Verschlüsselte Internet-Telefonie mit OSTN

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Chemnitzer Linux-Tage 2015



Über Mich



Über Mich

- Bildungswissenschaft/Psychologie
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Geek, Nerd, Hacker seit knapp 20 Jahren
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`



Forschungsprogramme des MIS

- Psychologie der Sicherheit
  - Social Engineering
  - Security Awareness, Sicherheit in Organisationen
  - Didaktik der Sicherheit
  - Didaktik der Kryptographie
- Lehrerfortbildung
  - Lernfelder: Fachinformatiker IT-Sicherheit
  - Lernfelder: IT-Sicherheit für Kaufleute
  - Lernfelder: IT-Sicherheit für Elektroberufe
- IT-Sicherheit in KMU
  - empirische Grundlagenforschung
  - didaktische Aufbereitung
  - Schulungen



Schulungs- und Beratungsangebote

- Sicher unterwegs im Internet
- Anonymität und Überwachung im Internet
- Security Awareness Kampagnen konzipieren
- Netzwerke absichern/Penetration Testing
- Die psychologischen Grundlagen des Social Engineerings
- Der digitale Untergrund: zur aktuellen Bedrohungslage im Internet
- Kryptographie - Konzepte, Methoden und Anwendungen
- Strategien im Wirtschaftskrieg
- Selbstschutz in Krisengebieten



Informationstechnologie und Sicherheitspolitik

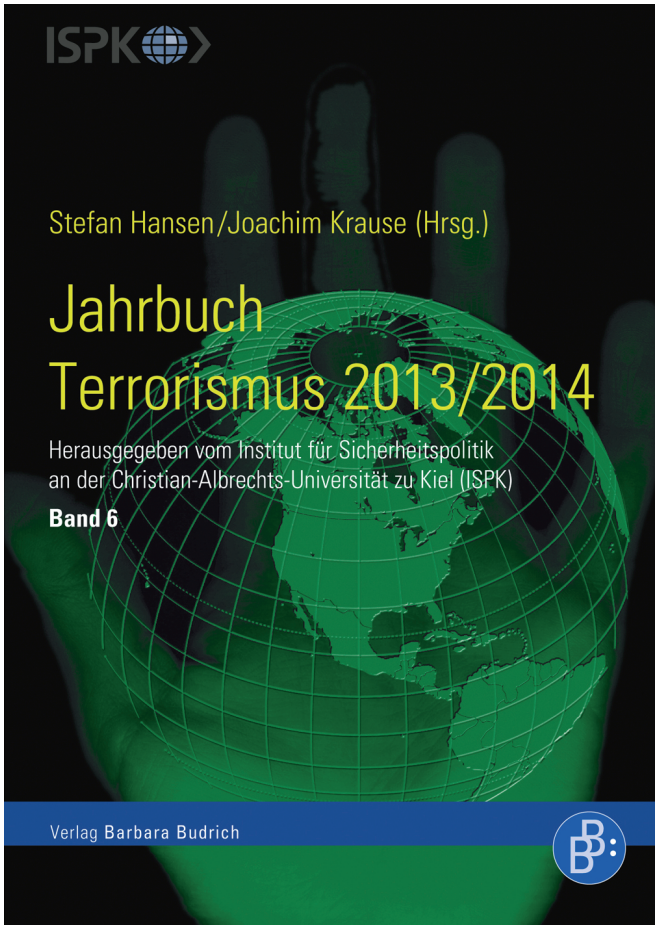
Sambleben, J. und Schumacher, S. (Herausgeber)



sicherheitsforschung-magdeburg.de/buecher.html

Jahrbuch Terrorismus 2013/2014

Hansen, S. und Krause, J. (Herausgeber, Institut für Sicherheitspolitik Kiel)



Stefan Schumacher:
Cyber-Terrorismus:
Reale Bedrohung oder Mythos?
S. 159 – 180

Inhaltsverzeichnis

1 Einführung

2 Kryptographie

3 OSTN/OSTEL.co

4 Clients

5 Fazit



Telefonie

- Telefone (Festnetz, DECT, GSM, Satellit) können abgehört werden
- nicht geeignet zur sicheren Datenübertragung
- Verschlüsselung nicht-trivial, da konstanter Datenstrom
- Hardwarelösungen teuer und kaum verbreitet
- Hardware schwer zu aktualisieren
- Softwarelösungen billiger und einfach nachzurüsten



Was ist Sicherheit?

