

OpenChaos-Reihe Digitale Verhütung

Teil 2: Sichere Kommunikation

Marcel Klein, Tobias Wolter

Chaos Computer Club Cologne e.V.

<http://koeln.ccc.de>

Köln

25.10.2007



Gliederung

- 1 Warum Kommunikationsverschlüsselung?
- 2 Praxis
- 3 Letzte Bemerkungen



Warum Kommunikationsverschlüsselung?

- Unverschlüsselte Netzwerke können leicht abgehört werden
- Passwörter können Dritten (Vierten, Fünften...) in die Hände fallen
- Die eigene Kommunikation kann verfolgt werden



Typische Probleme

- Man loggt sich von unterwegs aus auf einer Webseite ein
- An fremden Orten den Lieblings-IM nutzen
- Während eines Vortrages Mails lesen



Wichtige Hinweise

- Eine verschlüsselte **Verbindung** sichert nur die Authentifikation
- Eine verschlüsselte **Nachricht** sichert den Inhalt bis zum Empfänger



Wichtige Hinweise

- Eine verschlüsselte **Verbindung** sichert nur die Authentifikation
- Eine verschlüsselte **Nachricht** sichert den Inhalt bis zum Empfänger

Bei schlechten Systemen sind die Kommunikationsserver die Empfänger der Nachricht!



Praxis

Wir behandeln in diesem Vortrag:

- E-Mail
- Instant Messaging
- Sonstige Medien (IRC, VoIP, Datenaustausch, ...)



E-Mail

Für E-Mails gibt es inzwischen etablierte Methoden, wie man sie verschlüsselt.



E-Mail

Für E-Mails gibt es inzwischen etablierte Methoden, wie man sie verschlüsselt.

- Problem: Nutzer müssen diese auch aktiv nutzen, damit sie funktionieren.
- Oft wird mindestens eine Methode bereits durch die Software von Haus aus unterstützt, wenn man sie aber nicht konfiguriert bringt das nichts.



Verbindung

Es gibt zwei grundlegende Arten Verbindungen zu verschlüsseln:

- Auf Protokollebene, z.B. mit SSL/TLS
- Auf Netzwerkebene, sprich VPN



Verbindung

Es gibt zwei grundlegende Arten Verbindungen zu verschlüsseln:

- Auf Protokollebene, z.B. mit SSL/TLS
- Auf Netzwerkebene, sprich VPN

Merke:

VPN-Dienste müssen im selben Netzwerk sein.



OpenPGP

Benutzung von OpenPGP ist gerade bei Nerds populär, und recht vielfältig einsetzbar.

- E-Mails können signiert und verschlüsselt werden



OpenPGP

Benutzung von OpenPGP ist gerade bei Nerds populär, und recht vielfältig einsetzbar.

- E-Mails können signiert und verschlüsselt werden

Verschlüsselung sichert den Inhalt einer Nachricht, und Signieren die Authentizität.



OpenPGP

Benutzung von OpenPGP ist gerade bei Nerds populär, und recht vielfältig einsetzbar.

- E-Mails können signiert und verschlüsselt werden

Verschlüsselung sichert den Inhalt einer Nachricht, und Signieren die Authentizität.

- Vertrauen in Signaturen über Web of Trust (WoT)



X.509

Auch gerne bekannt als S/MIME oder einfach nur „Zertifikate“ oder „digitale Signatur“.

- Bietet auch Signierung und Verschlüsselung (PKCS #7)
- PKI: Zentrale Autoritäten (CA) erstellen und widerrufen Zertifikate



X.509

Auch gerne bekannt als S/MIME oder einfach nur „Zertifikate“ oder „digitale Signatur“.

- Bietet auch Signierung und Verschlüsselung (PKCS #7)
- PKI: Zentrale Autoritäten (CA) erstellen und widerrufen Zertifikate

Mailprogramme und Browser beinhalten oft Zertifikate, denen standardmäßig vertraut wird.



Vergleich PKI und WoT

PKI und WoT sind grundlegend andere Verfahren an das Problem ran zu gehen.

- PKI
 - Vorteile: einfache Handhabung, kein manueller Aufwand
 - Nachteile: anfällig gegenüber Sicherheitsproblemen, indirektes Vertrauen



Vergleich PKI und WoT

PKI und WoT sind grundlegend andere Verfahren an das Problem ran zu gehen.

