

Sicherheitsaspekte bei der Nutzung von VoIP



Grundregeln der Sicherheit

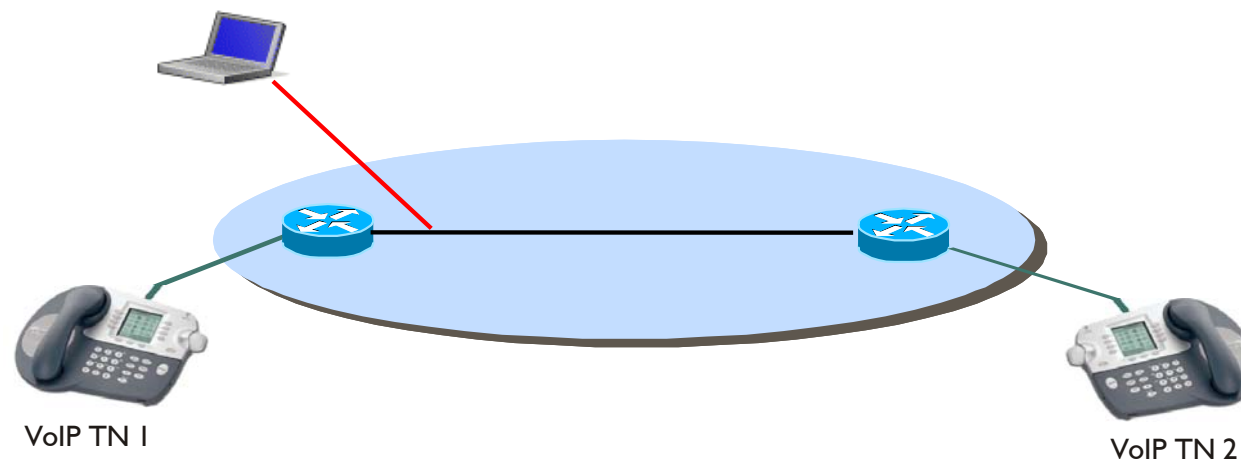
- Vertraulichkeit
 - Wer hat wann mit wem telefoniert
 - Abhörsicherheit der Gespräche

- Integrität / Authentizität
 - Integrität der Systemkomponenten
 - Anrufer ist der für den er sich ausgibt
 - Keine Wiederholung vorher aufgezeichneter Daten

- Verfügbarkeit
 - Ausfallsicherheit der Netzwerkinfrastruktur
 - Denial of Service Attacks
 - Quality of Service

