Vertrauliches Telefonieren durchs VPN

ifKom NW Jahrestagung 2007

Johannes Hubertz

hubertz-it-consulting GmbH

Düsseldorf, 14. November 2007

Gliederung

Vorstellung

Telefon – altbekannt, vertrauenswürdig

VoIP – neu und weniger vertrauenswürdig

H.323 – SIPv2 (RFC 3261)

SRTP – RFC 3711

VPN – kann man Virtuellem vertrauen?

IPsec – PKI und StrongSwan

OpenVPN – PKI und libssl

Angriffsmethoden

Zusammenfassung – Diskussion

Vorstellung: Johannes Hubertz

1973 Studium der Elektrotechnik in Aachen

1980 Honyewell Bull, Ersatzteilreparatur

1984 Entwicklung Sonderprodukte, Assembler, PLM

1994 Erstkontakt mit IP

1996 Xlink, root@www.bundestag.de, ...

1999 IT-Security Mgr. D-A-CH der Bull AG

2002 Entwicklung sspe für Steria GmbH

2005 Gründung der hubertz-it-consulting GmbH

...Weiterentwicklung und Betrieb von sspe

seit 1973 Bundesanstalt Technisches Hilfswerk in Köln-Porz

seit 2001 Segeln, am liebsten auf Salzwasser

Vorstellung: hubertz-it-consulting GmbH

Erkenntnisse aus dem Berufsleben

Bellovin and Cheswick: Firewalls and Internet Security, 1994

Fazit: Keep it simple!

Oder mit Einstein: So einfach wie möglich, aber nicht einfacher!

Etwas Erfahrung war Voraussetzung

Gründung am 8. August 2005, Sitz in Köln

Geschäftsinhalt: Dienstleistungen im Umfeld der IT-Sicherheit

Schwerpunkte: Netzwerk, Switches, Router, VPNs, Firewalls, Hochverfügbarkeit, X.509, Betrieb, Schulung, freie Software ...

Logo: Johannes Hubertz Certificate Authority als ASCII-7Bitmuster

Mitgliedschaft bei ECO e.V., guug e.V. und Kooperation mit der Bull GmbH

Wir sind käuflich ;-)

Aus der guten alten Zeit . . .

Kennen Sie das noch?

Die Post . . .

Das Fräulein vom Amt

Das Post- und Fernmeldegeheimnis Mit Freiheitsstrafe bis zu . . .

Der Staat – Garant vertraulicher Kommunikation

Leitungsvermittelte Ende-zu-Ende-Verbindung

Verfügbarkeiten weit jenseits von 99 Prozent

VSt mit eigener Stromversorgung, Batterien, K-Schalter, . . .

VoIP: Voice over Internet Protocol

Voice

Datenrate mindestens 8 kBit/s, besser 64 kBit/s
Latenzen ab 100 ms spürbar unangenehm

Internet Protocol, RFC 791

Paketorientiert – nur kleine Datenmengen zu einer Zeit
Verbindungslos – dynamische Routen
keine Sicherheit – in jeder Hinsicht

VoIP – Verfahren

- Unstandardisierte Verfahren

  Cisco Skinny
  Yahoo/Microsoft/ICQ/AOL Instant messengers (IM)
  Skype
  Google TALK (benutzt XMPP RFCs aus der Jabber Welt)

- Standardisierte Verfahren

  ITU International Telecommunication Union
  International organisation within the United Nations System
  governments and private sectors coordinate global telekom and services
  H.323 (V1) seit Mai 1997 (ITU-T)
  basiert auf H.320 Konzepten, H.225.0 (RAS & Q.931), H.245
  IETF Internet Engineering Task Force, open to any interested individual
  SIP – RFC 3261 ff., Juli 2002 seit 22. Feb. 1996 (draft-ietf-mmusic-sip00)
  basiert auf HTTP und SMTP Konzepten,
  benutzt SDP (Session Description Protocol, RFC 3264)

VoIP – unstandardisierte Verfahren

digma: Sichere Internet-Telefonie (VoIP)?

Frage: Welche Sicherheitsrisiken gehe ich beim Telefonieren mit Skype ein?

