Freie Universität Berlin

Vorlesung "Anwendungssysteme"

Informationssicherheit (Security)

Prof. Dr. Lutz Prechelt
Freie Universität Berlin, Institut für Informatik
http://www.inf.fu-berlin.de/inst/ag-se/

- 5 Aspekte: Integrität, Authentizität, Vertraulichkeit, Verfügbarkeit, Verbindlichkeit
  - Definitionen, Beispiele
- Arten von Angreifern
- Traditionelle Schutzmaßnahmen
- Vertrauen, Angriffsmodell
- Technische Schutzmaßnahmen
  - Digitale Signatur
  - Schwachstellen, Schadsoftware
- Sozio-technische Schutzmaßn.
  - Das Problem der Verfügbarkeit
  - Social Engineering

Definition "Informationssicherheit" (1)

Freie Universität Berlin

Definition aus der vorletzten Stunde (Einheit "Risiken")

- "Schutz (*security*):
  - Die Widerstandsfähigkeit eines Systems gegen absichtliche Angriffe. Das System ist sicher (geschützt, *secure*), wenn die Angriffe ohne Unfall überstanden werden
    - Bei Informatiksystemen insbesondere: Informationssicherheit
  - Teilaspekt von Sicherheit"

Spezialisierung heute:

- **Informationssicherheit** (information security):
  - Die Widerstandsfähigkeit eines Informatiksystems gegen absichtliche Angriffe auf die **Integrität**, **Authentizität**, **Verbindlichkeit**, **Verfügbarkeit** oder **Vertraulichkeit** v. Daten
    - Definitionen folgen
  - Wir nennen ein System **sicher**, wenn erfolgreiche Angriffe aufwändiger sind, als der Nutzen des Angreifers es gestattet.

Kriterien für Informationssicherheit (1)

Freie Universität Berlin

- **Integrität (integrity)**: betrifft die **Daten** selbst
  - Sind die Daten wirklich originalgetreu (z.B. seit Ihrer Erzeugung unverändert?)
- **Authentizität (authenticity)**: betrifft beteiligte **Personen**
  - Ist die Autorin der Daten wirklich die behauptete Person?
  - Dito für Leserin der Daten
- **Verbindlichkeit (non-repudiation)**: betr. beteiligte **Pers.**
  - Kann man auch dann nachweisen, dass die Autorin die Autorin war, wenn die das abstreiten möchte?
  - Dito für die Leserin
- **Verfügbarkeit (availability)**: betrifft **Zugang** z.d. Daten
  - Sind die Daten (für Befugte!) abrufbar, wenn man sie benötigt?
    - a) im gewünschten Moment oder b) überhaupt noch
- **Vertraulichkeit (privacy)**: betrifft **Zugang** z.d. Daten
  - Kann keine unbefugte dritte Person die Daten lesen?

Kriterien für Informationssicherheit (2)

- Integrität: War die ursprüngliche Nachricht wirklich X?
- Authentizität: Kommt X wirklich von Alice?
  Ist der adressierte Empfänger wirklich Bob?
- Verbindlichkeit: Kann Bob nachweisen,
  dass X von Alice kam?
- Verfügbarkeit : Kommt die Nachricht bei Bob an?
  Kann Bob sie abrufen und lesen?
- Vertraulichkeit: Können nur Alice+Bob die Nachricht lesen?

"Nein" → Problem!

Kriterien für Informationssicherheit (3)

Beispiele von Verletzungen der Eigenschaften

- Authentizität: Nachricht kommt von Bobs Ex-Freundin
- Vertraulichkeit: Bobs Freund Charlie hat die Nachricht gesehen
- Integrität: Charlie ändert sie zu "Ich hasse Dich"
- Verfügbarkeit : Charlie hat die Nachricht gelöscht
- Verbindlichkeit: Alice sagt "War nicht von mir."
  oder (f. Empfang): Bob sagt "Sorry, habe ich nie bekommen."

Echte Beispiele f. Verletzungen

Freie Universität Berlin

- Authentizität:
  - Ex-Freundin von X erzeugt drei Scheinidentitäten bei StudiVZ und schwärzt darüber die neue Freundin von X bei X an. (Wurde per Strafbefehl verurteilt. 2010.)
    - http://www.heise.de/newsticker/meldung/Geldstrafe-fuer-die-Nutzung-eines-offenen-WLAN-und-Stalking-auf-studiVZ-917915.html

- Verfügbarkeit:
  - Frau J will einer Zwangsheirat entgehen und sendet Nachricht an ihren heimlichen Geliebten R, dass sie deshalb vor der Hochzeit ein starkes Schlafmittel einnehmen wird.
    R erhält die Nachricht nicht, findet die schlafende J, hält sie für tot und bringt sich selber um.
    - (William Shakespeare: Romeo und Julia)

Kriterien für Informationssicherheit (4)

Beispiele von Verletzungen der Eigenschaften

- Authentizität: a) Den Account 'Alice' benutzt heute Eve.
  b) Auto-Angebot kommt gar nicht von Bob.
- Integrität: Da stand eigentlich € 1.600.
- Verfügbarkeit: Das Gebot kommt nicht an.
  Oder nicht rechtzeitig.
- Verbindlichkeit: Bob kann nicht nachweisen,
  dass Alice €5.600 geboten hat.