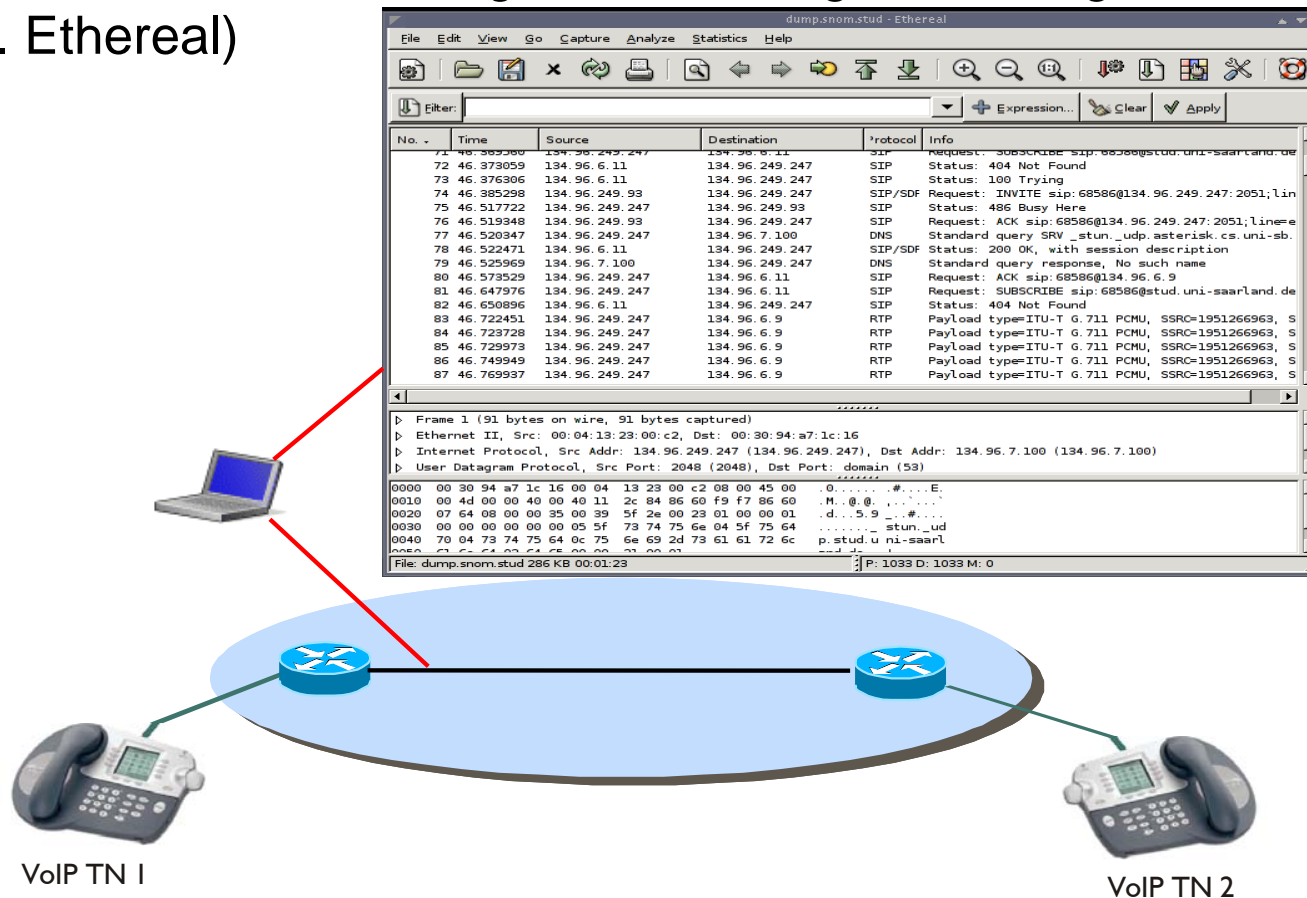
Vertraulichkeit – Mithören

- Datenpakete können relativ leicht mitgeschnitten werden
- Verbindungsinformationen und Gesprächsdaten somit verfügbar



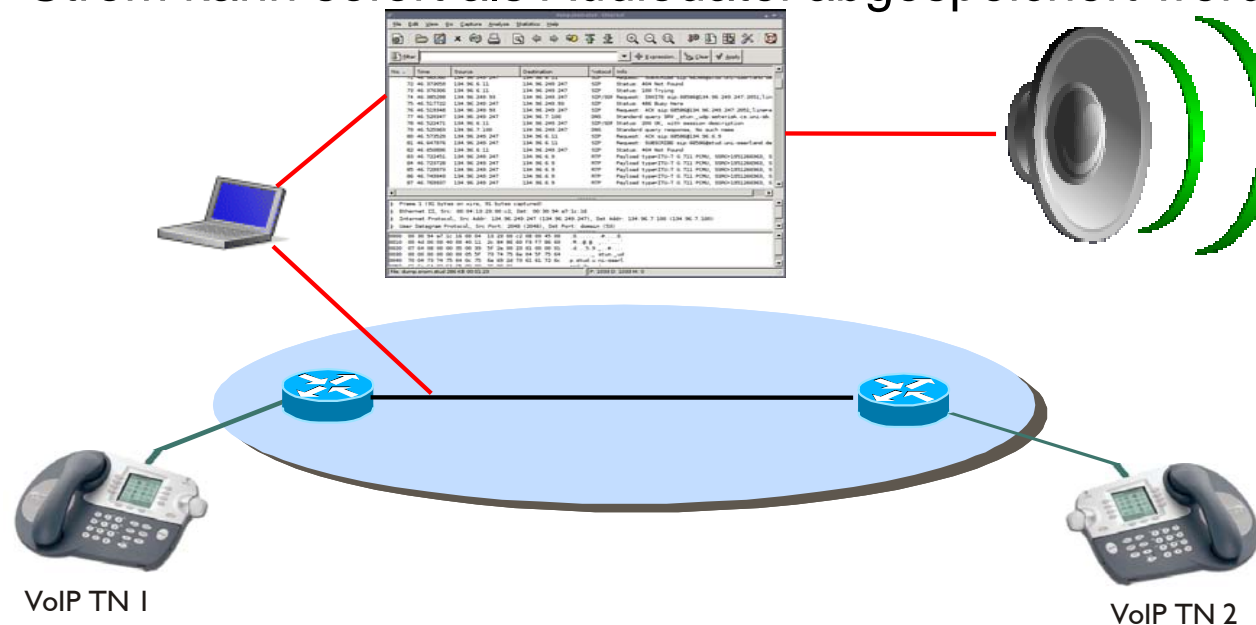
Vertraulichkeit – Mithören

- Automatische Auswertung mit frei verfügbaren Programmen (z.B. Ethereal)



