Sicherheit im Internet

Institut für Informatik (IAM), Universität Bern
Forschungsgruppe Rechnernetze und Verteilte Systeme (RVS)
http://www.iam.unibe.ch/~rvs/

Inhalt

- Was für Gefahren lauern auf den Internet Surfer?
- Abwehrmassnahmen:
  - Verschlüsselungstechnik.
  - Verhaltensregeln.

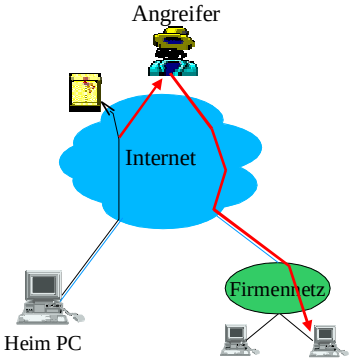
Bedrohungslage

- Bei der Internet Entwicklung wurde die Sicherheit vernachlässigt.
- PC Betriebssysteme waren nicht für den Netzwerkbetrieb gedacht.
- Jeder Rechner kann jeden anderen Rechner im Internet ansprechen.
- Die Daten werden ungeschützt über die Netze von ev. vielen verschiedenen Betreibern geleitet.

... Bedrohungslage

- Digitale Manipulationen hinterlassen keine Spuren.
- Keine sicheren Identitätsmerkmale.
- Unseriöse Datenhandhabung bei Internet Firmen.
  - Computerpannen.
  - Firmenkonkurse.
- Schlechtere Datenschutzbestimmungen in anderen Ländern.

Klassifizierung der Angriffe



- Angriffsziel:
  - Heim PC.
  - Campus− / Firmennetz.
- Angriffsmethode:
  - Passiv (ausspionieren).
  - Aktiv (eindringen).
    - Unter Vortäuschen falscher Identität.

Angreifer und Motive

- Hacker: Wissensdurst, Abenteuerlust, Vandalismus.
- Unzufriedene Mitarbeiter.
- Industriespionage.
- Behörden: Überwachung von gesetzesbrecherischen Aktivitäten, Zensur.
- Geheimdienste: Handel mit (militärischen) Informationen.

Viren und Trojanische Pferde

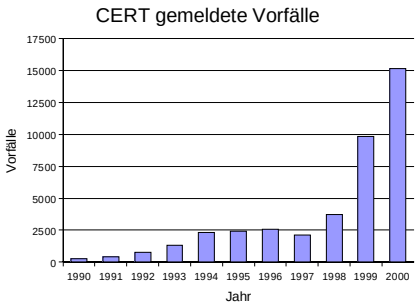
- Viren:
  - Kleine Programme, die sich selbstständig kopieren.
- Würmer:
  - Programme die sich selbstständig über ein Netzwerk verbreiten.
- Trojanische Pferde:
  - Killerprogramme, die sich als bekannte, scheinbar harmlose Programme tarnen.

Historische Beispiele

- Passive Angriffe:
  - Carnivore (FBI).
  - Echelon (NSA und westliche Geheimdienste).
- Aktive Angriffe:
  - Morris' Internet Wurm (legte 1988 ca. 10% Internets lahm).
  - "I LOVE YOU" E−Mail Wurm.
  - Fluten von www.yahoo.com.
  - Ausspionieren von Microsoft's neuer Entwicklung.

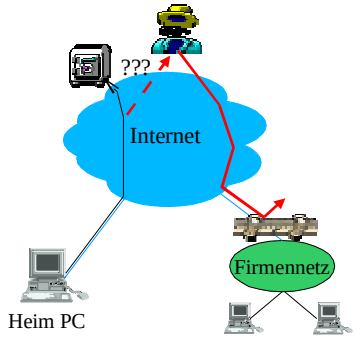
CERT Melde− und Info Stelle

- Akademische Organisation (neutral).
- Aus dem Internet− Mutterprojekt DARPA erwachsen (1988).
- Dunkelziffer viel höher!
- www.cert.org