Beispiele f. Verletzungen

- Authentizität:
  - **Phishing**: "Hier spricht Deine Bank.
    Wir haben Deine Daten verbummelt und brauchen Deine Hilfe.
    Gib bitte hier Deine PIN und TAN ein."
    - Verletzung der Authentizität *bewirkt* Verletzung der Vertraulichkeit
  - **Kreditkartenbetrug**: Buchungen mit geklauten Kartennummern
- Integrität/Authentizität/ Verfügbarkeit:
  - Am 24.12.1987 überwies ein holländischer Bankangestellter sich selbst 6,7 Millionen Dollar unberechtigt auf ein Schweizer Konto
    (fehlende Integrität)
  - Überweisungen mussten von 2 Personen autorisiert werden (4-Augen-Prinzip), aber er kannte das Passwort eines Kollegen (verletzte Authentizität).
  - Flog auf, weil die Überweisung wegen technischen Versagens nicht durchlief
    (verletzte Verfügbarkeit)

Motivationen von Angreifern

Warum greift jemand Daten oder ein Informatiksystem an?

1. Persönliche Bereicherung (Kriminelle)
2. Wirtschaftsspionage, staatliche Spionage (Firmen, Geheimdienste)
3. Wirtschaftssabotage, staatliche Sabotage (dito) "Cyber-Krieg"

4. Neugierde (irgendjemand)
   - auf die Daten oder auf den Angriff
5. Jugendlicher Übermut (*Script-Kiddies*)
6. Böswilligkeit (z.B. s. oben: Ex-Freundin)

7. Gerechtigkeitssinn ("Robin Hood")
8. Auf Risiken hinweisen (z.B. Chaos Computer Club)

Traditionelle Schutzmaßnahmen (Beispiele)

Freie Universität Berlin

In der physischen Welt von Daten ohne Computer
(d.h. persönliche Begegnung, Dokumente auf Papier):

- Authentizität: Ausweis, Unterschrift, Stempel, Briefbogen

- Verbindlichkeit/ Integrität: Dokumentechte Tinte, Notar

- Vertraulichkeit/ Integrität/ Verfügbarkeit: Wertschrank (Tresor)

- Verbindlichkeit: Unterschrift

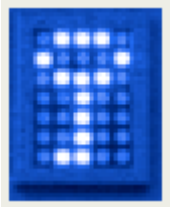
Vertrauen

Freie Universität Berlin

- Beim Entwurf eines Informatiksystems muss man entscheiden, wem vertraut werden darf (d.h. "X ist sicher")
  - Welchen Personen(kreisen), welcher Hardware, welcher Software

Warum?

1. Manche Absicherungen schließen einander aus
   - Variante 1: echte Passwörter
     - aber dann gilt: Passwort verloren → Zugang futsch
     - Vertraulichkeit/Integrität hoch, Verfügbarkeit heikel
   - Variante 2: jemand kann ein Passwort zurücksetzen
     - aber dann gilt: Ich muss demjenigen vertrauen.
     - Vertraulichkeit/Integrität geringer, Verfügbarkeit höher



Truecrypt

2. Übertriebene Absicherung ist unsinnig teuer oder unpraktisch
   - Wer sperrt beim Ablegen immer sein Handy?
   - Wer verschlüsselt alle seine Emails?

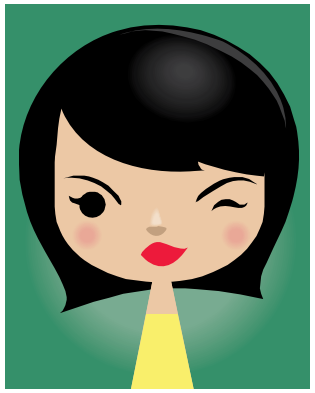
GnuPG

Grund: Lohnt oft (scheinbar) nicht!

