
1943 SIGSALY 1946
SPEECH ENCIPHERMENT SYSTEM

Worum geht's?

DEEPSEC

- Informations-Telefonie (IT)
- Sicherheit und Risiken
- Anleitungen für Skeptiker
- Strategien zur Schadensbegrenzung
- Tools

Sicherheit?

DEEPSEC

- *Integrität* der Verbindungs-/Gesprächsdaten
- *Vertraulichkeit* der Verbindungs-/Gesprächsdaten
- *Identität* der Gesprächsteilnehmer
- *Verfügbarkeit* der Infrastruktur

Geschäftsmodell für Startups

DEEPSEC

1. Gründe VoIP Dienstleister Unternehmen
2. „Networking“ mit anderen VoIP Unternehmen
3. „Anpassen“ von Geräten in deren Netzwerk
4. Dirigieren aller Anrufe über fremde Netzwerke
5. Rechnung für Dienste stellen, die andere bezahlen

„It's so easy a caveman can do it.“
– Robert Moore, Techniker, verhaftet.

Hauptgrund für Attacken im Moment!

Geschäftsmodell für Provider

DEEPSEC

- Telecom Italia
  »*Prosecutors say the spy ring taped the phone conversations of politicians, industrialists and even footballers.*« – BBC Artikel (21.9.2006)
- »*According to Telecom Italia's own investigation, their procedure and machines used for the legal wiretaps had a number of flaws and it was technically possible to spy on the telephone conversations, without leaving any trace.*« – EDRi-Gram #4.15
- Gespräche lassen sich verkaufen wie jede andere Ware.

Geschäftsmodell für Unbekannte DEEPSEC

- Ericsson entdeckt am 4. März 2005 trojanische Pferde im Lawful Interception Subsystem von Vodafon Greece.
- Kostas Tsalikidis, Leiter Network Design bei Vodafon Greece, erhängt sich am 9. März 2005
- Vodafon deaktiviert Subsystem und löscht versehentlich alle Logs und Spuren.
- Software im Subsystem hörte Telefonate von über 100 Regierungsmitgliedern ab – umgeleitet auf Pre-Paid Handys.
- Täter sind unbekannt.
- Hintergrund: The Athens Affair (IEEE Spectrum, Juli 2007)

Schlußfolgerungen

Unified Hacking

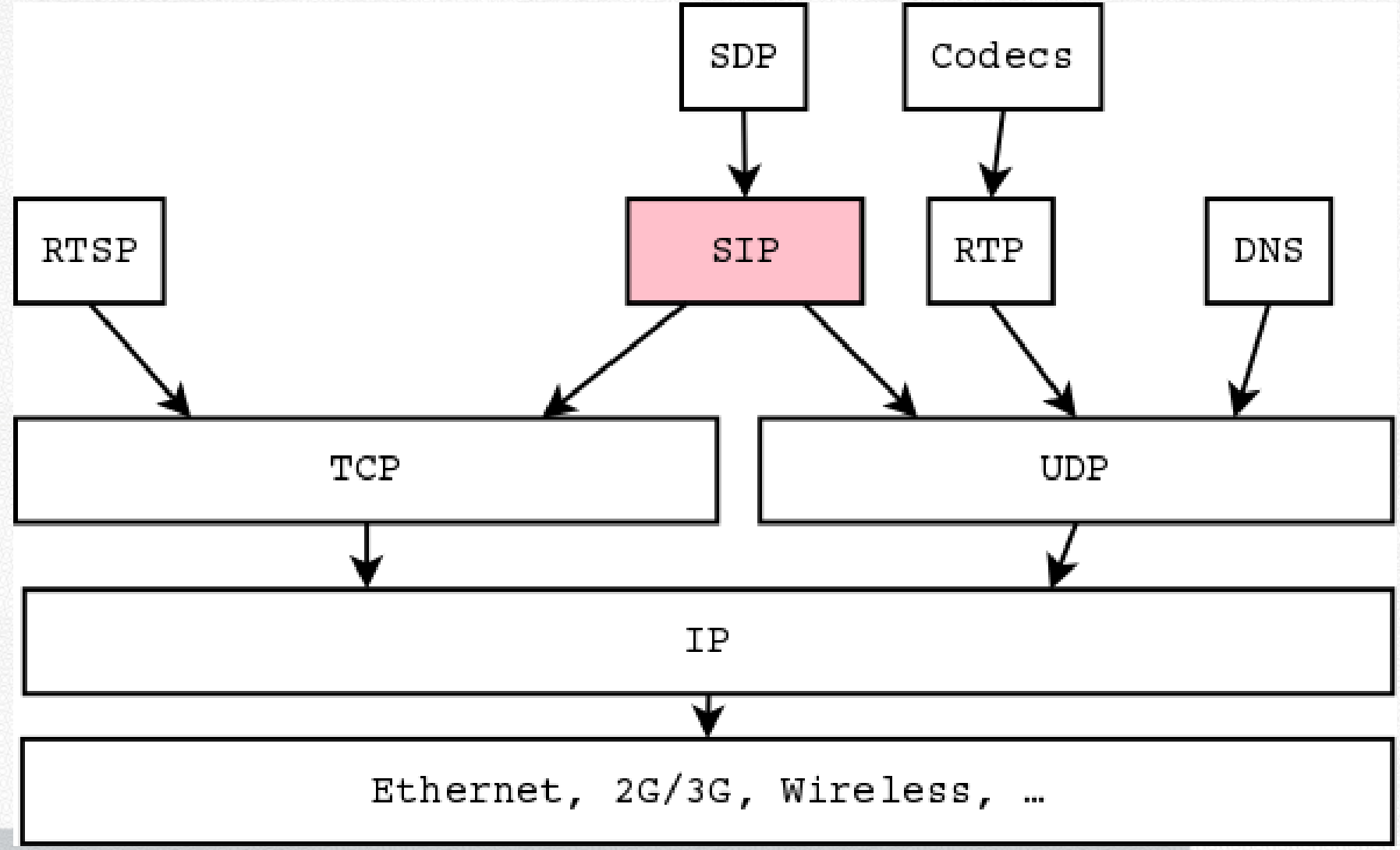
DEEPSEC

- VoIP vereint Schwachstellen von
  - IPv4 & IPv6
  - HTTP, E-Mail
  - Audio & Video Codecs
- Gateways zu PSTN, ISDN, 2G/3G/4G - „Ruf doch mal an!“
- »größter gemeinsamer Nenner«
- Sicherheitskatastrophe

Was ist VoIP?

DEEPSEC

- Signalisierung
  - Session Initiation Protocol (SIP)
  - H.323
  - Inter-Asterisk™ eXchange (IAX)
- Audio-/Videodaten
  - Session Description Protocol (SDP)
  - Real-time Transport Protocol (RTP)
  - Real-Time Transport Control Protocol (RTCP)
  - IAX

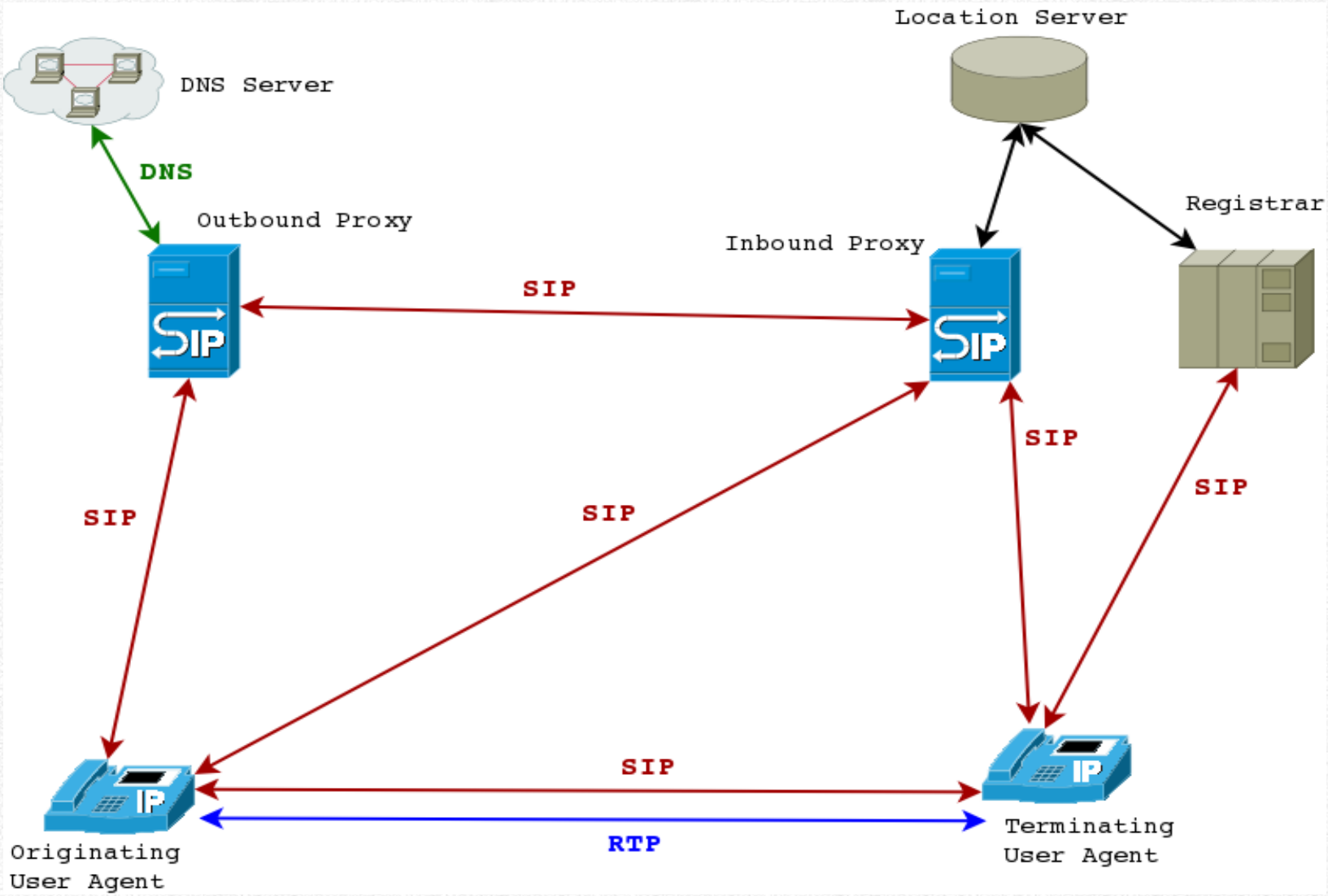

SDP
Codecs
RTSP
SIP
RTP
DNS
TCP
UDP
IP
Ethernet, 2G/3G, Wireless, …

SIP Komponenten

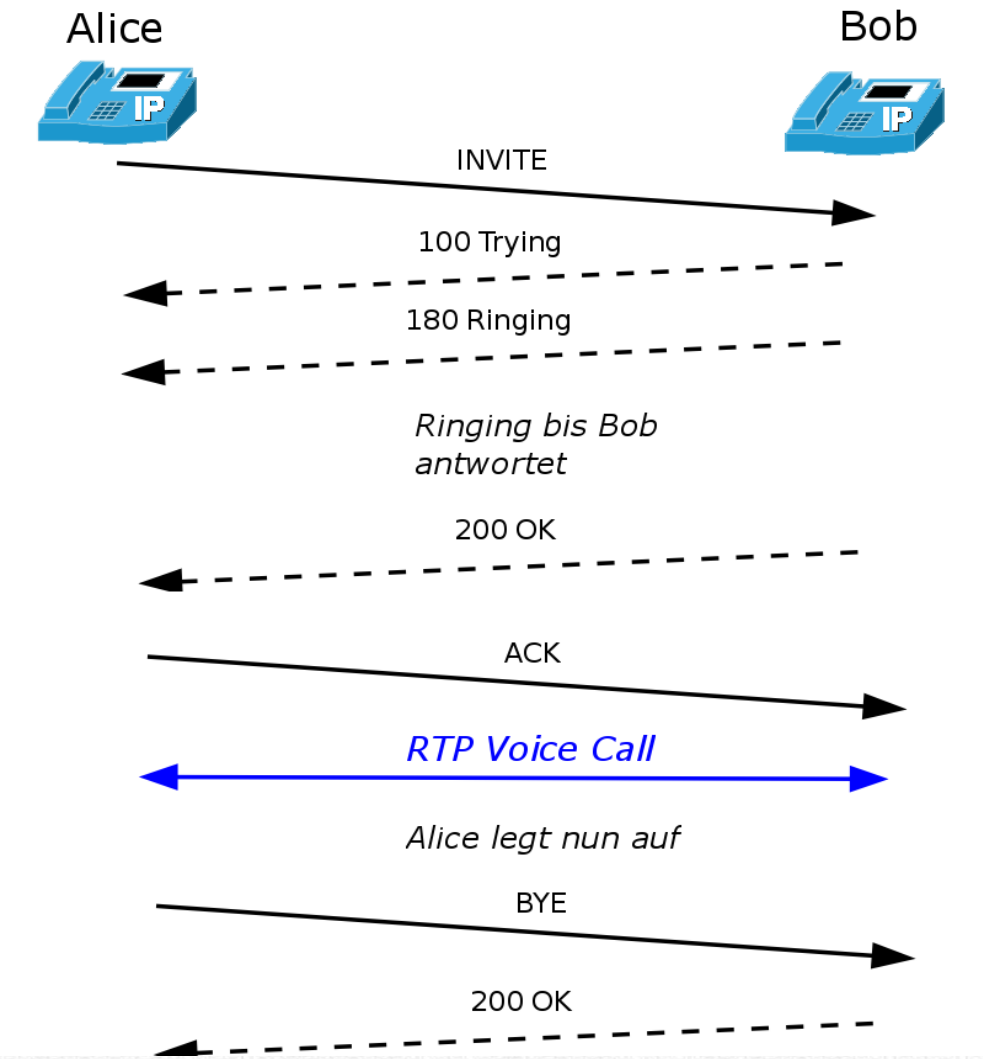
DEEPSEC

- User Agent (Soft-/Hardphone)
- Registrar / Registration Server
- Redirect Server
- Proxy Server
- SIP-fähige Endpunkte sind immer Server **und** Client