Abwehrmassnahmen

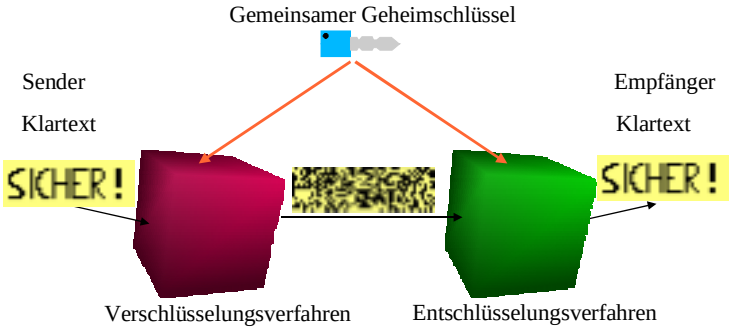
- Verschlüsselung der Übertragenen Daten.
- Zugangskontrollen.
  - Zu Rechnern.
  - Zu Netzen (Firewall).
- Überwachung (Logging).
- Umsichtiges Verhalten.



Verschlüsselungstechnik
(Kryptographie)

- Unkenntlichmachung und Wiederherstellen von Information.
- Seit Menschengedenken betrieben.
- Kriegsentscheidend.
- Blütezeit mit dem Informationszeitalter.
- Ein Schlüssel (Zahl) wird mit der zu verschlüsselnden Information verrechnet.

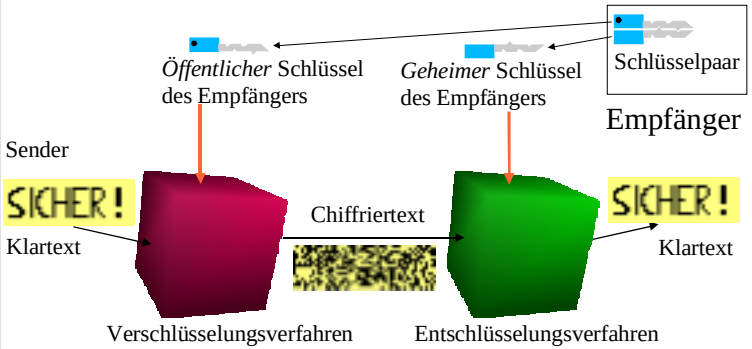
Symmetrische Verschlüsselung



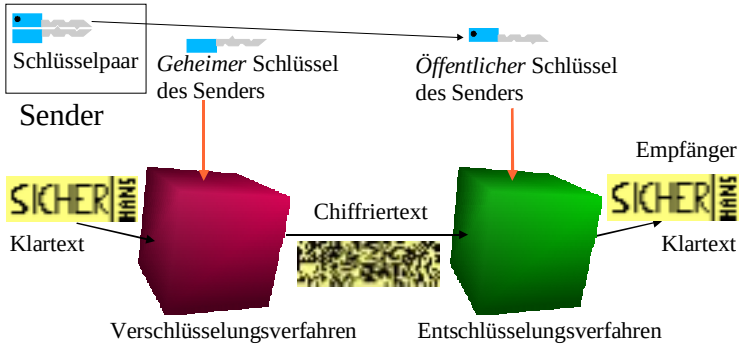
Asymmetrische Verfahren

- Schlüssel aus zwei ungleichen Teilen (Schlüsselpaar).
- Was mit dem einen Teil verschlüsselt wird, kann nur mit dem anderen entschlüsselt werden.
- Ein Teil öffentlich (z.B. Auf Web Seite), der andere Teil geheim.
- Anwendung: Verschlüsselung und Authentifikation.

