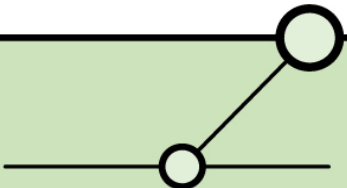


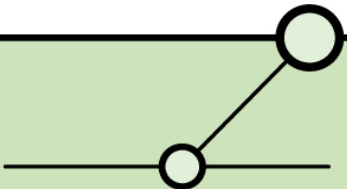
VoIP Security

www.ernw.de

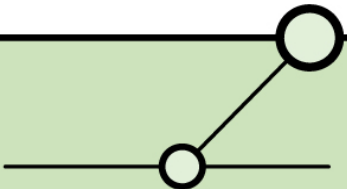


Agenda

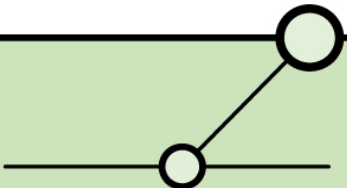
- Grundlagen & Terminologie
- Sicherheitsziele
- Threats & Vulnerabilities
- Angriffsmethoden
- Gegenmassnahmen



- **Grundlagen & Terminologie**
- Sicherheitsziele
- Threats & Vulnerabilities
- Angriffsmethoden
- Gegenmassnahmen

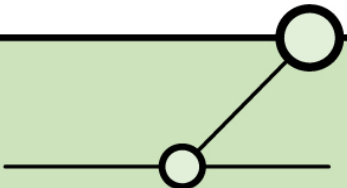


- Der Transport von ‚paketierten‘ Telefonverbindungen über IP-Netzwerke. Meist (aber nicht nur) Audio-Daten.
- Kann innerhalb von abgeschlossenen Netzeinheiten stattfinden
(=> dann spricht man oft von *VoIP*) oder über das Internet (=> Terminus ist hier üblicherweise *IP Telephony*)
- VoIP ist kein Protokoll.
Eher ein Sammelbegriff für verschiedene Technologien.

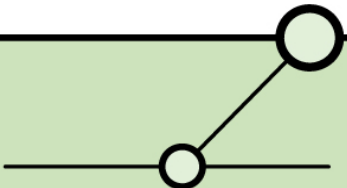


Bestandteile typischer VoIP-Szenarios

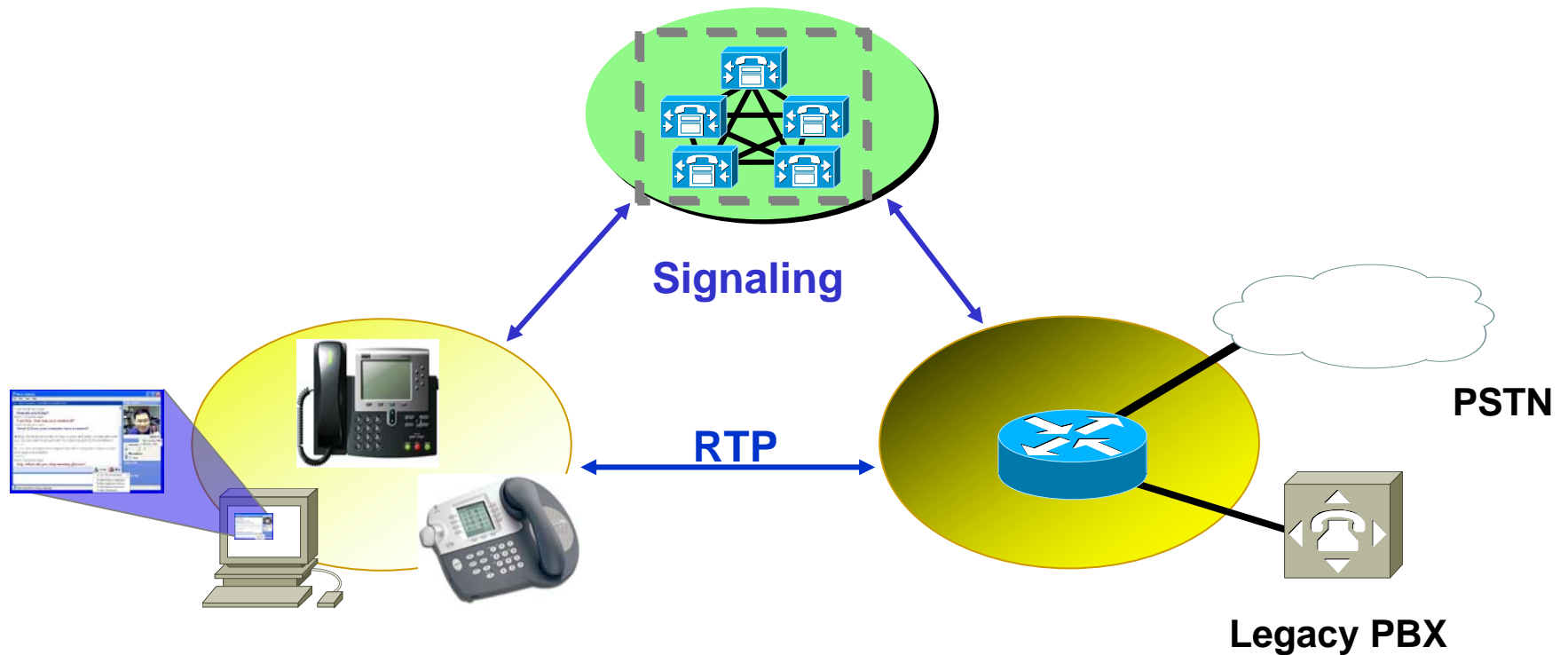
- Protokolle (Transport, Signalisierung, Management/Infrastruktur)
- Komponenten (dedizierte VoIP-Devices, Kopplungs-Geräte)
- Verbindungen (öffentliche, nicht-öffentliche Strecken)
- Endgeräte (Hardphones, Softphones, Legacy Devices)
- User („Faktor Mensch“)