Angriffsmodell für Email-Versenden

Freie Universität Berlin

- Zur Gestaltung eines sicheren Systems ist deshalb festzulegen, wo man mit was für Angriffen rechnet



Alice

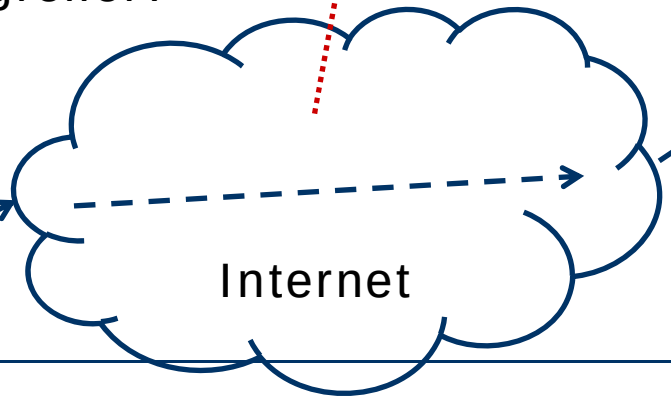
Ist Alice böswillig?
Handelt sie unter Zwang?

Hat jemand unbefugt Zugriff auf den Server? (Mensch, SW)

Belauscht jemand die Übertragung?
Verfälscht jemand die Übertragung (man-in-the-middle)?

Pass-wort

Meldet eine SW die Nachricht an einen fernen Angreifer?



Belauscht jemand die Pass-worteingabe?
Evtl. eine HW/SW?

u.s.w.

Technische Schutzmaßnahmen (Beispiele)

Freie Universität Berlin

In der digitalen Datenwelt:

- Authentizität: Besitz von Geheimnissen (Passwort, Signaturschlüssel)
- Vertraulichkeit: Verschlüsselung, Zugriffsschutz/Rechte
- Integrität: Entdeckung von Veränderungen (Verschlüsselung, digitale Signatur) phys. Zugriffsschutz auf Speicher/Leitung
- Verfügbarkeit: Betriebsabsicherung, Redundanz
- Verbindlichkeit: digitale Signatur, Protokolldaten

Crashkurs: Digitale Signatur

Freie Universität Berlin

Inhalt des Crashkurses (je 1 Folie):

- Verschlüsselung
- Symmetrische Verschlüsselung
- Asymmetrische Verschlüsselung
- Digitale Unterschrift (digitale Signatur)
- Public-Key-Infrastruktur
- Ermöglichte Sicherheitseigenschaften

- Dieser Crashkurs deckt nur ab, was jede/r Softwareingenieur/in wissen sollte
  - unzählige Details fehlen
  - Siehe die Veranstaltungen von Prof. Volker Roth

Verschlüsselung

Freie Universität Berlin

- Sei gegeben eine Nachricht **K** ("Klartext"), die geheim gehalten werden soll
- und zwei Funktionen
  - **V** ("Verschlüsselung") mit V(K) = **C** ("Chiffretext")
  - **E** ("Entschlüsselung") mit E(C) = K
- so, dass C jedem unbefugten Empfänger ("Angreifer") unverständlich ist
  - C sieht aus wie eine Folge von Zufallsbits: total redundanzfrei
- dann nennt man (V,E) ein Verschlüsselungsverfahren

- Offensichtlich müssen sich Sender und Empfänger auf das Paar (V,E) einigen und E geheim halten
  - Solche Verfahren wurden bereits in der Antike erfunden

Symmetrische Verschlüsselung

Freie Universität Berlin

Modernerer Ansatz:

- V und E sind beide allgemein bekannt
  - fast jede/r hat sie als Software vorinstalliert

AES

- aber sie sind parametrisiert mit einer großen Zahl S ("Schlüssel")
  - V_S, E_S
  - $E_S(V_S(K)) = K$, aber es gibt viele mögliche S (z.B. 2^{128} Stück), die ein Angreifer durchprobieren muss
    - Wie lange dauert das? → Überschlagsrechnung

- Sender und Empfänger müssen sich nun nur noch auf S einigen ("Schlüsselvereinbarung")
  - → ermöglicht den häufigeren Austausch der Verschlüsselung
    - Verfahren heißt *symmetrisch*, weil Sender und Empfänger denselben Schlüssel S benutzen
  - **Aber wie vereinbart man einen solchen Schlüssel, ohne belauscht zu werden?**

Asymmetrische Verschlüsselung

Freie Universität Berlin

Noch modernerer Ansatz:

- V und E sind beide allgemein bekannt
  - viele Personen haben sie als Software auf ihrem Computer
- aber sie sind parametrisiert mit zwei verschiedenen großen Zahlen P und Ö, die zusammengehören
  - $E_P(V_Ö(K)) = K$
  - Das Verfahren heißt asymmetrisch, weil Sender und Empfänger verschiedene Schlüssel benutzen
  - P heißt der private Schlüssel (*private key*) und ist geheim
    - Er wird nie (nie! nie!!) irgendjemandem weitergegeben
  - Ö heißt der öffentliche Schlüssel (*public key*) und wird quasi im Telefonbuch bekannt gegeben → Schlüsselvereinbarung entfällt!
  - Jeder Benutzer hat sein eigenes Paar (P, Ö)
- Somit kann jeder dem Empfänger eine Nachricht senden, die nur dieser entschlüsseln kann

