:  
<http://csrc.nist.gov/pcig/CHECKLISTS/voip-checklist-v2r2-2-20060519.pdf>