A.Steffen: Der proprietäre Skype Client, dessen Software bisher nur bruchstückhaft analysiert worden ist, hat zwar vorbildlich eine Peer-to-Peer Verschlüsselung, sowie eine zentralisierte Benutzerauthentisierung realisiert, dass selbst die Strafverfolgungsbehörden keine Möglichkeit sehen, Skype-Gespräche abzuhören. Aber wer weiss, ob die Skype-Besitzerin Ebay gewisse Masterschlüssel nicht schon an den Meistbietenden versteigert hat?

digma: Zeitschrift für Datenrecht und Informationssicherheit,
6.Jahrgang, Heft 3, September 2006, Seite 138ff.

VoIP – unstandardisierte Verfahren, Teil 2

A.Kerkhoff (1883)

Die Geheimhaltung der Algorithmen soll **nichts,** die Geheimhaltung der Schlüssel jedoch alles zur Sicherheit beitragen

Ingenieurskunst?

Kommerzielle Verschlüsselungsgeräte enthalten Hintertüren, (un)absichtlich eingebaut durch Hersteller und/oder andere. Reverse Engineering ermöglicht, aus den Geräten einen Quelltext zu rekonstruieren, um zielgerichtet Hintertüren zu finden und anschließend missbrauchen zu können. Kommerzielle Werkzeuge (Softwaredebugger, Logikanalysatoren etc.) sind am Markt, eine einfache Gewinn- und Verlustrechnung lässt die Rendite vorab schätzen ...
(Ortsabhängige Legalität beachten!)

Moderne Kryptographie

Je mehr Augen den Quellcode einsehen können, umso weniger Hintertüren bleiben unentdeckt. Quelloffenheit $\Longleftrightarrow$ überprüfbare Sicherheit $\Longleftrightarrow$ Vertrauen

VoIP – standardisierte Verfahren

H.323 V1,V2 Feb.1998	H.245 über TCP Q.931 über TCP RAS über UDP
H.323 V3,V4,V5 Nov.2000 Jul.2003	H.245 über UDP/TCP Q.931 über UDP/TCP RAS über UDP
SIP V1,V2 Jul.2002	UDP und TCP meist nur UDP

