Grundlagen der Verschlüsselung

(Email & Festplatten & Kurznachrichten)

8. Mai 2015

base on: https://github.com/kaimi/cryptoparty-vortrag/

Übersicht

Festplattenverschlüsselung

- Verlust des Geräts / der Festplatte
  - Notebook verloren
  - Einbruch
- alle unverschlüsselten Daten sind sofort zugreifbar
  - z.B. der OpenPGP-Schlüssel

- Verlust des Geräts / der Festplatte
  - Notebook verloren
  - Einbruch
- alle unverschlüsselten Daten sind sofort zugreifbar
  - z.B. der OpenPGP-Schlüssel
  - oder die Steuererklärung

- Verlust des Geräts / der Festplatte
  - Notebook verloren
  - Einbruch
- alle unverschlüsselten Daten sind sofort zugreifbar
  - z.B. der OpenPGP-Schlüssel
  - oder die Steuererklärung
  - oder die Partyfotos vom letzten Wochenende

- Verlust des Geräts / der Festplatte
  - Notebook verloren
  - Einbruch
- alle unverschlüsselten Daten sind sofort zugreifbar
  - z.B. der OpenPGP-Schlüssel
  - oder die Steuererklärung
  - oder die Partyfotos vom letzten Wochenende
  - ... you name it

- Lösung: Verschlüsselung der Festplatte
- **wichtig:** schützt nur zuverlässig, wenn
  - das Kennwort („Passphrase“) stark genug ist
  - das Gerät aus ist, wenn es verloren geht
  - Standby schützt nicht!

Festplattenverschlüsselung

Windows

- nur manche Varianten können Verschlüsselung von Haus aus (Enterprise, Ultimate)
- Abhilfe schafft TrueCrypt
- nachträgliche Verschlüsselung der Festplatte möglich

Mac OS

- Mac OS kann von Haus aus Festplattenverschlüsselung (FileVault)
- nachträgliche Verschlüsselung der Festplatte möglich
- für einzelne Dateien/Ordner: TrueCrypt

Linux

- Linux bietet Festplattenverschlüsselung bei der Installation an (LUKS)
- für einzelne Dateien/Ordner: TrueCrypt

Übersicht

Emailverschlüsselung

Wie funktioniert Email?

- im Grunde eine einfache Textdatei
  - Metadaten
  - Inhalt
- wird von Server zu Server weitergereicht
- und auf dem Server des Empfängers gespeichert
- Abruf per Browser oder Mailprogramm
- in der Regel bleiben die Mails auf dem Server gespeichert

Wie funktioniert Email?

- Webmail per Browser ist in der Regel verschlüsselt
  - HTTPS
  - Schlossymbol im Browser
- Zugriff per Mailprogramm sollte das auch sein
  - „SSL, immer“
  - „TLS, immer“
- Übertragung zwischen den Servern
  - leider oft unverschlüsselt
  - als Nutzer kaum nachprüfbar

Wie funktioniert Email?

- nicht sicherer als eine Postkarte
- Mails liegen unverschlüsselt auf dem Server des Providers
- Zugriff möglich durch
  - Angestellte
  - Einbrecher (physisch oder über das Netz)
  - Strafverfolgungsbehörden
  - Geheimdienste
  - ... oder einfach durch eine Panne

Emailverschlüsselung

Was kann ich verschlüsseln?

Verschlüsseln lässt sich nur der **Inhalt** der Mail, nicht die Metadaten!

- Absender
  - Emailadresse
  - Anschlusskennung (IP-Adresse)
- Betreff
- Datum und Uhrzeit
- Empfänger

bleiben immer unverschlüsselt.

OpenPGP

- OpenPGP ist ein freier Standard
- asymmetrisches Verschlüsselungsverfahren
- ermöglicht:
  - Vertraulichkeit (Verschlüsselung)
    - liest jemand mit?
  - Authentisierung (Signaturen)
    - ist mein Gegenüber der, für den er sich ausgibt?

OpenPGP

jeder braucht 2 zusammengehörige Schlüssel:

- öffentlicher Schlüssel
  - wird veröffentlicht oder den Partnern zur Verfügung gestellt
  - Verschlüsselung
  - Überprüfung einer Signatur
- geheimer Schlüssel
  - **niemals** aus der Hand geben
  - Entschlüsselung
  - Signatur

Schlüsselerstellung

- man braucht nur einen Namen und eine Emailadresse
- ... und das richtige Programm
- öffentlichen Schlüssel bekanntmachen
  - selbst zum Download anbieten, z.B. auf der eigenen Homepage
  - Hochladen auf einen Schlüsselserver

Schlüsselerstellung

- man braucht nur einen Namen und eine Emailadresse
- ... und das richtige Programm
- öffentlichen Schlüssel bekanntmachen
  - selbst zum Download anbieten, z.B. auf der eigenen Homepage
  - Hochladen auf einen Schlüsselserver

Das ist im Grunde alles, was man braucht. Aber:

Achtung

Jeder kann zu **beliebigen** Namen und Emailadressen einen Schlüssel erzeugen!

Noch leichter lässt sich in einer Email eine gefälschte Absenderadresse angeben.