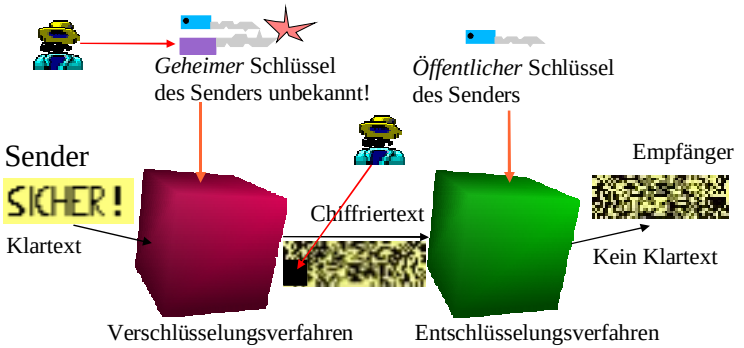
Asymmetrische Verschlüsselung



Authentifikation: Verifizieren des Absenders



Entlarvte Betrugsversuche: Falscher Absender Vortäuschen oder Daten Ändern



Sicherheit der Verfahren

- Symmetrische Verschlüsselungsverfahren: 3DES, IDEA, Blowfish, RC4.
- Asymmetrische Verfahren: RSA, ElGamal.
- Bei bekannten, als sicher geltenden Verfahren ist die verwendete Schlüssellänge ausschlaggebend.
  - PIN auf EC−Karte: bis 97': 56 Bit−verschlüsselt.
    - Knackbar mit 100'000 $ in 3.5 Stunden.
  - PIN auf EC−Karte: 112 Bit−verschlüsselt.
    - Knackbar mit 10 Mio. $ in 100'000'000'000 Jahren.

Einsatz der Verfahren

- Verschlüsselungsmechanismen sind integrierte Bestandteile von sicheren Anwendungen (z.B. PGP für E−Mail, Netscape fürs Web Surfen).

Quellenangaben

- *Applied Cryptography*, Bruce Schneier, John Wiley & Sons, Inc
- http://www.counterpane.com
- http://www.faqs.org/faqs/cryptography−faq/

Generelle Verhaltensregeln bei der Internetbenutzung

- Sich der Gefahren bewusst sein.
- Mit einigen einfachen Regeln, lässt sich Sicherheit deutlich erhöhen.
- Kompromiss zwischen Sicherheit und Komfort.

Computerhygiene

- Sicherheitsprogramme wie Virenscanner und Firewalls regelmässig aktualisieren.

- Der Sicherheitsgrad von Anwendungen und Betriebssystem lässt sich oft hoch−konfigurieren.

- Kein automatisches "Starten" von Mails oder anderen Anwendungen.
- Sicherheitskopien der wichtigen Daten.

Gefahren durch Programme

- Kein Starten von Programmen und Dateien unbekannter/zweifelhafter Herkunft.
  - Download aus dem Internet.
  - Benutzung fremder Datenträger (auch leerer).
  - Öffnen von Attachments (I LOVE YOU).

Passwörter

- Passwörter/ PINs niemals weitergeben, oder ungeschützt aufschreiben (Brieftasche, Agenda, unter Tastatur).
- Keine realen Wörter/Silben, Daten, Adressen.
- Nicht zu kurz (mehr als 6 Buchstaben).
- Komplizierte Passphrasen: "TiMd,S'idiS,".
- Passwörter regelmässig ändern.
- Verschiedene Passwörter für verschiedene Systeme/Sicherheitsstufen verwenden.

Persönliche Daten

- Keine persönlichen oder finanziell relevanten Daten (Kreditkarten Nummer) in ungeschützte Web Formulare eintragen.
- Ihr Surf−Aktivität ist grundsätzlich über mehrerer Wochen rückverfolgbar.
- Immer daran denken, dass evtl. Millionen Menschen Zugriff auf die Information haben!

Gesicherte Web Verbindung

- Schloss−Icon zeigt gesicherte Verbindung an (Verschlüsselung).
- Wesentlich sicherer als normale Kreditkarten−benutzung.
- www.fortify.com [SSL check]

Email

- Niemals auf Spam Mails antworten !
- Keine verdächtigen Mails öffnen:
  - unbekannter Absender.
  - unbekannte Attachments.
  - seltsame Anrede etc.
- Sicherheitshalber Rückfragen!
- Viruswarnungen per Email sind oft Kettenbriefe.
- Vertrauliche Nachrichten verschlüsseln.

Fragen?

Institut für Informatik (IAM), Universität Bern
Forschungsgruppe Rechnernetze und Verteilte Systeme (RVS)
http://www.iam.unibe.ch/~rvs/