VoIP – Handelnde Personen

Alice

Bob

Provider

VoIP – beteiligte Geräte

Softphone

SIP-Phone

SIP-Proxies

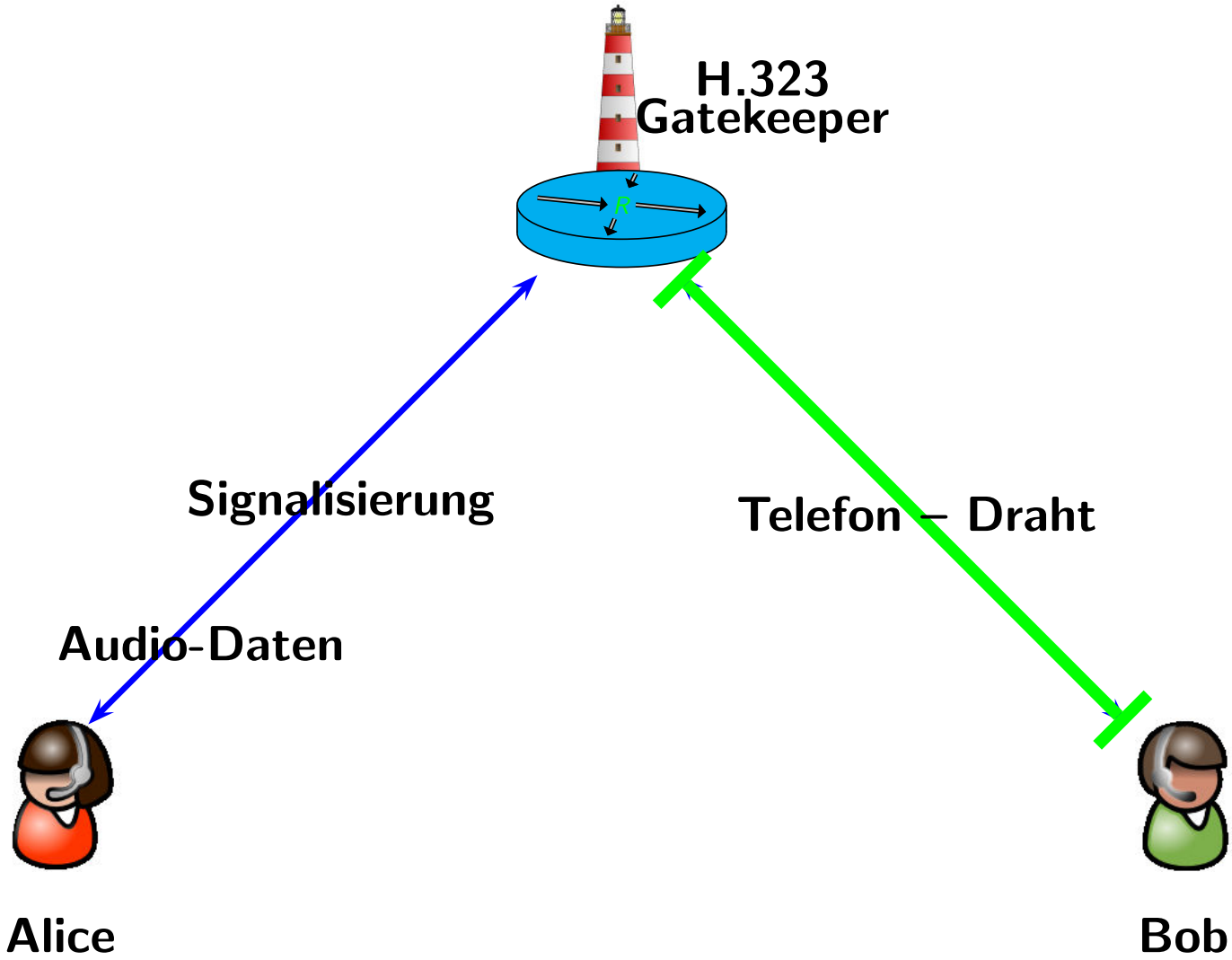
eigene Router, Switches

Firewalls, VPN-Devices

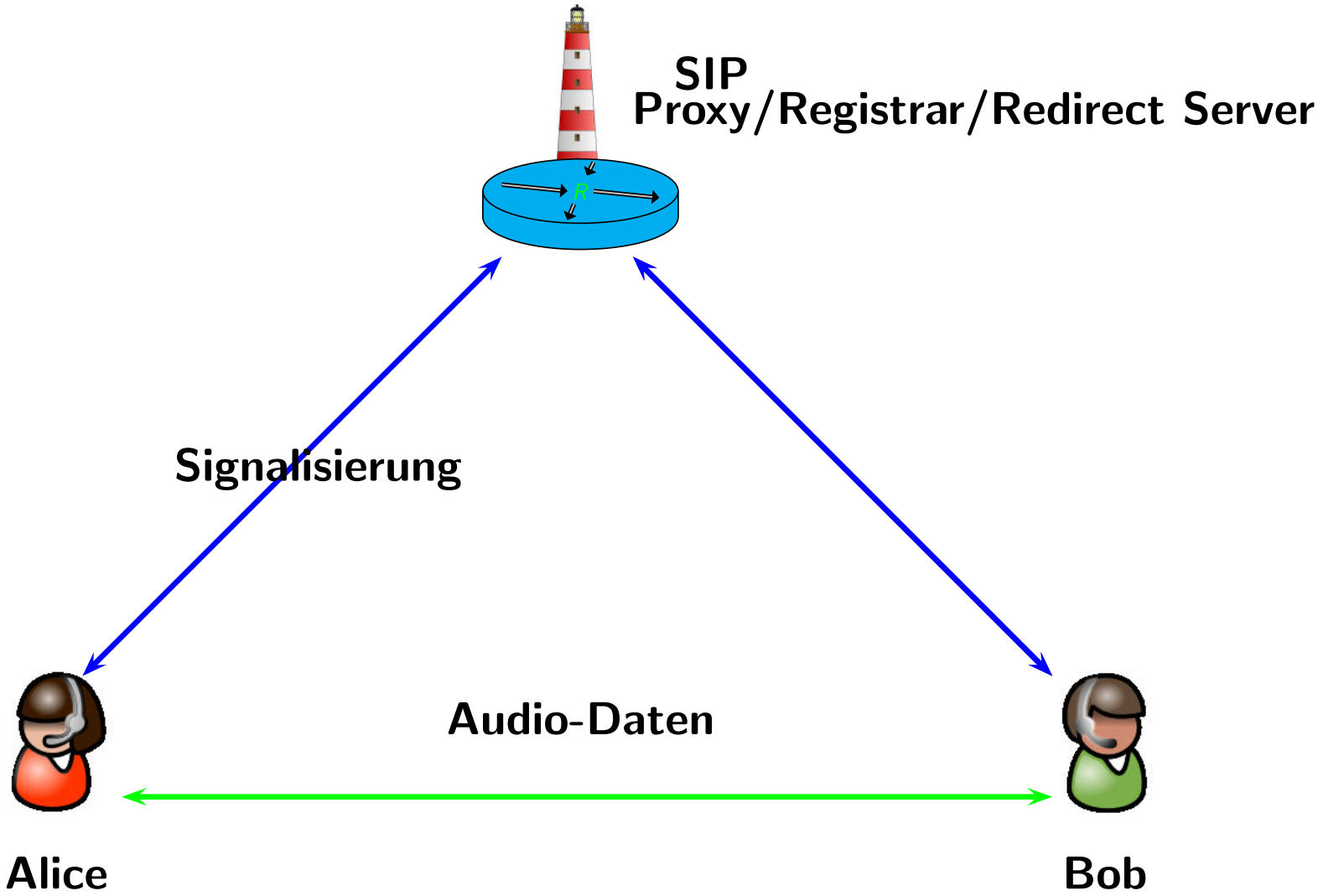
ISP-Router

Telefonanlagen

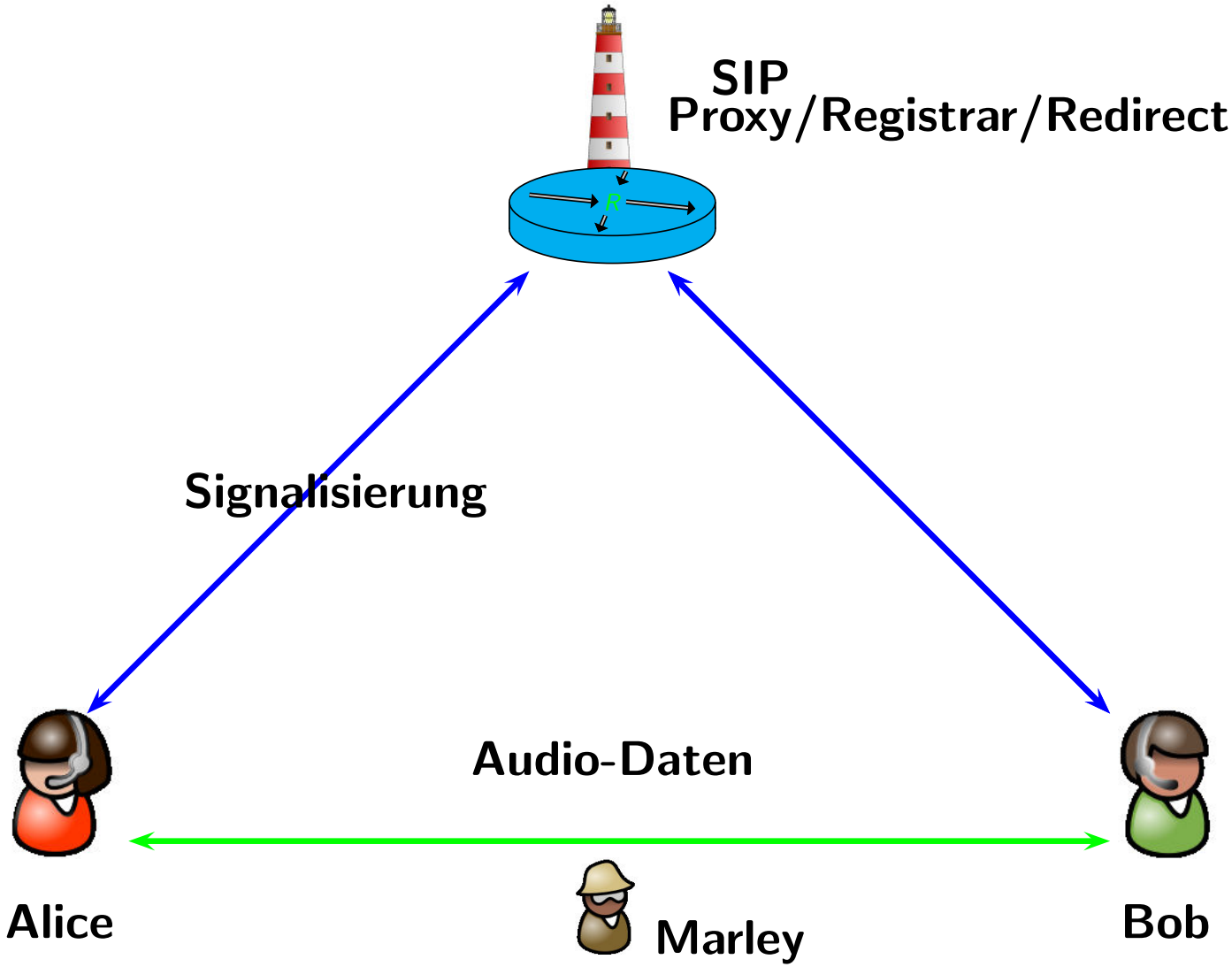
VoIP – how ITU likes it



VoIP – how it works



VoIP – how it works



Marley: „man in the middle“ und seine Werkzeuge

Netzwerkeinbruch ist sein Geschäft

Brecheisen und Dietrich sind nicht mehr gefragt

Arbeitszelte und Straßeneinstiege bleiben ungenutzt

Einbruch geschieht meist völlig unbemerkt

Standardmethoden (Virenscanner) sind wirkungslos

Umleitung des Datenstroms um Lauschangriff zu ermöglichen

Hilfsmittel: Bundes- oder andere Trojaner, Individualsoftware

