Vorlesung Datensicherheit

WS 2002/2003

Dr. Frank Bourseau

Dr. Jens Fricke

Personalia

- Dr. Frank Bourseau
- Studium der Mathematik und Physik
- Diplom und Promotion in Mathematik an der Universität Bielefeld
- Danach Berater im Datenbankbereich
- Seit 3 1/2 Jahren im IT-Sicherheitsbereich
- Seit 1. Jan. 2002 bei der dvg Hannover

Personalia

- Dr. Jens Fricke
- Studium der Physik und Mathematik
- Diplom und Promotion in Physik an der Universität Göttingen
- Seit 1998 Systementwickler und IT-Sicherheitsberater
- Seit 1. Feb. 2001 bei der dvg Hannover

Inhalt der Vorlesung (1)

- Kapitel 1: Sicherheitsmanagement
  - Bedrohungen und Risiken
  - Standards und Vorgehensweisen
- Kapitel 2: Kryptographie
  - Symmetrische Kryptographie
  - Hash Algorithmen, Message Digests
  - Public Key Kryptographie

Inhalt der Vorlesung (2)

- Kapitel 3: Netzwerksicherheit
  - Überblick über TCP/IP
  - Sichere elektronische Kommunikation (Email, IP, Web)
  - Firewalls
- Kapitel 4: Authentifizierung
  - Passwörter
  - Token
  - Biometrische Verfahren
  - Kerberos

Sicherheitsmanagement

- Kapitel 1: Sicherheitsmanagement
  - Bedrohungen und Risiken
  - Standards und Vorgehensweisen

Heise News Ticker 23.10.02

Heise News Ticker 23.10.02

Sicherheitsmanagement

- Sicherheitsbegriff
- Schwachstellen, Bedrohungen, Risiko
- Sicherheitsstandards
- Policies, Sicherheitsmanagement
- Praxisbeispiele

Sicherheitsbegriffe

- Datensicherung (Backup)
  - Schutz vor Datenverlust
- Datenschutz (Privacy)
  - Kontrollierte Weitergabe personenbezogener Informationen, informationelles Selbstbestimmungsrecht, Anonymität
- Informations-Sicherheit (Security)
  - Maßnahmen zur Abwehr von Bedrohungen auf ein System und Informationen
- Betriebssicherheit, passive Sicherheit (Safety)

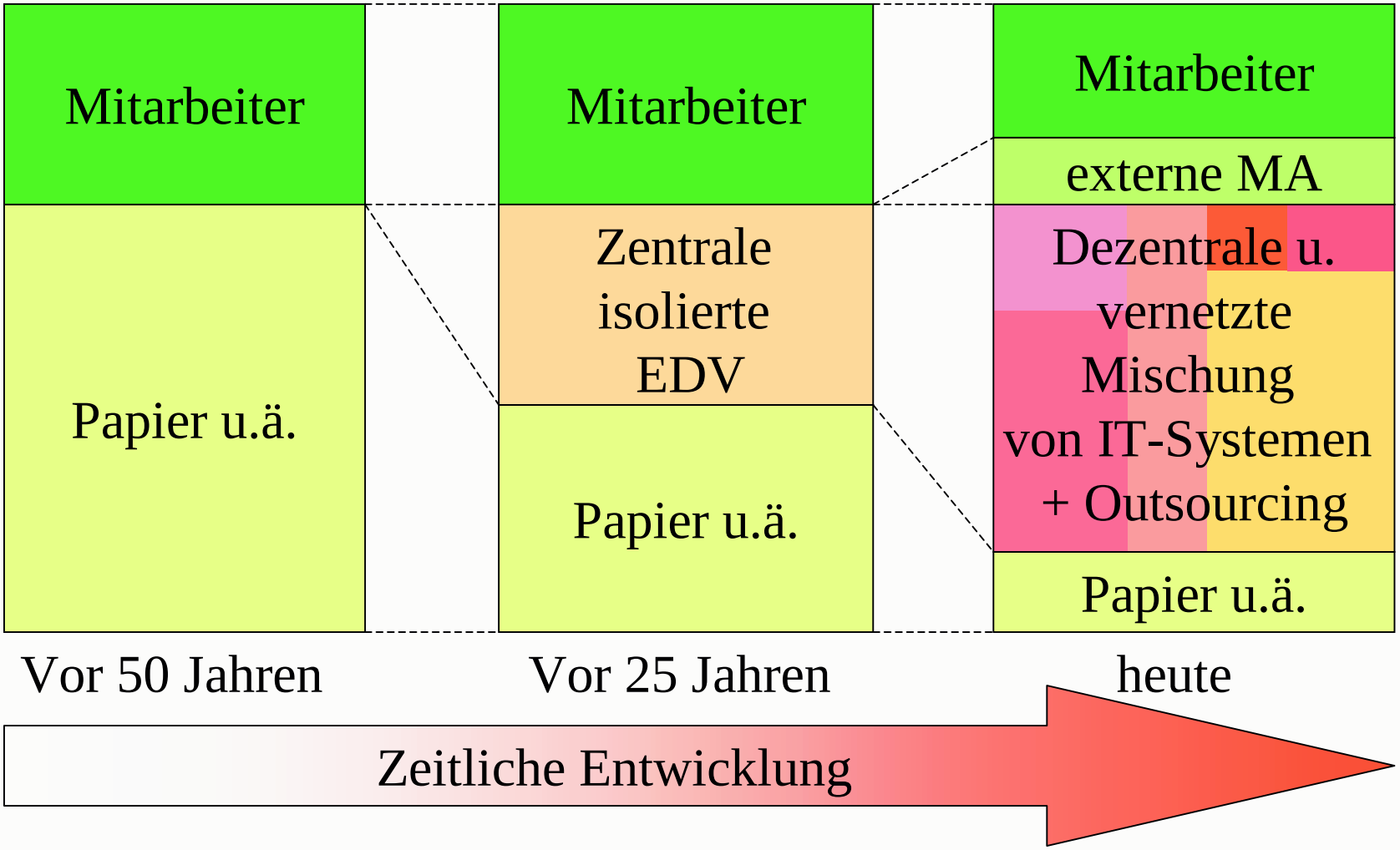
Was ist Sicherheit? (1)

- Ist es sicher zu fliegen?
- Jedes komplexe System hat Schwachstellen (Cockpittüren offen)
- Bedrohung: Flugzeugentführung
- Risiko = Bedrohung x Wahrscheinlichkeit für Eintritt

Was ist Sicherheit? (2)

- Subjektive Größe
- Vom Betrachter abhängig
- Nicht direkt sicht- oder messbar
- Idealerweise bleibt sie unbemerkt
- Schwer zu „verkaufen“
- 100% Sicherheit nicht erreichbar

Informationsverteilung



Die Herausforderungen

- Sicherheitsadministration
- Zunahme von technischen Sicherheitslösungen
- Rechte- und Rollenverwaltung
- Verschiedenste Plattformen
- Zunahme von Schnittstellen
- Externe und interne Prüfungen
- Gesetzliche Anforderungen
- Finanzielle Bewertung von Sicherheitsmaßnahmen, Kostenfaktor?
- Risikoabschätzungen
- ...