Schlüsselüberprüfung

- jeder Schlüssel hat einen eindeutigen Fingerabdruck
- Austausch des Fingerabdrucks über einen getrennten Kanal
  - am besten: persönlich
  - Telefon
  - ganz altmodisch per Brief
  - **nicht** über das Netz

Schlüsselüberprüfung

- jeder Schlüssel hat einen eindeutigen Fingerabdruck
- Austausch des Fingerabdrucks über einen getrennten Kanal
  - am besten: persönlich
  - Telefon
  - ganz altmodisch per Brief
  - **nicht** über das Netz

Was ist, wenn ich eine Email bekomme, den Schlüssel aber noch nicht kenne?

Übersicht

Kurznachrichtenverschlüsselung

- Ähnlicher Ablauf wie bei Email

- Ähnlicher Ablauf wie bei Email
- Austausch von (kurzen) Textnachrichten

- Ähnlicher Ablauf wie bei Email
- Austausch von (kurzen) Textnachrichten
  - Client - Server - Server - Client

- Ähnlicher Ablauf wie bei Email
- Austausch von (kurzen) Textnachrichten
  - Client - Server - Server - Client
- Auch Verschlüsselung im Grunde sehr ähnlich wie Email

- Ähnlicher Ablauf wie bei Email
- Austausch von (kurzen) Textnachrichten
  - Client - Server - Server - Client
- Auch Verschlüsselung im Grunde sehr ähnlich wie Email
- Aber: Andere Protokolle & Programme

Kurznachrichtenverschlüsselung

Jabber

Auf dem PC

- Addressen wie bei Email: d3non@jabber.chaos-darmstadt.de
- Viele öffentliche Server und Clients möglich
  - eigenen Server hosten möglich
  - Viele Clients unterstützen auch andere Protokolle (ICQ, ...)

Jabber + OTR

OTR: Off-The-Record (wie bei Journalisten)

- Vergleichbar mit OpenPGP + mehr coole Features
- wie bei OpenPGP: geheimer + öffentlicher Schlüssel
- Manuelle Verifikation des Schlüssels
  - Per Fingerprint ..
  - ... oder geheimer Sicherheitsfrage

Smartphones

- oft Telefonnummer als Identität
- OpenSource + Verschlüsselt + Auditiert?
  - TextSecure (Android) bzw Signal (iOS)
  - Sogar verschlüsselte Telefonie (Redphone)
- Alternativ: auch Jabber + OTR
  - Xabber (Android), ChatSecure(Android + iOS)

Übersicht

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern
  - Trojaner können den Inhalt vor der Verschlüsselung lesen

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern
  - Trojaner können den Inhalt vor der Verschlüsselung lesen
  - Keylogger erfassen sowohl die Eingabe des Klartextes als auch der Passphrase

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern
  - Trojaner können den Inhalt vor der Verschlüsselung lesen
  - Keylogger erfassen sowohl die Eingabe des Klartextes als auch der Passphrase
- ... und hilft nur begrenzt gegen die Staatsgewalt

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern
  - Trojaner können den Inhalt vor der Verschlüsselung lesen
  - Keylogger erfassen sowohl die Eingabe des Klartextes als auch der Passphrase
- ... und hilft nur begrenzt gegen die Staatsgewalt
  - Totalüberwachung &-speicherung, bis der Code geknackt ist

Bin ich jetzt sicher?

- absolute Sicherheit gibt es **nicht**!
- Technik kann immer nur eine Hilfe sein
- Verschlüsselung ist ein wichtiger Baustein
- ... bietet aber keinen Schutz vor Trojanern oder Keyloggern
  - Trojaner können den Inhalt vor der Verschlüsselung lesen
  - Keylogger erfassen sowohl die Eingabe des Klartextes als auch der Passphrase
- ... und hilft nur begrenzt gegen die Staatsgewalt
  - Totalüberwachung &-speicherung, bis der Code geknackt ist
  - im Zweifel Zwangsmittel

Übersicht

Festplatten

- TrueCrypt https://www.truecrypt71a.com/
  - Wichtig: Version 7.1a
  - Auditierung http://istruecryptauditedyet.com/
- Nachfolger Veracrypt https://veracrypt.codeplex.com/

Email

- GnuPG http://gnupg.org/
  - Win http://www.gpg4win.de/
  - OSX https://gpgtools.org/
- Thunderbird http://www.thunderbird-mail.de/
  - Enigmail https://addons.mozilla.org/de/thunderbird/addon/enigmail/

Kurznachrichten

- Jabber
  - Pidgin https://pidgin.im/
  - OTR https://otr.cypherpunks.ca/
  - Xabber
    https://play.google.com/store/apps/details?id=com.xabber.android
  - ChatSecure (Android)
    https://play.google.com/store/apps/details?id=info.guardianproject.otr.app.im
  - ChatSecure (iOS) https://itunes.apple.com/de/app/chatsecure-encrypted-messenger/id464200063?mt=8
- TextSecure https://whispersystems.org/
  - Textsecure
    https://play.google.com/store/apps/details?id=org.thoughtcrime.securesms
  - RedPhone
    https://play.google.com/store/apps/details?id=org.thoughtcrime.redphone
  - Signal(iOS) https://itunes.apple.com/de/app/signal-private-messenger/id874139669?mt=8