SIP Interaktion



SIP Gesprächsaufbau

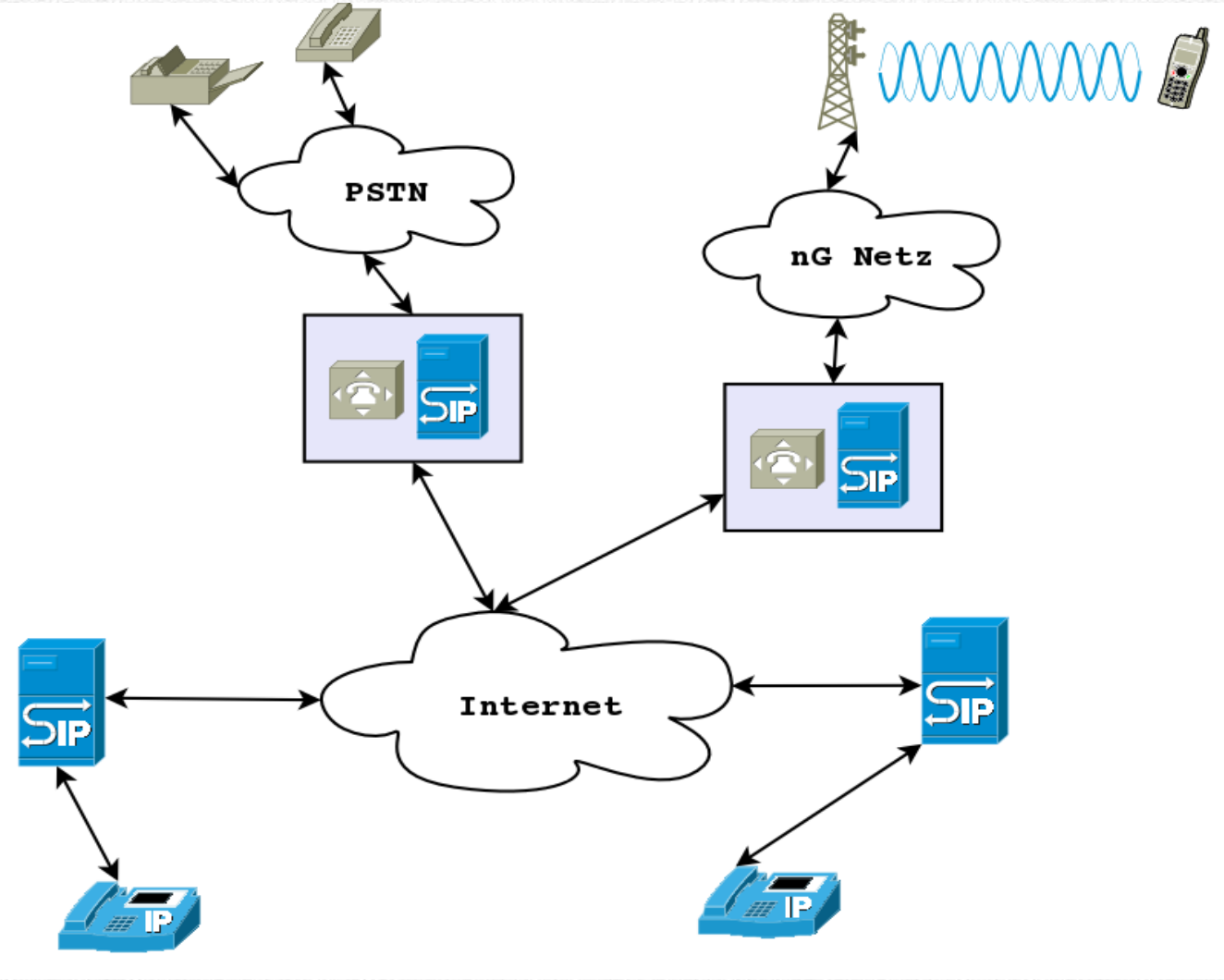


SIP Nachricht

DEEPSEC

```
REGISTER sip:pbx.deepsec.net SIP/2.0
Route: <sip:23.23.23.1:5060;lr>
CSeq: 1 REGISTER
Via: SIP/2.0/UDP 172.16.17.30:5060;branch=z9hG4bK422da326-0f71-e011-8313-028037ec0200;rport
User-Agent: Ekiga/3.2.7
From: <sip:42@pbx.deepsec.net>;tag=64ada126-0f71-e011-8313-028037ec0200
Call-ID: be8aa126-0f71-e011-8313-028037ec0200@nephtys
To: <sip:42@pbx.deepsec.net>
Contact: <sip:42@172.16.17.30>;q=1, <sip:42@10.15.1.2>;q=0.750, <sip:42@10.23.23.2>;q=0.500, <sip:42@10.42.23.2>;q=0.250
Allow: INVITE,ACK,OPTIONS,BYE,CANCEL,SUBSCRIBE,NOTIFY,REFER,MESSAGE,INFO,PING
Expires: 3600
Content-Length: 0
Max-Forwards: 70
```

SIP Gateways



Angriffsziele

- DoS / DDoS
- TDoS
- Signalisierung
- Audio-/Videostream

DoS / DDoS / TDoS

- Erschöpfen von Bandbreite
- Fluten mit Signalisierung
  - UAs läuten
  - UAs melden sich ab / stürzen ab / rebooten
- Fluten mit Audio/Video
  - „satanische Botschaften“
  - Stören von Gesprächen

Layer 2 / IPv4 / IPv6

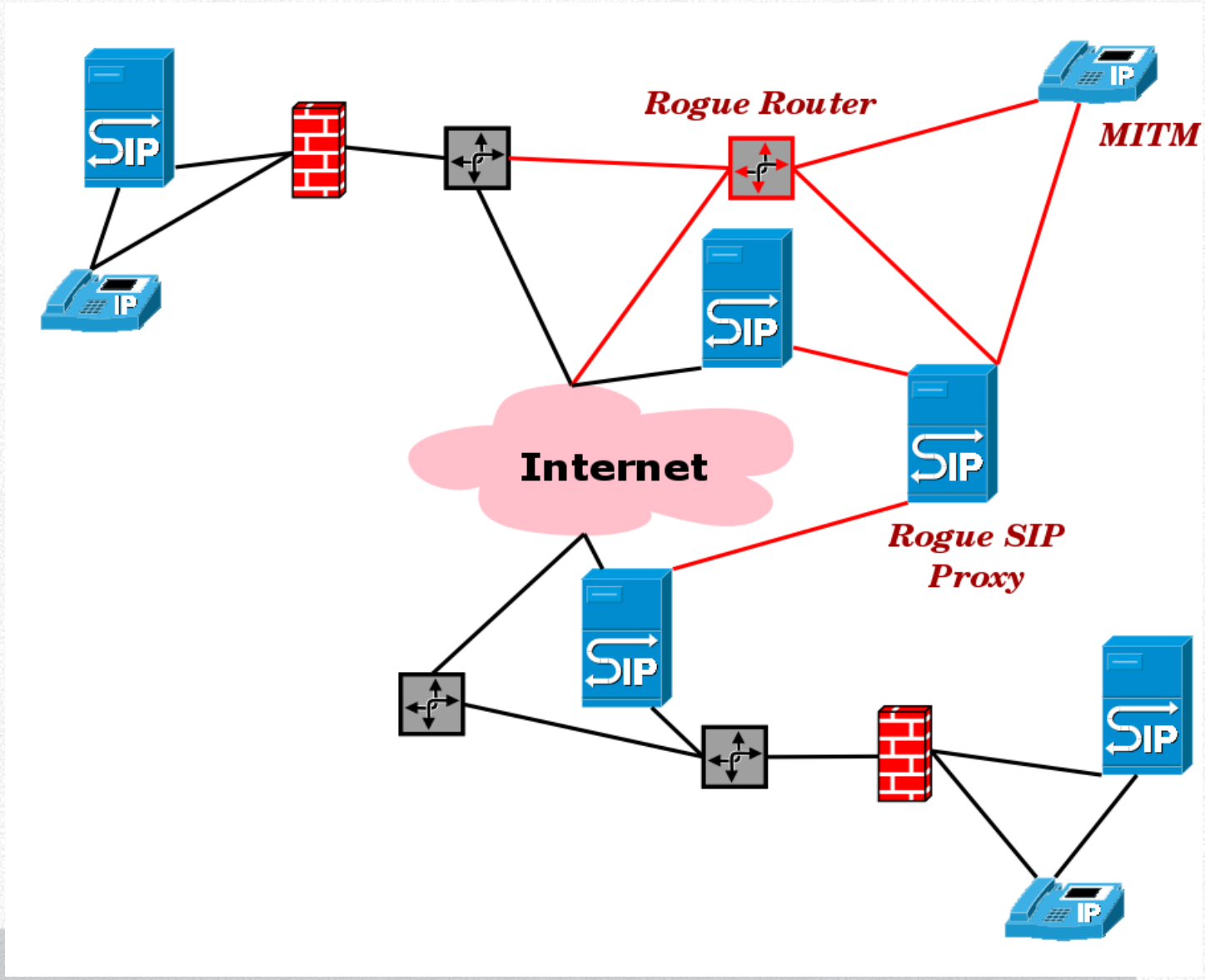
- Fehlkonfigurationen
- VLAN Hopping
- ARP Spoofing, IP Spoofing (SIP benutzt UDP)
- DNS Hijacking / Spoofing
- DHCP Exhaustion
- Routing Attacken
- Management Interfaces
- Provisioning (TFTP, …)

Client Konfiguration

DEEPSEC

- Hardphones holen Konfiguration vom Netzwerk
- Angriff auf Provisioning Server
  - TFTP
  - Webserver
- SNMP
- Management Interfaces

Mittelsmannattacken



Signalisierung

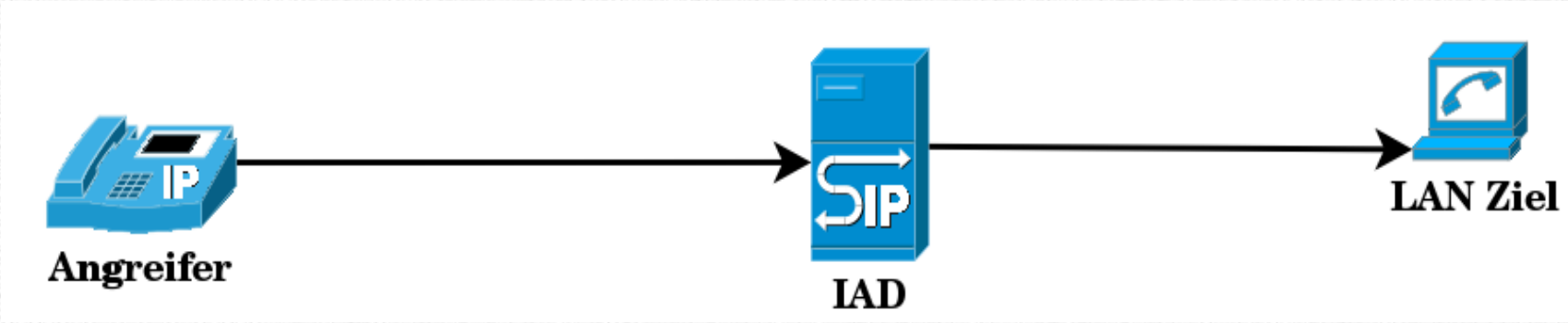
- Aufzählen von Benutzerkonten
- Abfangen & Knacken von Paßworten
- Man-In-The-Middle Attacken
- Hijacking von Registrierungen
- Spoofing (Caller-ID / Registrare / Proxy Server)
- DoS
  - BYE
  - REGISTER / un-REGISTER

Aufklärung

DEEPSEC

- War Dialling für digitale PBX
  - Identifizieren von SIP-fähigen Geräten
  - Identifizieren von Anschlüssen
- Fingerprinting
- Aufzählen von Anschlüssen/Konten
- Trend: Portscans auf Port 5060 beliebter als Port 22
  - Gesucht werden Spender für Gesprächsguthaben
  - „Calling Cards“

- SIP hält Zustand in der Nachricht
  - Entlasten des Netzwerk Cores
- Entspricht *Source Routing* bei IP
  - Sender gibt Weg vor
  - Requests/Responses in LANs schicken
  - Mediadaten in LANs schicken



SIP Authentisierung

DEEPSEC

- SIP verwendet Digest Authentication
  - Challenge-Response mit MD5 wie bei HTTP
  - WWW-Authenticate: Digest algorithm=MD5, realm="deepsec.net", nonce="4c97916f"
  - Authorization: Digest username="23", realm="deepsec.net", nonce="4c97916f", uri="sip:pbx.deepsec.net", algorithm=MD5, response="4e920a4c1c2a7147950c447b13b9b6e5"
- Mitschneiden ermöglicht Offline Brute Force Attacke
- Viele SIP-fähige Geräte lecken Digest Auth Information
- Brute Force Attacken zunehmend leichter
  - GPUs (hunderte von Cores pro PC)
  - Cloud Brute Forcing

SIP Digest Auth Leak

1. Ziel ist per SIP erreichbar
2. Angreifer sendet INVITE Kommando an Ziel
3. Ziel läutet, Hörer wird abgenommen und wieder aufgelegt
4. Ziel sendet BYE an Angreifer
5. Angreifer schickt »407 Proxy Authentication Required« an Ziel
6. Ziel schickt Digest Authentication Antwort und zweites BYE
7. Angreifer hat alle Informationen für Brute Force Attacke
8. Let's rent some virtual servers…

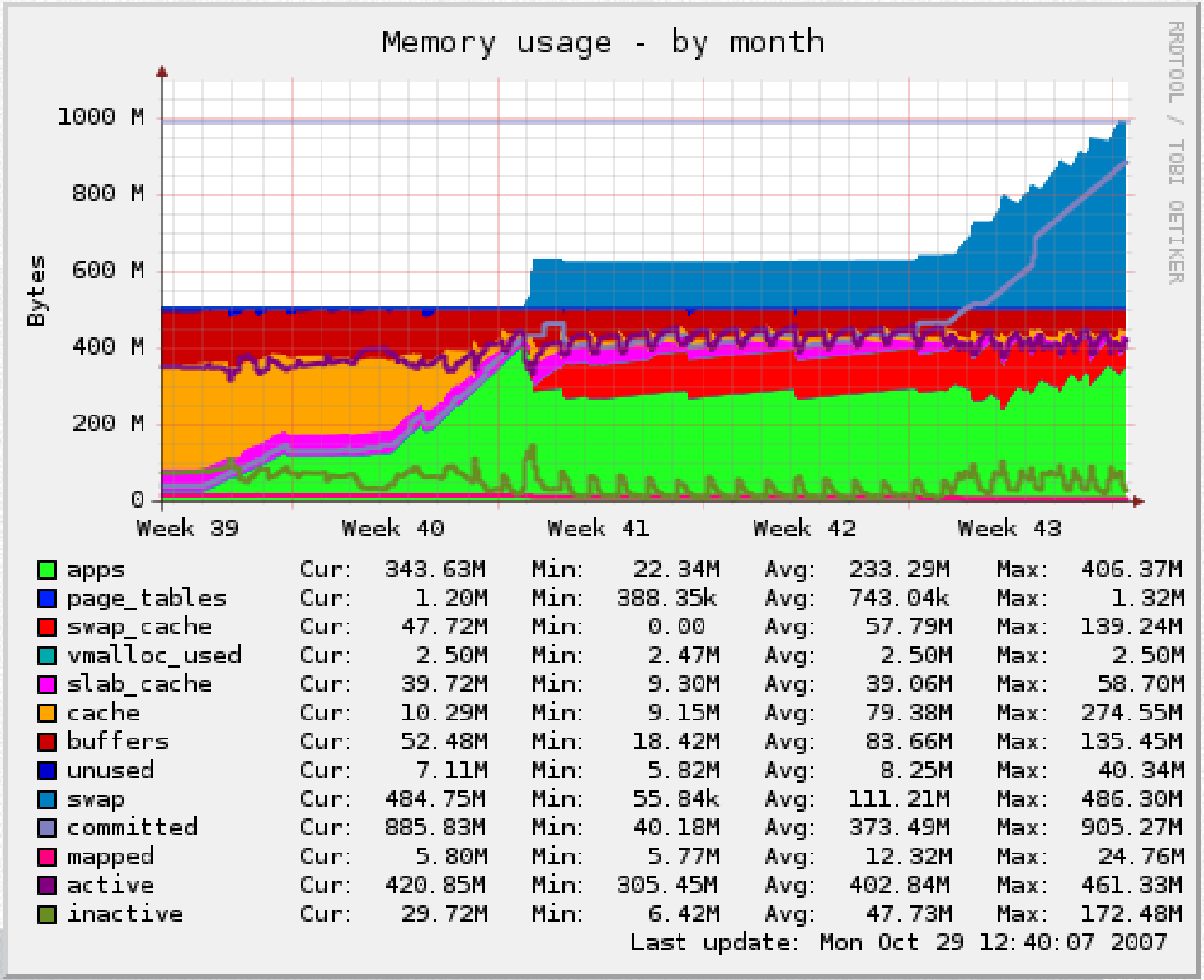
SIP Firewall Inspection

DEEPSEC

- SIP ähnelt HTTP
- Viele Firewall/NAT-Devices sind »SIP aware«
  - INVITE http://x.com/sip:bob@fasel.com/SIP/2.0 HTTP/1.1
  - INVITE sip:bob@x.com SIP/2.0
- Öffnen von UDP Ports ins LAN via SIP
  - Laden von JavaScript in Browser im LAN
  - JavaScript sendet SIP URLs ins Internet
  - NAT-FW öffnet Tore für UDP Traffic

SIP Testen

- Protokollsicherheitsforschung
- PROTOS Test Suites von Codenomicon
- Fuzzing und entworfene ungültige Nachrichten
- Für SIP und andere Protokolle verfügbar
  - Bitte Developern schenken und sie quälen!