- PKI
 - Vorteile: einfache Handhabung, kein manueller Aufwand
 - Nachteile: anfällig gegenüber Sicherheitsproblemen, indirektes Vertrauen
- WoT
 - Vorteile: sicherer, weniger anfällig gegenüber Sicherheitsproblemen
 - Nachteile: sehr aufwändige Pflege



Instant Messaging

An der IM-Front ist Verschlüsselung noch eher ein Randthema:

- Sehr geringe Unterstützung bei Programmen
- Nicht wirklich viele Benutzer



Verbindung

- Jabber unterstützt SSL
- MSN benutzt SSL für die Authentifizierung
- Sonst eher mau



OpenPGP

- Nachrichten-Verschlüsselung mit OpenPGP
- Wird von Jabber und den meisten Jabber-Clients auf Protokollebene unterstützt
- Für andere Clients gibt es Plugins



Off-the-Record Messaging (OTR)

- Neueres Verfahren zur sicheren Kommunikation
- Tolle Features:
 - Verschlüsselung
 - Authentifikation
 - Bestreitbarkeit
 - „Perfect Forward Secrecy“



Off-the-Record Messaging (OTR)

- Sehr einfach
- Arbeitet mit jedem Protokoll zusammen, welches Text überträgt
- Bietet keine Verschlüsselung der Metadaten einer Konversation, nur des Inhalts



Off-the-Record Messaging (OTR)

- Sehr einfach
- Arbeitet mit jedem Protokoll zusammen, welches Text überträgt
- Bietet keine Verschlüsselung der Metadaten einer Konversation, nur des Inhalts

Vorsicht:

OTR bei Google Talk schaltet nur das Logging aus!



Vergleich zwischen OTR und OpenPGP

- OpenPGP macht es einfacher, ohne abgehört zu werden auch mit Dritten zu reden (bei gutem Web of Trust)
- OTR braucht den Austausch von Fingerprints über andere Medien, damit Authentifizierung gewährleistet ist
- Bei OTR weiß man nie genau wer mit wem redet, bei OpenPGP sieht man es sofort
- Bei OTR können Nachrichten im Nachhinein „hinzugefälscht“ werden, ohne daß man einen Hauptschlüssel hat



IRC

- Diverse Implementation von einfachen Strom- und Blockchiffren (AES, twofish, blowfish, ...)
- Theoretisch auch wiederum kein Problem, OpenPGP und OTR zu benutzen
- Für z.B. irssi wird gerade ein otr-Plugin geschrieben



IRC

- Diverse Implementation von einfachen Strom- und Blockchiffren (AES, twofish, blowfish, ...)
- Theoretisch auch wiederum kein Problem, OpenPGP und OTR zu benutzen
- Für z.B. irssi wird gerade ein otr-Plugin geschrieben

OpenPGP in einem Channel benutzen ist eher nicht empfehlenswert.



VoIP

Wenn man VoIP nicht verschlüsselt, dann ist es kein großes Problem die Gespräche abzuhören.

- Theoretisch gibt es verschiedene Möglichkeiten eine VoIP-Kommunikation zu verschlüsseln:
 - Mit VPNs auf Netzwerkebene
 - Auf Protokollebene, z.B. mit SRTP, ZRTP oder Skype...



VoIP

Wenn man VoIP nicht verschlüsselt, dann ist es kein großes Problem die Gespräche abzuhören.

- Theoretisch gibt es verschiedene Möglichkeiten eine VoIP-Kommunikation zu verschlüsseln:
 - Mit VPNs auf Netzwerkebene
 - Auf Protokollebene, z.B. mit SRTP, ZRTP oder Skype...

Ein VPN-Tunnel verschlüsselt nur die Verbindung zwischen Netzen, die Kommunikation innerhalb des LANs bleibt unverschlüsselt.



Secure Real-Time Transport Protocol (SRTP)

- Verwendet AES
- Schlüsselaustausch erfolgt über das Signalisierungsprotokoll
- Wird von manchen Hard- und Softwarephones unterstützt
- Muss von beiden Endpunkten unterstützt werden



ZRTP

- Als Protokoll wird SRTP benutzt
- ZRTP wird zum Austausch des SRTP-Sessionkeys verwendet
- „Perfect Forward Secrecy“



Skype

- Benutzt AES
- Kein offenes Protokoll
- Die Verschlüsselung dient zum Schutz des Protokolls und nicht des Users



Datenaustausch

- Steganographie ermöglicht es, Nachrichten in Dateien zu verstecken
- Bietet Verschlüsselung und vor allem Unklarheit



Datenaustausch

- Steganographie ermöglicht es, Nachrichten in Dateien zu verstecken
- Bietet Verschlüsselung und vor allem Unklarheit

Ohne Vorkenntnis über die Datei und den Algorithmus ist es nicht-trivial, festzustellen, ob ein Datei steganographische Informationen enthält.



Datenaustausch

- Steganographie ermöglicht es, Nachrichten in Dateien zu verstecken
- Bietet Verschlüsselung und vor allem Unklarheit

Ohne Vorkenntnis über die Datei und den Algorithmus ist es nicht-trivial, festzustellen, ob ein Datei steganographische Informationen enthält.

- Keine Authentifizierung



Letzte Bemerkungen

- Verschlüsselung ist ein sich konstant änderndes Feld; die Aussagen in diesem Vortrag könnten morgen schon ungültig sein.
- Es gibt wenige universell anwendbare Verfahren, die mit an Sicherheit grenzender Wahrscheinlichkeit unknackbar sind (OTP).
- Dies stellte natürlich nur einen groben Überblick dar.



Referenzen

- <http://www.cypherpunks.ca/otr/>
- <http://www.gnupg.org/>