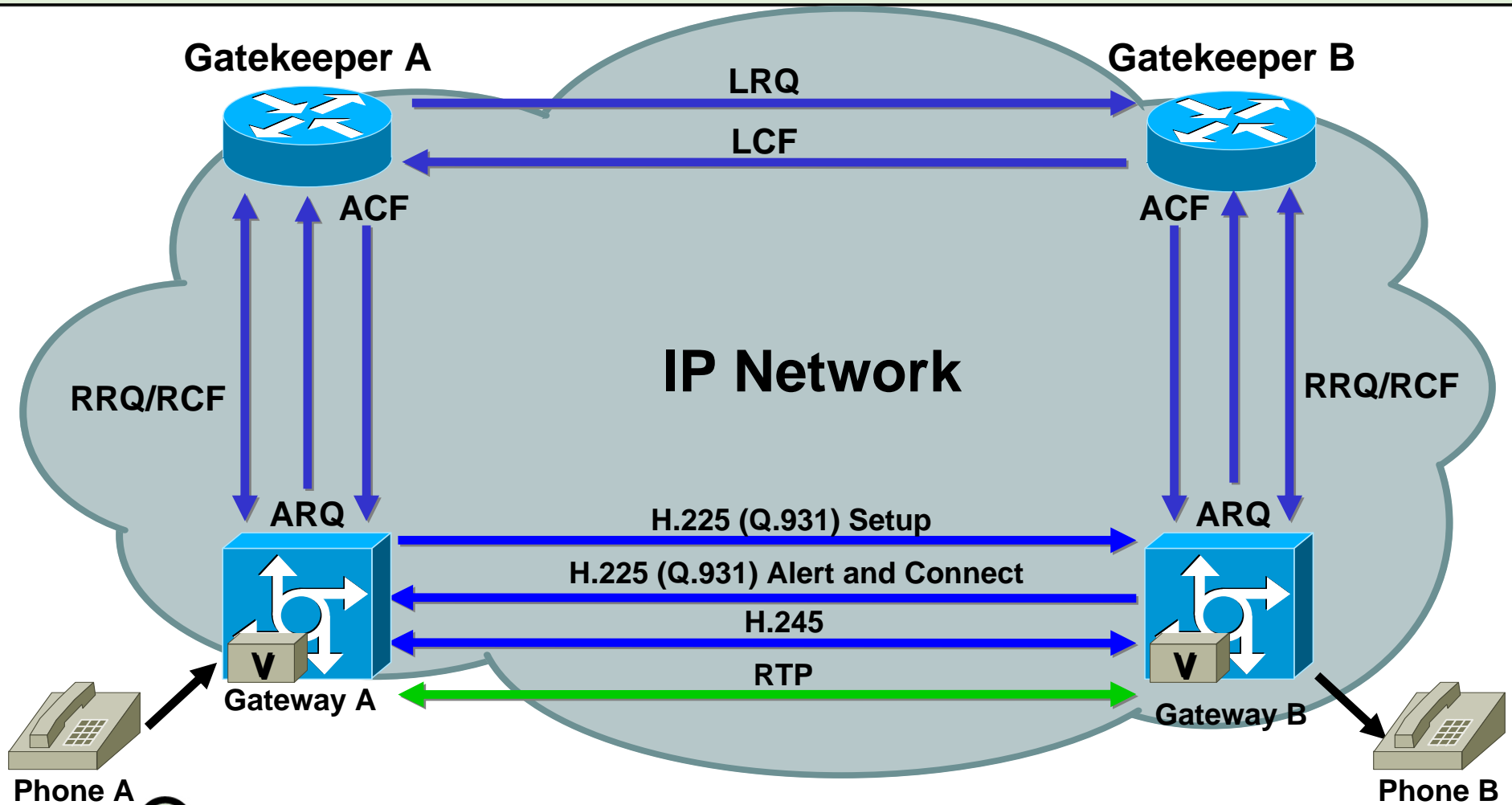
- Transport (von Nutzdaten):
Real-Time Transport Protocol [RTP, RFC 1889]
+ ggf. *RTP Control Protocol [RTCP]*
- Signalisierung (*Location of Users, Session Setup & Negotiation* etc.):
 - *H.323* [Urheber: ITU]
 - *Session Initiation Protocol [SIP, RFC 2543/3261]*
 - *Skinny/SCCP* [Cisco-proprietär]
- Management/Infrastruktur [DNS, SNMP et.al.]