VIVA-Kriterien

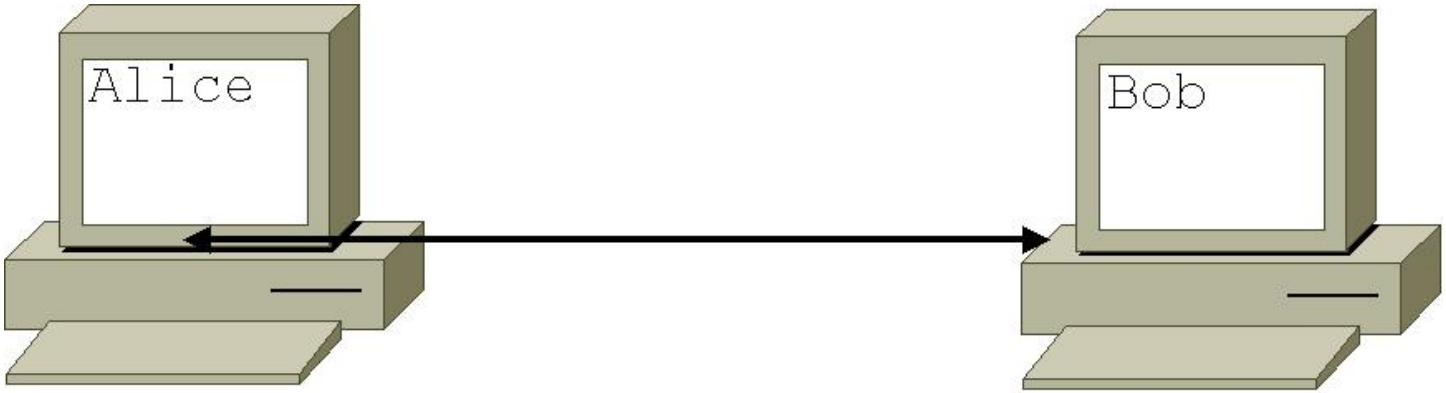
- Vertraulichkeit: Geheimhaltung, Zugriffsschutz der Daten
- Integrität: Verläßlichkeit, Daten sind unverändert
- Verfügbarkeit: Daten sind vorhanden/verwertbar
- Authentizität: Verbindlichkeit, Daten stammen vom vorgegebenen Absender