Audio-Software, ettercap, tcpdump, wireshark, ...

Legalität klärt die jeweilige örtlich zuständige Behörde

Wo ist Marley?

In den unendlichen Weiten des Internet ...

Die IETF bietet Hilfestellung

SRTP – VoIP mit etwas Vertraulichkeit

März 2004: RFC 3711 – Secure Real-Time Protocol

AES Counter Mode, 128 bit keys

kein Transport-overhead $\Longrightarrow$ gleicher Bandbreitenbedarf

kein Schlüsselaustausch enthalten

MIKEY ist in RFC 3830 seit August 2004 beschrieben

kommerzielle Geräte bald am Markt?

kommerzielle Geräte $\Longrightarrow$ Hintertüren, Schlüsselhinterlegung, ...

Hintertüren hatten wir schon

PS: Paranoid zu sein bedeutet nicht, dass keiner hinter einem her wäre.

Virtual Private Network

Virtual – virtuelles Netz, also kein reales, physikalisches Netzwerk

Private – privates, verschlüsseltes Netz, im Gegensatz zum Öffentlichen

VPN – zusätzliches Netzwerk auf bestehendem, zumeist dem Internet

VPN – Hersteller-Konsortium schuf FreeSwan – Referenz für IPsec auf IPv4

VPN – bewährte und verfügbare Technologien: IPsec-, SSL-, Obscure-VPNs

FreeSwan – kompatibel zu (fast) allen kommerziellen VPN-Lösungen

FreeSwan – beendet, StrongSwan ist Nachfolge-Projekt aus der Schweiz

StrongSwan – starke Authentisierung mit z.B. 2048 bit RSA-Keys (X.509)

VPN – Mechanismen

normale IP-Pakete werden verschlüsselt

vorangestellter zusätzlicher Header erlaubt normalen Versand

Empfang: zusätzlicher Header nach Plausibilitätsprüfung entfernt

Das IP-Paket wird entschlüsselt und an seine Ziel-IP zugestellt

Transparent für den Endanwender, Sicherheit hängt an vielen Faktoren

RFC4303 IP Encapsulation Payload (ESP)