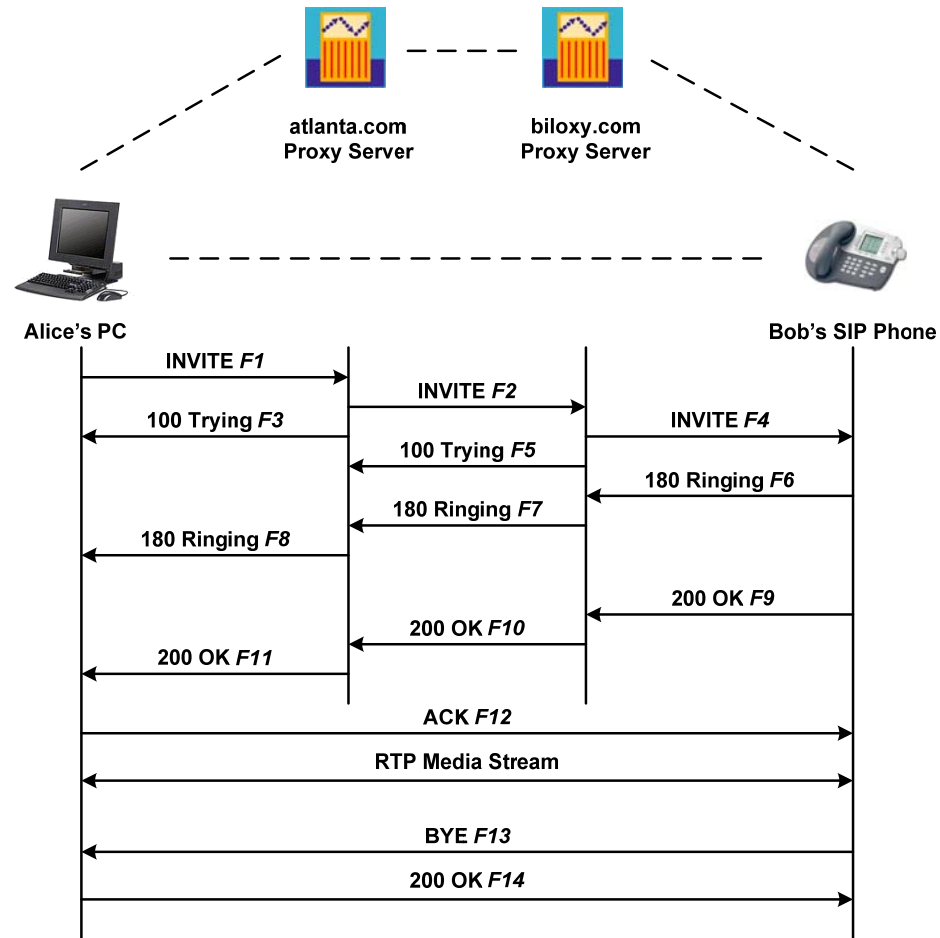
Zusammenwirken der Protokolle



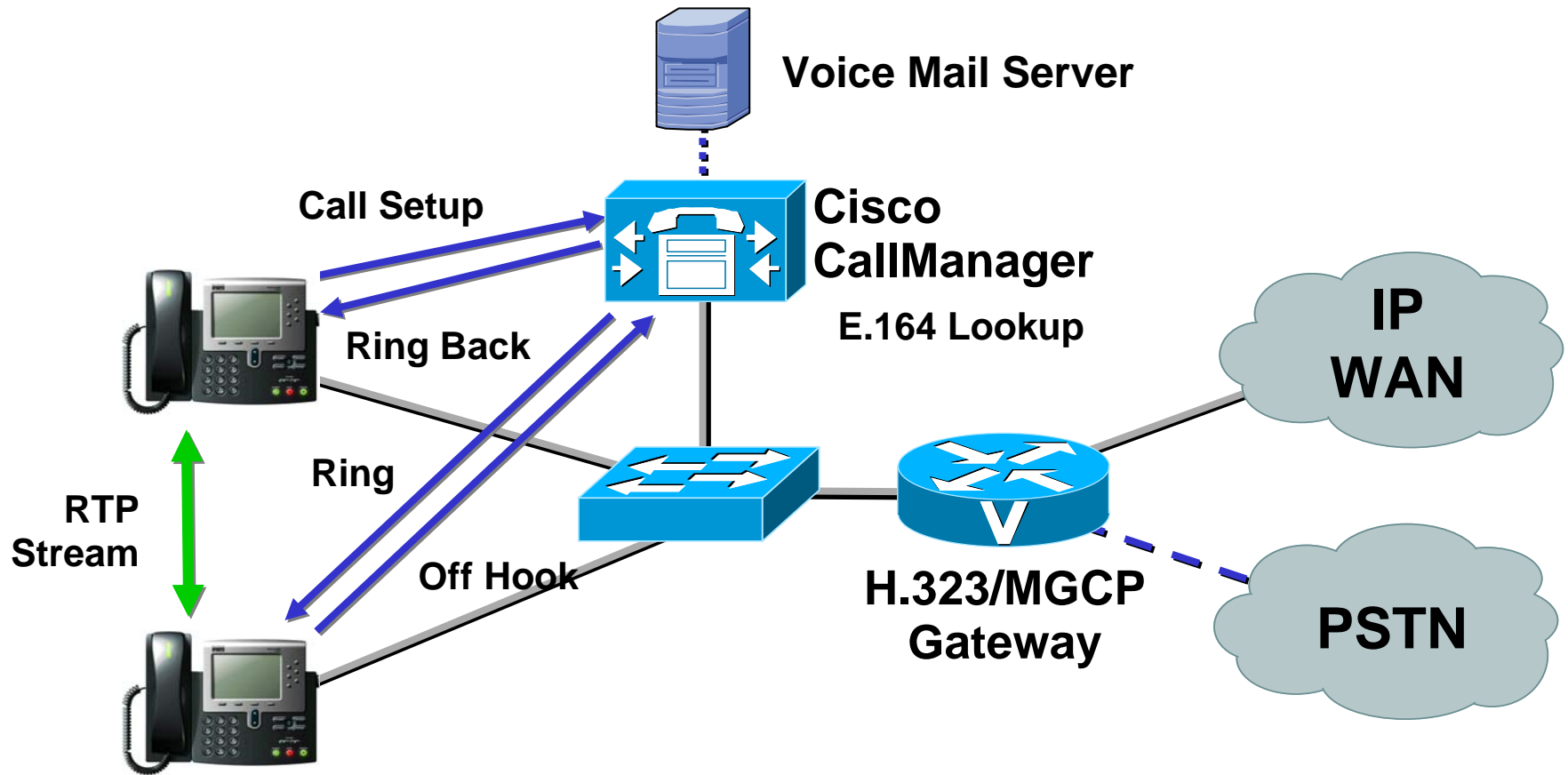
Beispiel H.323



Beispiel SIP

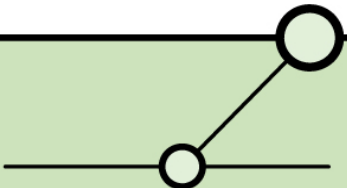


Beispiel Skinny

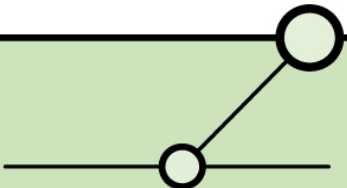


Komponenten

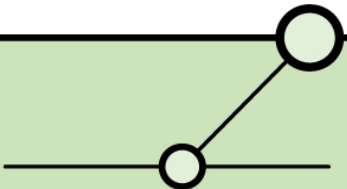
- Dedizierte VoIP-Devices, e.g.
H.323 Gatekeeper, Multipoint Controller
SIP Proxy, Redirector
Voice-Mail Server
TRIP Location Server
- Kopplungskomponenten zu anderen Netzen, z.B.
GGSN/SGSN zu GPRS/UMTS-Netzen
- Infrastruktur-Komponenten (etwa Backbone Router)



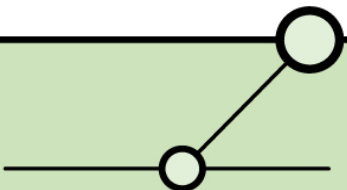
- Hardphones: dedizierte Telefone mit VoIP-Fähigkeiten, etwa Cisco 7960.
- Softphones: Software-Applikationen, die auf PCs laufen und VoIP-Funktionalität zur Verfügung stellen.
- Legacy Devices: traditionelle Telefon-/Fax-Geräte, die über geeignete Schnittstellen (etwa Cisco NM-2V+VIC-2FXS) in VoIP-Netze integriert werden.



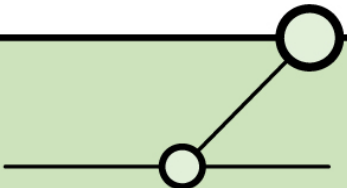
- Grundlagen & Terminologie
- **Sicherheitsziele**
- Threats & Vulnerabilities
- Angriffsmethoden
- Gegenmassnahmen



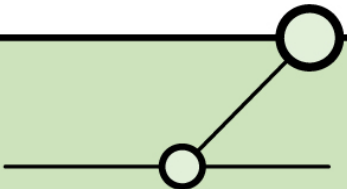
- Verfügbarkeit
- Vertraulichkeit
- Integrität (?)
- Authentizität
- Non-Repudiation
- Einhaltung gesetzlicher Bestimmungen
 - Datenschutz
 - *Lawful Interception*



- Enduser:
Vertraulichkeit (das „emotionale Moment“)
- Organisation:
Verfügbarkeit, Vertraulichkeit, Datenschutz
- Carrier/Dienst-Anbieter:
Non-Repudiation (Abrechnungs-Betrug!), Lawful Interception,
„Kundenbindung durch Vertrauen“