Memory usage - by month
RRDTOOL / TOBI OETIKER
Bytes
1000 M
800 M
600 M
400 M
200 M
0
Week 39
Week 40
Week 41
Week 42
Week 43
apps Cur: 343.63M Min: 22.34M Avg: 233.29M Max: 406.37M
page_tables Cur: 1.20M Min: 388.35k Avg: 743.04k Max: 1.32M
swap_cache Cur: 47.72M Min: 0.00 Avg: 57.79M Max: 139.24M
vmalloc_used Cur: 2.50M Min: 2.47M Avg: 2.50M Max: 2.50M
slab_cache Cur: 39.72M Min: 9.30M Avg: 39.06M Max: 58.70M
cache Cur: 10.29M Min: 9.15M Avg: 79.38M Max: 274.55M
buffers Cur: 52.48M Min: 18.42M Avg: 83.66M Max: 135.45M
unused Cur: 7.11M Min: 5.82M Avg: 8.25M Max: 40.34M
swap Cur: 484.75M Min: 55.84k Avg: 111.21M Max: 486.30M
committed Cur: 885.83M Min: 40.18M Avg: 373.49M Max: 905.27M
mapped Cur: 5.80M Min: 5.77M Avg: 12.32M Max: 24.76M
active Cur: 420.85M Min: 305.45M Avg: 402.84M Max: 461.33M
inactive Cur: 29.72M Min: 6.42M Avg: 47.73M Max: 172.48M
Last update: Mon Oct 29 12:40:07 2007

Audio-/Videodaten

- Mithören
- Einfügen von Audiodaten
- Ersetzen von Audiodaten
- DoS für Gespräche

Mithören & Mitsprechen

- RTP Streams sind »Klartext«
- Streams haben IDs und Sequenznummern
  - Synchronization Source Identifier (SSRC)
  - Sequence Number
  - Timestamp
- Dekodieren sehr leicht
- Audioinjektion möglich
  - Verwendung gleicher IDs
  - Manipulieren der Timestamps

RTP DoS

- RTP-fähige Empfänger müssen RTP dekodieren
- Stören mit Fake-RTP Paketen
  - SSRC Nummer notwendig
  - Fluten
- Senden von RTCP BYE Paketen

Verschlüsselung

- IPsec
- Secure RTP (SRTP)
- SIPS (=SIP+SSL/TSL)
- SIP + S/MIME
- H.323 + stunnel (SSL/TLS)
- <u>Aber:</u>
  - Ende-zu-Ende schwierig bis unmöglich
  - Signalisierung separat von Audio/Video!

Verschlüsselung ZRTP

DEEPSEC

- ZRTP bietet PGP-ähnliche Features
- Signalisierung mit SIP, H.323, Jingle und DHT
- Ende-zu-Ende Verschlüsselung
- Integritätscheck mit Codes, die vorgelesen werden
- ZRTP/S Erweiterung für GSM, UMTS, ISDN, PSTN, SATCOM, UHF/VHF Funk

Verschlüsselung einsetzen?

DEEPSEC

- Sicherheitslevel bestimmt Verschlüsselung
  - Gespräche / Daten klassifizieren
  - Sicherheitsstufen einführen
- Höchste Sicherheit nur gegeben, wenn
  - man selbst alle beteiligten Schlüssel kontrolliert,
  - Ende-zu-Ende Verschlüsselung vorliegt.
- Absicherungen eigener Infrastruktur leichter möglich

Gegenmaßnahmen

DEEPSEC

- Telefonie per Policy bewerten (Awareness!)
- VoIP- & Daten-Netzwerke strikt trennen
  - impliziert keine Softphones!
- SIP Traffic strikt filtern (Whitelisting)
- Proxies verwenden (um UAs abzuschotten)
- IP Adressen in SIP ignorieren (RTP verwenden)
- Verschlüsselung einsetzen wo möglich
- Regelmäßiges Auditing / Pen Testing
  - Testen neuer UAs / Systeme vor Einführung

…as we know, there are known knowns. There are things we know we know. We also know there are known unknowns. That is to say we know there are some things we do not know. But there are also unknown unknowns -- the ones we don't know we don't know.
– *Donald Rumsfeld, 12.2.2002, Department of Defense news briefing*

Über uns…

DEEPSEC

The DeepSec IDSC is an annual European two-day in-depth conference on computer, network, and application security. We aim to bring together the leading security experts from all over the world. DeepSec IDSC is a non-product, non-vendor-biased conference event. Intended target audience: Security Officers, Security Professionals and Product Vendors, IT Decision Makers, Policy Makers, Security-/Network-/Firewall-Admins, Hackers and Software Developers.

Web: https://deepsec.net/
Blog: http://blog.deepsec.net/

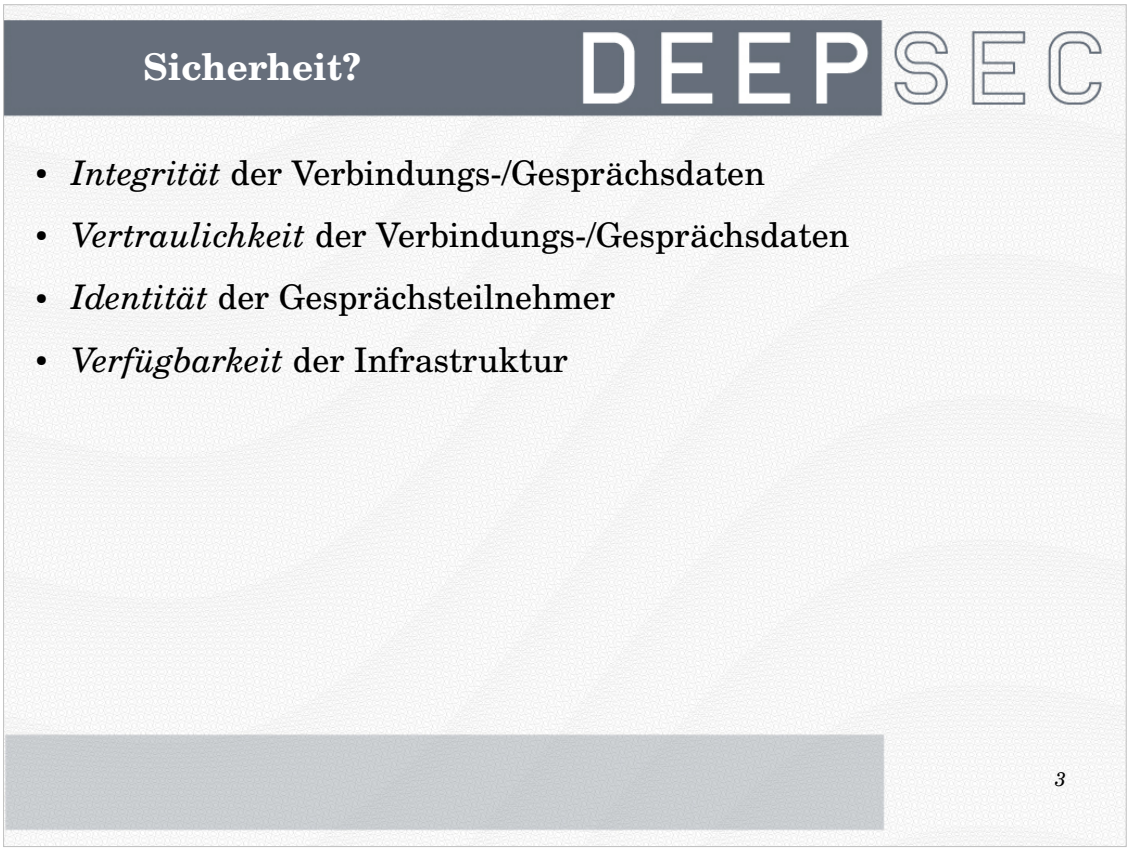
Tools

- Perl, Python, C/C++ ☺
- sipvicious
- sipsak
- smap
- nmap
- Backtrack 4 Live-CD
- VoIP Hacking Exposed

Das Bild zeigt ein SIGSALY Telefon. Es wog 50 Tonnen, hatte 40 Racks und wurde von den Allierten ab 1943 für verschlüsselte Telefonate eingesetzt. Ein dutzend dieser Telefone wurden unter den Hauptquartieren verteilt (unter anderem hatte General Douglas MacArthur eine „mobile“ Variante auf einem Schiff der US Navy im Pazifik). Die kryptographische Qualität war sehr hoch. Deutsche Einheiten fingen SIGSALY Kommunikation ab, dachten jedoch es sei ein komplexes telegrafisches Kodierungssystem.

Das Bild stammt aus dem National Cryptologic Museum der NSA.

Es sei angemerkt, daß im Rahmen dieses Vortrags nur ein Teil der tatsächlich eingesetzten Protokolle betrachtet werden kann. Cisco hat ein eigenes Protokoll, daneben gibt es H.323 und eine Vielzahl von Protokollen in SS7 und Mobilfunknetzwerken. Dazu gibt es noch Insellösungen wie Skype oder andere Messenger-Dienste, die auch Audio-/Videokommunikation ermöglichen (wie beispielsweise XMPP-Clients wie Ekiga).



In den seltensten Fällen werden alle Kriterien immer für alle Kommunikationen gleich wichtig sein. Es macht daher sehr viel Sinn eine Klassifizierung einzuführen und nicht alle Daten über die höchste Sicherheitsstufe zu leiten. Dieser Ansatz ist sehr verbreitet und wird auch beim Militär eingesetzt.

Achtung, Gefahr!

Beschrieben im Artikel von The Register (2006):

„Two men were arrested yesterday and charged with wire and computer fraud. They are accused of secretly routing phone calls into VoIP services without paying for them.

Edwin Pena, a 23-year old man living in Miami, started two companies offering wholesale phone services - smaller telco providers often buy bulk packages of minutes from such companies. But Pena wasn't buying wholesale telco minutes, he was getting them by hacking into various VoIP providers. Robert Moore, 22-years-old from Spokane, Washington, allegedly helped him.

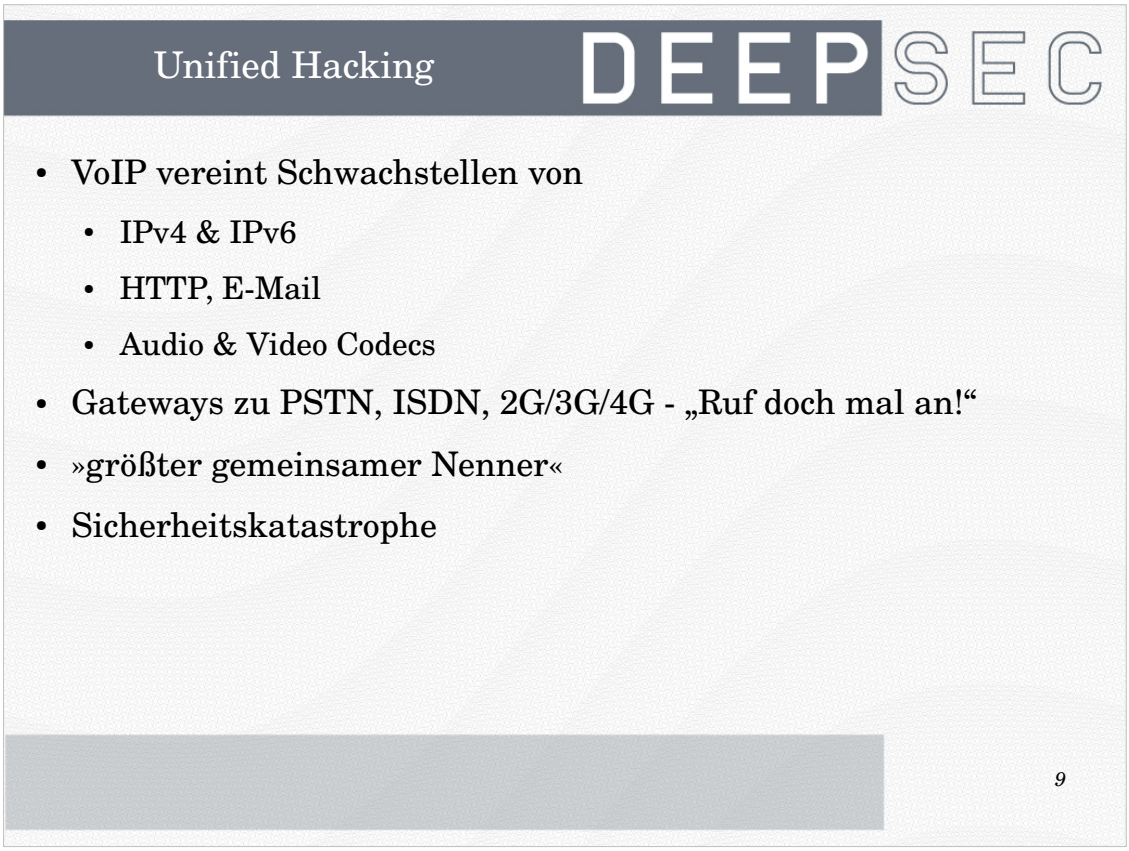
To cover their tracks the two routed calls through unprotected network ports at other companies to route calls onto providers. Over three weeks, the two routed half a million phone calls to a VoIP provider in Newark via a company based in Rye Brook. Federal investigators believe the two made as much as $1m from the scam. …“

Die Deutsche Telekom hatte 2008 diesbezüglich ihren eigenen Skandal, der auf der Webseite einer Detektei beschrieben ist:
„Die Deutsche Telekom soll, so die Staatsanwaltschaft Bonn, mindestens 55 Personen, darunter Aufsichtsräte der Telekom und T-Mobile, ein Vorstandsmitglied der Telekom sowie Betriebsratsangehörige und weitere Mitarbeiter der Telekom abgehört oder mit illegalen Methoden ausgeforscht haben. Ebenso betroffen von dieser Spitzelaffäre sind auch sieben Journalisten sowie weitere Personen, zu denen unter anderem auch der Gewerkschaftschef Frank Bsirske gehört.“

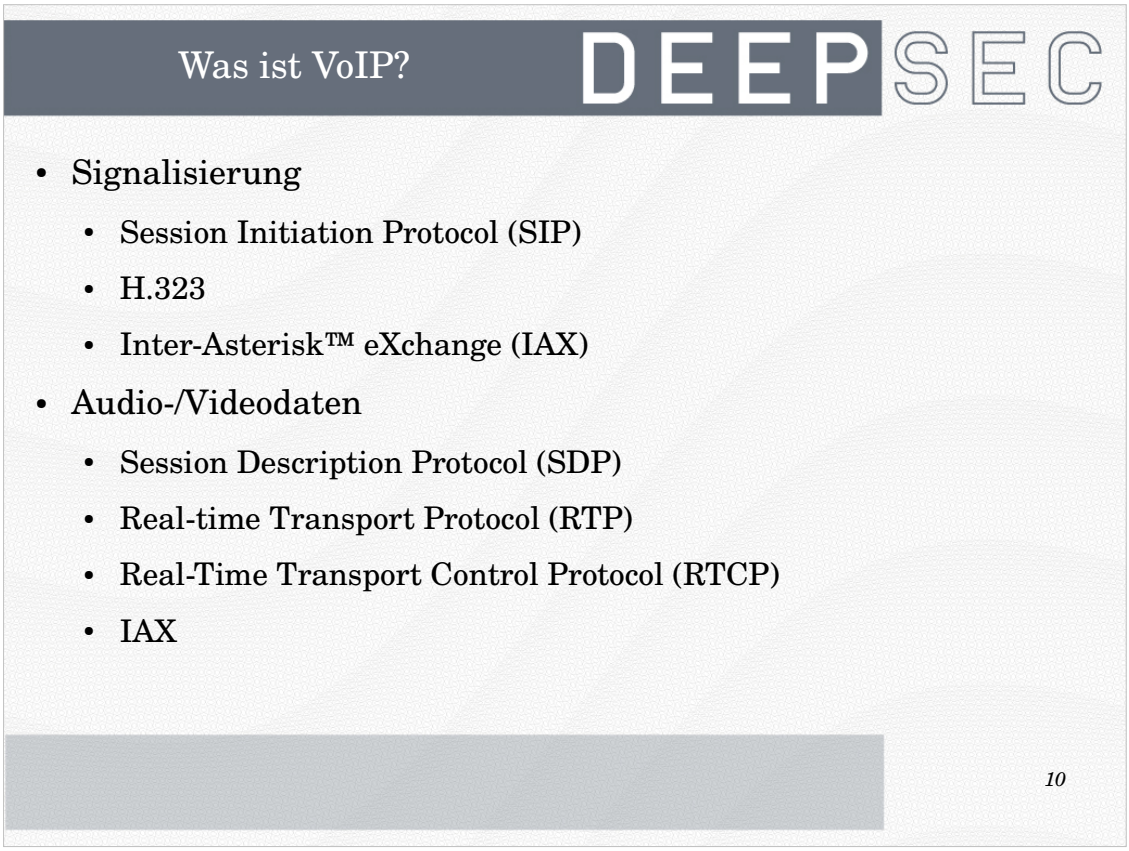
Das illustriert sehr schön, daß Mittelsmannattacken verbreiteter sind denn je. Infrastruktur muß immer hinterfragt und kontrolliert werden.