Vertraulichkeit – Mithören

- Datenpakete können relativ leicht mitgeschnitten werden
- Verbindungsinformationen und Gesprächsdaten somit verfügbar
- Automatische Auswertung mit frei verfügbaren Programmen (z.B. Ethereal)
- RTP-Strom kann sofort als Audiodatei abgespeichert werden



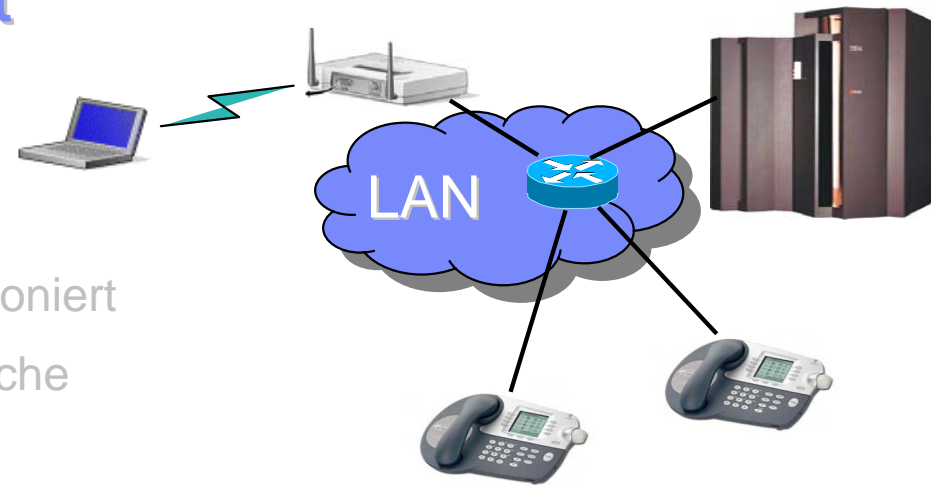
VoIP-Sicherheit – Protokolle

- Netzwerkverbindung sichern
 - IPSec, VPN
 - Nicht von Endgerät zu Endgerät
- Sichere Übertragungsprotokolle verwenden
 - Secure SIP, SRTP
 - Bereits in manchen Endgeräten implementierter Standard



Grundregeln der Sicherheit

- Vertraulichkeit
 - Wer hat wann mit wem telefoniert
 - Abhörsicherheit der Gespräche
- Integrität / Authentizität
 - Integrität der Systemkomponenten
 - Anrufer ist der für den er sich ausgibt
 - Keine Wiederholung vorher aufgezeichneter Daten
- Verfügbarkeit
 - Ausfallsicherheit der Netzwerkinfrastruktur
 - Denial of Service Attacks
 - Quality of Service



Grundregeln der Sicherheit

- Vertraulichkeit
 - Wer hat wann mit wem telefoniert
 - Abhörsicherheit der Gespräche

- Integrität / Authentizität
 - Integrität der Systemkomponenten
 - Anrufer ist der für den er sich ausgibt
 - Keine Wiederholung vorher aufgezeichneter Daten

- Verfügbarkeit
 - Ausfallsicherheit der Netzwerkinfrastruktur
 - Denial of Service Attacks
 - Quality of Service

Gefährdungen – Kosten

- Durch Erschleichen von Zugangsinformationen
- Fehlerhafte Rufnummernpläne
 - Häufig bei selbst installierten TK-Anlagen
 - Ankommende Anrufe können externe Rufnummern erreichen
- ENUM mit tel-URIs
 - ENUM = tElephone NUmber Mapping
 - Liefert weitere Informationen zur Rufnummer, z.B. Erreichbarkeit über VoIP
+49 681 302 68588
`sip:68588@enum.rz.uni-saarland.de`
 - Problem: auch `tel:<teure 0190-Hotline>` denkbar