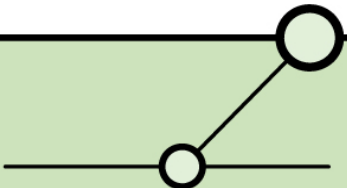


- Grundlagen & Terminologie
- Sicherheitsziele
- **Threats & Vulnerabilities**
- Angriffsmethoden
- Gegenmassnahmen



(Main) Threats

- Abhören von Verbindungen/Sniffing
 - durch Angreifer
 - ‚Lawful‘ (⇔ Anwälte, Journalisten, Beratungsinstitutionen)
- Denial-of-Service
- Kompromittierung von Komponenten
 - => Abhören
 - => Umleiten
- Spoofing
 - => Verlust der Authentizität (Telefon-Banking)
 - => Abrechnungsbetrug



Auf Protokoll-Ebene:

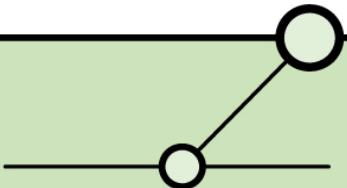
- Implementierungs-Schwächen (?)
- (Hochgradig) Dynamische Kommunikationsbeziehungen
- Fehlende immanente Sicherheitsfeatures (?)

Auf Komponenten-Ebene:

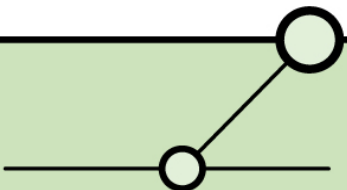
- Unsichere Default-Konfigurationen
- *Design without security in mind*, insbesondere an Kopplungskomponenten
- Seiteneffekte von VoIP Security-Problemen auf ‚Nicht-VoIP Devices‘

Auf Endgeräte-Ebene:

- Unsichere Default-Konfigurationen
- (Zu) wenig Sicherheits-Features
- Malicious Code ?



- Implementierungs-Schwächen:
Seit den Analysen der *Oulu University Secure Programming Group* [1] zu SIP und H.323 kaum mehr vorhanden.
- (Hochgradig) Dynamische Kommunikationsbeziehungen:
Signalisierung und Transport werden durch unterschiedliche Protokolle geregelt. Dabei werden die von RTP verwendeten Ports im Rahmen der Signalisierung dynamisch (innerhalb einer grossen Port-Range) ausgehandelt.
=> Regelung/Kontrolle durch Paketfilter schwierig.
- Fehlende immanente Sicherheitsfeatures (?):
die meisten Protokolle weisen (inzwischen) Sicherheits-Mechanismen (SIP/TLS) oder sichere Varianten (*SRTP*, RFC 3711) auf.



Vulnerabilities, Protokoll-Probleme (SCCP)

Cisco Security Advisory: Vulnerability in Cisco IOS Embedded Call Processing Solutions - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address <http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml> Go Links

More information about Cisco's IOS Telephony Service (ITS) and Cisco CallManager Express (CME) can be found here:

<http://www.cisco.com/en/US/products/sw/voicesw/ps4625/index.html>

More information on Cisco's Survivable Remote Site Telephony (SRST) can be found here:

<http://www.cisco.com/en/US/products/sw/voicesw/ps2169/index.html>

ITS, CME and SRST are features that allow a Cisco device running IOS to control IP Phones using the Skinny Call Control Protocol (SCCP). SCCP is the Cisco CallManager native signaling protocol.

Certain malformed packets sent to the SCCP port on an IOS device configured for ITS, CME or SRST may cause the target device to reload. This issue is documented in Cisco bug ID CSCee08584.

The following commands can be used to determine if ITS or CME are running. A device that does not have ITS or CME enabled will display:

```
Router#show telephony-service
telephony-service is not enabled
```

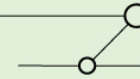
A device that has ITS or CME enabled will show something similar to:

```
Router#show telephony-service
CONFIG (Version=3.0)
=====
Cisco CallManager Express
ip source-address 192.168.1.1 port 2000
max-ephones 2
max-dn 2
max-conferences 8
max-redirect 5
time-format 12
date-format mm-dd-yy
keepalive 30
timeout interdigit 10
timeout busy 10
timeout ringing 180
edit DN through Web: disabled.
```

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

Done Trusted sites

Vulnerabilities, Protokoll-Probleme (H.323)



The screenshot shows a Microsoft Internet Explorer browser window with the address bar containing <http://www.securityfocus.com/bid/10111/discussion/>. The page title is "SecurityFocus HOME Vulns discussion: Microsoft Windows H.323 Remote Buffer Overflow Vul".

The page content includes a navigation menu with links for Home, Foundations, Microsoft, UNIX, IDS, Incidents, Virus, Pen-Test, Firewalls, Bugtraq, Newsletters, and Mailing Lists. A search bar is located at the top right.

The main content area is titled "VULNERABILITIES" and features a sub-header "Microsoft Windows H.323 Remote Buffer Overflow Vulnerability". Below this, there are tabs for "info", "discussion", "exploit", "solution", "credit", and "help". The "discussion" tab is selected.

