Security, Privacy and Freedom

Albert Weichselbraun

Inhalt

- Privatsphäre im Internet – Sniffing, Logging & Co
- Computer-Forensik
- Peer to Peer Netzwerke

Ziele dieser Einheit:

- De-Mystifying „Anonymity“
- Awareness

Privatsphäre im Internet – eine Demonstration

- Sniffing
- Spoofing and Man in the Middle Attacks
  - ARP Spoofing
- Logging (an Routern, Webserveren, etc.)
  - Vergleich: *whois*
- Social Networking (Facebook, StudiVZ, ...)

Bedeutung von Privacy

- Freiheit

  „No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.“

  [Universal Declaration of Human Rights, Article 12]
- Industriespionage

  Beispiel: Echelon

  SWIFT
- Kriminalität

  Phishing (mit Kontextinformationen ▸ Spear Phishing)

  Mithören von Passwörtern

  Verfolgen und Mitprotokollieren von Benutzeraktionen

Bedeutung von Privacy

- Rasterfahndung, Gefährdungseinschätzung von Flugpassagieren (US Ampel) arbeiten mit Information Retrieval Methoden
  => Feature Selection
  => Annahme:
  ähnliche Features = ähnliche Eigenschaften
- Sicherheit: 99.9% => 60 mil. Fehlklassifikationen
- **Verantwortung** liegt bei wem?
  Vergleiche: Rasterfahndung in .de;
  Computerdurchsuchung

Verschlüsselung und Authentifizierung

- **Zielsetzungen:**
  - der Inhalt der Kommunikation soll geheim bleiben (=> Verschlüsselung)
  - Zertifizierung der Identität (=Authentifizierung)
- Trotz Verschlüsselung weiter bekannt, mit wem man kommuniziert!

Authentifizierung

- über Zertifikate
- diese bestätigen die Authentität von
  Benutzern (PGP, gnupg)
  Programmen (signierte Applets)
  Webseiten und Inhalten (Telebanking)
- Zwei Ansätze:
  a) **Zentral**: Zertifizierungsstellen
  (zum Beispiel: VeriSign, ...)
  b) **Dezentral**: Web of Trust (PGP, gnupg)

Verschlüsselung

- **Zwei Prinzipien:**
  a) symetrische Verschlüsselung
  b) asymetrische Verschlüsselung
  -> öffentlicher/privater Schlüssel
- Für Web-/E-Mail: meist symetrisch, nachdem der Session-Key via asymetrische Verschlüsselung ausgetauscht wurde.
- Programme für den Privatanwender:
  gnupg/PGP – Frontends für die meisten E-Mailprogramme verfügbar (z.B. Enigma für Thunderbird)

E-Mail Verschlüsselung mit Enigma

- Installation von Enigma
- Erstellen eines eigenen Key-Paars
- Importieren von öffentlichen Schlüsseln
- Signieren einer E-Mail
- Verschlüsseln einer E-Mail

Übungsaufgabe*

- Senden Sie eine signierte E-Mail mit den folgenden Daten:

  ```
  Subject: Test
  Dieses E-Mail stammt sicher von ...
  ```

  an ihren Nachbarn.
- Senden Sie die selbe E-Mail verschlüsselt an xyz@localhost und an ihren Nachbarn.

Anonymität

- Verschlüsselung sichert **nicht** die Privatsphäre
- Usertracking:
  1px Images (Ping)
  Cookies
  JavaScripts (Vergl. Google-Analytics)
- Möglichkeiten diese zu verbessern/schützen:
  Anonyme Remailer (E-Mail)
  Java Anon Proxy (JAP) (Web)
  Tor (TCP/IP Traffic)
  Browser Plugins (NoScript)
- Steganographie -> Fourier Analyse, ...
  steghide (Beispiel: Homepage; Pwd: 123)

Beispiel: steghide

- Verstecken von Daten:

  ```
  steghide embed -cf picture.jpg -ef secret.txt
  ```
- Extrahieren von Daten

  ```
  steghide extract -sf picture.jpg
  ```
- **Übungsaufgabe:**
  Senden Sie Ihrem Nachbarn/Ihrer Nachbarin eine versteckte Nachricht via E-Mail

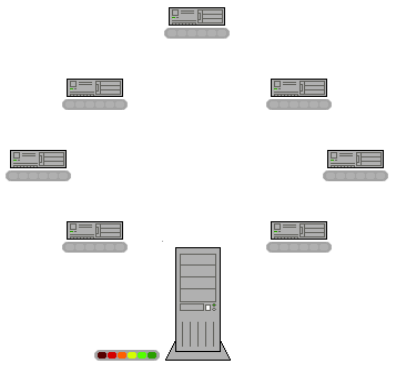
Hard Disk Encryption

- Beispiel: Löschen von Daten
  (A -> B -del-> C)
- Anwendung – rechtliche Rahmenbedingungen
- Nachteile: Backups, Data-Recovery
- Software:
  Truecrypt (Linux, Windows)
  LUKS (=Linux Unified Key Setup)
- Vorgangsweise (/dev/urandom, cryptsetup, ...)

Peer to Peer Netzwerke

- Beispiele: Bittorrent, eDonkey, Gnutella
- Vorteile:
  a) geringe Bandbreite benötigt, um hohe Datenmengen zu verteilen
  b) Dezentral
- Nachteile:
  Sharing von urheberrechtlich geschützter Inhalten
  => schlechter Ruf
- Funktionsweise von bittorrent
  a) Tracker – verwaltet Informationen zu den Dateien
  b) Peers - Herunterladen

Funktionsweise: bittorrent



Quelle: Wikipedia

Conclusions

- Privacy, Security and Freedom are NOT for free.
- Technologie kann helfen, die Privatsphäre zu sichern, wenn man diese richtig einsetzt.
- Gesetzgeber tw. nicht kompetent
  -> vergleiche: Verbot von Hacking/Reverse Engineering
- Fokus <-> Werte

„darf nicht so sehr darauf fokusiert sein den Krieg mit allen Mitteln zu gewinnen, dass man dabei in Kauf nimmt, jene Werte für die man kämpft, zu zerstören...“