Über *The Athens Affair* findet man im Internet reichlich Artikel. Die Lektüre des zitierten Artikels aus dem IEEE Spectrum ist sehr zu empfehlen. Solche Geschichten kennt man normalerweise nur aus Kriminalromanen, aber es gibt tatsächlich gute Gründe für Kriminelle Netzwerk zu kompromittieren. Im besagten Fall dürfte wohl auch ein gesundes Maß an Korruption im Spiel gewesen sein. Bitte also immer auf zufriedene und glückliche Mitarbeiter achten. ☺

Slippery when insecure. Beware!

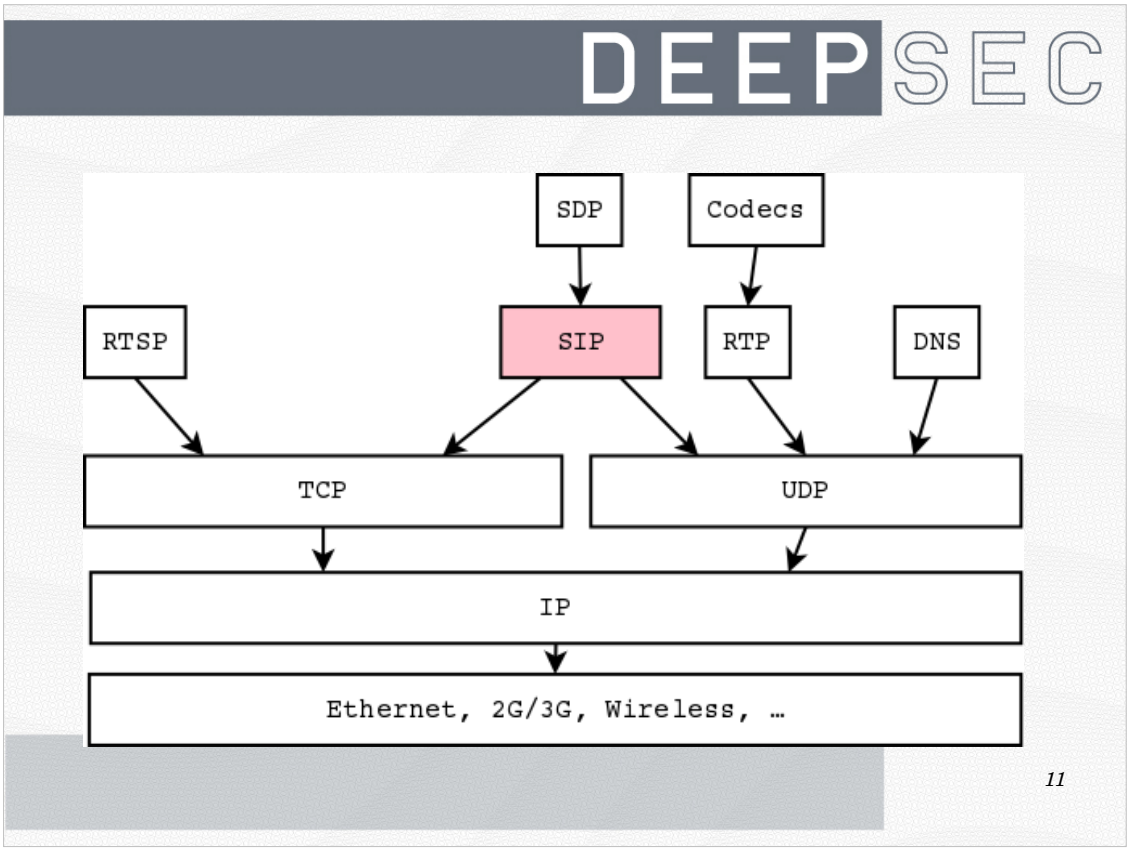


Voice over IP besteht aus einer Vielzahl von Protokollen, die allerlei Probleme mit sich bringen. Darüber hinaus ist Audio-/Video naturgemäß komplexer und damit anfälliger für Fehler in der Implementierung. VoIP läßt sich also mit der Summer aller Attacken auf alle Komponenten angreifen, was sicherheitstechnisch ein Alptraum ist, speziell da man bei Anrufen wie bei E-Mail oder Webauftritten in der Regel für die Welt erreichbar sein muß.
Ein gezieltes Whitelisting ist nur ganz selten möglich.



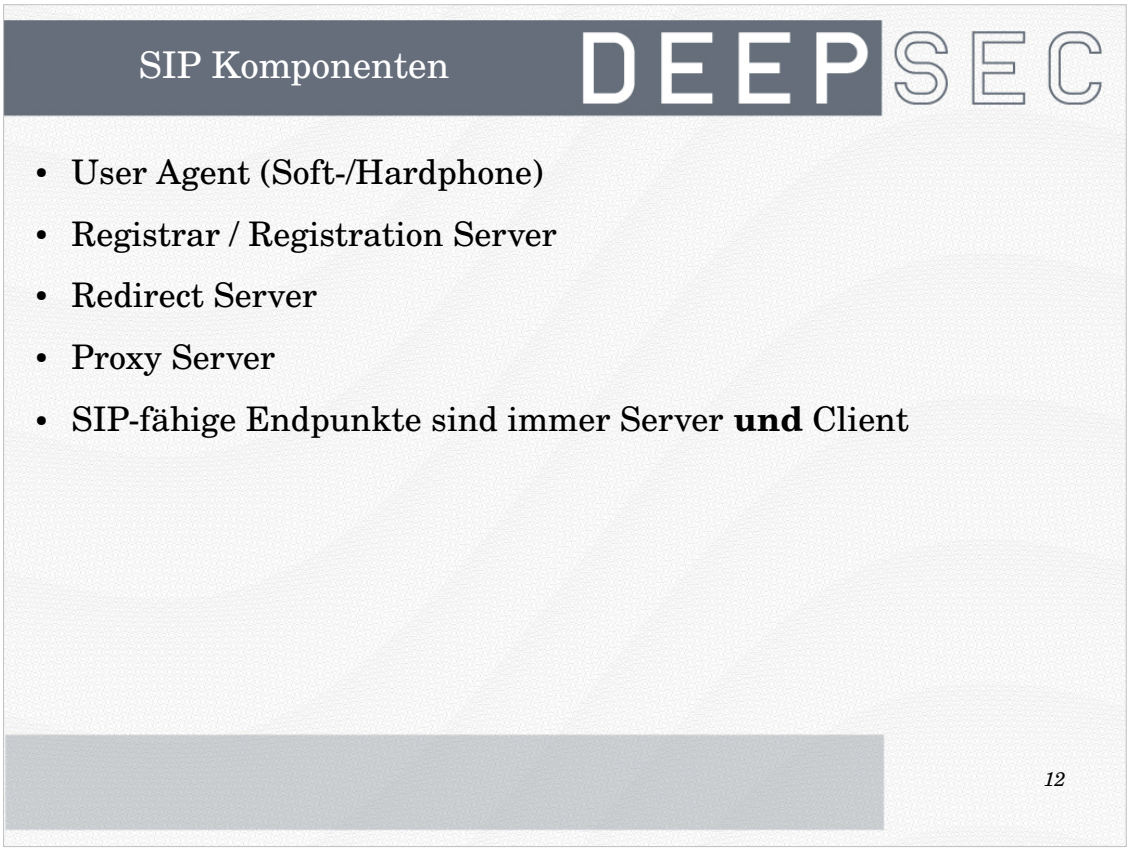
VoIP teilt sich in die Signalisierung und in die eigentlichen Gesprächsdaten auf. Die Signalisierung kümmert sich um die Vermittlung der Gespräche, Ortsangaben (sprich wie ist der Client gerade zu erreichen) und Aushandlung des Medienstreams.

Die Audio-/Videodaten werden von anderen Protokollen gehandhabt und werden im Idealfall immer zwischen den Gesprächsteilnehmern ausgetauscht (was aufgrund NAT oder Proxies nicht immer möglich ist).

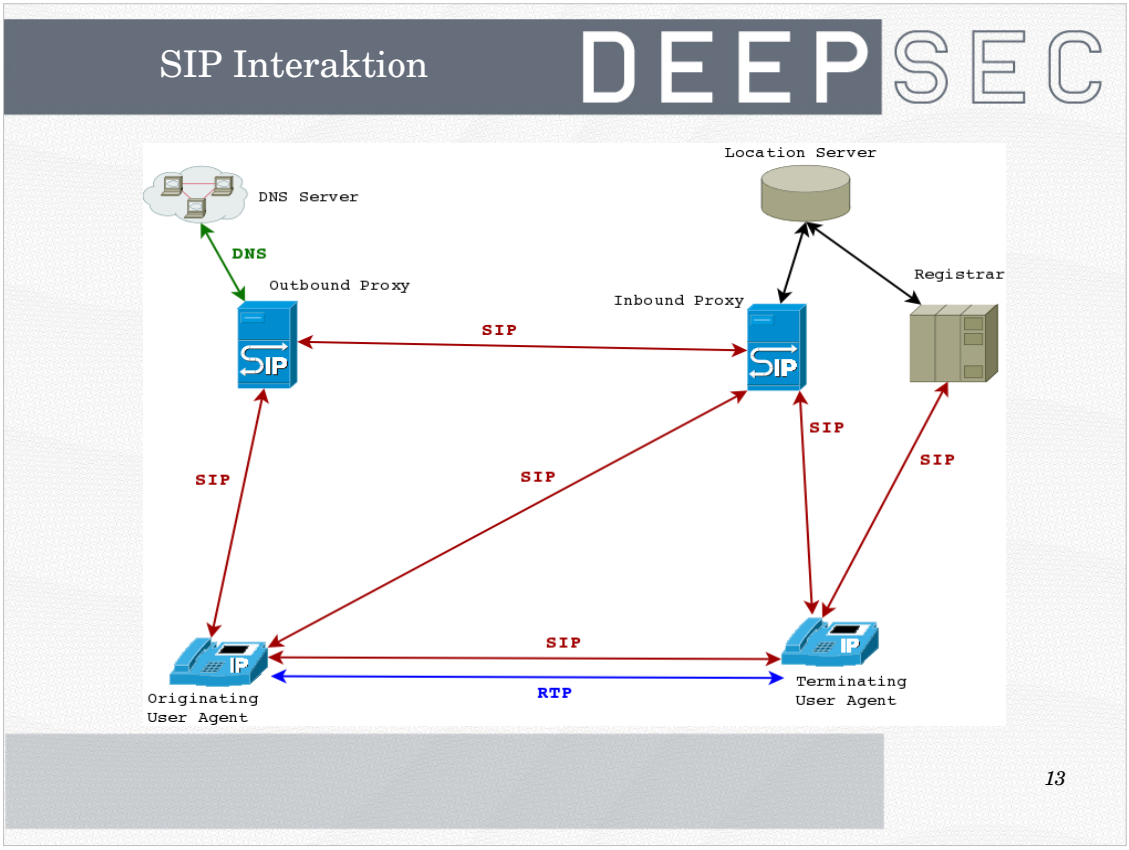


SIP ist für die Verwendung über UDP und TCP spezifiziert. Der Großteil aller SIP-fähigen Komponenten implementiert es leider nur über UDP, was das Fälschen von Paketen sehr leicht macht.

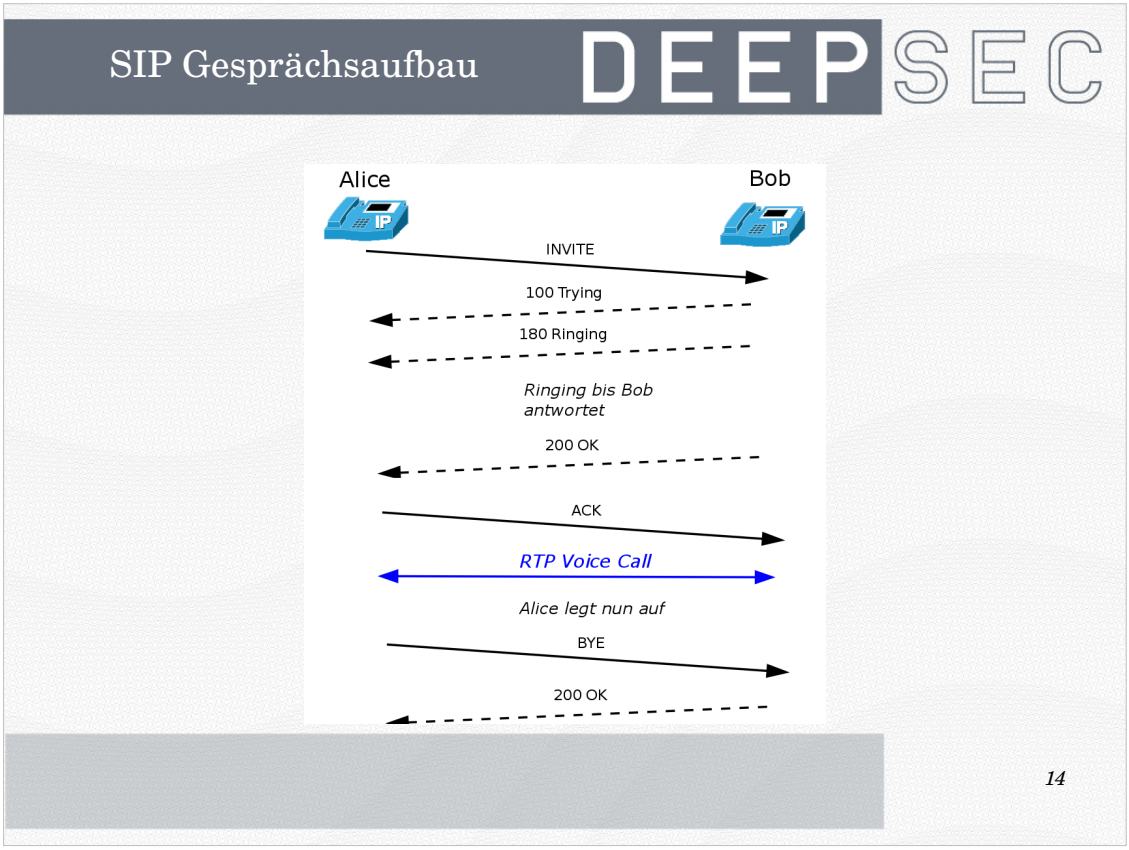
SDP wird wie der Text einer E-Mail in eine SIP Nachricht eingebettet und beschreibt welche Audio-/Videoparameter die Endgeräte unterstützen. In der SIP Nachricht können auch noch Informationen über tatsächlich IP-Adressen oder NAT stehen.



