Sicherheit im Internet

Andreas Maag, dipl. phys.
maagical GmbH

Programm heute

1. Teil

- Was ist Sicherheit?
  - Persönlichkeitsschutz und Demokratie, Persönlichkeits-Klau
  - Diebstahl
  - Spam
- Beispiele
  - Online Einkaufen
  - Email versenden
- "So einfach geht es" (ein Hacking-Versuch)

2. Teil

- Lösungen
  - "sicheres" Verhalten
    - sicherere Passwörter
    - SSL etc.
  - "sichere" Systeme

Sicherheit (im Internet)

Welche Sicherheit meinen wir? Was sind die Gefahren

- wir wollen keine unberechtigten Zugriffe auf Computer
- kein Spam, keine Viren
- kein Diebstahl (Geldabzocke, Phishing)
- keine Trojaner die Daten ausspähen (E-Banking, Persönlichkeits-Klau, Big-Brother)

Privatsphäre vs. Geheimhaltung

(Warum wollen wir Sicherheit? wir haben ja nichts zu verbergen?)

- Eine Privatangelegenheit ist etwas, bei dem man nicht will, dass es die ganze Welt weiss, aber eine geheime Angelegenheit ist etwas, von dem man nicht will, dass es irgendjemand weiss.

Privatsphäre

Beispiele:

- Wenn ich im Laden ein Magazin kaufen und bar zahle, so muss der Verkäufer nicht wissen, wer ich bin, wieviele Kinder ich habe, was meine politische Einstellung zu Bush ist, etc ....
- Wenn ich meinen Email-Provider beauftrage eine Meldung zu versenden, so muss mein Provider nicht wissen an wen ich sende oder was ich sage oder was andere zu mir sagen. Mein Provider muss nur wissen wie die Meldung zum Absender gelangt und wieviel Geld er verlangen darf. Wenn ich meine Identität durch den darunterliegenden Mechanismus (Email versenden) aufdecken muss, so habe ich keine Privatsphäre. Ich kann mich nicht selektiv öffnen, ich muss **immer** alles von mir öffnen.

Warum Anonymität:

- Darum braucht Privatsphäre in einer offenen Gesellschaft anonyme Transaktionssysteme. Bis jetzt war Bargeld das primäre solche System. Ein anonymes Transaktionssystem ist keine heimliches Transaktionssystem. Eine anonymes System befähigt Individuen ihre Identität aufzudecken wann sie es wollen und nur wann sie es wollen, es ist die Essenz der Privatsphäre. (Stichwort Freiheit)

Quelle: http://www.activism.net/cypherpunk/manifesto.html "A Cypherpunk's Manifesto"
(Übersetzung aus: http://www.bpb.de/publikationen/0WLS2D,13,0,5_2_Kryptografie.html Bundeszentrale für politische Bildung Deutschland)

Bemerkungen

- Es gibt keine endgültige Sicherheit - Sicherheit ist ein Prozess, es gibt keine einfachen Lösungen - auch kein einfaches Delegieren)

- "Es betrifft nicht nur mich selbst" (Bsp: Strassenverkehr)
  Beispiele:
  - Brief an andere (durch 3te gelesen) -> Mobbing
  - Missbrauch des eigenen PC als Spam-Plattform (oder noch kriminellere Machenschaften - Bot-Netze)

Am Beispiel: Online Einkaufen

Warum die Sicherheit z.B. der Kreditkartennummer nicht nur an einem Punkt hängt ....

- Fishing
- Auf dem eigenen Computer sitzt ein Troyaner, der alle Eingaben mitlesen kann und wegsendet
- Der eigene Computer Präsentiert alle Daten auf dem Internet (Standardeinstellung gewisser Windows)
- Sniffing (jemand spioniert z.b. über das WLAN eine ungesicherte Verbindung)
- Man-in-the-middle-Attacke
- Online Shop / Abrechnungsfirma / KK-Firma wird geknackt (Juni 05, 40 Mio....)

Beispiel: Email versenden oder

Wer schreibt seine Liebesbriefe auf Postkarten?

