Betriebssysteme und Sicherheit – Sicherheit

Einführung Sicherheit

About Myself

- Temporary professor (Lehrstuhlvertreter) at the chair of privacy and data security
- 10 years experience
- Still with SAP in Security & Trust Research
- Main expertise: „Applied Cryptography“
  - Secure Multi-Party Computations
  - Security of business applications

About the Chair

- Staff
  - ~5 Assistants (PostDocs)
  - ~2 PhD
- Strong reputation and profile in privacy
  - Anonymous Communication
    - Projects AN.ON, JAP
- Courses Offered
  - 5 lectures (including this one)
  - 2 seminars
  - 3 praktika
- Bachelor, master, diploma thesis topics !!

Literature

- **Slides**
- In the library
  - Charles P. Pfleeger, Shari Lawrence Pfleeger. Security in Computing. 4th edition. Prentice Hall, 2006.
  - Matt Bishop. Computer Security: Art and Science. Addison-Wesley, 2002.
  - Bruce Schneier. Applied Cryptography. 2nd edition. John Wiley & Sons, 1996.
  - Douglas Stinson. Cryptography Theory and Practice. 3rd edition. CRC Press, 2005.
- Online
  - Ross Anderson. Security Engineering. http://www.cl.cam.ac.uk/~rja14/book.html
  - Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Cryptography. http://www.cacr.math.uwaterloo.ca/hac/. Copyright!

Terms

- **Privacy**: Protection of human beings against misuse of their person related data
- **Data Security**: Protection of data (and its processing) against unauthorized access and deletion

Terms II

- **Security**: Protection against an adversary who purposefully attacks data
- **Safety**: Protection against technical and human failure

Goals of Data Security

- Confidentiality
  - Data must be only made available to authorized persons or systems
- Integrity
  - Data is correct, complete and current
  - Data must be only modified by authorized persons or systems
- Availability
  - Data must be accessible, when needed

Confidentiality

- „Need to know“ or „Need to access“ basis
- Hard to prevent, but easy to check (binary yes/no)
- Can be prevented, but cannot be undone

Integrity

- Concerned with modification
- More difficult to measure
  - Context-dependent
  - Leads into availability (deletion)
- Cannot be prevent (in general), but can be undone

Availability

- Implies „timely“ availability
- Not completely understood yet
- We can say available, if
  - Timely request response
  - Fair allocation of resources (no starvation!)
  - Fault tolerant (no total breakdown)
  - Easy to use in the intended way
  - Provides controlled concurrency (concurrency control, deadlock control, ...)

Case Study

- Case: Sending an e-mail over the Internet
- Threats to
  - Confidentiality
  - Integrity
  - Availability

Threats

- Interception
  - an unauthorized party (human or not) gains access to an asset
- Interruption
  - an asset becomes lost, unavailable, or unusable
- Modification
  - an unauthorized party changes the state of an asset
- Fabrication
  - an unauthorized party counterfeits an asset

Defenses

- Prevent attack
  - Block attack / Close vulnerability
- Deter attack
  - Make attack harder (can't make it impossible?)
- Deflect attack
  - Make another target more attractive than this target
- Detect attack
  - During or after
- Recover from attack

Why Data Security?

- Social Importance
  - Privacy
- Economic Importance
  - Risk

Privacy

- Privacy is a basic human right
- Implementation of privacy in an electronic world
  - Informational self-determination
    - Appropriation (purpose binding)
    - Approval
    - Necessity

Privacy Enforcement

- Why is a legal regulation not enough?
  - Technical limits
    - Privacy/Confidentiality breach cannot be undone
      - „The Internet does not forget“
  - Legal limits
    - Prosecution requires proof
      - Whistle blower

Technical Privacy

- Data Minimization Principle
  - Only necessary data should be collectable
- Relation to confidentiality
  - Data remains secret to owner / origin
- Verifiability
  - Adversary model $\rightarrow$ Data Security

Risk Analysis

- Identication of potential threats
- Financial assessment of threats
- Determination of protection mechanisms

Risk Analysis Approach

- What is to be protected?
  - Identification of (also immaterial) assets
- What are potential threats?
- What is the potential damage?
- What is the probability of occurrence?

Assessment

- Risk: Forgery of e-mail sender
- Damage: x EUR
- Probability of Occurence: y %
- Assessment $x \cdot y/100$

Why is it so difficult?