Ein *User Agent* ist in der Regel ein Endgerät mit Hörer und Mikrofon.
Ein *Registrar* nimmt Anmeldungen von UAs entgegen und führt Buch über deren Erreichbarkeit und deren Ort im Netzwerk.
Ein *Redirect Server* ist ein User Agent, der SIP Codes aus dem Bereich 3xx ausgibt und SIP Nachrichten umleitet, ganz analog zu den HTTP Redirect Codes. Man kann damit ein VoIP Netzwerk besser skalieren.
Ein *Proxy Server* entspricht voll und ganz dem HTTP Pendant. Beispielsweise könnte man über einen solchen Proxy User Agents im LAN die Registrierung an einem externen Server erlauben.



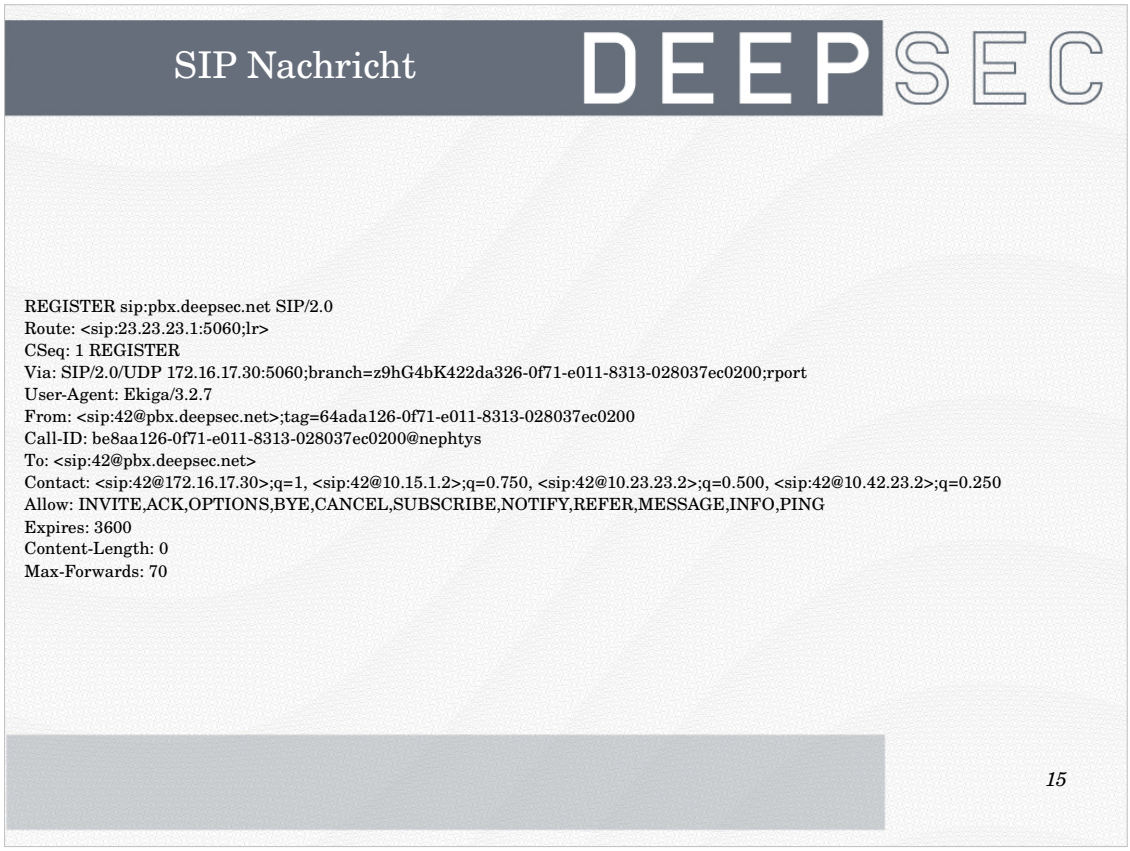
Die Grafik illustriert welche Komponenten in einem SIP Netzwerk präsent sein können. Alles außer den beiden User Agents ist optional, denn man könnte auch zwei UAs per statischer Konfiguration und Cross-Over-Kabel per SIP vernetzen.
Durch die „Ausuferung“ der Komponenten sieht man hier schon ganz gut, daß Angreifer sehr viele Optionen haben. Beispielsweise könnten sie auch einen DNS Server angreifen, versuchen eine Domain umzuleiten und dann alle SIP Nachrichten auf einen eigenen Server umleiten.



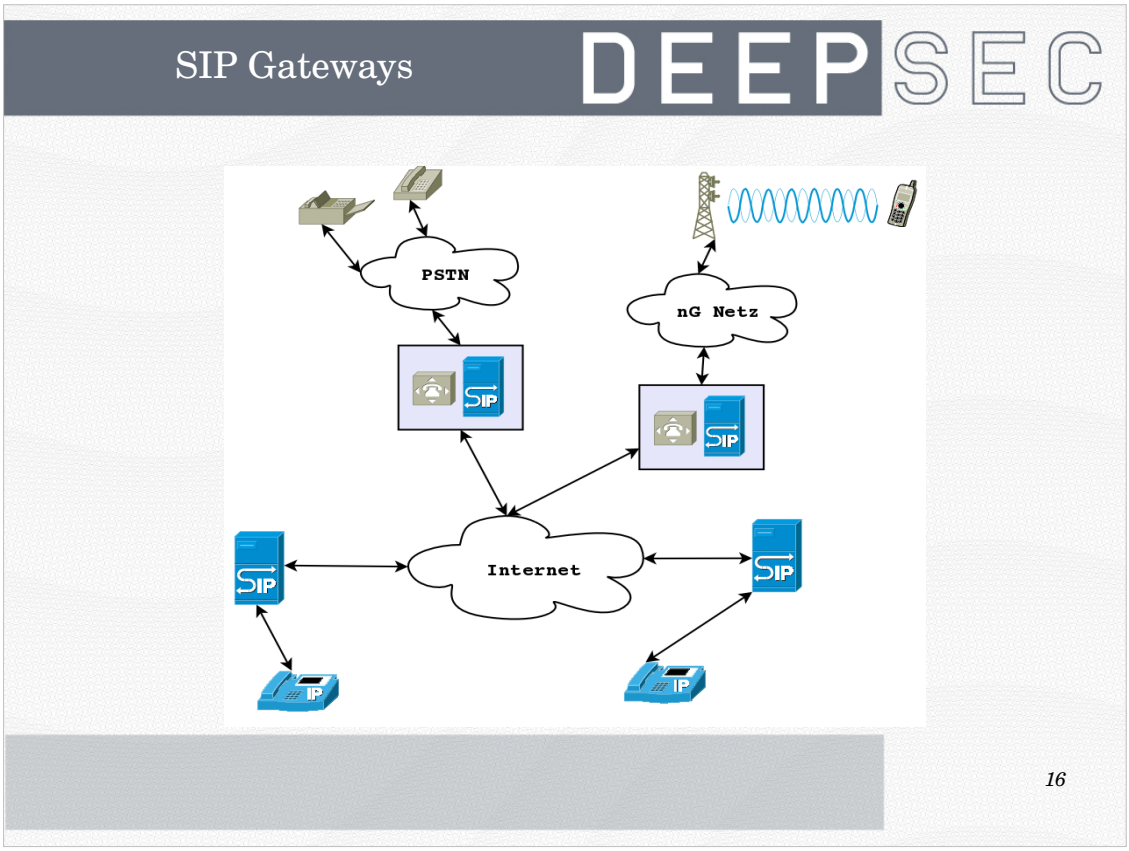
Die Abbildung zeigt die typische Abwicklung eines Anrufs. Eine SIP INVITE Message leitet immer eine Vermittlung eines Anrufs ein. Der angerufene UA generiert RINGING Nachrichten bis abgehoben wird. Bekommt man 200 OK, so kann man sprechen. Per SIP wird dann noch der Weg der Medien ausgehandelt. BYE Nachrichten beenden das Gespräch.

Es ist nie eine schlechte Idee SIP-fähigen Komponenten testweise mal während Gesprächen BYE Kommandos zu schicken bzw. fremden UAs INVITE Nachrichten zu senden. Angreifer würden das auch tun, und so weiß man was passiert bevor es jemand anderer weiß.

Obiger Dialog läßt sich übrigens mit dem Wireshark Tool sehr gut darstellen und dekodieren.



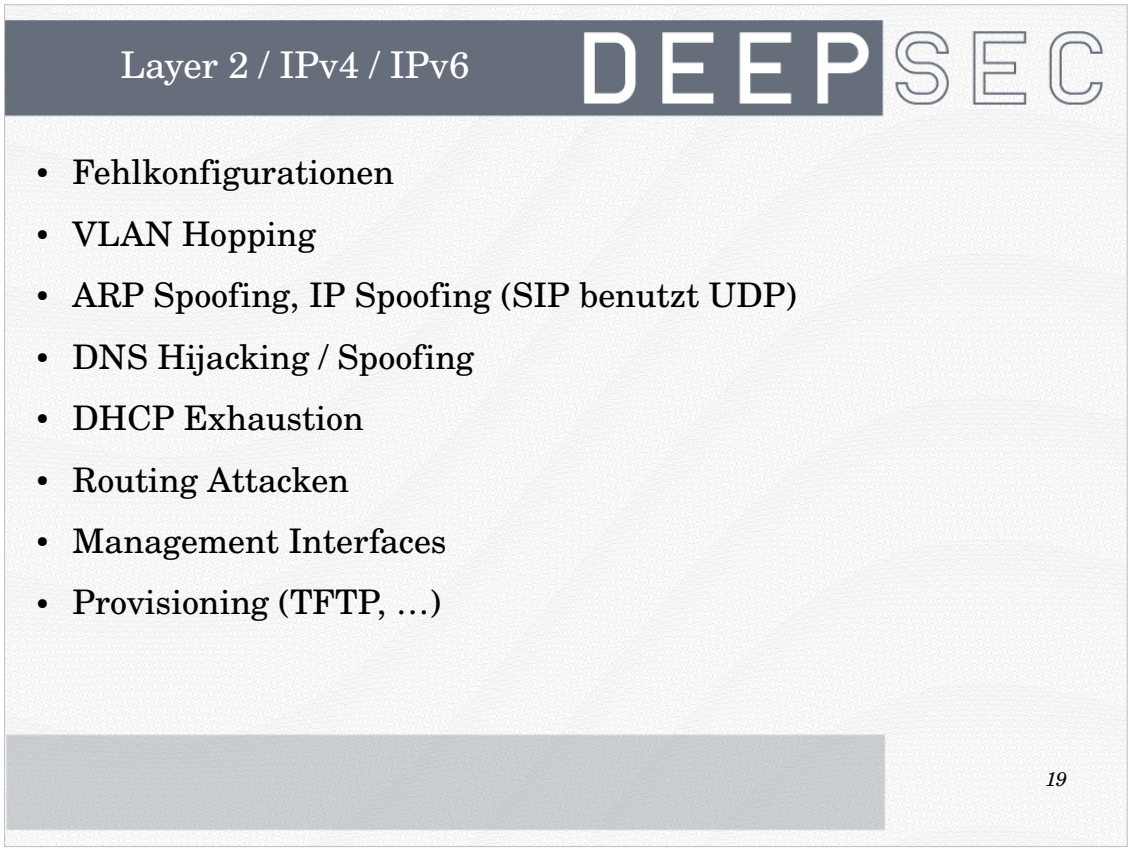
So sieht eine SIP Nachricht aus. Sie entspricht HTTP Requests bzw. E-Mails. Aus pädagogischen Gründen wird empfohlen einmal den eigenen SIP Verkehr aufzuzeichnen und mit Wireshark anzuschauen.



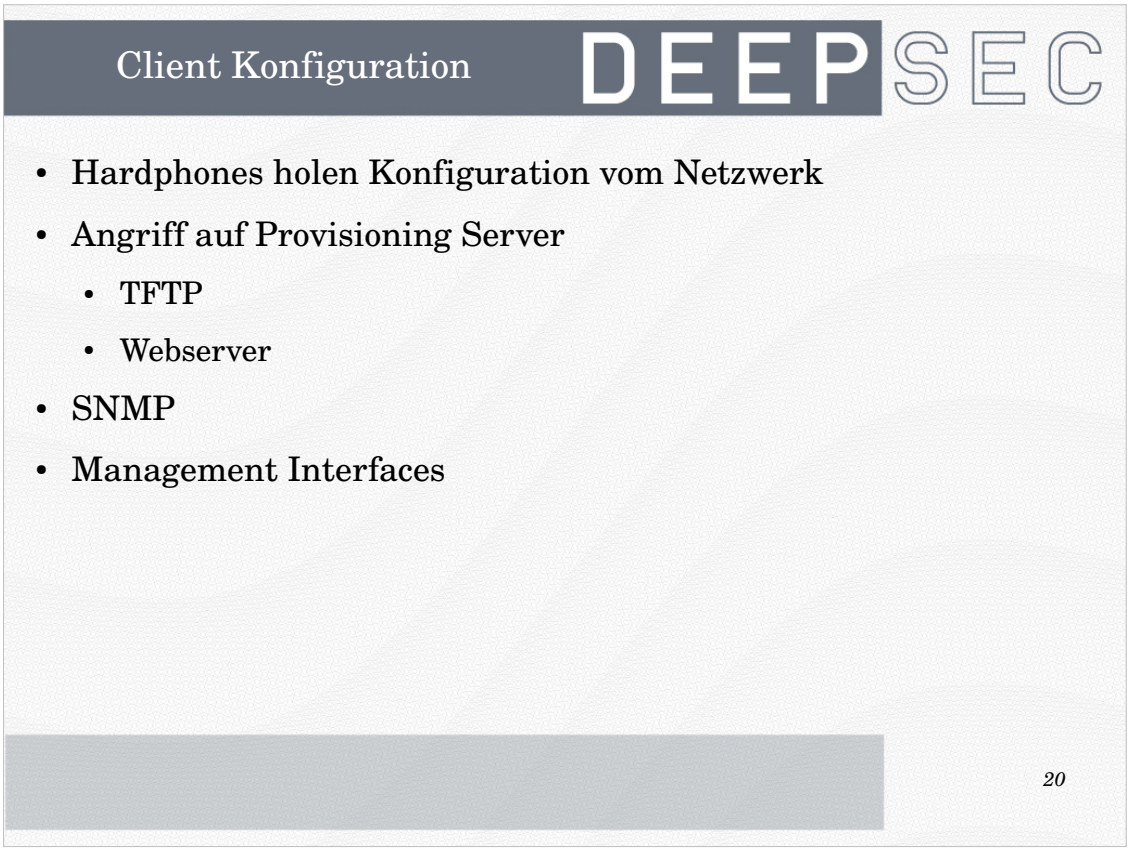
VoIP Gateways (nicht nur solche, die SIP sprechen) verbergen sich an Übergängen zu anderen Netzwerken und auch in Netzwerken selbst (beispielsweise wenn eine Organisation intern VoIP ausschließlich verwendet). Das Bild illustriert ganz gut, daß es sehr viele Übergänge geben kann, die mitunter die Gesprächsqualität verringern. Das ist insbesondere der Fall, wenn QoS-lose Netzwerke durchquert werden müssen, oder wenn die Audio-/Videodaten konvertiert werden müssen.