nur mit Krypto sicherzustellen



Man-in-the-Middle

Staatstrojaner

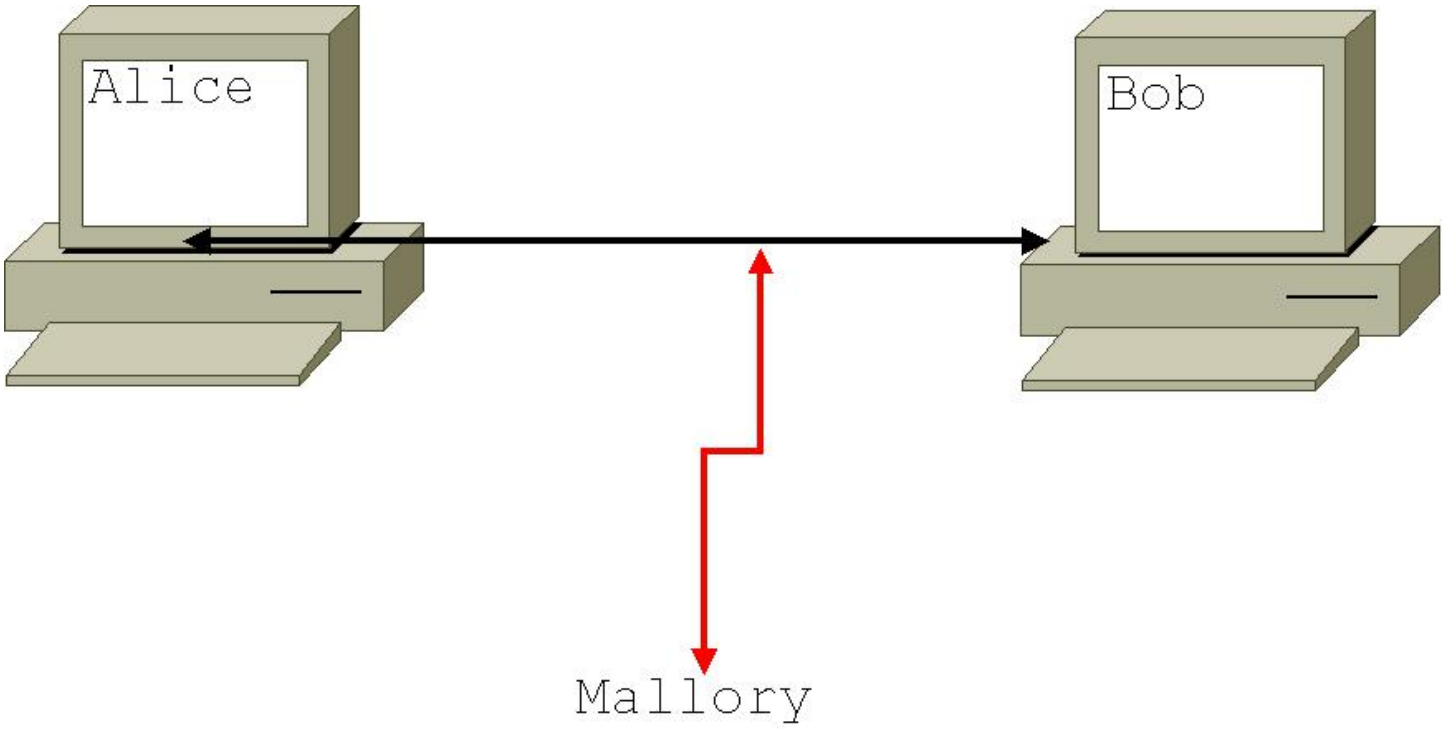


Mallory

unverschlüsselte Kommunikation kann abgefangen und ausgewertet werden