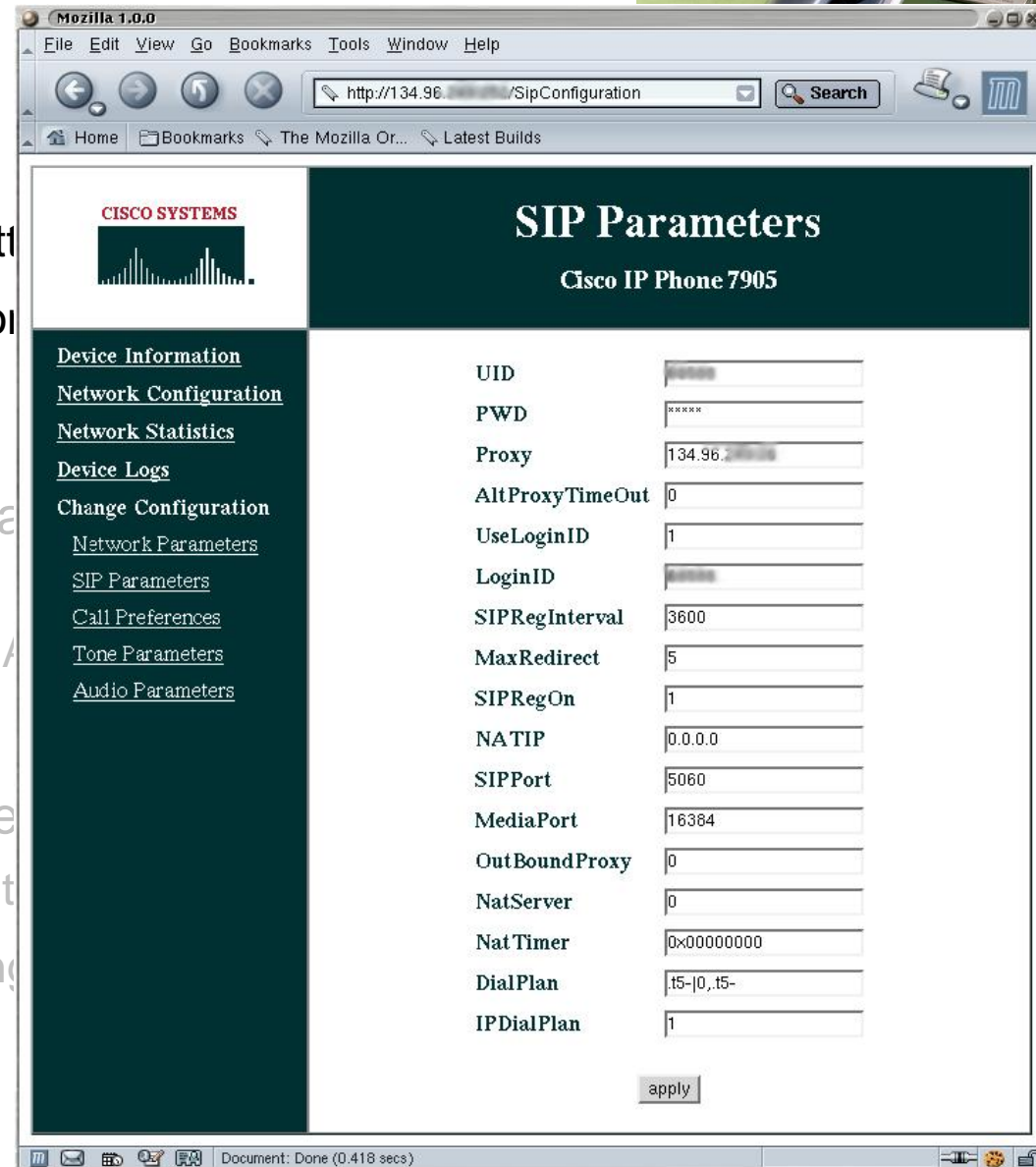
VoIP-Sicherheit – Endgeräte

- Integrierte Webserver
 - Meist nur http, kein https
 - Erlauben Konfiguration, Einsicht von Verbindungsdaten, Initiieren von Anrufen
- Telefone laden Konfiguration beim Einschalten aus Datei vom Server
 - TFTP-Protokoll ohne Authentifizierung und Verschlüsselung
- Konfigurationszugang per Telnet
 - Keine sichere Authentifizierung
 - Keine Verschlüsselung



VoIP-Sicherheit – Endgeräte

- Integrierte Webserver
 - Meist nur http, kein https
 - Erlauben Konfiguration
 - Initiieren von Anrufen
- Telefone laden Konfiguration aus Datei vom Server
 - TFTP-Protokoll ohne Authentifizierung
- Konfigurationszugang per Webbrowser
 - Keine sichere Authentifizierung
 - Keine Verschlüsselung



VoIP-Sicherheit – Endgeräte

- Integrierte Webserver
 - Meist nur http, kein https
 - Erlauben Konfiguration, Einsicht von Verbindungsdaten, Initiieren von Anrufen
- Telefone laden Konfiguration beim Einschalten aus Datei vom Server
 - TFTP-Protokoll ohne Authentifizierung und Verschlüsselung
- Konfigurationszugang per Telnet
 - Keine sichere Authentifizierung
 - Keine Verschlüsselung