RFC4305 Cryptographic Algorithm Implementation Requirements for ESP

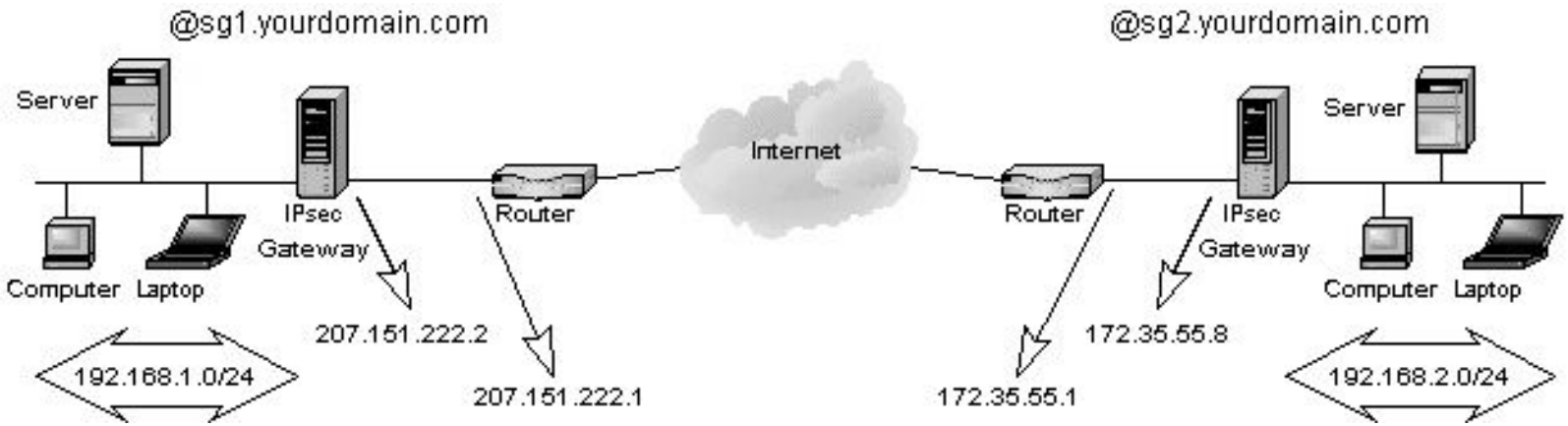
Schlüssel müssen auf vertraulichem Wege ausgetauscht werden

Schlüssel müssen regelmässig gewechselt werden

RFC4306 Internet Key Exchange (IKEv2) Protocol

RFC4307 Cryptographic Algorithms for Use in the IKEv2

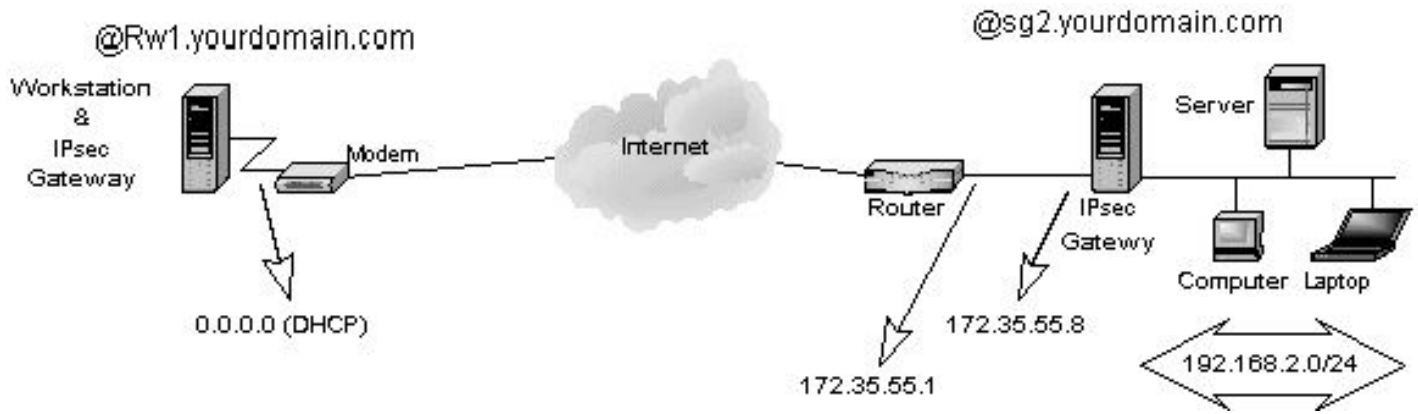
VPN – Beispiel



Eine Firma mit zwei Standorten vernetzen . . .