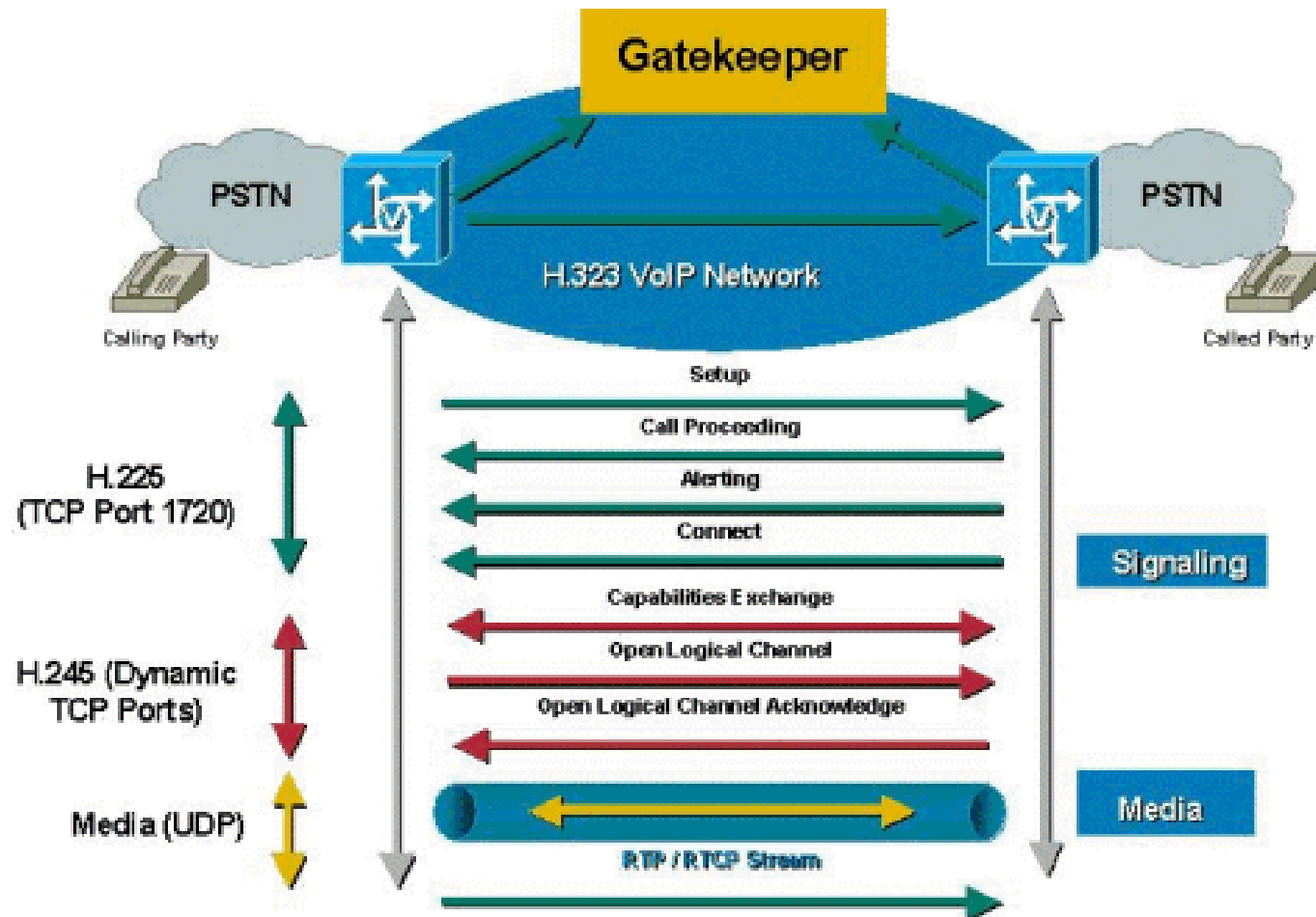
The text of the article states: "The Microsoft Windows H.323 protocol implementation is prone to a remote buffer overflow. Successful exploitation could allow for execution of arbitrary code." and "This vulnerability could only be exploited if an H.323 application such as NetMeeting were running on the system."

At the bottom of the article, there is a "Disclaimer | About The Vulnerability Database" link and an email address: vuldb@securityfocus.com.

On the right side of the page, there is a red box with the text "FREE Webinar on Penetration Testing".

The browser's status bar at the bottom shows "Done" and "Trusted sites".

Dynamische Ports, Beispiel H.323 (1)



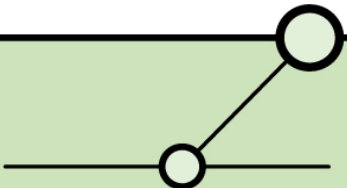
Dynamische Ports, Beispiel H.323 (2)

```
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

- Unsichere Default-Konfigurationen, z.B.:
 - *Cisco Call Manager* auf MS IIS mit unzureichenden Berechtigungen
 - *Cisco Call Manager* mit *Auto Registration* per default *enabled*.
- *Design without security in mind*, insbesondere an Kopplungskomponenten
=> ‚Kinderkrankheiten‘, die nicht mehr auftreten *dürften*.
- Seiteneffekte von VoIP Security-Problemen auf ‚Nicht-VoIP Devices‘



Vulnerabilities, (neue) Komponenten

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

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

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

Done Trusted sites

Vulnerabilities, Kopplungskomponenten

http://www.atstake.com/research/advisories/2003/a031303-2.txt - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media

Address http://www.atstake.com/research/advisories/2003/a031303-2.txt Go Links

Security Advisory

Advisory Name: Nokia SCSN (DX200 Based Network Element) SNMP issue
Release Date: 03/13/2003
Application: Nokia SCSN (DX200 Based Network Element)
Platform: DX200
Severity: An attacker is able to read SNMP options with any community string
Author: Ollie Whitehouse [ollie[at]atstake.com]
Vendor Status: Vendor has removed support for this protocol
CVE Candidate: CVE Candidate number applied for
Reference: www.atstake.com/research/advisories/2003/a031303-2.txt

Overview:

Nokia's (<http://www.nokia.com>) SCSN (Serving GPRS support node) is the platform which exists between the legacy GSM network and the new IP core of the GPRS network. This enables operators to deploy high speed data access over the top of their GSM network with minimal upgrades to their BSCs (Base Station Controllers), thus making the transition from a 2.0G to a 2.5G network.

Due to its position in the network (i.e. between the RF network and the IP network) the SCSN will have interfaces on the SS7 signaling network and the IP core network as well as connections to the BSCs. For this reason, the SCSN can be considered a key part of the infrastructure of any mobile operator looking to deploy GPRS.

A vulnerability exists in the SNMP (Simple Network Management Protocol) daemon of the DX200 based network element that allows an attacker to read SNMP options with ANY community string.

This is a good example of why network elements which introduce IP functionality to legacy networks should have their functionality verified in terms of impact on security before deployment in a production environment. !!

Proof of Concept:

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

Done Internet

Vulnerabilities, Seiteneffekte

To determine if your Cisco IOS device is processing H.323 traffic and is possibly vulnerable, it is necessary to understand the three different ways that Cisco IOS software processes H.323 traffic.

1. H.323 Endpoints

This includes H.323 Gateway, H.323 Gatekeeper, and H.323 Gatekeeper with Proxy, as well as releases that may run the H.323 process by default without being configured. Please continue with the following steps to determine if your device is affected.

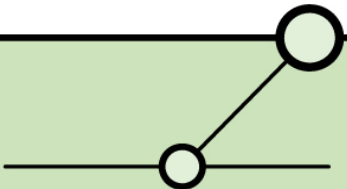
From the enable prompt, run the **show process cpu** command and look for a process called CCH323_CT. In later versions of Cisco IOS software, you can execute the **show process cpu | include CCH323**.