Man-in-the-Middle

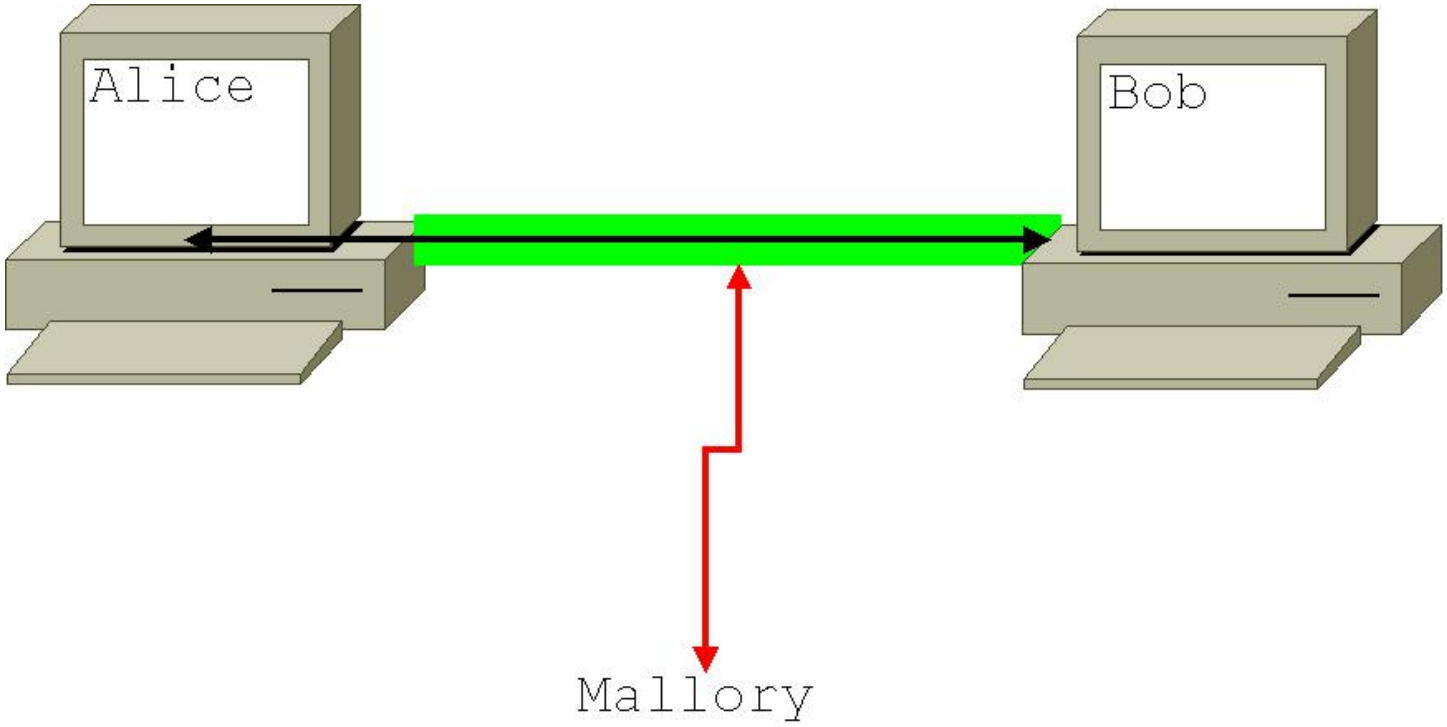
Staatstrojaner



Lösung: Verschlüsselung zwischen den Endpunkten (Skype, VPN, GnuPG, SSL) ermöglicht Authentifikation und Vertraulichkeit