Was ist z.B. zu bedenken?

Spionage

Loss of Reputation

Rechtliche (Geschäftsführer-)Haftung

Hintertüren

Viren

Cracker

Social Engineering

Datenintegrität

Spoofing

Softwarepflege

Denial of Service

Datenschutz

Erpressung

Datendiebstahl

Geschäftsgeheimnisse

Verfahrensfehler

Vertraulichkeit

Trojanische Pferde

Verschlüsselung

IT-Sicherheit

- Sicherheit der Informationstechnik?
- Was ist das schützenswerte Gut, die Informationstechnik?
- Nein: Zu schützen sind Informationen und zwar vor Diebstahl, Veränderung, Abstreitbarkeit, etc.
- Da viele Informationen innerhalb von Technik verwaltet, übertragen, gespeichert werden, spielt Technik eine entscheidende Rolle.
- Genauso wichtig sind z.B. Menschen und ihr Sicherheitsbewusstsein!

Sicherheitsbewusstsein (1)

- Als Bill Clinton das US-Signaturgesetz ratifizierte, unterschrieb er in aller Öffentlichkeit elektronisch mit seinem Passwort „Buddy“.
- Wenigen ist bewusst, dass Email (ohne Zusatzfunktion) keinerlei Sicherheit bietet.
- Passwörter werden unter Tastaturen notiert.
- Passwörter werden zu einfach gewählt.
- Sicherheit wird als Hindernis empfunden.

Sicherheitsbewusstsein (2)

- Eine Vielzahl der möglichen Gefährdungen ist nur mit bewusster oder unbewusster „Unterstützung“ der Mitarbeiter möglich.
- Das Management und die Mitarbeiter müssen die Risiken ihrer Aktionen erkennen können.
- Ein angemessenes Sicherheitsbewusstsein ist die Basis jeder Sicherheitsmaßnahme.
- Wertewandel erforderlich.

Schutzziele

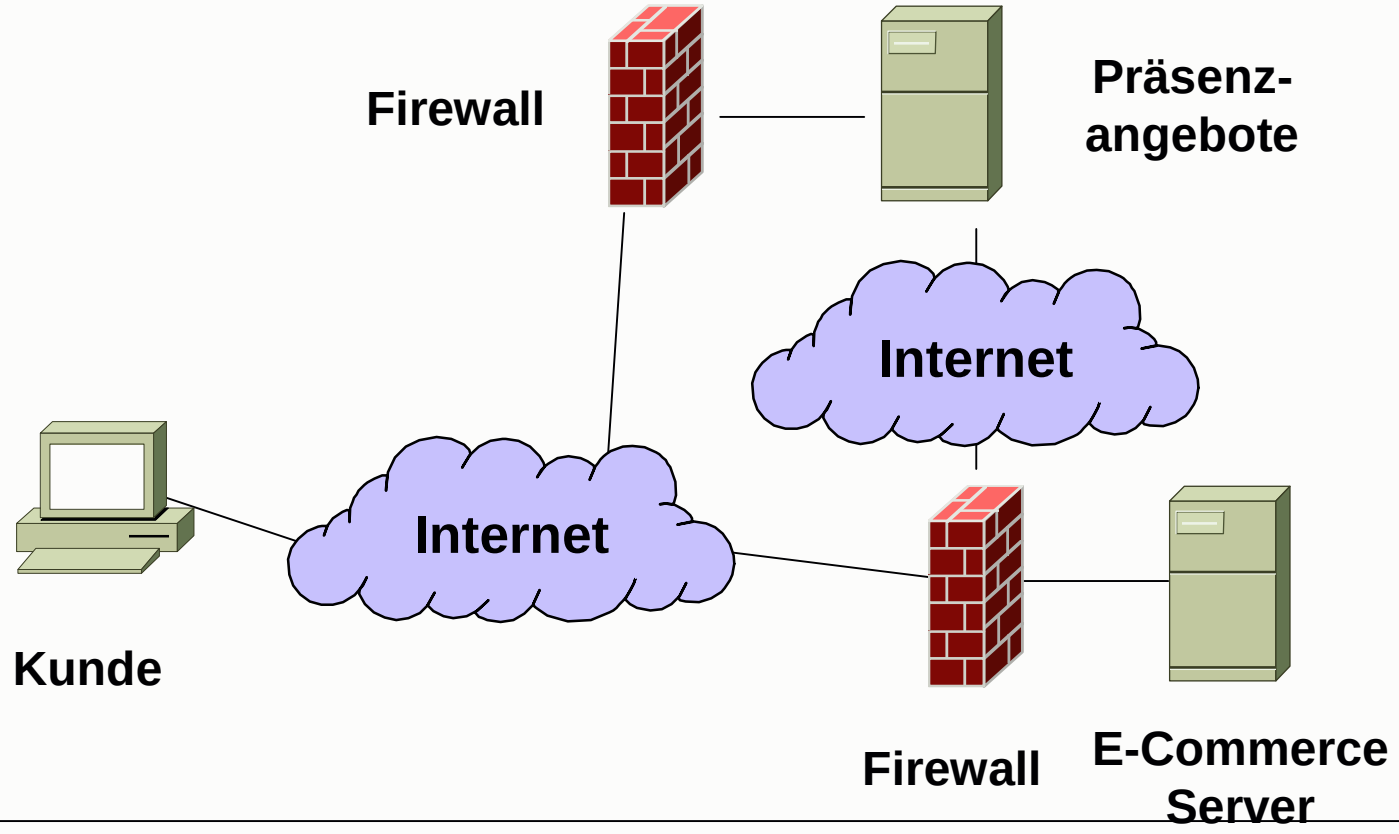
- Informationsintegrität
  - Schutz vor unautorisierter und unbemerkter Modifikation von Daten
- Informationsvertraulichkeit
  - Schutz vor unautorisierter Informationsgewinnung
- Verbindlichkeit
  - Schutz vor unzulässigem Abstreiten durchgeführter Handlungen
- Verfügbarkeit
  - Schutz vor unbefugter Beeinträchtigung der Funktionalität von Komponenten

Widersprüche?