```
Router# show process cpu | include CCH323
112 Mve 60F3E5E0 295112 239401 123220072/24000 0 CCH323_CT
```

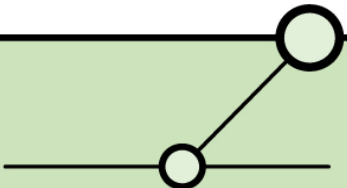
Note: Only images with a "PLUS" feature set (such as IP PLUS, ENTERPRISE PLUS) support voice and will have the CCH323_CT process running. In 12.0, the "PLUS" feature set has the CCH323_CT process running by default on the 2600 and 3600 platforms. Starting in 12.1, the process will run by default if you have a voice card or dsp card inserted.

- If you see the a process called CCH323_CT, your router is affected. Please consult the IOS table to determine which version is appropriate for your device. If you cannot immediately upgrade, the following workarounds may work for you
 - If you *are not* using H.323 within your network, an inbound access list to block TCP port 1720 will protect your router, but it is recommended that you upgrade as soon as is feasible.
 - If you *are* using H.323, then you can configure an access list to restrict TCP port 1720 traffic to known, trusted IP addresses. Again, upgrading as soon as is feasible is recommended.
- If you do not see the CCH323_CT process, you may still be vulnerable. Some configurations of H.323 Gatekeeper are vulnerable. Affected configurations are those gatekeepers configured for H.323 Proxy. To check to see if you are configured as a gatekeeper, check your configuration for the line "proxy h323" in the global configuration. If you have "proxy h323" configured, then you are vulnerable.
 - If you *are not* using GK proxy functionality, you can disable proxy functionality by doing the following configuration.
Note: This will drop all calls being managed by the gatekeeper. Perform this only when you can safely stop gatekeeper functionality.

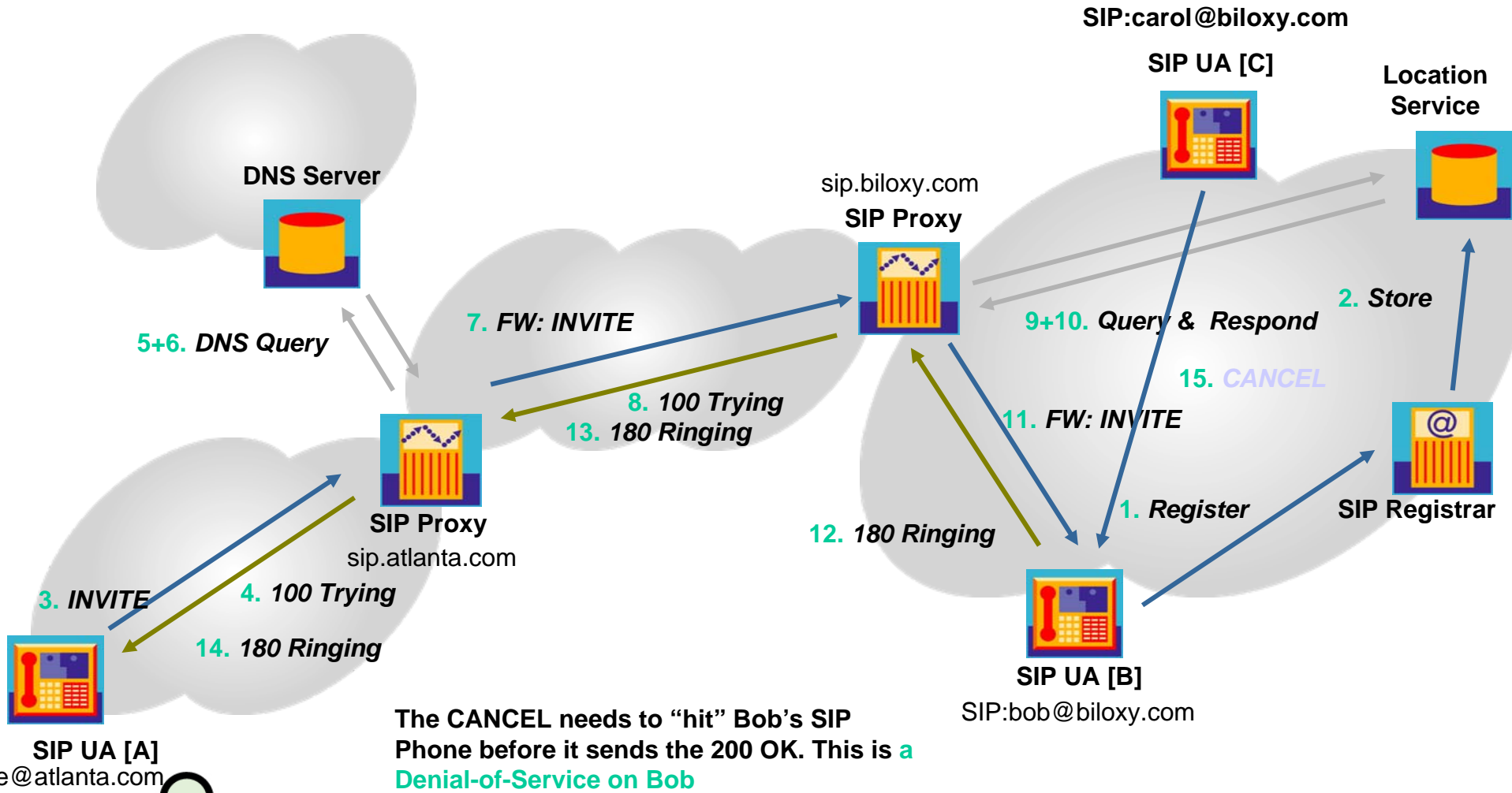
- Grundlagen & Terminologie
- Sicherheitsziele
- Threats & Vulnerabilities
- **Angriffsmethoden**
- Gegenmassnahmen



- Sniffing:
Da RTP per default unverschlüsselt überträgt, kann ein Angreifer mit Zugriff auf den Netzwerk-Verkehr (üblicherweise im lokalen Netz per ARP-Spoofing) VoIP-Sitzungen abhören.