Was könnte man denn alles kompromittieren oder zerstören? Bei VoIP gibt es aufgrund der vielen Komponenten das Richtige für jeden Geschmack.

Denial of Service Attacken kennt man aus dem IP-Bereich. In der Regel wird eine Leitung geflutet, was sämtliche Datentransmissionen stark stört. Bei VoIP sind diese Transmissionen zeitkritisch, daher fällt das sehr ins Gewicht.
Bei VoIP reicht es mitunter aus sehr viele Signalisierungsnachrichten zu schicken, um z.B. alles was läuten kann zum Läuten zu bringen. Schafft man es durch Signalisierungsattacken nur die Telefonie gezielt lahmzulegen, so spricht man von einer TDoS Attacke.
Man kann auch versuschen laufende Gespräche zu manipulieren oder zu stören, wenn man deren ID kennt. Dann ist es tatsächlich möglich Audio hineinzumischen bzw. auszutauschen.

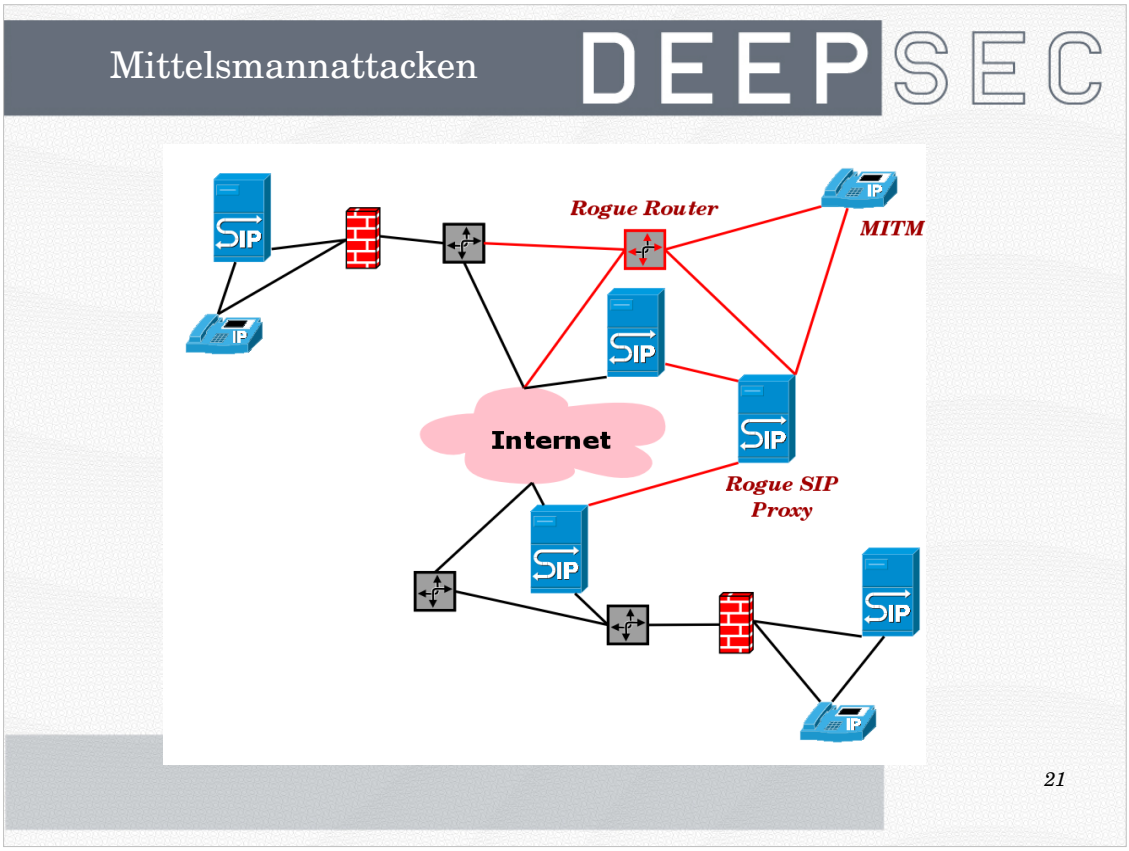


Man kann natürlich auch konservativ sein und nur den IP Teil attackieren. Dafür gibt es reichhaltige Möglichkeiten, Angriffswerkzeuge und Gelegenheiten.



Alle User Agents müssen konfiguriert werden. Hat man ausreichend viele davon, so kommt man um eine automatische Konfiguration nicht herum. Schafft man diese Management-Komponenten zu kompromittieren, so kontrolliert man alle UAs. TFTP ist sehr verbreitet für das Verteilen und Sichern von Konfigurationen, und für TFTP gibt es eine Reihe von Attacken. Ähnlich ist es bei eingebauten Web-Interfaces oder anderen Verwaltungszugängen.

Alle Zugänge dieser Art müssen abgesichert werden/sein.



Hier ist eine Mittelsmenschattacke skizziert, die nicht in der Nähe der UAs stattfindet. Router sind immer ein willkommenes Ziel (speziell bei IPv6 lassen sich Router Advertisements fälschen). Der DNS entscheidet welche SIP Server angesprochen werden (über die SRV Records). Dann gibt es noch Signalisierungsattacken, die Gespräche umleiten können.

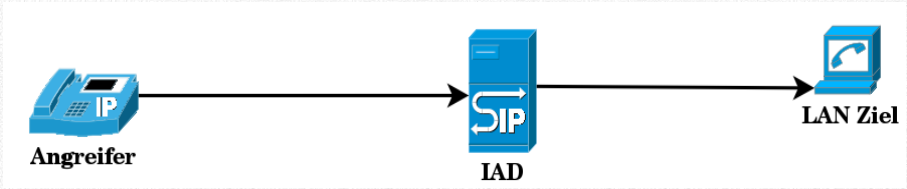
Die Signalisierung ist die wichtigste Komponente von VoIP. Durch die Vererbung von HTTP und E-Mail ergeben sich für SIP exakt dieselben Probleme zusätzlich zu den SIP-inherenten Möglichkeiten für Angreifer.

Alle Attacken beginnen ausnahmlos mit einer Aufklärung. Das schließt Portscans und Fingerprinting ein. Die Portscans auf Port 5060/UDP haben mittlerweile die Scans nach SSH Servern überholt. Der Hintergrund ist die Suche nach offenen PBX, UAs oder Proxies über die man dann Gesprächsguthaben verkaufen kann. Das Geschäftmodell ähnelt dem der eingangs vorgestellten VoIP Dienstleister.

SIP Source Routing

DEEPSEC

- SIP hält Zustand in der Nachricht
  - Entlasten des Netzwerk Cores
- Entspricht *Source Routing* bei IP
  - Sender gibt Weg vor
  - Requests/Responses in LANs schicken
  - Mediadaten in LANs schicken

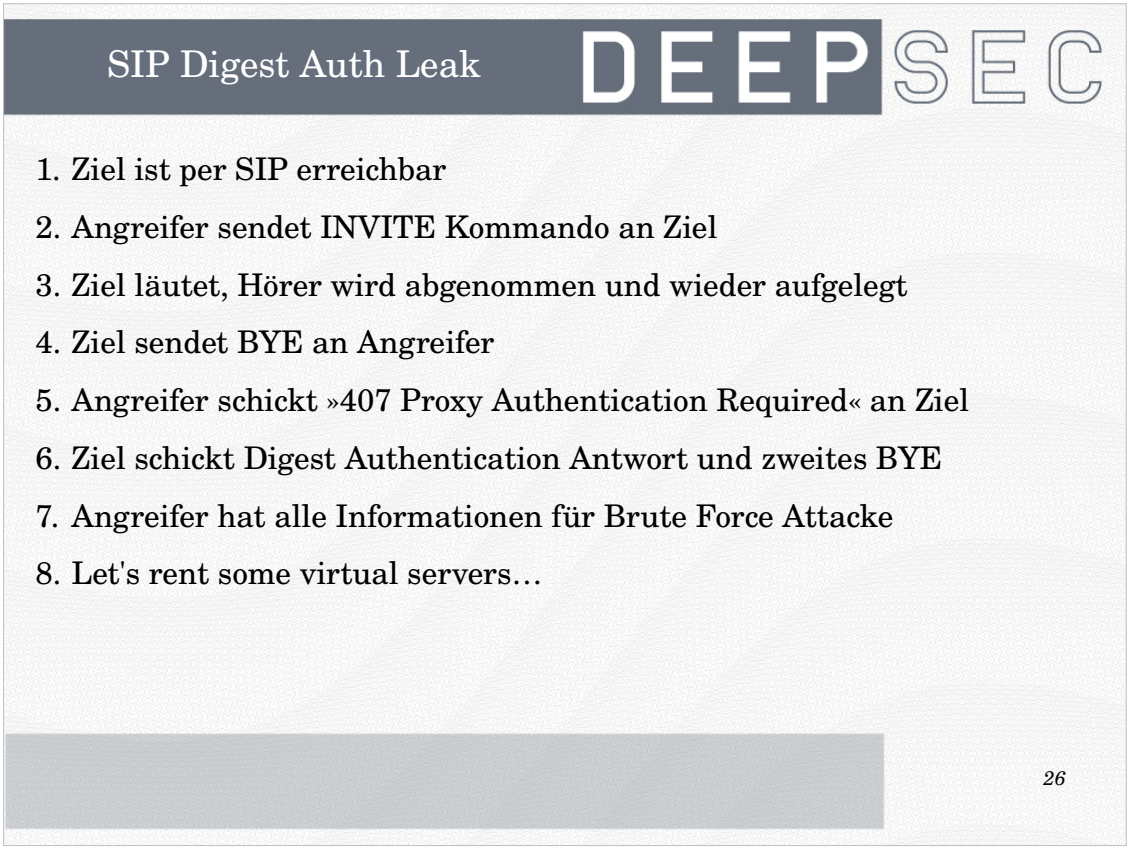


Source Routing sollte allen Netzwerkadministratoren ein Begriff sein. SIP benutzt es per Design, um den Netzwerk Core möglichst zustandsarm/-frei zu halten. Die Idee ist dadurch die Skalierbarkeit leichter zu machen. Dadurch entstehen allerdings Probleme, da der Sender eine SIP Nachricht bestimmen kann wohin diese Nachricht übertragen werden soll. Findet man SIP-fähige Gateways oder UAs, so kann man damit SIP Nachrichten in LANs schicken. Speziell die „kleinen“ SIP Appliances oder SOHO Geräte fragen da nicht viel nach oder überprüfen Anfragen.

Die SIP Authentisierung besteht aus HTTP Digest Authentication, welche Challenge-Response mit Nonces und MD5 Hashes einsetzt. SIP Server können von Client s eine solche Authentisierung einfordern, ganz analog wie es Webserver mit dem HTTP Code 401 tun.

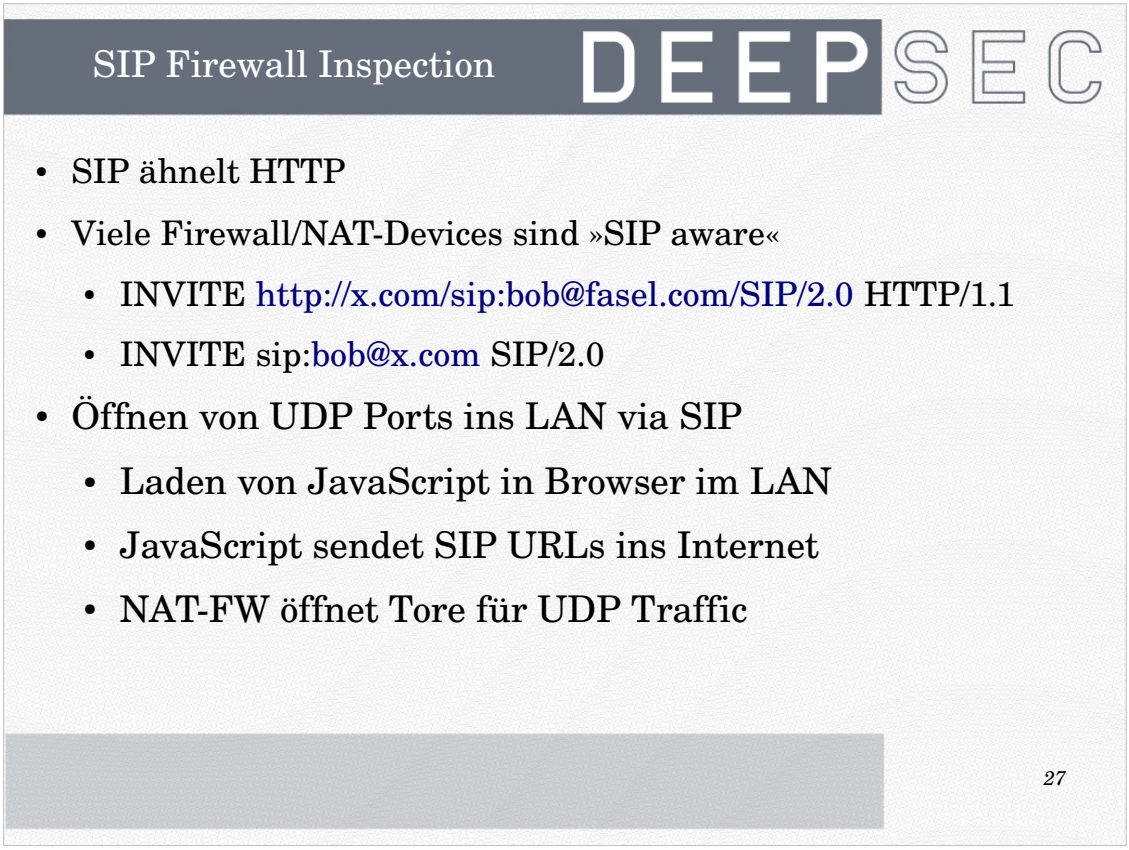
MD5 gehört zu den betagten Hash-Algorithmen, die nicht mehr verwendet werden sollten. Kollisionen sind bereits bekannt, und die zunehmende Performance von Servern erlaubt Brute Force Attacken. Ein Angreifer muß dazu nur zwei SIP Nachrichten abfangen.

Eine Autorisierung findet in SIP üblicherweise nicht statt.



Das SIP Digest Auth Leak wurde von Sandro Gauci zuerst beschrieben. Dabei nimmt man einen Gespächsaufbau zu einem UA auf. Dieser UA muß für Externe erreichbar sein (eine Telefonnummer bietet sich an). Nach erfolgreichem Gesprächsaufbau beendet man das Gespräch aber und fordert vom „gegnerischen“ UA eine Authentisierung. Da SIP UAs sowohl Client wie auch Server sind, besteht eine sehr hohe Chance auf eine Antwort mit MD5 Digest. Man hat damit alle Zutaten für eine Offline Brute Force Attacke.