Man-in-the-Middle

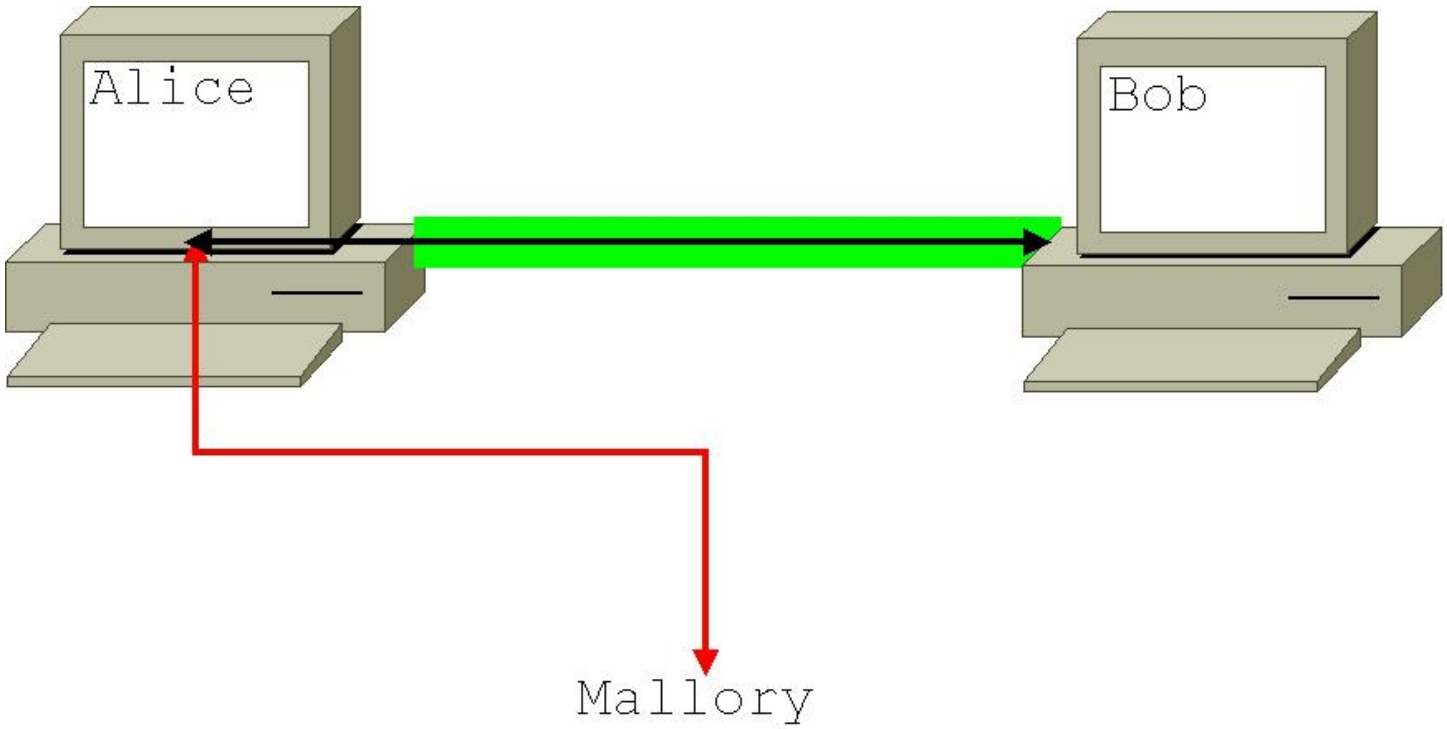
Staatstrojaner



Ausweich: Man-in-the-Middle-Attacke im System A oder B

Man-in-the-Middle

Staatstrojaner



abschöpfen der Daten auf dem Zielsystem selbst, bevor diese verschlüsselt werden

Inhaltsverzeichnis

1 Einführung

2 Kryptographie

3 OSTN/OSTEL.co

4 Clients

5 Fazit



RTP

- RFC 3550: RTP: A Transport Protocol for Real-Time Applications
- kontinuierliche Ende-zu-Ende-Übertragung von AV Daten in Echtzeit
- Paketverlust einkalkulierbar
- Daten kodieren, paketieren, versenden, idR über UDP
- QoS über RealTime Control Protocol (RTCP) möglich
- genutzt u.a. in H.323 und VoIP/SIP oder XMPP/Jingle



SRTP

- RFC 3711: The Secure Real-time Transport Protocol (SRTP)
- Ziele: Verschlüsselung, Authentifizierung, Integrität sicherstellen, Replay verhindern
- AES mit 2 Stream Cipher Modes, nötig um Paketausfälle zu überleben
- 2 Cipher (NULL) verschlüsselt nicht und muss implementiert werden



SRTP

- Integritätssicherung mit HMAC-SHA1
- über der Nutzlast und Headerdaten inkl. Sequenznummer generiert
- auf 80 oder 32 Bit gekürzt, wird in jedes Paket integriert
- Empfänger protokolliert Indizes und vergleicht neue Indizes mit alten um Replay zu verhindern
- erfordert zwingend ständig laufende Integritätssicherung
- beinhaltet keinen Schlüsselaustauschalgorithmus



ZRTP

- RFC 6189: ZRTP: Media Path Key Agreement for Unicast Secure RTP
- ZRTP: Z und RTP (Z = Zimmermann)
- Schlüsselaustauschprotokoll für Ende-zu-Ende-Geräte in VoIP-Netzen
- ZRTP/S Variante für alte Telefonnetze inkl. GSM, UMTS, ISDN, PSTN, SATCOM, UHF/VHF
- implementiert Diffie-Hellman-Schlüsselaustausch



ZRTP

- Diffie-Hellman-Schlüsselaustausch
- erzeugt geteiltes Geheimnis, welches genutzt wird um Schlüssel und Salz für eine SRTP Sitzung zu erzeugen
- benötigt keine PKI oder zentrale Server
- verschlüsselt opportunistisch
- zusätzliches geteiltes Geheimnis wird in der 1. Sitzung gespeichert (Challenge Response vorlesen)