Bild von http://jixen.tripod.com

VPN – Beispiel

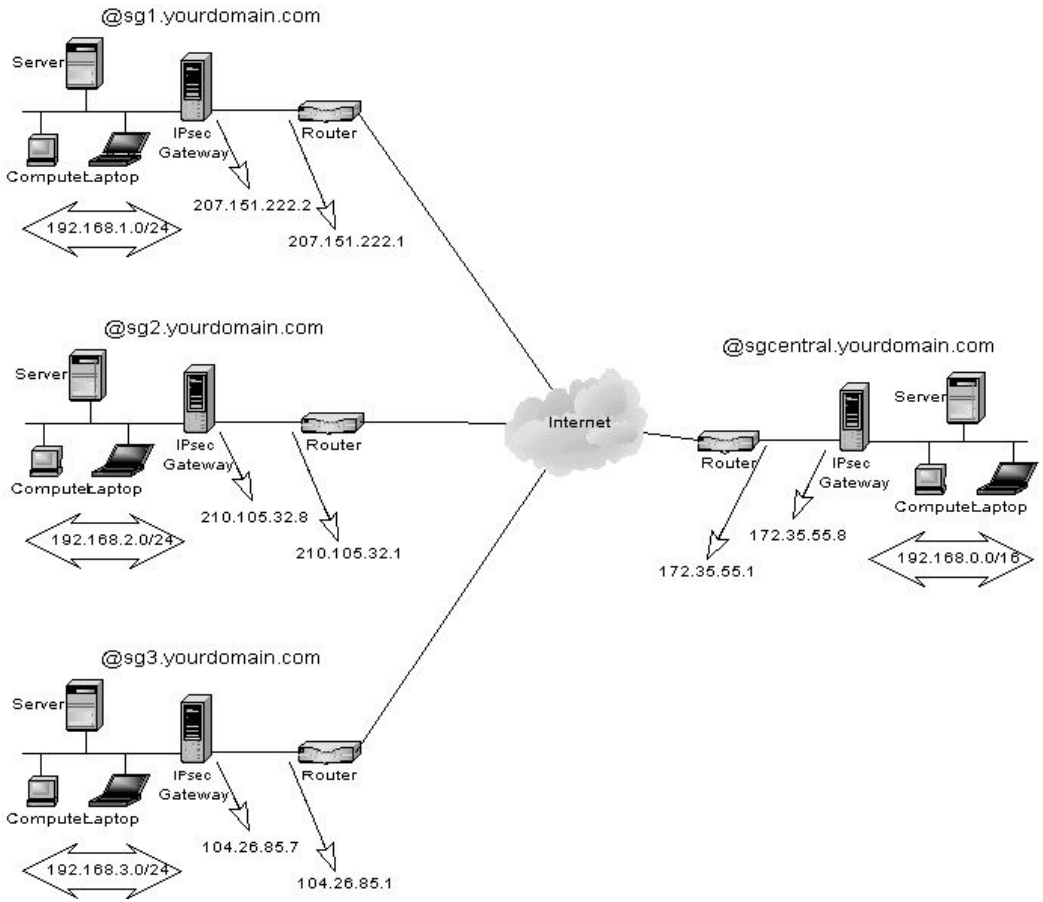


Einen Außendienstler mit der Zentrale verbinden . . .

Bild von http://jixen.tripod.com

VPN – Beispiel

beliebig viele Standorte verbinden,



voll-vermascht, teil-vermascht, sternförmig, wie Sie wollen . . .

Bild von http://jixen.tripod.com

VPN – aktuelle Software

http://www.strongswan.org	http://www.openvpn.net
	
IPsec	SSL-VPN
RFC-konform	RFC-konform
Hersteller-kompatibel	nicht Hersteller-kompatibel
UDP, ESP, NAT	UDP, TCP, NAT
Passworte, X.509	X.509
Verschlüsselung im Kernel	Verschlüsselung im Userland

neue Produkte, neue Kryptographie, mehr Sicherheit?

Bruce Schneier, amerikanischer Krypto-Experte, in „Secrets and Lies“:

Jeder, der eine eigene kryptographische Grundfunktion erstellt, ist entweder ein Genie oder ein Narr. Angesichts des Genie/Narr-Verhältnisses stehen die Chancen nicht gut.