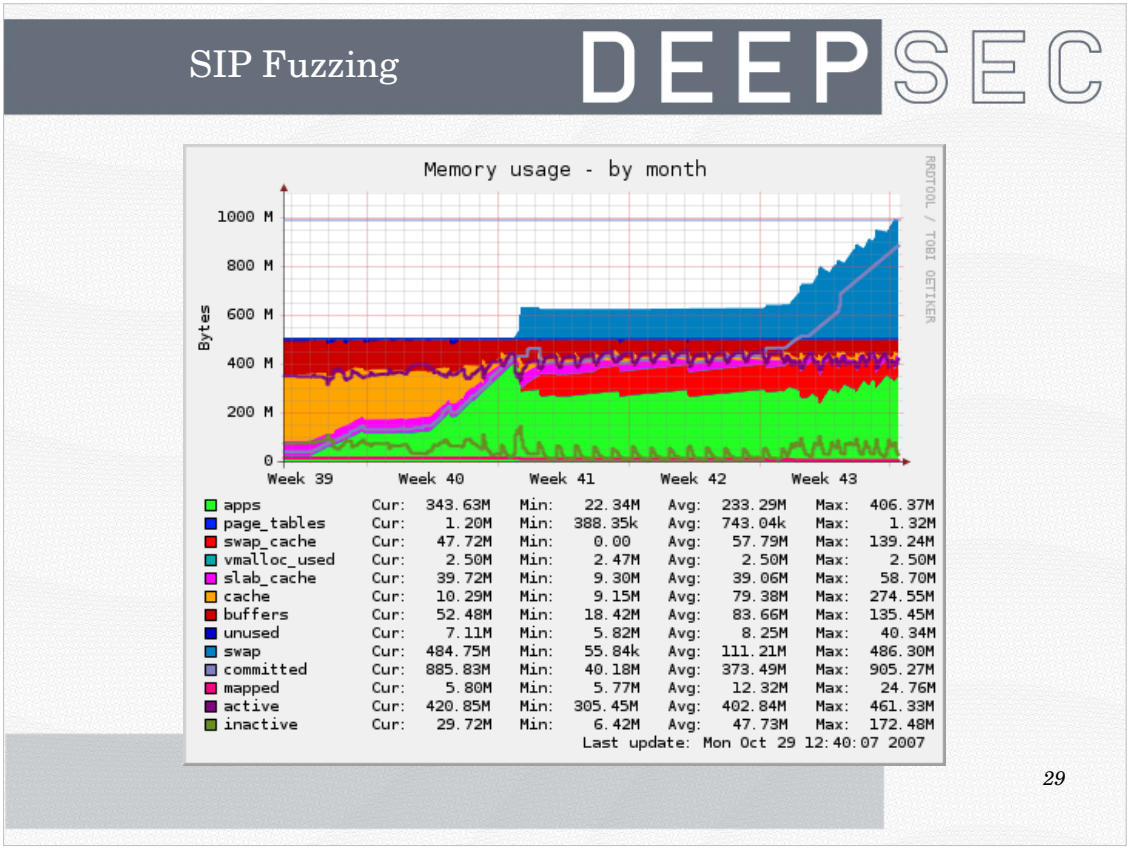
Laut Sandro Gauci sind ca. 60% aller UAs für eine solche Attack anfällig.



Firewalls und Proxies sind oft die erste Hürde für Angreifer. Manche Produkte beherrschen auch die Inspektion und das geregelte Durchleiten von SIP Nachrichten. Tatsächlich ergeben sich jedoch Schlupflöcher, die sich ausnutzen lassen, ganz speziell bei den vielen „Feld-, Wald- und Wiesenfirewalls“, die im Umlauf sind.
Angreifer können dadurch mittels SIP Nachrichten an Firewall-/NAT-Router unter Umständen ins LAN schauen und die Nachrichten dorthin schicken lassen. Man kann auch versuchen mittels JavaScript SIP-ähnliche URIs in HTTP Anfragen zu verpacken, um dann weitere Aktionen zu setzen.

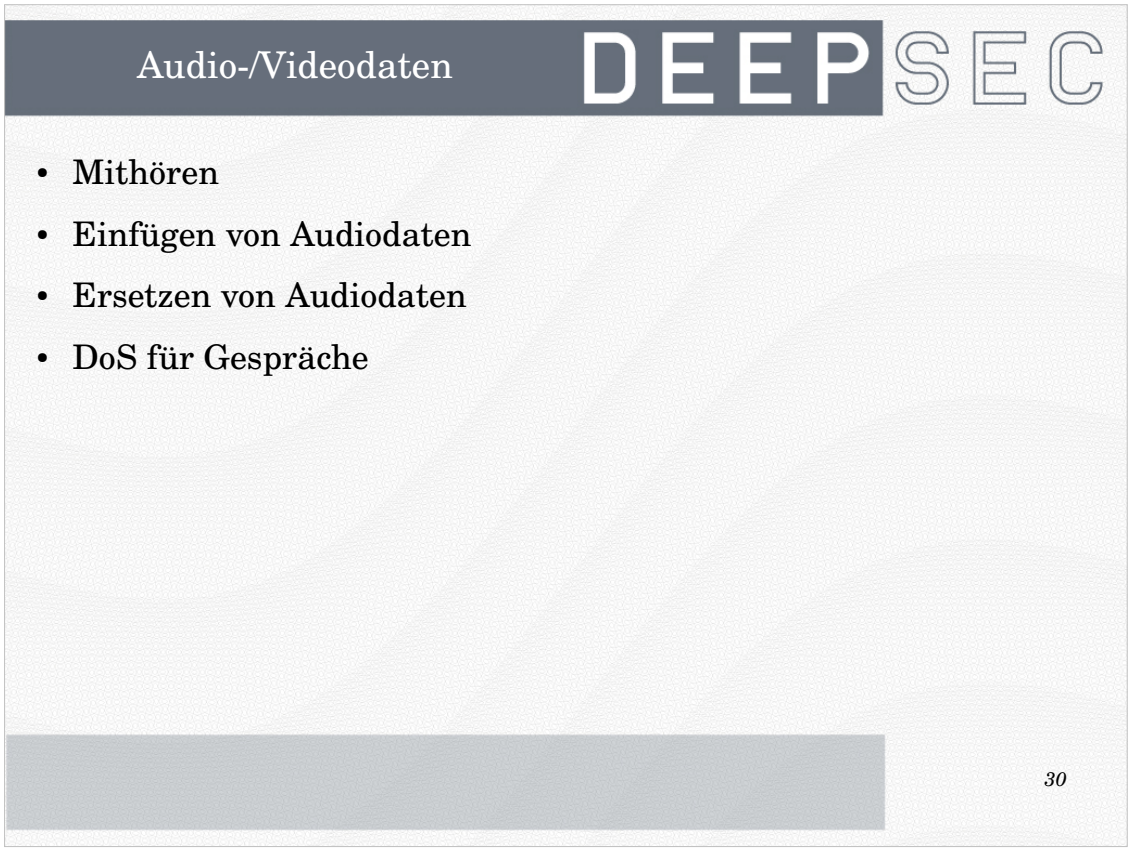
Protokolle werden nicht immer spezifikationsgemäß implementiert und können in ihrer Implementation, abgebildet in Software, Fehler enthalten. Es gibt Sicherheitsexperten, die mit den Implementationen Protokolltests durchführen. Die PROTOS Test Suites sind ein Beispiel dafür. Sie wurden gezielt für Protokolltests und die Analyse auf *data driven attacks* entwickelt. Die PROTOS Test Suit für SIP enthält gezielte SIP Nachrichten, die prüfen sollen, ob ein SIP Gerät mit den ungültigen Daten fertig werden.

Die PROTOS Suites kann man selbst herunterladen und einsetzen.



Man sieht hier die Speichernutzung eines GNU/Linux® Servers, der einen Asterisk™ Server beherbergt. Die blauen Flächen stellen verwendeten Auslagerungsplatz dar. Darunter befindet sich die Nutzung des physischen Speichers, farblich kodiert nach Zweck.

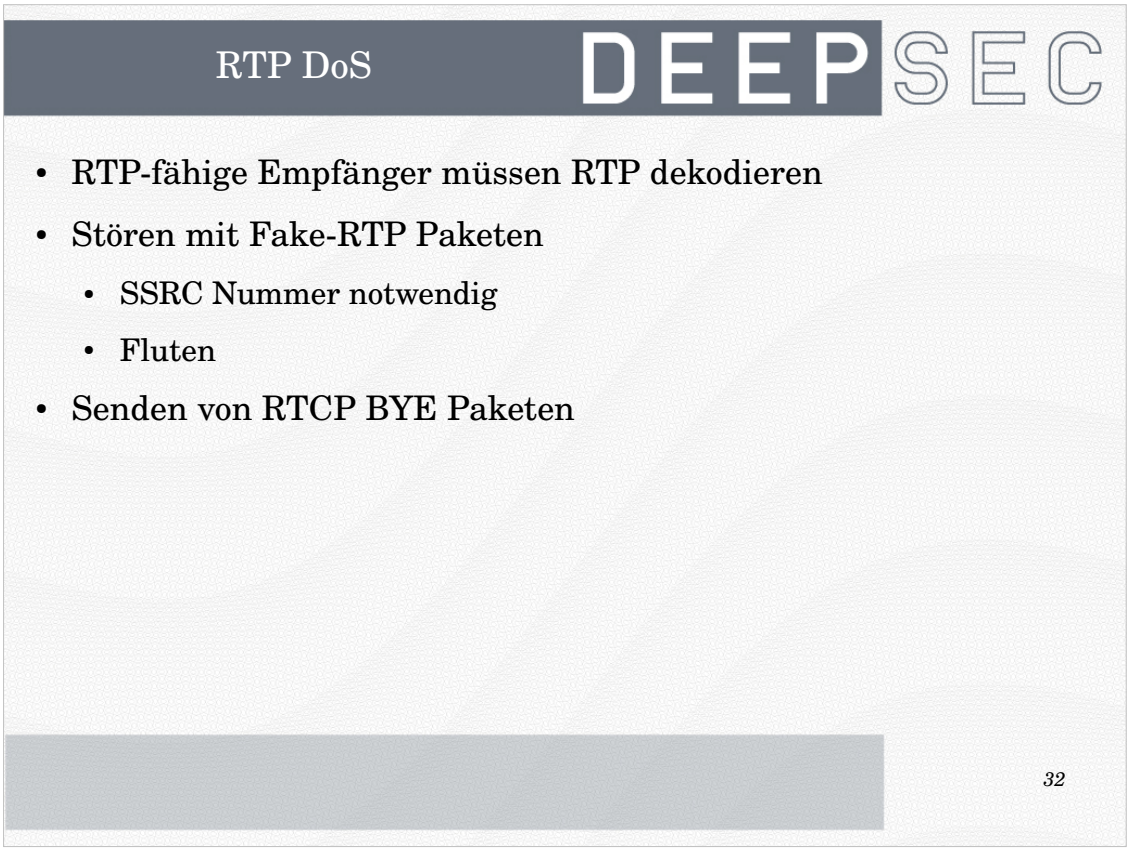
Der Server wurde einem PROTOS Test unterzogen. Monate später gab das System die Funktion aufgrund vollständiger Erschöpfung des physikalischen und virtuellen Speichers auf. Zwischen „Attacke“ und Auswirkung vergingen ca. 5 Wochen. Das entspricht einer verzögerten DoS Attacke ganz ohne Paketflut und Überlasten der Internetanbindung.



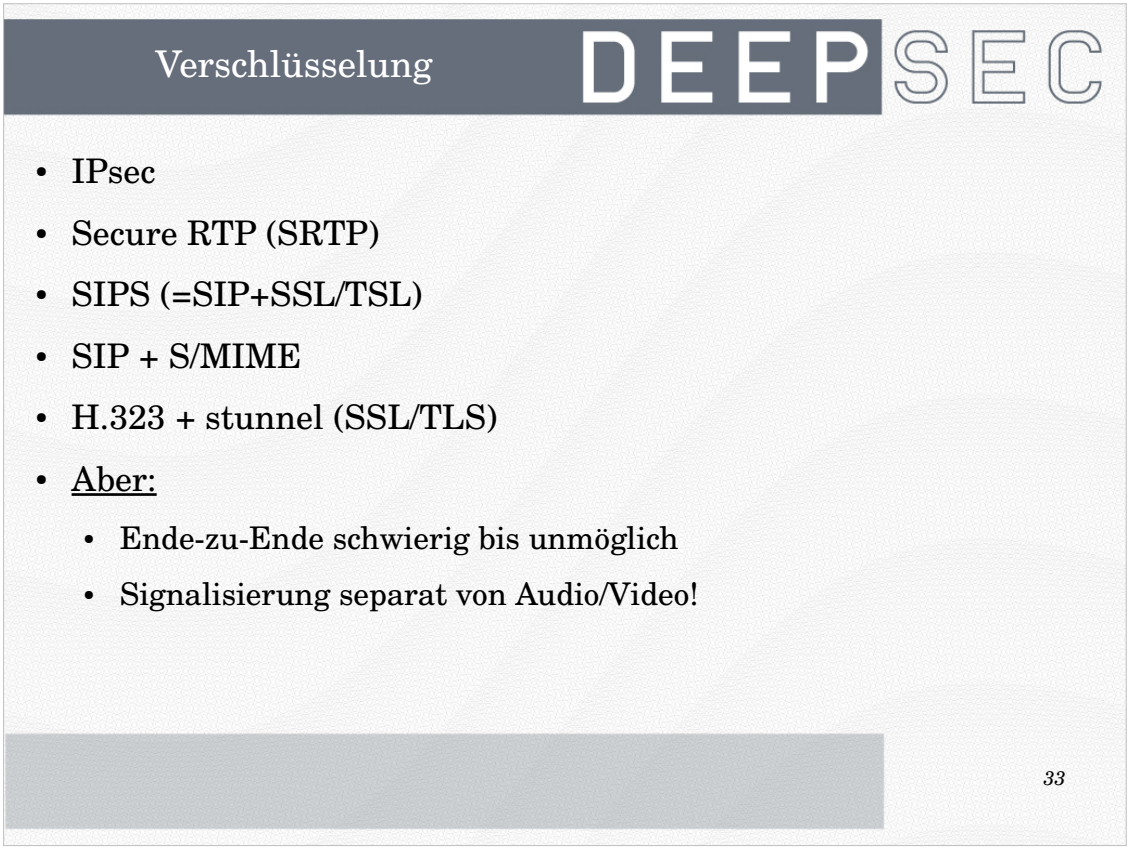
Die Audio-/Videodaten sind im Klartext und mit IDs sowie Sequenznummern versehen, d.h. jeder Mitschnitt kann leicht dekodiert werden. Durch Kenntnis der Charakeristika lassen sich auch Mediendaten ersetzen bzw. einfügen. Diese Attacken erfordern gutes Timing und Kenntnis der Session-IDs. Für das Einfügen von Mediendaten muß der Angreifer nicht in der Mitte sitzen, das läßt sich durch Verwendung gefälschter Pakete und passender Zeitstempel auch erledigen.

Mithören & Mitsprechen

- RTP Streams sind »Klartext«
- Streams haben IDs und Sequenznummern
  - Synchronization Source Identifier (SSRC)
  - Sequence Number
  - Timestamp
- Dekodieren sehr leicht
- Audioinjektion möglich
  - Verwendung gleicher IDs
  - Manipulieren der Timestamps



Das Real Time Control Protocol (RTCP) wurde bisher nicht ausführlich betrachtet. Es transportiert Status- und Statistiknachrichten, kann auch zum Beenden von RTP Streams verwendet werden.