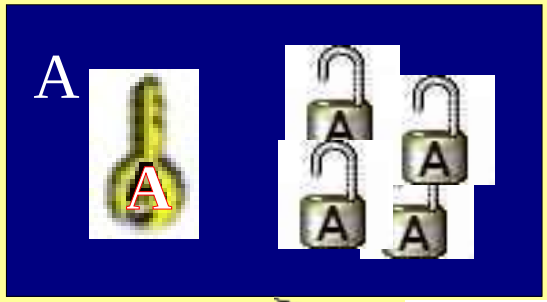
- Ein Email unternimmt u.U. einen langen Weg bis zum Absender
  - es muss seinen Weg "selber" finden ("packetorientiertes" Internet)
  - es gibt keine Garantie, dass es ankommt (protokollbedingt)
  - Anti-Spam Massnahmen schmeissen u.U. gute Mails weg (hotmail)
- Ohne "harter" Verschlüsselung/Signatur gibt es keine Garantie dass die Mail vom vermuteten Absender kommt

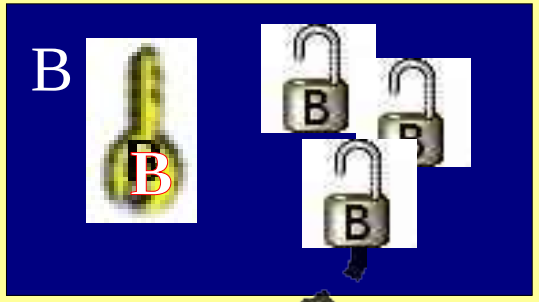
Funktionsweise der Verschlüsselung

public key / öffentlicher Schlüssel

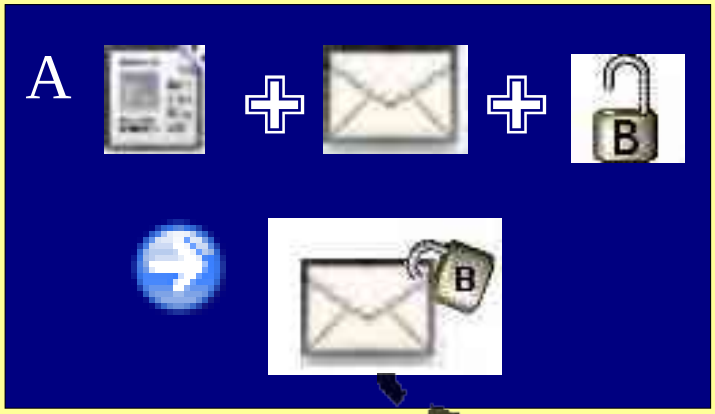
secret key / privater Schlüssel

A soll Brief/Email/Dokument an B verschlüsseln





A braucht den "öffentlichen Schlüssel" von B



B

nur B hat den privaten Schlüssel um das Couvert zu öffnen

A überträgt auf unsicherer Leitung den Brief

Funktionsweise Signieren

Das signieren ist im Prinzip genau umgekehrt zum Verschlüsseln

- *"A will Brief an B signieren"*
  - A braucht nur eigenen privaten Schlüssel
  - B braucht öffentlichen Schlüssel von A
- A macht einen Fingerabdruck des Inhalts des Briefs und verschlüsselt diesen "verkehrt" mit seinem privaten Schlüssel (so dass es nur mit dem öffentlichen Schlüssel von A entschlüsseln werden kann)
- B kann die Signatur mit dem öffentlichen Schlüssel von A prüfen und sehen dass der Fingerabdruck korrekt ist

Lösungen

- Sichereres Verhalten
  - gute Passwörter
  - Emails verschlüsseln = Briefe zukleben
  - so wenige Daten von sich bekannt geben wie möglich (Persönlichkeitsklau / Datenschutz)
  - kritische Informationen (z.B. Kreditkartennummer) nur auf verschlüsselten Wegen übermitteln (SSL/https / gnupg/gpg / pgp / S/Mime, ssh ...)

- Sicherere Systeme brauchen
  - Linux und nicht Windows, Win XP+SP2 eher als Windows 2000/98
  - nicht als Administrator auf dem PC arbeiten (leider noch bei XP die Default-Einstellung)

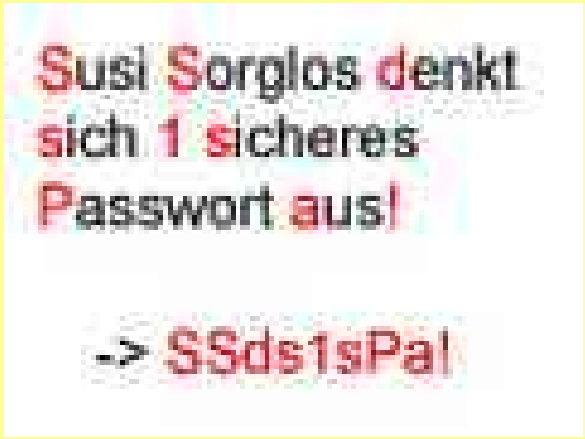
Passwörter einfach merken

Gut sind alle Passwörter, die man nicht einfach so erraten kann.

Tipp: Zum Beispiel eine Abkürzung für einen Satz wie:

"An warmen Sommertagen regnet es eher selten." =
AwSrees.