Bekannte Tools: *Vomit (*NIX)*, *Cain & Abel (Windows)*, *Ethereal*.
- Call-Hijacking/MITM
- Denial-of-Service:
Gegen Protokolle (meist SIP), Komponenten oder Endgeräte.
- Angriffe gegen Endgeräte/-Management:
Aufgrund fehlender Sicherheits-Features (etwa fehlender Authentifizierung), schlechter Default-Konfiguration (e.g. aktiviertem Telnet-Zugang) oder mangelhafter Management-Strukturen (Konfig per TFTP etc.). Siehe etwa [4] gegen ältere Cisco 7960-Modelle.



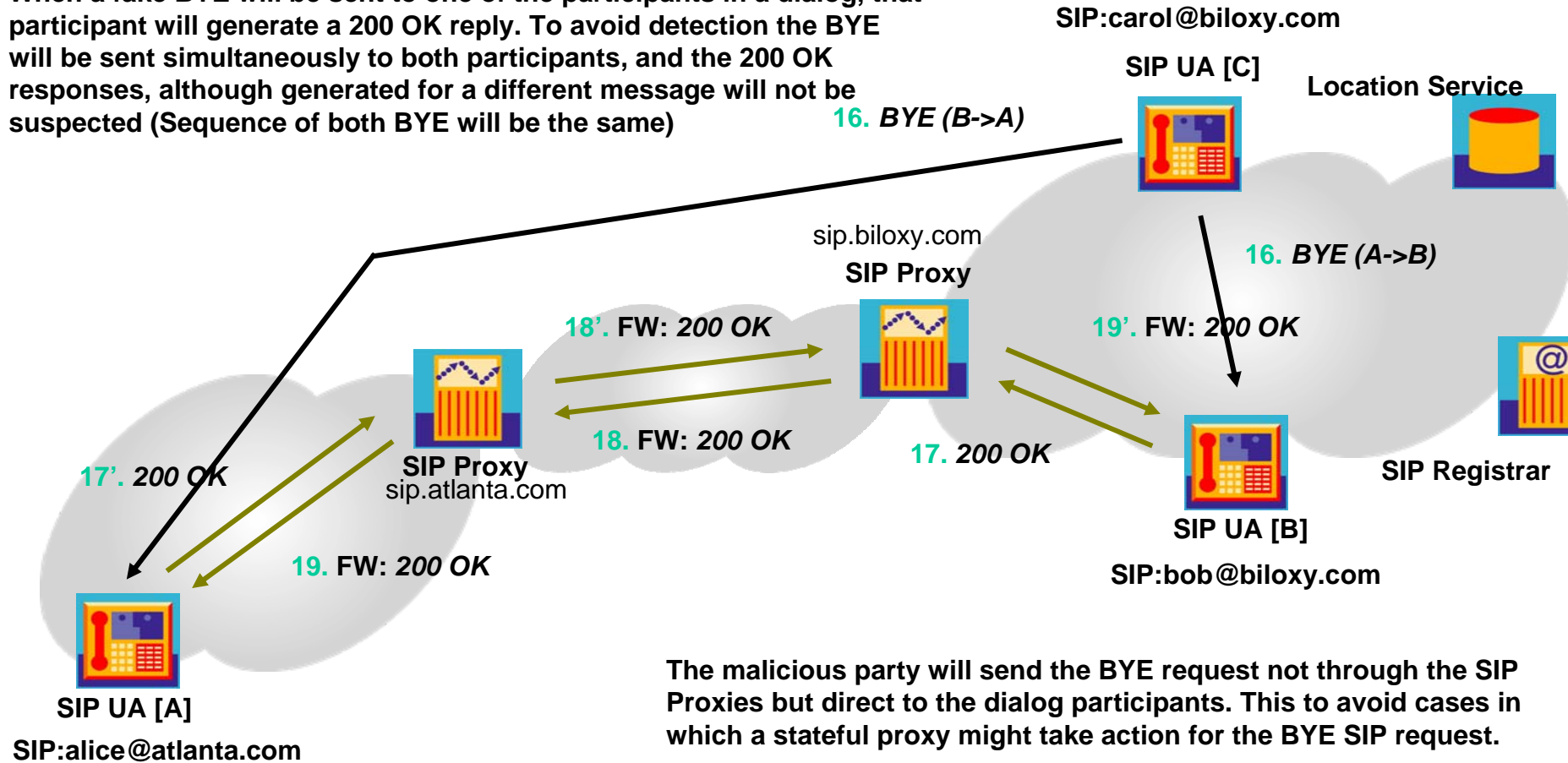
Angriffsmethoden, DoS gegen SIP (aus [3])



The CANCEL needs to "hit" Bob's SIP Phone before it sends the 200 OK. This is a Denial-of-Service on Bob

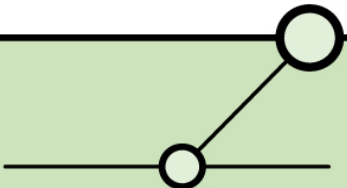
Angriffsmethoden, DoS gegen SIP (aus [3])

When a fake BYE will be sent to one of the participants in a dialog, that participant will generate a 200 OK reply. To avoid detection the BYE will be sent simultaneously to both participants, and the 200 OK responses, although generated for a different message will not be suspected (Sequence of both BYE will be the same)



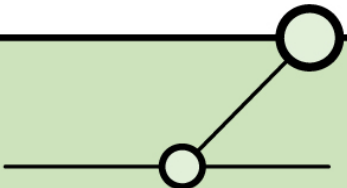
The malicious party will send the BYE request not through the SIP Proxies but direct to the dialog participants. This to avoid cases in which a stateful proxy might take action for the BYE SIP request.

- Grundlagen & Terminologie
- Sicherheitsziele
- Threats & Vulnerabilities
- Angriffsmethoden
- **Gegenmassnahmen**

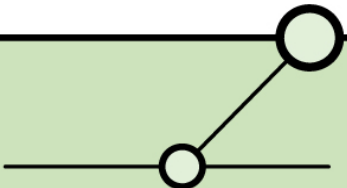


Die ‚Klassiker‘:

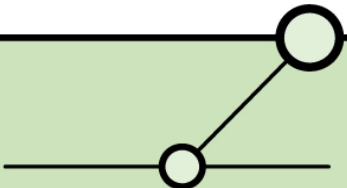
- Segmentierung
- Authentifizierung
- Verschlüsselung
- Sicheres Management



- Datenverkehr und VoIP/IP Telephony MÜSSEN logisch getrennt werden [(Voice) VLANs, MPLS et.al.]. Dies ist aber meist aus QoS/TE-Gründen schon gegeben.
- Daten- & Telefonie-Devices MÜSSEN in unterschiedlichen Segmenten sein, mit wohldefinierten Kommunikationsbeziehungen zwischen den Segmenten.
- Beim Einsatz von Firewalls SOLLTEN diese ausreichend intelligent sein, um Kommunikations-Beziehungen (Signalisierung/Transport, Multipoint-Verbindungen etc.) zu verstehen. Ein Beispiel für eine gute Implementierung ist die *Check Point Firewall-1*.