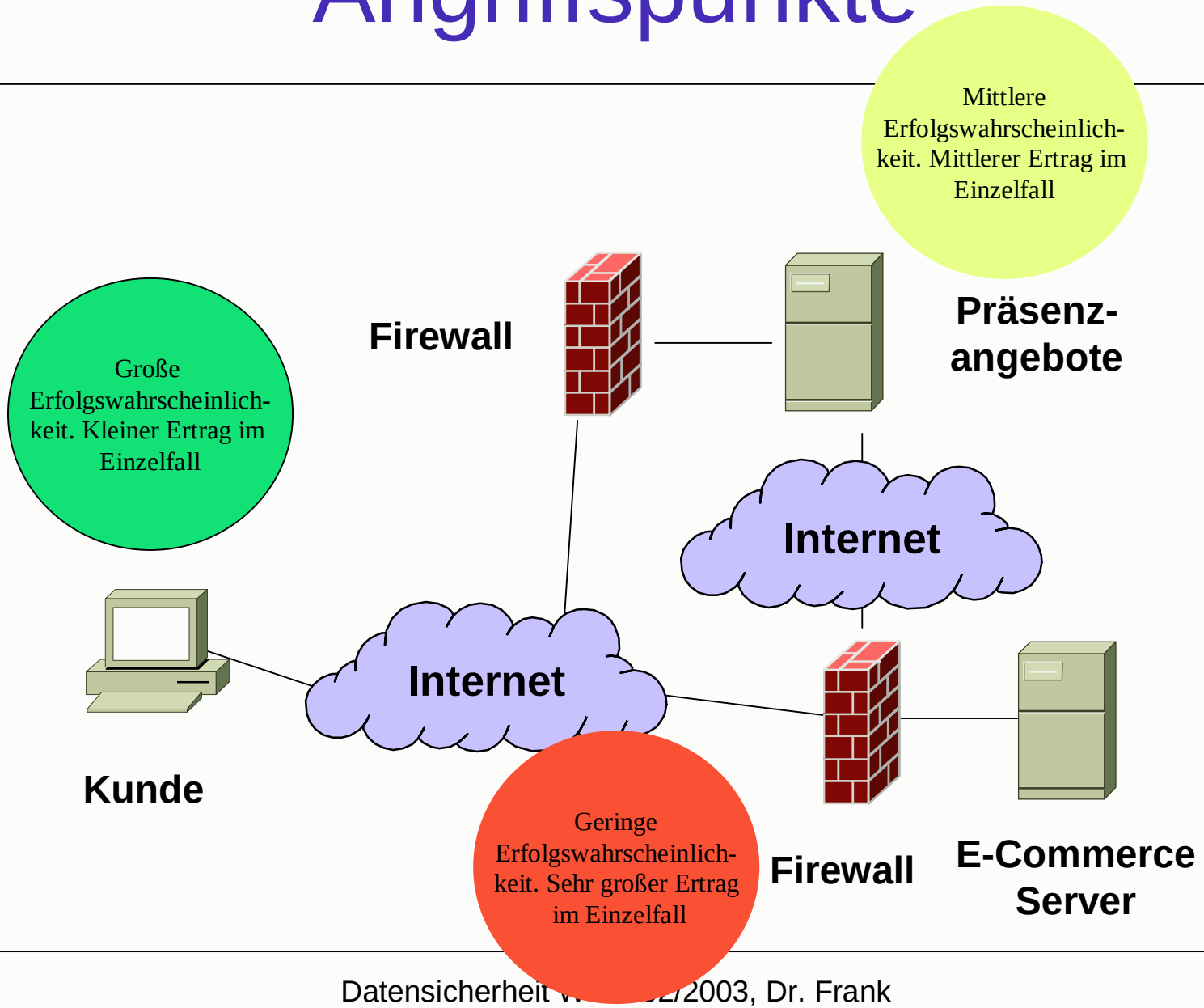
- Vertraulichkeit vs. Verfügbarkeit
  - Angenommener Schadensfall: Hacker im System
  - Abwägung zwischen Abschalten des Systems (Vertraulichkeit vor Verfügbarkeit) oder Weiterbetrieb (Verfügbarkeit vor Vertraulichkeit)
- Integrität vs. Vertraulichkeit
  - Dürfen Mitarbeiter verschlüsselte Kanäle aus dem Unternehmen benutzen (SSL, PGP, S/MIME) oder müssen alle Inhalte kontrolliert werden?
  - Wie sind diese Ziele vereinbar?
- Jedes Unternehmen muss eigenen Weg festlegen.
  → IT-Sicherheitsziele und -politik

Sicherheit ist komplex!

Z.B. angenommenes praktisches Szenario:
E-Commerce- und weiterer Internet-Auftritt
bei verschiedenen Web-Hostern:

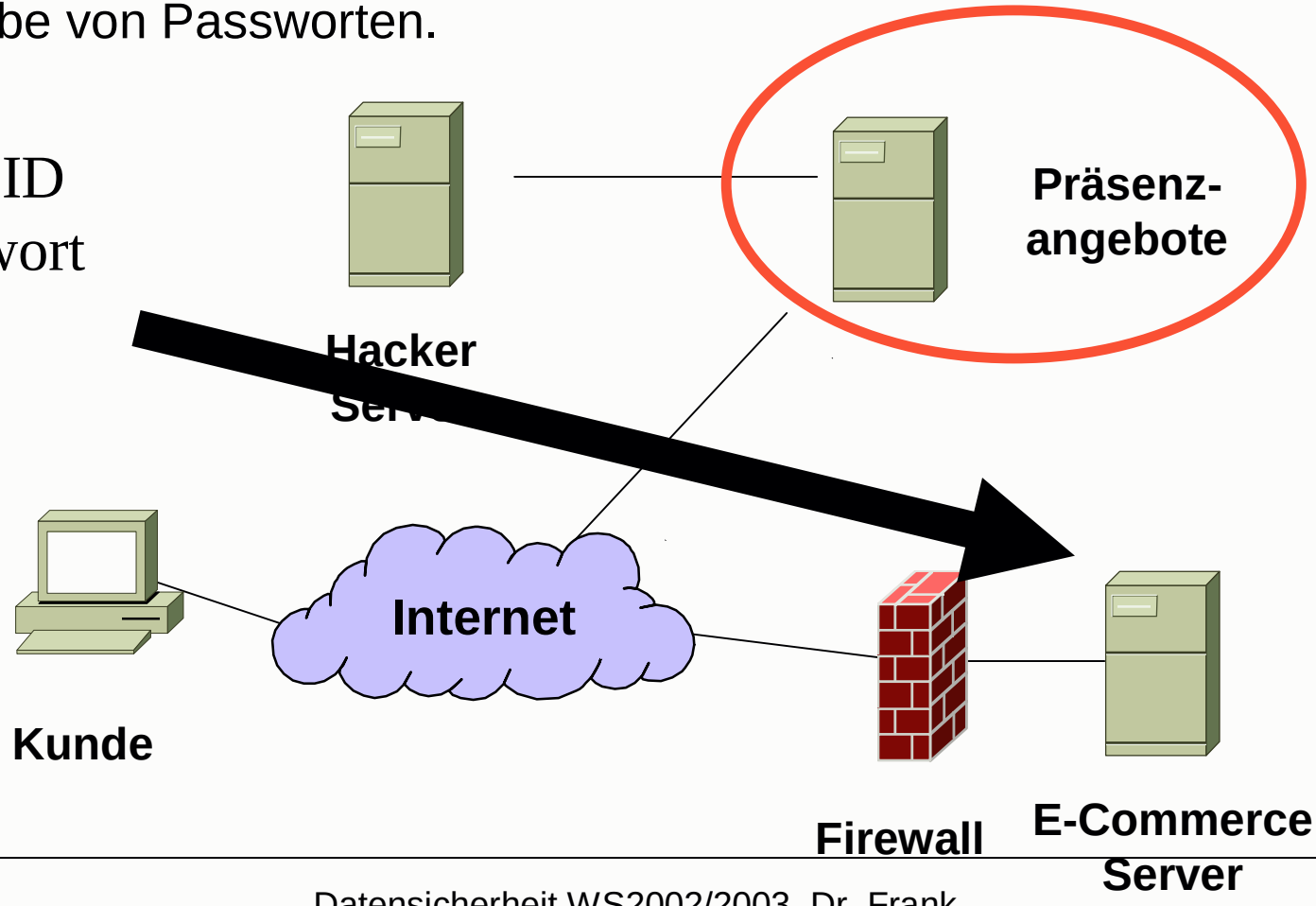


Angriffspunkte



Mögliches Szenario

Hacker übernehmen nicht direkt E-Commerce Server, sondern den weniger gesicherten Werbe-Auftritt und verleiten arglose Kunden zur Eingabe von Passworten.



Schwachstelle

- Verwundbarkeit, Mangel in einem System
- Beispiel Technik
  - E-Mail wurde nur zur Kommunikation im Rechenzentrum entworfen.
- Beispiel Mitarbeiter
  - Notieren sich Passwörter unter Tastatur.
- Führt aus sich selbst heraus noch nicht zu einem Schaden.

Bedrohung

- Umstand, der unter Ausnutzung einer Schwachstelle zu einem Schaden führt.
- Beispiel Technik
  - Abfangen von Emails mit Angeboten durch eine Konkurrenzfirma und Unterbieten
- Beispiel Mitarbeiter
  - Unzufriedener Mitarbeiter manipuliert Personalakten o.ä.

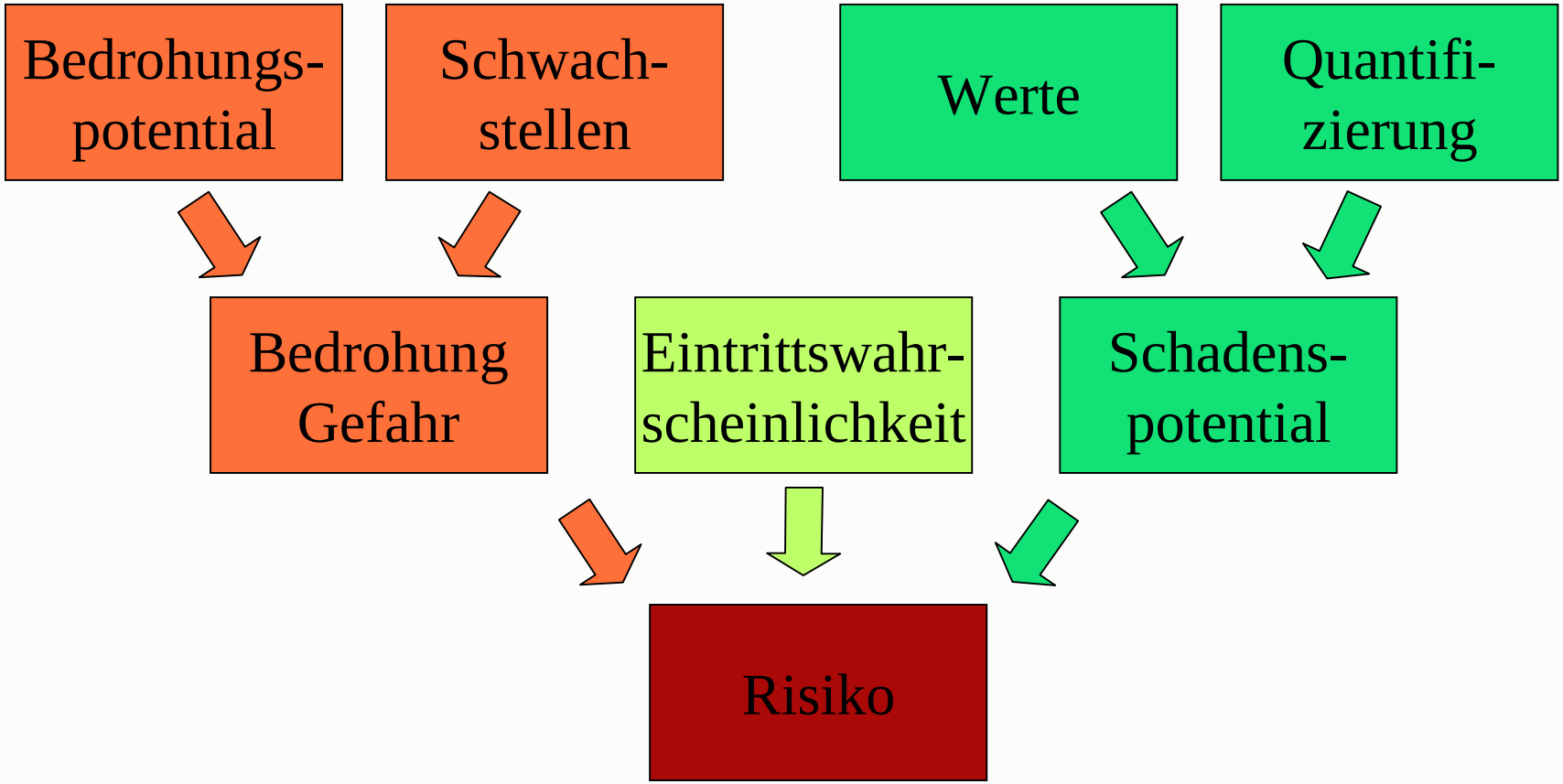
Bedrohungen

- Passive Angriffe, z.B. Abhören von Datenleitungen, Sniffer Attack
- Aktive Angriffe, z.B. Modifizieren, Replay, Spoofing, Denial of Service
- Absichtliches oder unabsichtliches Fehlverhalten
  - z.B. Programmierfehler: Absicht oder Versehen
- Bedrohungen sind nur schwer erkennbar.