Digitale Unterschrift (digitale Signatur)

Freie Universität Berlin

Jetzt kommt ein toller Kniff:

- Asymmetrische Verschlüsselung funktioniert auch "andersrum":
  - $E_{Ö}(V_P(K)) = K$
  - Dann kann also jeder mit Ö die Nachricht entschlüsseln
- Wozu ist das gut?
  - Ich sende Nachrichten der Form "Von prechelt@inf.fu-berlin.de: $V_P(K)$", wobei $P = P_{Prechelt}$
  - jetzt kann jeder Empfänger nachprüfen, dass die Nachricht wirklich von Prechelt kommt
  - denn dann (und nur dann) kann man sie mit $Ö_{Prechelt}$ entschlüsseln
  - Kein Angreifer kann die Nachricht gezielt verfälschen.
- Asymmetrische Kryptographie ist die genialste Mathe-Erfindung der letzten 100 Jahre

Public-Key-Infrastruktur (PKI)

Zwei Probleme bleiben übrig:

- Das ganze bricht zusammen, falls
  (a) ein Angreifer A das Telefonbuch fälschen kann
  - und der Welt sein eigenes $Ö_A$ als $Ö_{Prechelt}$ unterjubelt, oder aber
- (b) jemand meinen privaten Schlüssel ausspioniert

- (a) Deshalb müssen Telefonbucheinträge wiederum unterschrieben sein
  - von jemand, dem alle vertrauen und dessen Ö quasi jeden Tag in der Tagesschau etc. durchgesagt wird, so dass es niemand verfälschen kann.
  - → *Zertifizierungsstellen* (Certification Authorities, CAs)
  - Der ganze technisch-organisatorische Rahmen samt Verfahren heißt ***Public-Key-Infrastruktur (PKI)***
- (b) Schlüssel P darf niemals vertrauenswürdige Hardware verlassen → nicht PC, sondern Chipkarte führt Signatur durch

Ermöglichte Sicherheitseigenschaften

Freie Universität Berlin

Verschlüsselung ➔

- Vertraulichkeit (privacy)
- Integrität (integrity)

Signatur ➔

- Authentizität (authenticity)
- Verbindlichkeit, Nicht-Abstreitbarkeit (non-repudiation)

- Man kann Signatur und Verschlüsselung auch beide anwenden und somit alle 4 Eigenschaften zugleich erreichen

- **Aber:** Verfügbarkeit???
  - Wird durch Verschlüsselung gesenkt (Schlüsselverlustrisiko)!

(Ende des Crashkurses über digitale Signatur)

Freie Universität Berlin

Noch zwei Anmerkungen:

- Zur Verschlüsselung:
  - Asymmetrische Verschlüsselung ist sehr rechenaufwändig,
  - deshalb verschlüsselt man in der Praxis größere Datenmengen stets symmetrisch
  - und benutzt asymmetrische Verfahren nur für die dazu nötige Schlüsselvereinbarung.

- Zur Signatur:
  - Zur digitalen Signatur verwendet man deshalb ebenfalls nicht das ganze Dokument
  - sondern signiert nur eine Prüfsumme (z.B. 256 bit lang).
  - Dafür gibt es spezielle *kryptografische Hashfunktionen*

SHA-256

Und nun?

- Mit diesen technischen Maßnahmen kann im Prinzip eine recht gute Informationssicherheit erreicht werden

- Risiken drohen vor allem aus zwei Quellen:
  - Menschliches Verhalten derjenigen Beteiligten, die Vertrauen genießen (müssen)
    - dazu später mehr
  - Aushebeln der technischen Mechanismen durch Schadsoftware

Schadsoftware

Ausgangspunkt:

1. Computer ist universell, kann beliebig programmiert werden
2. Aktivität von SW entzieht sich weitgehend der Beobachtung

- Wenn also SW auf den Rechner gelangt, die nicht vertrauenswürdig ist, können viele Sicherheitsmechanismen unwirksam werden
- Solche Schadsoftware (*malware*) ist inzwischen ein Massenmarkt für Kriminelle
  - http://en.wikipedia.org/wiki/Malware