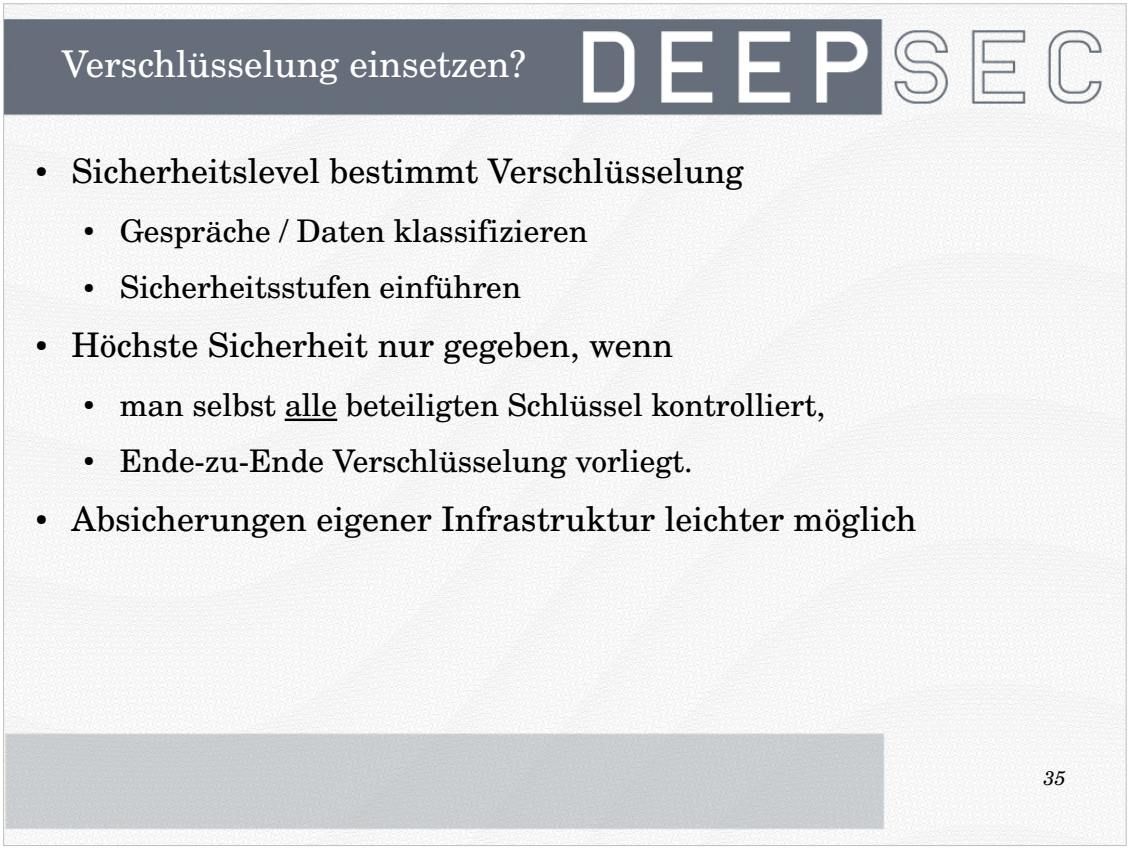


VoIP Transmission lassen sich mit bereits unter IP verfügbaren Mitteln absichern. Das Hauptproblem liegt, ähnlich wie bei verschlüsselten E-Mails, im Vertrauensverhältnis der Zertifikate/Schlüssel und in der Mischung der UAs. Dazu kommt noch, daß Signalisierung und Mediadaten getrennt abzusichern sind. SIPS nutzt wenig, wenn dann wieder RTP ohne Verschlüsselung vermittelt wird.

Ein großes Problem ist die Ende-zu-Ende-Verschlüsselung, die aufgrund der Vielfalt der Endgeräte nur in definierten Fällen möglich ist (z.B. VoIP UA zu VoIP UA, VoIP zu GSM/PSTN/… geht nicht ohne großen Aufwand oder spezielle Produkte).

ZRTP versucht die Eigenschaften von PGP auf VoIP zu übertragen. Man kann es mit bestehenden Signalisierungsprotokollen sowie Jingle (XMPP/Jabber Erweiterung) oder Distributed Hash Tables (DHT, verbreitet bei Bittorrent Clients) einsetzen. Es versucht mittels Codes, die vorgelesen werden müssen, ein Vertrauensverhältnis aufzubauen.

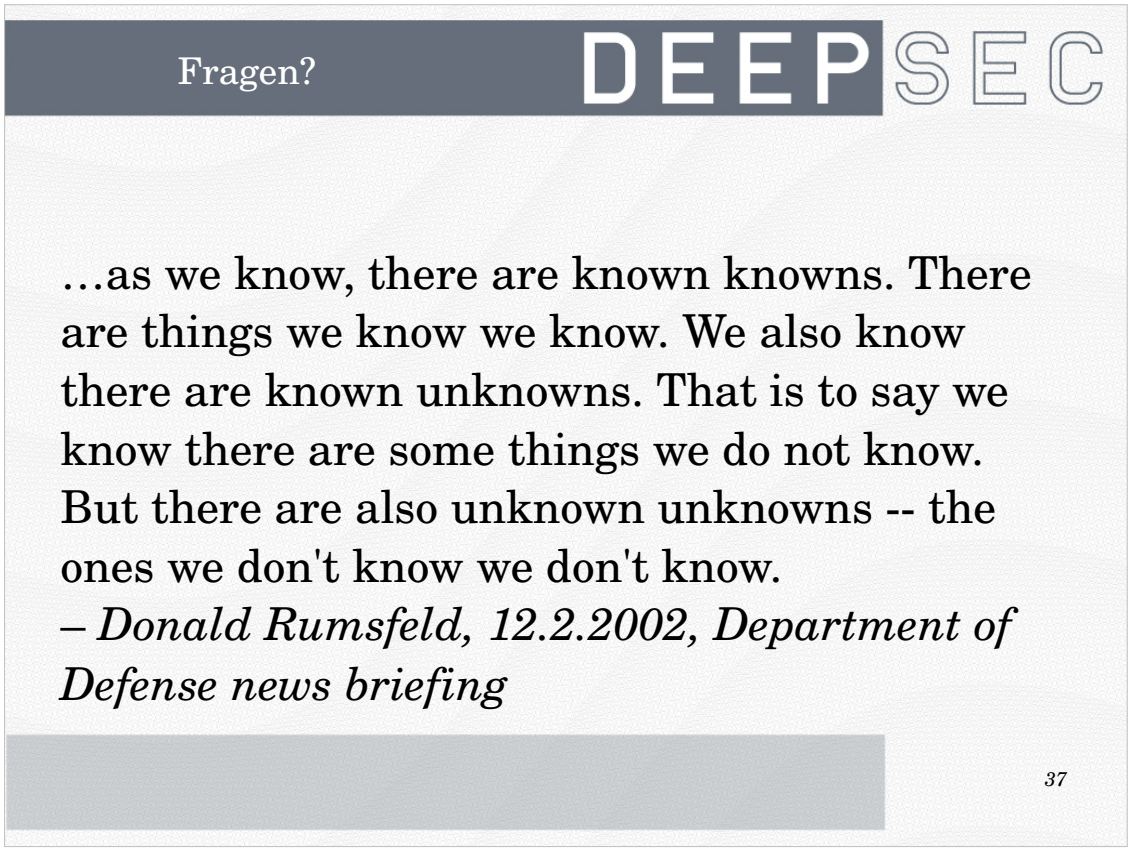
Für ZRTP gibt es eigene Clients und Plugins für bestehende PBX Systeme (wie z.B. Asterisk™).



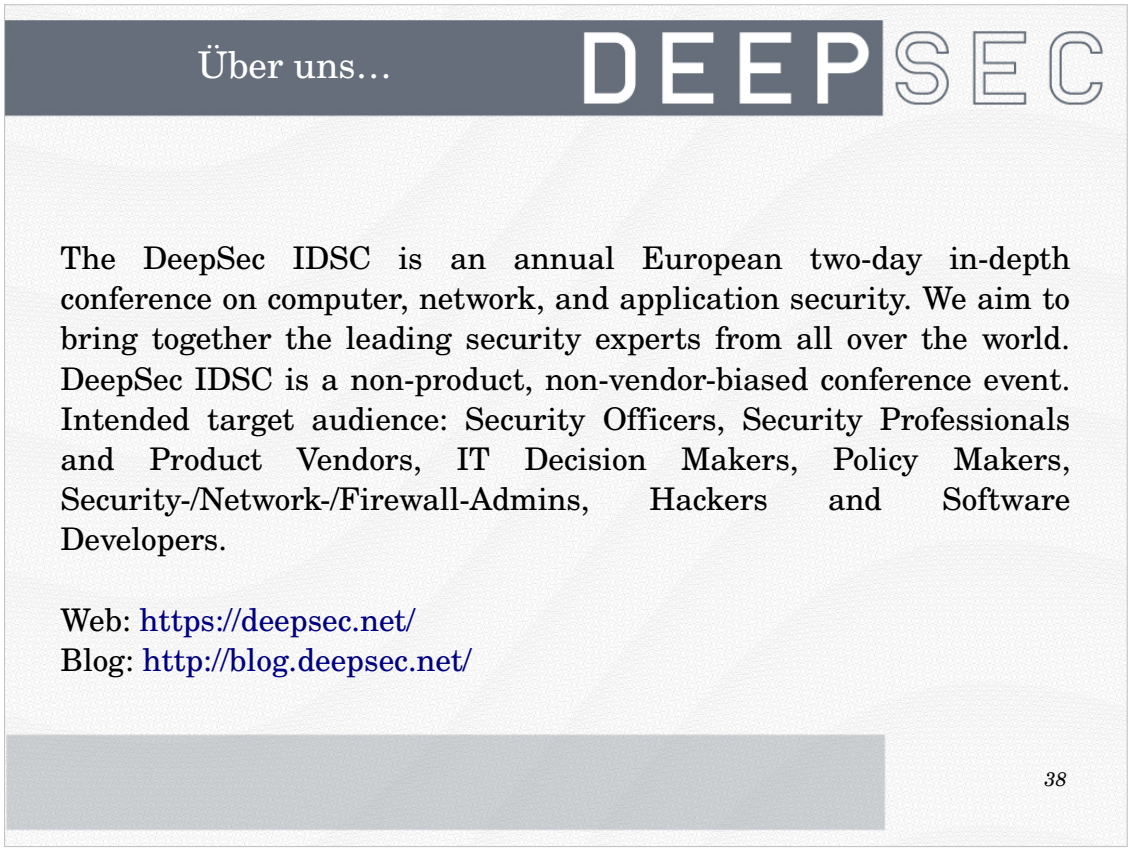
Wer auf die Forderung nach mehr Sicherheit nur „Verschlüsseln“ sagen kann, der/die hat die Probleme nicht verstanden. Verschlüsselung per se ist keine Lösung, die automatisch mehr Sicherheit bietet. Man muß betrachten welche Benutzergruppen über welche Wege kommunizieren müssen. Es ist immer einfacher die eigene Infrastruktur und geschlossene Gruppen zu verbinden. Die Probleme beginnen spätestens dann, wenn man mit dem Rest der Welt kommunizieren muß. Die Problematik ist bei VoIP daher exakt so wie bei Instant Messaging (IM) oder E-Mail.

Diese Liste ist unvollständig. Erster Schritt muß immer eine Analyse und Festlegung sein wer mit wem wie sicher kommunizieren muß. TANSTAAFL.

Zusätzlich darf man nie vergessen ständig die Sicherheitsmaßnahmen zu überprüfen. Insbesondere die schlechten Erfahrungen mit Protokolltests und Scans bzw. Verhalten unter Last und absichtlichen falschen Signalisierungsnachrichten zeigen, daß UAs und eingesetzte Software so ausgiebig wie möglich getestet werden muß bevor sie in Produktion geht – ganz analog zu den anderen Bereich der IKT.

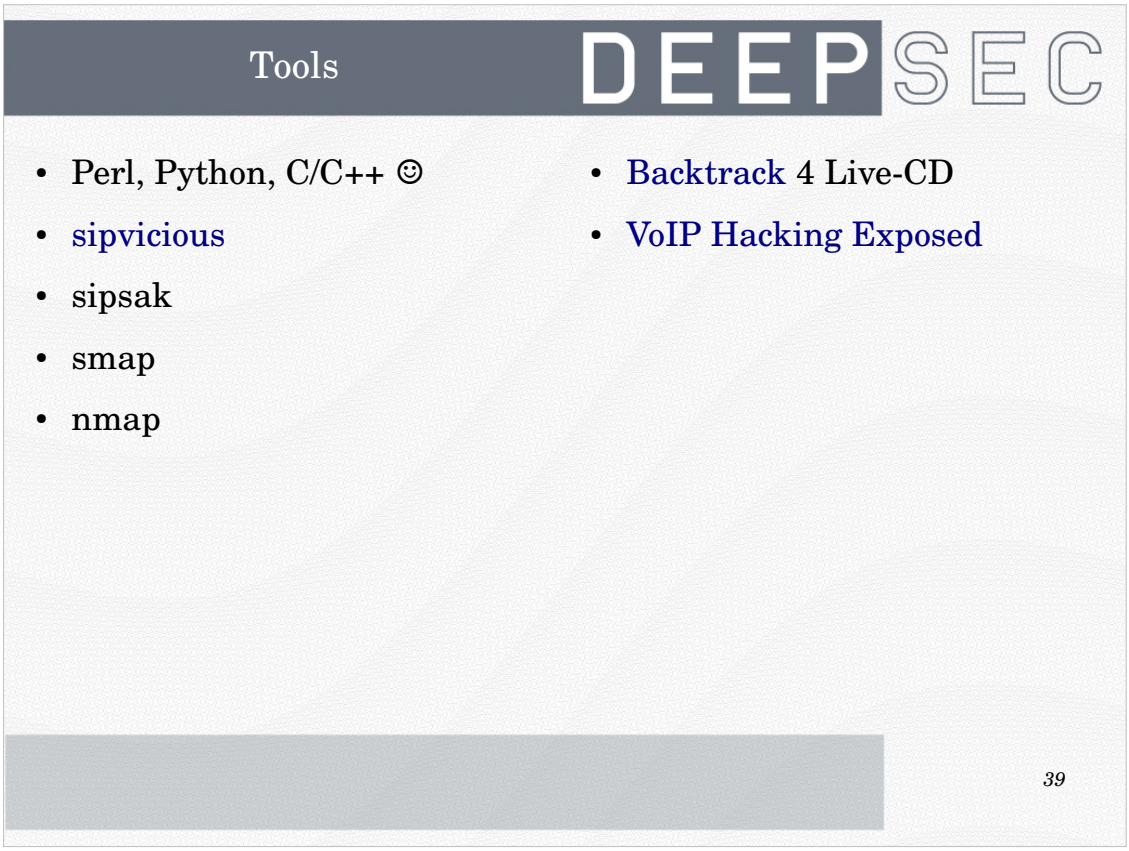


Herr Rumsfeld macht deutlich wie wichtig das ständige Hinterfragen von vermeintlichen Tatsachen und Fakten ist, auch wenn das Zitate aus einem anderen Kontext stammt.



Wir freuen uns über jegliches Feedback, Kommentare im Blog, interessierte Sponsoren für die jährliche DeepSec Konferenz, Teilnehmer, Anregungen für Sicherheitsthemen, eigene Erfahrungen und sonstigen regen Austausch. Wir bieten bei Anrufen keine sichere Kommunikation, man kann uns aber verschlüsselt Nachrichten via E-Mail oder Webseite zukommen lassen.

Danke für Ihre Aufmerksamkeit!



Hier sind einige Tools vorgestellt, die man verwenden kann und die von uns verwendet wurden. Wie überall im Bereich Sicherheit gilt: Wenn es keine Tools gibt, so schreibt man sich welche. Die Protokolle sind meist offen, Standards lassen sich nachlesen, ansonsten bemüht man Sniffer und etwas Reverse Engineering. (Ja, es gibt keine Abkürzungen, weder für Angreifer noch für Verteidiger.)