Angreifer

- Über 50% aller bekannten Angriffe erfolgen durch Mitarbeiter
  - Mangelhafte Kenntnisse, Bereicherung, Frust, Fahrlässigkeit
  - Ehemalige Mitarbeiter, deren Accounts nicht gelöscht werden
  - Bekannte Administratorenzugänge
- Hacker, systematische Zerstörung, Spieltrieb
- Wirtschaftsspionage, Geheimdienste
  - Z.B. Echelon-System der National Security Agency (NSA)

Risikoanalyse

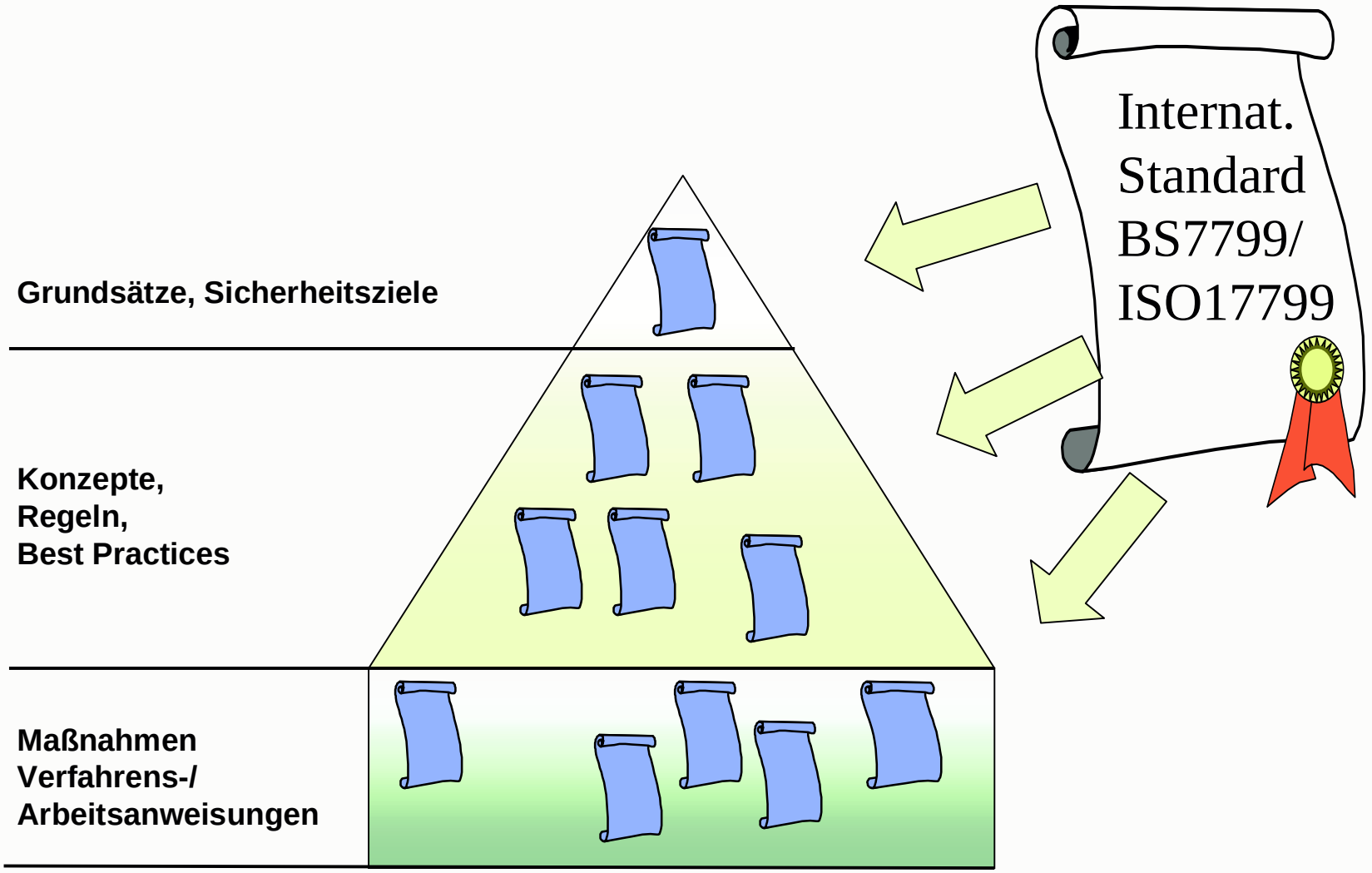


Risiko = potentieller Schaden x Eintrittswahrscheinlichkeit

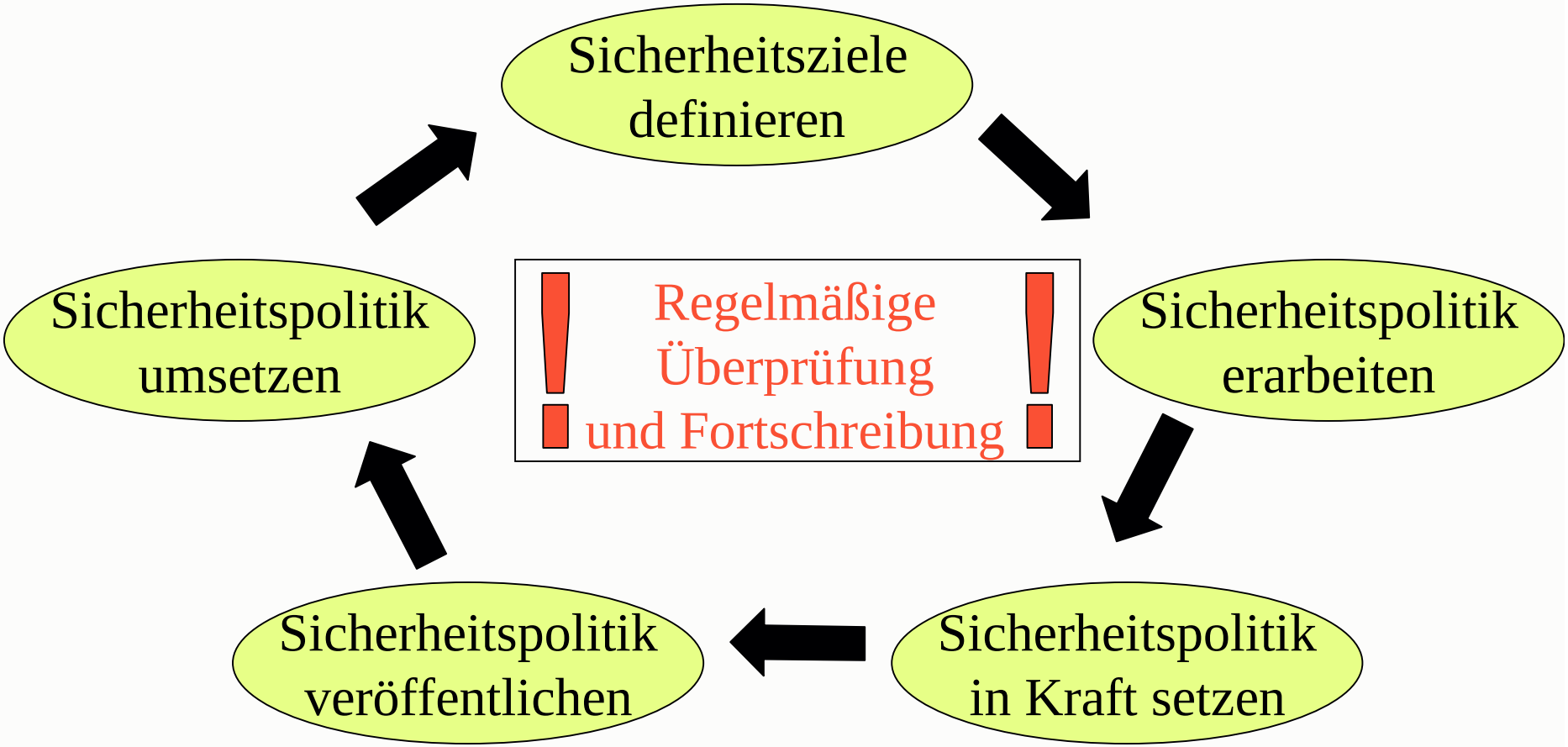