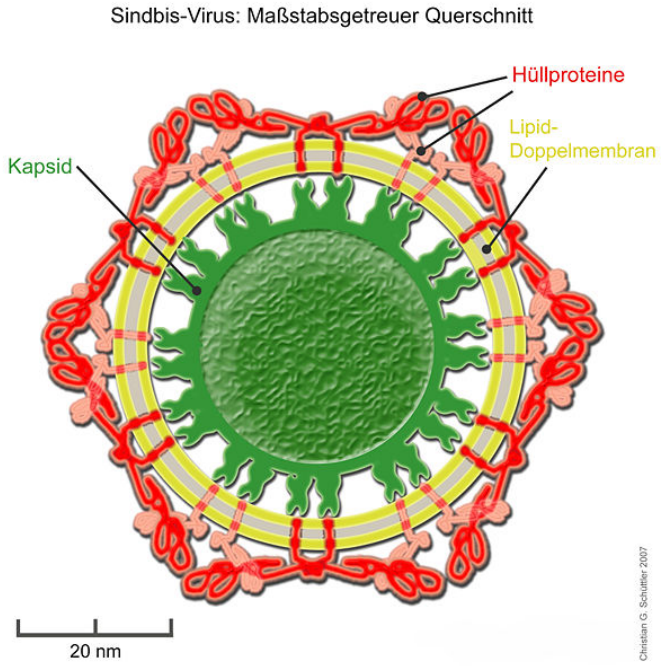
- Es folgen Begriffsklärungen zu Schadsoftware

Aspekte von Schadsoftware

1. Verbreitungsweg
   - Wie gelangt die Schadsoftware zu dem Rechner, der kompromittiert werden soll?

2. Methode des Eindringens (Erlangung der Kontrolle)
   - Wie kommt es dazu, dass die Schadsoftware auf diesem Rechner tatsächlich ausgeführt wird?

3. "Nutzlast" (Schadkomponente)
   - Was tut die Schadsoftware dann?

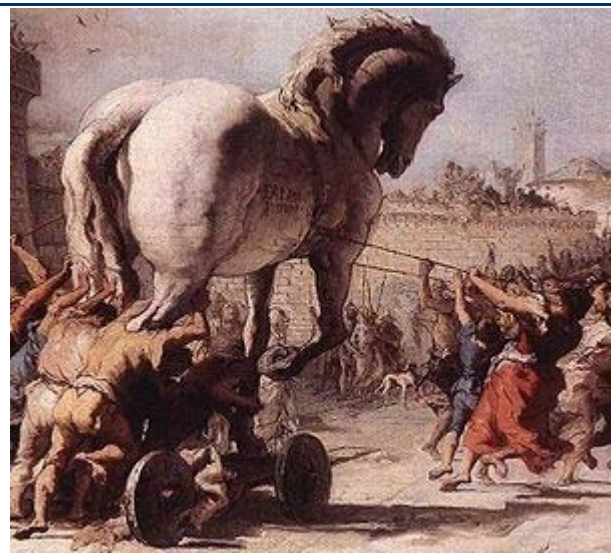


1. Verbreitungswege

Freie Universität Berlin

- Virus
  - Biologie: Ein Organismus, der als Parasit in eine Zelle eindringt und diese dazu "umprogrammiert", ihn zu vervielfältigen.
  - Informatik: Software, die einen Computer ungewollt so verändert, dass er (a) evtl. etwas unerwünschtes tut und (b) das Virus weiterverbreitet.
- Wurm
  - Ein Virus, das sich aktiv selbst über ein Netzwerk verbreitet
- Trojanisches Pferd
  - Ein Schadprogramm, das ein Benutzer selbst freiwillig aufruft, weil er es für etwas Harmloses hält
  - Auftreten insbesondere als (1) Email-Anhang oder (2) Webseite ("drive-by infection" per Javascript, Flash o.ä.)

2. Eindringmethoden (1)



1. "Absichtliche" Ausführung
   - Trojanisches Pferd

Alle anderen Eindringmethoden setzen eine Schwäche der SW (Verletzlichkeit, *vulnerability*) voraus:

2. Standardpasswörter (Hersteller-Voreinstellung)
   - Häufig bei Hardwarekomponenten (Router u.ä) und bei Infrastruktur-SW (DBMS, Webserver u.ä.)
     - Viele Beispiele: http://www.phenoelit-us.org/dpl/dpl.html (inzwischen offline)
   - Herkunft: Konfigurationsfehler

2. Eindringmethoden (2)

Freie Universität Berlin

3. Pufferüberlauf

- Ablauf geht ungefähr so: 4000 Bytes Eingabedaten →
  in Stringvariable (Länge 200 Bytes) auf dem Stapel →
  überschreibt andere Stapelinhalte, insbes. Rücksprungadresse →
  Rücksprung an angreifergewählte Adresse (auch auf Stapel) →
  Eingabedaten werden als Programm interpretiert →
  Angreifer kann beliebige Operationen ausführen
- Verbleibender Schutz: Angreifer gewinnt nur soviel Privilegien wie das angegriffene Programm sie hatte
- Besonders bedroht sind Programme in C (z.T. auch C++), die noch Bibliotheken verwenden, die Überläufe nicht prüfen
  - betrifft sehr viel Systemsoftware
- Herkunft: Programmierfehler