- Auch die Verweigerung von Gratuitous ARPs (*Ignore GARP*), wie sie Cisco-Telefone praktizieren, ist eine Segmentierungs-Massnahme.
- *Segmentation/Isolation + Defense-in-Depth rule...*

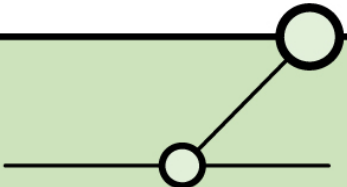


- Es MÜSSEN in allen Szenarien geeignete Authentifizierungs-Mechanismen implementiert sein.
- Endgeräte anhand von MAC-Adressen und/oder Zertifikaten.
- Komponenten (e.g. *Call Manager*) anhand von Zertifikaten.
- User-Authentifizierung SOLLTE möglichst eindeutig sein (etwa Hotel-WLAN nur mit KK etc.). Ggf. sind hier auch Vorgaben im Rahmen der *Lawful Interception* zu beachten.
- Authentifizierung & Nachvollziehbarkeit/Revisions-Anforderungen sind unmittelbar miteinander verknüpft.
- *Clients are malicious...*

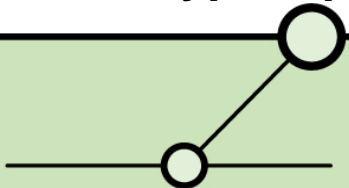
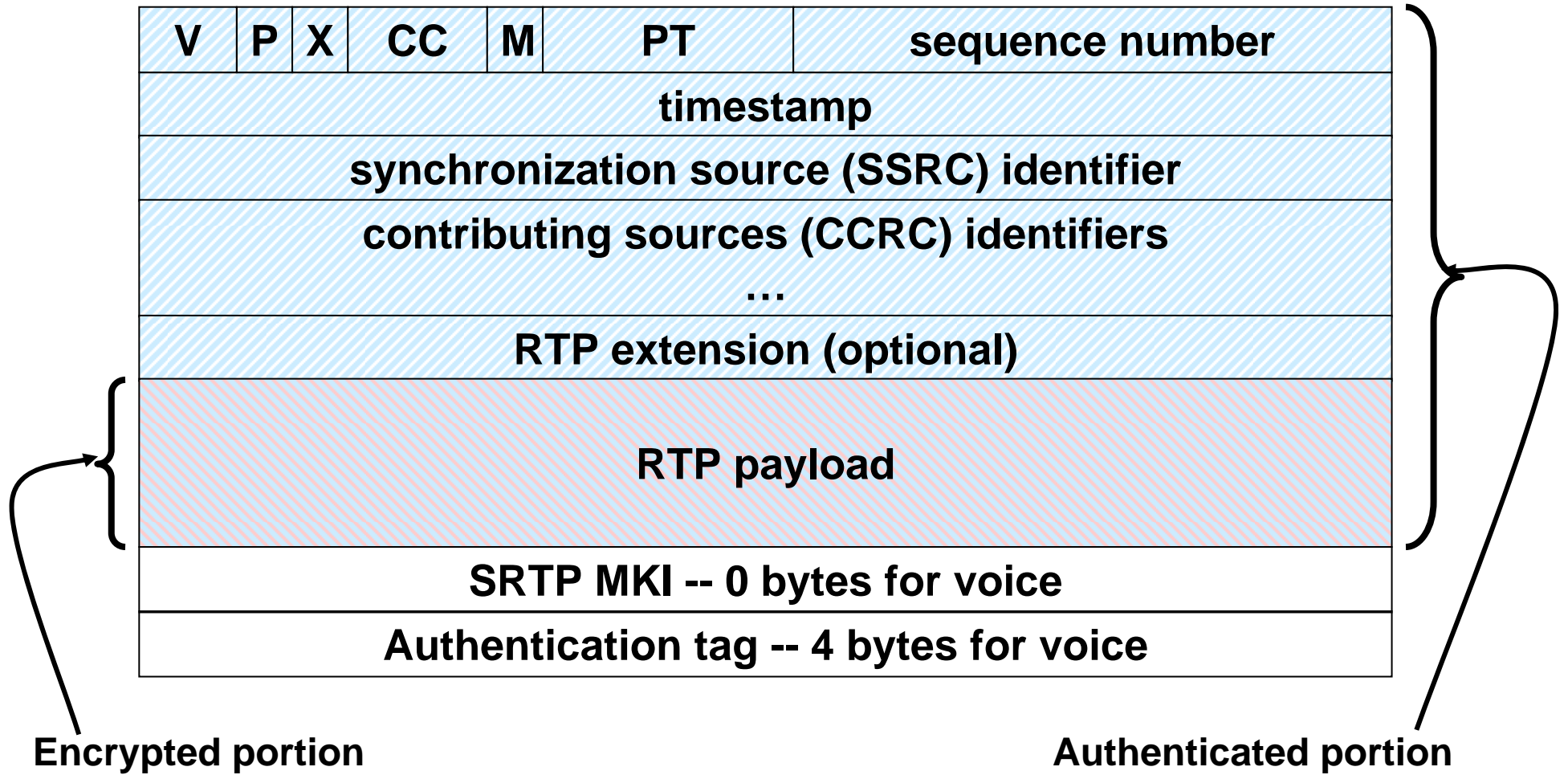


Verschlüsselung

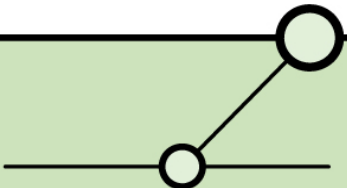
- SRTP ist inzwischen ‚Produktions-reif‘.
- IPsec ist oft nicht geeignet.
- Geeignete Protokolle lösen meist auch noch andere Anforderungen (Authentizität, Anti MITM, Anti Replay).
- Vielfach sind Revisions-Anforderungen nur durch Verschlüsselung erfüllbar.



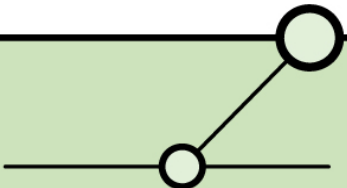
SRTP



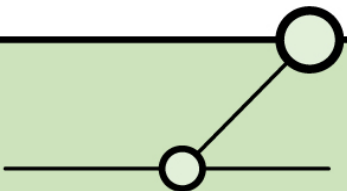
- Out-of-Band
- Stark authentifiziert
- Verschlüsselt
- Zum Management zählt etwa auch die Verteilung von (signierten) Images an Endgeräte.
=> *Change and Configuration Management*
- Unterstützt durch Segmentierung & Filterung.
- Monitoring & Intrusion Detection.



- VoIP/IP Telephony basiert auf verschiedensten Protokollen/Komponenten/Faktoren. Mit unterschiedlichen Sicherheits-Anforderungen und ‚Reifegraden‘.
- Es ergeben sich eine Reihe (altbekannter) *Threats*, aber ‚neuer‘ *Vulnerabilities*.
- Dem korrekten Design der Umgebungen und ihrer Kommunikationsbeziehungen kommt eine hohe Bedeutung zu.
- VoIP/IP Telephony Implementierungen können mit aktueller Technologie durchaus sicher gestaltet werden.



Fragen?



Danke für Ihre Aufmerksamkeit!