Sicherheitsstrategie (Sec. Pol.)

- Festlegung der Schutzziele
  - Z.B. Vertraulichkeit der Kundendaten
  - Z.B. Verfügbarkeit des Web-Auftritts
- Regeln und Maßnahmen zur Gewährleistung des Erreichens der Schutzziele
  - Rahmenbedingungen (Gesetze, Richtlinien)
  - Organisatorische Maßnahmen (Rollentrennung, Clean Desk)
  - Technische Maßnahmen (Verschlüsselung, Firewalls)

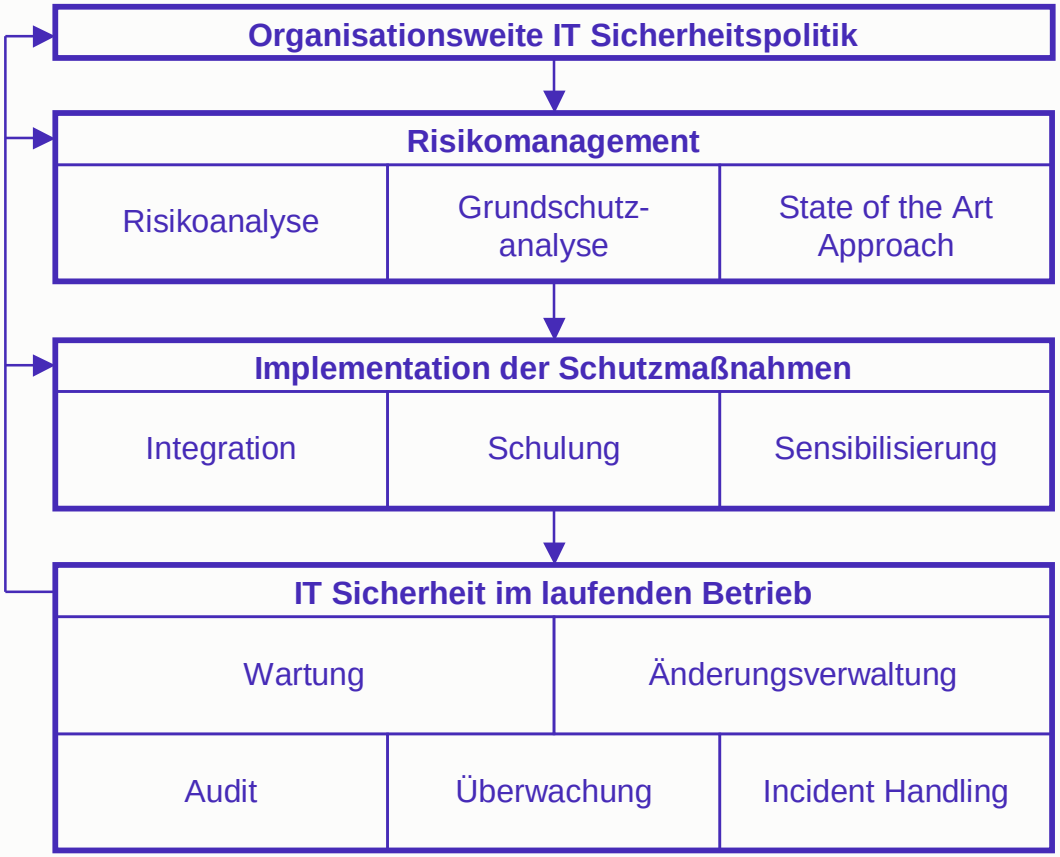
Sicherheitspolicies



Weiterentwicklung

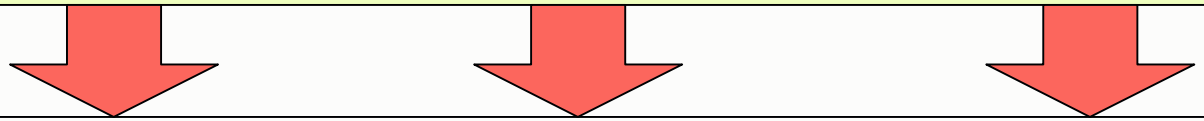


Der IT-Sicherheitsprozess



Gesetze, Regeln etc.

- KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich)
- „Basel II“ (s. nächste Folie)
- MaIT (Mindesanforderungen an die IT, Bundesamt für Finanzdienstleistungsaufsicht)
- ...



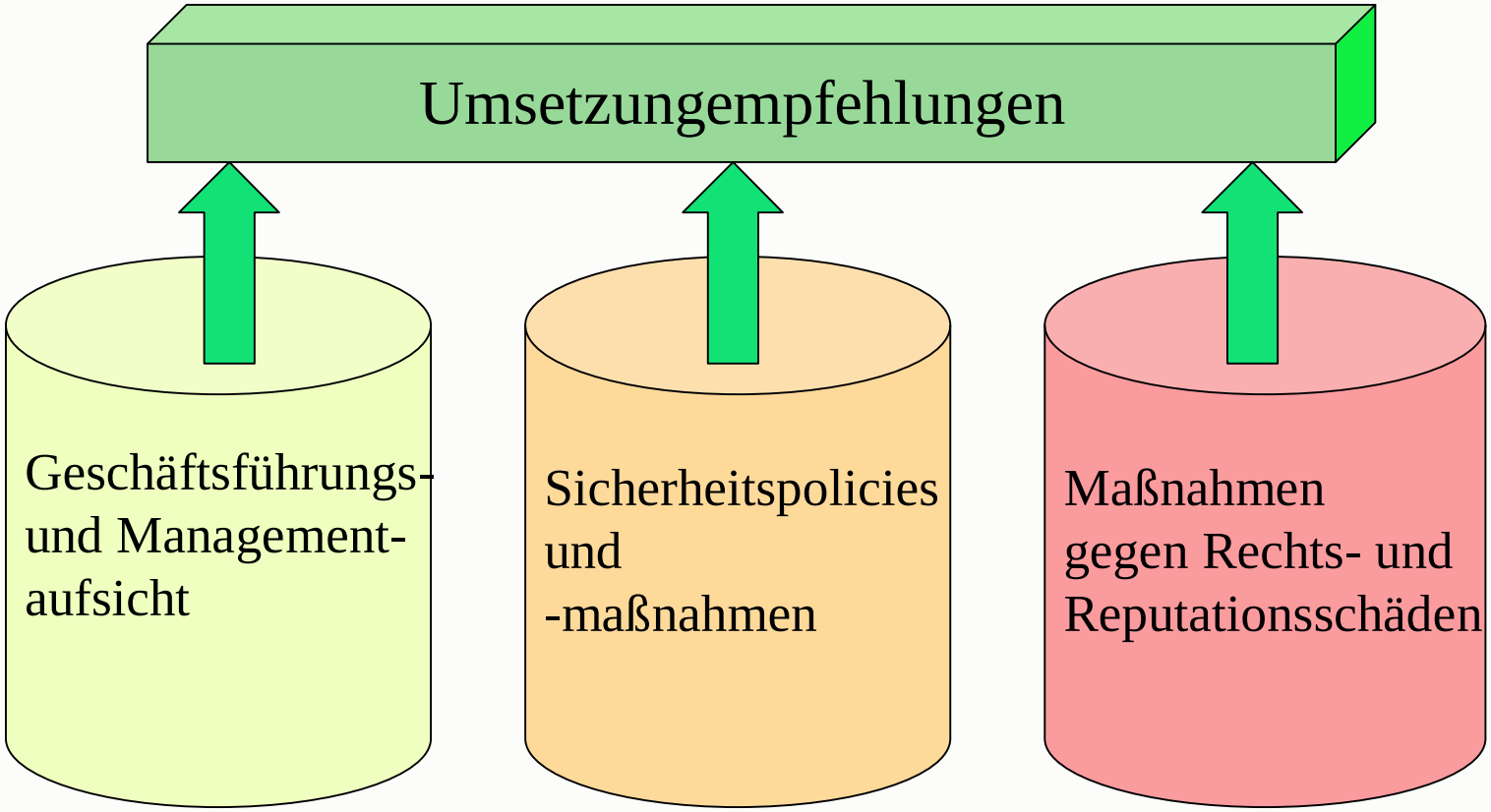
- Geschäftsführungsverantwortung
- Sicherheitspolitik
- Sicherheitsorganisation
- Risikoanalyse und -management
- Katalog technischer und organisatorischer Sicherheitsmaßnahmen

„Basel II“ für Banken (1)

- Basler Ausschuss für Bankenaufsicht = Zentralbanken der G10 + ESP + LUX
- Basel I = Basler Eigenkapitalvereinbarung von 1988
  - Rahmen zur Messung des Kreditrisikos
  - Mindestkapitalanforderungen
  - Rechtlich unverbindlich
  - Umsetzung in rechtlich verbindliche EU-Richtlinie
- Basel II (neuer Entwurf voraussichtlich gültig ab 2005)
  - Mindeskapitalanforderungen (Eigenkapitalbedarf hängt direkt ab von Kredit- und **operationellen Risiken**)
  - Aufsichtliches Überprüfungsverfahren
  - Marktdisziplin (Weitgehende Offenlegungsverpflichtungen des eigenen Risikomanagements)

Basel II: Richtlinien (2)

Risikomanagement-Prinzipien für Electronic Banking



Managementaufgaben (3)

- Effektive Managementaufsicht über E-Banking Aktivitäten
- Etablierung eines Management-Kontrollsystems zur Überwachung der wesentlichen Sicherheitsprozesse einer Bank
- Etablierung eines nachhaltigen Überwachungsprozesses zum Management der Beziehungen zu Outsourcern und sonstigen Geschäftspartnern im E-Banking-Prozess

Policies und Maßnahmen (4)

- Angemessene Maßnahmen zur Authentisierung und Autorisierung
- Angemessene Maßnahmen zur Nicht-Abstreitbarkeit und Verfügbarkeit
- Angemessene Maßnahmen zur Trennung von Verantwortlichkeiten innerhalb von E-Banking-Systemen, Datenbanken und Anwendungen
  - Funktionstrennung zwischen Entwicklung und Administration
  - Test auf Umgehbarkeit von Funktionstrennungen
  - ...
- Schutz der Integrität
- Klare Auditrichtlinien
- Schutz der Vertraulichkeit

Rechts- und Imageschäden (5)

- Informationen zur Identifikation und den Regeln der Bank auf den Webseiten
- Einhaltung der Datenschutzrichtlinien
- Effektive Kapazitäts-, Wiederanlauf und Notfallplanung zur Aufrechterhaltung der Verfügbarkeit
- Angemessene Planung zur Reaktion auf unvorhergesehene Vorfälle, z.B. interne oder externe Angriffe auf E-Banking-Systeme

Umsetzungsempfehlungen (6)

- Sicherheitsprofile
- Sensitivitätsklassifizierung
- Zugangskontrollen zur Durchsetzung von Funktionstrennung
- Virus Scanning Software
- Intrusion Detection
- Penetrationstests
- Übereinstimmung der Policies des Outsourcers mit den eigenen
- Periodische Reviews aller Sicherheitsfunktionalitäten auch von Outsourcern
- ...