2. Eindringmethoden (3)

Freie Universität Berlin

4. Injektionsangriffe
   - SW verwendet Benutzereingabe in einem interpretierten Kommando (z.B. als Dateiname), filtert aber Metazeichen nicht richtig aus
   - Triviales Beispiel: system("cp $tempfile $target").
     $target ist Benutzereingabe und enthält "meinbild.jpg; rm –rf /"
   - Herkunft: Entwurfs- oder Konfigurationsfehler

5. (Es gibt noch einige andere, eher seltenere Typen)

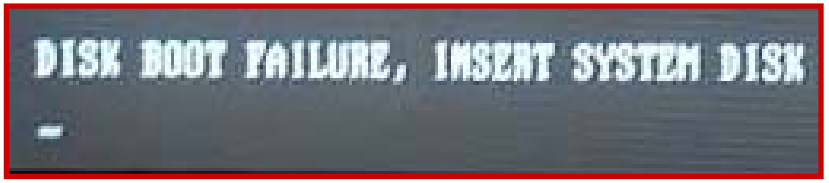
Quellen:

- http://www.owasp.org
- http://www.sans.org/top-cyber-security-risks/?ref=top20

3. Arten von Schadkomponenten

Freie Universität Berlin

- Daten ausspionieren ("Spyware")
  - Insbes. Passwörter, Konto-/Kreditkartennummern u.ä.
  - Bei Wirtschafts- und Staatsspionage aber auch Nutzdaten
- Rechner fernsteuerbar machen ("Bot-Armee")
  - Rechner nimmt dann übers Netz Aufträge des Angreifers entgegen und verschickt z.B. Spam oder macht bei Dienstverweigerungs-Angriffen mit (denial-of-service attack)
- Daten zerstören
  - früher häufig: Bootblock löschen



- Daten verfälschen
  - eher selten. Ausnahme:
- Erpressung ("Ransomware")
  - Benutzerdateien verschlüsseln, Schlüssel gegen Geld verraten
- Dienstverweigerung
  - z.B. Rechner stürzt immer wieder ab

Sozio-technische Schutzmaßnahmen

Freie Universität Berlin

Als Ergänzung für die digitale Datenwelt:

- Authentizität: persönliche Bekanntschaft
- Integrität: Plausibilitätsprüfung, ggf. Rückfrage
- Verfügbarkeit:
  - Rückfallkanäle (z.B. Brief, Telefon)
  - informelle Redundanz (Kopien streuen)
  - Abschwächung oder Umgehung von Zugriffsschutzmechanismen
- Vertraulichkeit: Kulturelle Schranken (Privatsphäre u.ä.)
- Verbindlichkeit: Kulturelle Schranken (Ehrlichkeit)

Spannungsverhältnis Schutz/Verfügbarkeit

Wichtig!

1. Alle schützenden Eigenschaften erschweren die Verfügbarkeit
   - Authentisierung, Verschlüsselung, Signatur sind alle anfällig für Schwierigkeiten
   - Wenn beides sehr wichtig ist, wird der Entwurf schwierig!
     - Drastisches Beispiel: Abschuss von Atomraketen
     - http://www.crypto.com/blog/titans
2. Angriffe sind bei sicheren Systemen eher selten

⇩

- Deshalb werden öfter diejenigen sozialen Mechanismen eingesetzt, die die *Verfügbarkeit* stützen
  - "Hm, die Technik ist mal wieder im Weg. OK, ich helfe Ihnen..."

⇩

- Das wiederum kann ein Angreifer ausnutzen: **Social Engineering**

Social Engineering

Freie Universität Berlin

- Social Engineering ist ein von Menschen an Menschen durchgeführter Angriff auf Informatiksysteme (u.a.)

- Er zielt hier auf die Herausgabe wichtiger Informationen
  - z.B. Passwörter
  - oft über erhebliche Umwege, viele Angriffsschritte

- Er basiert darauf, eine Berechtigung zu suggerieren, die gar nicht wirklich gegeben ist
  - Eine Variante des Betrugs

Video dazu (ca. 8 Minuten)