ISBN 3-89864-302-6, S.110

Kein Bedarf für Neues

- OpenVPN und StrongSwan skalieren ausgezeichnet.
- Vertraulichkeit skaliert deutlich schlechter. ;-)
- Moderne Hardware und KnowHow schaffen vertrauliche Umgebungen

IPsec-VPN – vertrauenswürdige Transportmethode

Linux ab Kernel 2.4

FreeSwan-Patch, X.509-Patch für FreeSwan-Patch, später StrongSwan-Patch
Ab StrongSwan 4.0 auch IKEv2, kompatibel zu kommerziellen IPsec-Produkten
Kann mit X.509-Zertifikaten umgehen, eine PKI kann genutzt werden.

Kommerzielle IPsec-Implementierungen

Teuer, untereinander nicht immer kompatibel,
Mißtrauen ist spätestens dann angesagt, wenn der Administrator etwas einstellt und das Gerät anderes mit der Gegenseite aushandelt.

OpenVPN – auch vertrauenswürdig

Linux, M$-Windows

OpenVPN erledigt die Verschlüsselung als Anwender-Prozess, plattformunabhängig mit OpenSSL bzw. libssl. Stellt wie auch IPsec eine Route in einen Tunnel bereit. Benötigt X.509-Zertifikate, eine vorhandene PKI kann genutzt werden.

Kommerzielle SSL-VPN-Devices

Meist kostengünstiger als IPsec-VPN-Geräte.
Untereinander nicht kompatible SSL-VPN Lösungen sind am Markt, Zertifikatshandhabung nicht immer zukunftsweisend ...

Verschlüsselungs-Funktionen

OpenSSL wird im Internet gewartet und regelmässig gepflegt. StrongSwan ebenso. In beiden Implementierungen können Fehler vorhanden sein, die jedoch bei Bekanntwerden bisher stets kurzfristig behoben wurden.

Anriffsszenarien gegen VPN-Telefonie

Was kann Marley dagegen noch tun?

DoS und dDoS geht immer

Telefonieren mit Nebengeräuschen verdeckt Stimmidentität

Lauschen im Voice-Datenstrom ist nicht unmöglich, Marley hat Werkzeuge

Lauschen im Client-PC setzt Rootkit auf dem PC voraus (Bundestrojaner?)

Social Engineering kann bei Implementierung sehr hilfreich sein

VoIP via VPN – Schlussfolgerungen

Telefonieren Sie unbesorgt im Festnetz, Internet oder Mobil via VoIP vom Softphone

Vertrauliche Inhalte jedoch ausschliesslich über VPNs

Vertrauliche VPNs funktionieren nur mit vertraulichen Systemen

Vertrauliche Systeme funktionieren mit offengelegten Quelltexten

Offengelegte Quelltexte können sichere, vertrauenswürdige Systeme bilden

Sicherheit des Gesamtsystems ist nur so gut wie die des schwächsten Gliedes

Bruce Schneier: Sicherheit ist ein Prozess

Keep it simple!

Quellen

Guido Schuster, I. f. Kommunikationssysteme, Hochschule für Technik Rapperswil, Voice over IP und Internet-Telephonie, Folien VoIP 30.8.05

Andreas Steffen, Sichere Internet-Telefonie? entnommen aus: digma, Zeitschrift für Datenrecht und Informationssicherheit, 6.Jahrgang, Heft 3, September 2006, Seite 138ff.

Bruce Schneier, Secrets and Lies, Heidelberg: dPunkt.verlag GmbH, ©2004

http://ietf.org/rfc/rfc.3261.txt – SIP

http://ietf.org/rfc/rfc.3711.txt – SRTP

http://ietf.org/rfc/rfc.3550.txt – RTP

http://ietf.org/rfc/rfc.3830.txt – MIKEY

http://strongswan.org/ – StrongSwan, Andreas Steffen

http://www.openvpn.net/ – OpenVPN Homepage und Wiki

Ich bedanke mich für Ihre Aufmerksamkeit

hubertz-it-consulting GmbH jederzeit zu Ihren Diensten

Ihre Sicherheit ist uns wichtig!

Frohes Schaffen

Johannes Hubertz

`it-consulting _at_ hubertz dot de`

powered by LaTeX 2ε
and PSTricks