- How do you assess damage to immaterial assets?
- How do you assess probability of occurence?
  - Prior experience
  - „Build security in from the start“

Assessment of Protection Mechanism

- Assessment without protection x EUR
- Assement with protection y EUR
- Cost of protection z EUR
- Savings by mechanism x – y – z EUR

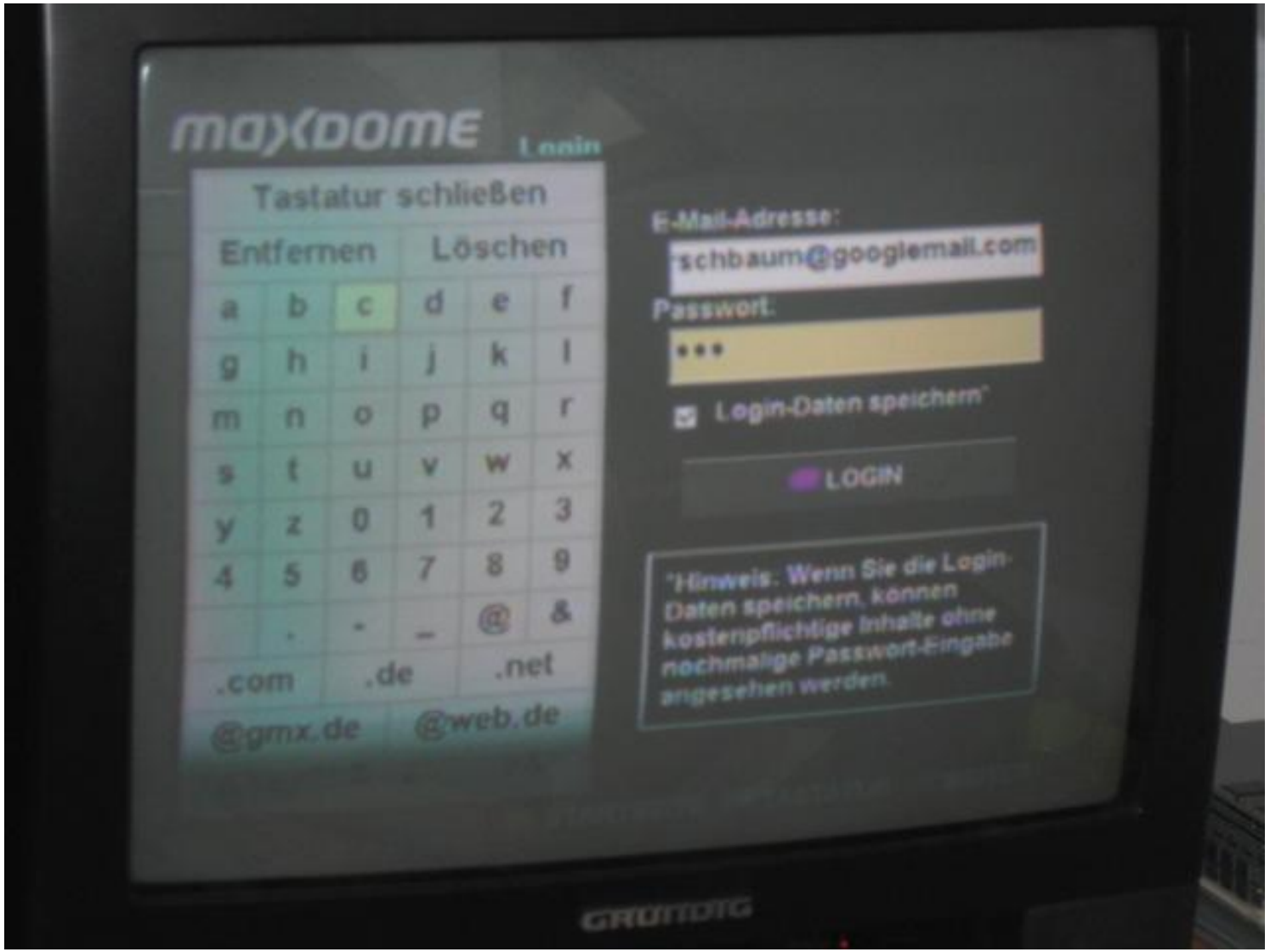
How do we assess effectiveness?

- What path will the attacker take?
  - Easiest penetration principle
  - Weakest link
- Given two protection mechanisms for the same threat does their effect add up?
  - In general no; Composition is difficult

Example I

Source: Bruce Schneier‘s Blog

Example II


maxdome
Login
Tastatur schließen
Entfernen
Löschen
a b c d e f
g h i j k l
m n o p q r
s t u v w x
y z 0 1 2 3
4 5 6 7 8 9
. - _ @ &
.com .de .net
@gmx.de @web.de
E-Mail-Adresse:
schbaum@googlemail.com
Passwort:
Login-Daten speichern
LOGIN
Hinweis: Wenn Sie die Login-Daten speichern, können kostenpflichtige Inhalte ohne nochmalige Passwort-Eingabe angesehen werden.
GRUNDIG

Dealing with Risk

- Reduce
  - Development of protection mechanisms
- Avoid
  - Redesign system
- Transfer
  - Insurance
- Bear