Rechtliche Grundlagen: Betrug

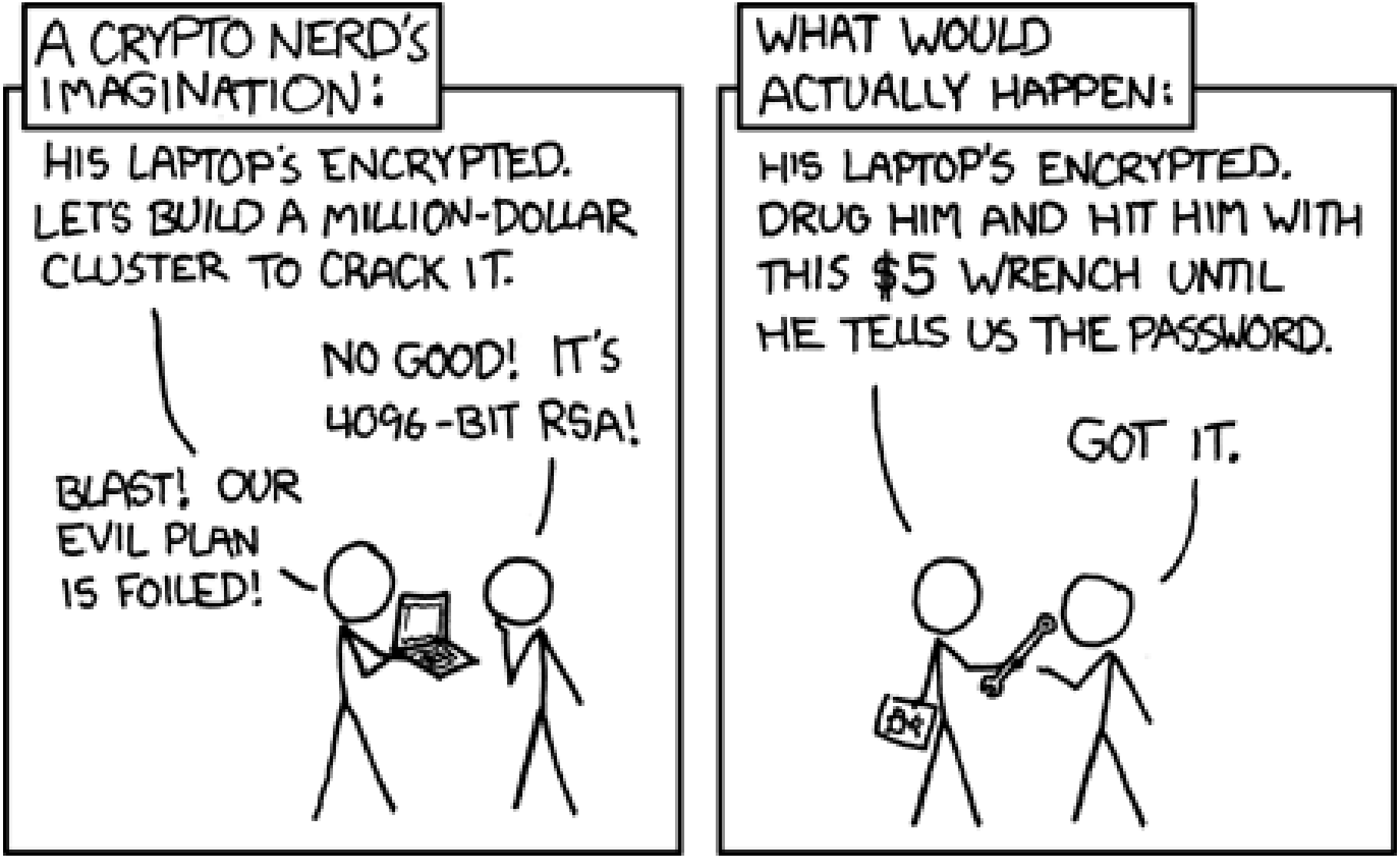
- §263 StGB (Betrug):
  - "Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, daß er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält"
    - Freiheitsstrafe bis 5 Jahre, Geldstrafe
- §267 StGB (Urkundenfälschung):
  - "Wer zur Täuschung im Rechtsverkehr eine unechte Urkunde herstellt, eine echte Urkunde verfälscht oder eine unechte oder verfälschte Urkunde gebraucht"
    - Freiheitsstrafe bis 5 Jahre, Geldstrafe
- Der Versuch ist strafbar

Rechtliche Grundlagen: Computersabotage

Freie Universität Berlin

- §303a StGB (Datenveränderung):
  - "Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert"
    - Freiheitsstrafe bis 2 Jahre, Geldstrafe
- §303b StGB (Computersabotage):
  - Beschädigung von Daten, Datenträgern, Computeranlagen
  - "Handelt es sich um eine Datenverarbeitung, die für [...] ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ..."
    - Freiheitsstrafe bis 5 Jahre, in besonders schweren Fällen bis 10 Jahre
- Der Versuch ist strafbar

(Mit Gewalt geht's noch einfacher):



Ausblick: Datenschutz

Was wir hier noch weitgehend ignoriert haben:

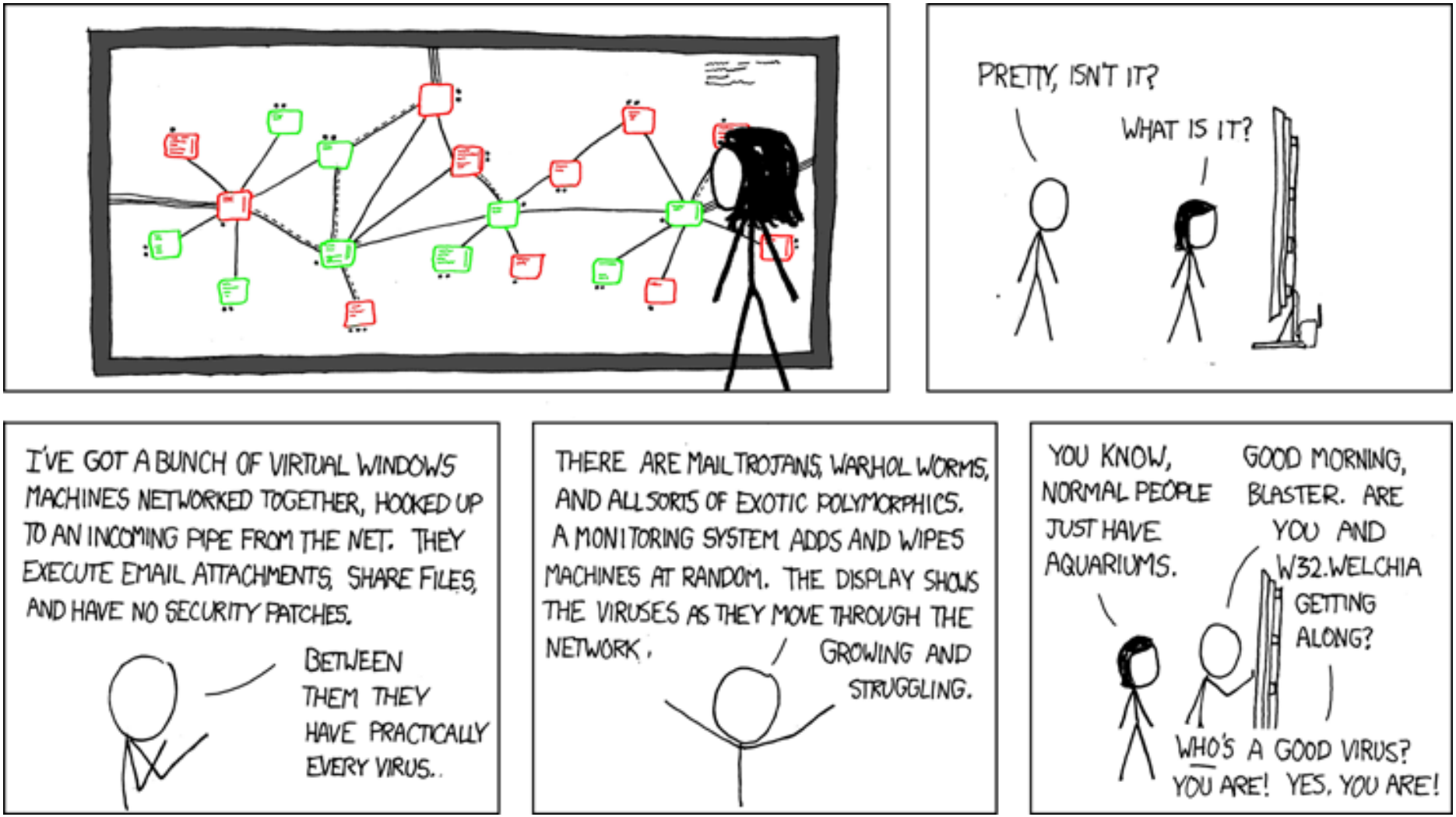
- Vertraulichkeit betrifft nicht nur Inhaltsdaten
  - Schon allein die Tatsache, dass Alice überhaupt etwas an Bob geschickt hat (Verkehrsdaten), kann der Vertraulichkeit bedürfen

- Vertraulichkeit betrifft manchmal nicht pauschal die Daten, sondern nur manche (oder fast alle) ihrer Verwendungen
  - z.B. soll meine Apothekerin wissen, dass ich Fußpilz habe, bis sie mir ein Fußpilzmittel verkauft hat – und soll es dann wieder vergessen
  - Mein Name ist dabei allenfalls für eine Versandapotheke relevant

➔ **Datenschutz** siehe nächste 2 Stunden

Danke!

xkcd



http://xkcd.com/350/