Wer dann auch noch Sonderzeichen und Ziffern verwendet, hat ein sicheres Passwort. Und kann es sich auch noch gut merken.



Passwort-Checks:
https://passwortcheck.datenschutz.ch/check.php?lang=de
http://www.internet-kompetenz.ch/sicherheit/crackmaster/

Links

- Verschlüsselungssoftware
  - www.gnupg.org
  - http://www.gaponline.de/software/win/thunderbird/verschlues.html (gpg mit Mozilla Thunderbird)
- Dokumentation
  - http://www.schneier.com/crypto-gram.html (monatlicher Newsletter zur Sicherheit, mit interessanten Beispielen zur "Sicherheitssituation" in den USA)
  - http://syndikat.ch/navi17/detail634/ (Grundsatzpapier zu Datenschutz und Personendaten-Geheimnis)
  - Überwachung
    - Echelon / Onyx
      - http://www.medienheft.ch/kritik/bibliothek/k22_BaerDavid_18.html
      - http://www.heise.de/tp/r4/artikel/7/7213/1.html
  - cronopios.org/seguridad/sicherheitsstunde.pdf (dieses Dokument)

Zitate

- http://www.securityfocus.com/columnists/337:
  Don't do any online banking unless you have a router, a firewall, the latest anti-virus, the latest Windows patches, the latest Windows OS, three anti-spyware applications, and you fully understand what "phishing" means. If you don't know what these are, what you're doing or how to properly configure, secure and operate your own server, turn your computer off. Or buy a Mac or Linux desktop and slip under the radar.
  (Mache keine Online-Bankgeschäfte falls du keinen Router, Firewall, nicht die letzte Anti-Virus Software, die letzten Windows Flicke, das letzte Windows System und die letzte Anti-Spyware Applikation hast und wenn du nicht vollständig verstanden hast was „Phishing“ bedeutet. Falls Du nicht weiss was das ist, was du tust oder wie du deinen eigenen Server richtig konfigurierst, sicherst und betreibst – schalte deinen Computer aus. Oder kauf einen Mac oder installiere Linux um unter dem Radar durchzukommen.)
- http://www.schneier.com/crypto-gram-0506.html
  More than 1,000 new worms and viruses were discovered in the last six months alone.
- http://syndikat.ch/navi17/detail634/:
  Die Haltung „Wer nichts zu verbergen hat, hat auch nichts zu befürchten" verkennt vier Gefahren:
  - Wer Zugang zu Daten hat, kann diese manipulieren oder für Sonderinteressen missbrauchen. Beispiel: Der Arbeitgeber erfährt durch das Überwachen privater E-Mails von einer schweren Krankheit eines Mitarbeiters und entlässt diesen.
  - Der Gebrauch demokratischer Rechte kann mit starken Interessen von Personen, Institutionen oder Unternehmen kollidieren, die Zugang zu vertraulichen Informationen haben. Beispiel: In einem Betrieb bildet sich einen gewerkschaftliche Betriebsgruppe, die gegen die Entlassung eines Kollegen antreten will. Ihre Kommunikation wird durch den Arbeitgeber überwacht, die ‚Rädelsführer' werden ebenfalls entlassen.
  - Ein Anstieg der sozialen Spannungen oder eine Zunahme internationaler Konflikte kann rasch dazu führen, dass sich autoritäre Regimes bilden, die auf der Basis bestehender Datensammlungen reelle und potentielle Oppositionelle gezielt unterdrücken. Ständige Überwachung kann auch dazu führen, dass die Leute ihr Verhalten selbst zensurieren.
  - Menschen werden zunehmend definiert und fixiert durch die Daten, die über sie gespeichert werden. Die EDV „vergisst nicht und vergibt nicht": Wer zum Beispiel einmal als zahlungssäumig erfasst ist, erleidet möglicherweise für den Rest seines Lebens Nachteile.
  Fazit: Der ausreichende Schutz der Privatsphäre ist ein unabdingbarer Bestandteil der Menschenwürde, der freien Meinungsbildung und einer offenen, pluralen Gesellschaft.
- Aus dem AIDE (Advanced Intrusion Detection) Handbuch (http://www.cs.tut.fi/%7Erammer/aide/manual.html)

  General guidelines for security
  1. Do not assume anything
  2. Trust no-one,nothing
  3. Nothing is secure
  4. Security is a trade-off with usability
  5. Paranoia is your friend

  Generelle Sicheheitshilfslinien
  1. Mache keine Annahmen irgendwelcher Art
  2. Vertraue niemandem und nichts
  3. Nichts ist sicher
  4. Sicherheit erkauft sich mit schlechter Benutzerfreundlichkeit
  5. Paranoia ist dein Freund