Inhaltsverzeichnis

1 Einführung

2 Kryptographie

3 OSTN/OSTEL.co

4 Clients

5 Fazit



The Guardian Project

- 2009 gegründet
- entwickelt sichere Anwendungen für mobile Geräte
- Erweiterungen für Betriebssysteme
- sichere Mobilgeräte
- unterstützt u.a. durch Google, UCB, MacArthur Foundation et. al.
- betreibt OSTN/OSTEL.co



Open Source Telephony Network

- Open Source Implementierungen der ZRTP Bibliotheken
- Server-Betrieb
- Ostel.co als Vermittlungsserver
- kostenlos nutzbar, Account einrichten als »Telefonnummer«
- Clients entwickelt/unterstützt



Inhaltsverzeichnis

1 Einführung

2 Kryptographie

3 OSTN/OSTEL.co

4 Clients

5 Fazit



CSipSimple

- Client für Android-Geräte
- SIP/VoIP-Client
- unterstützt ZRTP, unter GPL
- ermöglicht Ende-zu-Ende-Verschlüsselung der Telefonie
- einfach zu installieren, nutzt Hardware im Handy/Tablet aus



Jitsi

- Java-Client für VoIP, Instant Messaging etc.
- Windows, Linux, Mac OS X, FreeBSD
- Android in Entwicklung
- Verschlüsselung mit ZRTP
- Telefonkonferenzen möglich
- andere Messenger (XMPP, ICQ, Google, Facebook etc.) integriert
- Ressourcenhungrig ...



weitere

- LinPhone: Linux, Windows, Android, iOS, OS X
- Twinkle: Linux (qt)
- Signal: iOS
- Redphone: Android, Forward Secrecy



Welcher Client?

https://www.eff.org/secure-messaging-scorecard

- Encrypted in transit?
- Encrypted so the provider can't read it?
- Can you verify contacts' identities?
- Are past comms secure if your keys are stolen?
- Is the code open to independent review?
- Is security design properly documented?
- Has there been any recent code audit?



Inhaltsverzeichnis

1 Einführung

2 Kryptographie

3 OSTN/OSTEL.co

4 Clients

5 Fazit



Fazit

- Angriffsmöglichkeiten im 1. Schlüsselaustausch
- Short-String-Authentication
- dDoS auf den Server $\rightsquigarrow$ keine Telefonate möglich
- eigener Server nicht wirklich nötig (dDoS)
- einfach zu bedienen und einzurichten
- hinreichende Sicherheit für nahezu alle Szenarien



Fazit

- Sicherheit durch Ende-zu-Ende Verschlüsselung
- Implementierung OK?
- Betriebssystem vertrauenswürdig?
- Trojaner im Linux? Google in Android?
- variable Bitrate? (VPN auf eigenen Server und Zufallsdaten dazu)



Magdeburger Journal zur Sicherheitsforschung

sicherheitsforschung-magdeburg.de/publikationen/journal.html

- Jens Kubieziel: Anonymität im Internet
- Stefan Schumacher: Timeo Danaos et dona ferentes: Zur Funktionsweise von Schadsoftware
- Michael »MiKa« Kafka und Rene »Lynx« Pfeiffer: Angriffe und Verteidigungsstrategien für vertrauliche Kommunikation über Funkdienste
- Dr. Georg Lukas: Why Android SSL was downgraded from AES256-SHA to RC4-MD5 in late 2010
- Dr. Georg Lukas: Java's SSLSocket: How Bad APIs Compromise Security



Webinar

- E-Businesslotse Mitteldeutschland
- montags, 19 Uhr, kostenlos und Online
  - 02.03 Wie Schadsoftware funktioniert und warum Virenscanner nichts taugen
  - 09.03 Open Source - Freie Software im Unternehmen
  - 23.03 Open Source – Linux, PostgreSQL, LibreOffice
  - 30.03 Einen sicheren Laptop mit Ubuntu einrichten
  - 13.04 Einbrechen wie die Hacker - Computer und Netzwerke auf Sicherheitslücken prüfen
  - 20.04 Abhörsichere Internet-Telefonie mit OSTN und OSTEL
  - 20.05 Mitarbeiter für IT-Sicherheit sensibilisieren



- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html



- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher
- ZRTP: 0xKaishakunin@ostel.co