VoIP-Sicherheit – Endgeräte

- Integrierte Webserver
 - Meist nur http, kein https
 - Erlauben Konfiguration, Einsicht von Verbindungsdaten, Initiieren von Anrufen
- Telefone laden Konfiguration beim Einschalten aus Datei vom Server
 - TFTP-Protokoll ohne Authentifizierung und Verschlüsselung
- Konfigurationszugang per Telnet
 - Keine sichere Authentifizierung
 - Keine Verschlüsselung



VoIP-Sicherheit – Endgeräte

```
rainer@precious:~$ telnet mein.ip-telefon
Trying mein.ip-telefon...
Connected to mein.ip-telefon.
Escape character is '^]'.

Password :*****

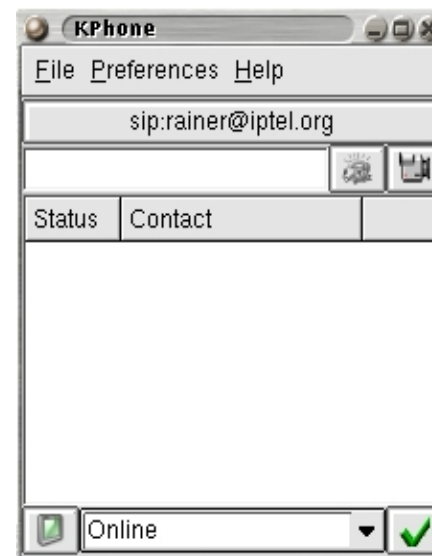
Cisco Systems, Inc. Copyright 2000-2003
Cisco IP phone  MAC: 0030:94c3:0904
Loadid: SW: POS3-06-0-00  ARM: PAS3ARM1  Boot: PC03M030  DSP: PS03AT38
SIP Phone> test

Test Command Definitions
-----
onhook  , hu - Handset Onhook
offhook , hd - Handset Offhook
key     , ky - Simulate Keystrokes
open    , op - Open the Test Session
close   , cl - Close the Test Session
show    , sh - Show Call Feedback
hide    , hi - Hide Call Feedback

SIP Phone> test open
TEST: Opening Session
SIP Phone> test hd
SIP Phone> test key 3841
```

VoIP-Sicherheit – Endgeräte

- Schlechte Standardpasswörter
 - “admin”, “0000”, “cisco”, ...
- Softwaretelefone durch Viren, Würmer und sonstige Malware gefährdet
 - Teilweise auch Speichern von Einstellungen und Anruflisten im Klartext auf dem PC (z.B. Windows-Registry)

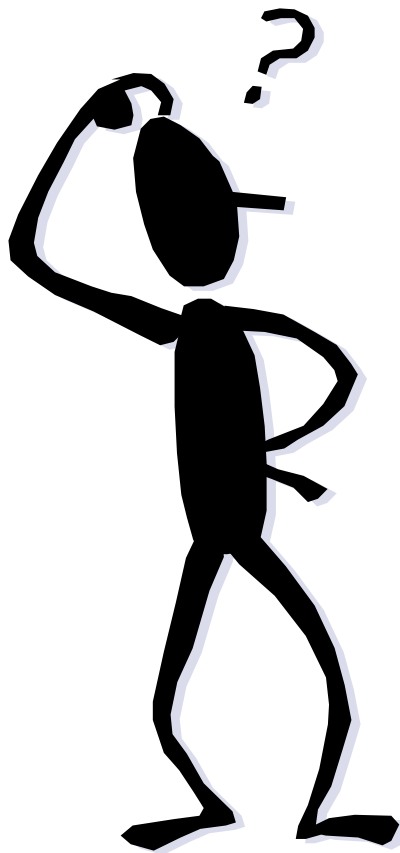


Herkömmliche TK-Welt

- Abhören bei der traditionellen Telefonie ebenso möglich
- Telefonie ist unverschlüsselt
- Fernwartungsfunktion herkömmlicher TK-Anlagen
- Fehlerhafte Rufnummernpläne und Berechtigungsstufen
- Auch hier sollten bei Schutzbedürftigkeit zusätzliche Sicherheitsmaßnahmen ergriffen werden

Zusammenfassung

- Sichere Protokolle verwenden
- Nicht benötigte Dienste deaktivieren
- Gute Passwörter verwenden
- Sicherheit des Gesamtsystems betrachten
- Sicherheitsmaßnahmen entsprechend der Bedrohungslage wählen



Fragen?

Sirrix Aktiengesellschaft
Im Stadtwald, Geb. 45
66123 Saarbrücken

Telefon (0681) 301 409 90
Telefax (0681) 301 409 91

a.alkassar@sirrix.com
<http://www.sirrix.com>