Standards

- Anwenderseitige Sicherheitsaspekte
- ISO/IEC TR 13335 1-5
- BSI IT Grundschutzhandbuch
- BS7799/ISO17799
- IT Infrastructure Library
- NIST Special Publication 800-12
- CoBit
- Canadian Handbook on IT Security
- IT Sicherheitshandbuch für die österreichischen Behörden

- Herstellerseitige IT Sicherheitsaspekte
- Orange Book
- ITSEC
- CommonCriteria
- FIPS 140

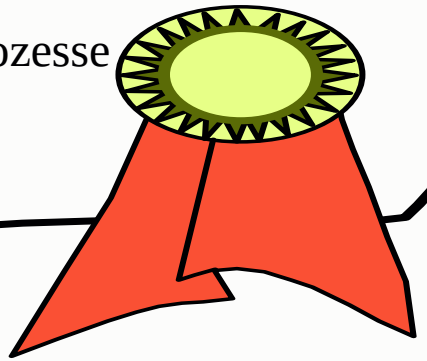
Wie können Standards helfen?

- Best Practice Ansätze liefern Vorgehensweisen zur Policyerstellung, Schwachstellenanalyse, Risikobewertung
  - BS7799 (ISO17799)
    - British Standards Institute (www.bsi-global.com)
    - Etablierung einer Sicherheitspolitik, Zertifizierungsmöglichkeit
  - ISO 13335
    - 5 Reports (Best Practice) zur Umsetzung der Sicherheitsstrategie (www.iso.ch)
  - „Grundschutzhandbuch“
    - Umfangreiche Maßnahmensammlung des deutschen BSI (www.bsi.de)
- Standards liefern Hilfestellung, umsetzen muss jedes Unternehmen eigenständig.

BS7799 (ISO 17799)

Maßnahmenkatalog nach BS7799

1. Sicherheitspolitik
2. Organisation der Sicherheit
3. Festlegung und Bewertung zu schützender Objekte und Prozesse
4. Physische Sicherheit und Infrastruktur
5. Netzwerk- und Systemmanagement
6. Personelle Sicherheit
7. Zugriffs- und Zugangskontrolle
8. Systementwicklung und -wartung
9. Aufrechterhaltung der Geschäftsprozesse
10. Einhaltung von Verpflichtungen (Compliance)



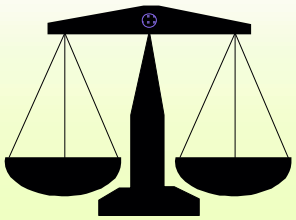
Security nach KISS-Prinzip

- Wer liest heutzutage mehrseitige „Gebrauchsanleitungen“?
- Auch Security verkauft sich nur nach KISS-Prinzip: „Keep it simple, stupid!“
- Sicherheitsarchitekturen und -standards sind etwas für Sicherheitsexperten, Prüfer, Revisoren, aber nicht für Anwender!
- Sicherheitsführer, -checklisten für den Alltag müssen kurz und prägnant sein: „Quick Manuals“ sind in.

Sicherheitsmanagement

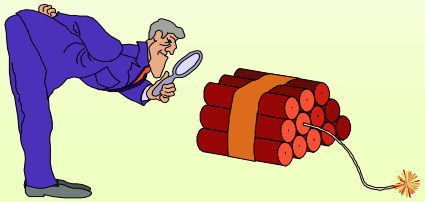
Gesetze, Normen Abkommen

§

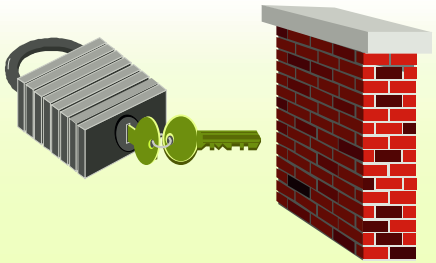


Sicherheits-ziele + -politik

Schwachstellenanalyse Risikobewertung Auditing



Sicherheitstechnik



Management-Attention, Organisation, Sensibilisierung

Return On Security Investment, Restrisiken

€

Sicherheitsmanagement ...

- fordert teure und hohe Sicherheitsanforderungen
- leitet punktuelle Sicherheitsmaßnahmen ein
- beschränkt sich auf Sicherheitstechnik
- stellt ein starres Regelwerk dar
- geht nur die Abteilung Sicherheit an
- reagiert nur auf offensichtliche Schwachstellen
- behindert den Wertschöpfungsprozess

- bewertet Bedrohungen und Risiken im Gesamtkontext
- leitet technische, organisatorische oder andere Maßnahmen zur Risikominimierung ein und berät bei deren Umsetzung
- passt sich Veränderungen im Unternehmen an und ist ein kontinuierlicher Prozess
- betrifft jeden Mitarbeiter
- sorgt für die Einhaltung eines stabilen Sicherheitsniveaus sowie gesetzlicher und sonstiger Anforderungen
- ist ein Business-Enabler

Kryptographie

- Kapitel 2: Kryptographie
  - Symmetrische Kryptographie
  - Hash Algorithmen, Message Digests
  - Public Key Kryptographie

Kryptographische Verfahren

- **Kryptographie**
  - Wissenschaft, die sich mit der Absicherung von Nachrichten beschäftigt.
- **Kryptoanalyse**
  - Kunst, Chiffretext aufzubrechen.
- **Kryptologie**
  - Zweig der Mathematik, der Kryptographie und Kryptoanalyse umfasst.
- **Steganographie**
  - Methode zum Verbergen der Existenz einer Nachricht.

Griechisch: steganos = verdeckt; kryptos = geheim; graphein = schreiben

Ziele der Kryptographie

- **Vertraulichkeit** (Confidentiality)
- **Datenintegrität** (Data integrity)
- **Authentifizierung** (Authentication) bzw. Authentizität
- **Verbindlichkeit** (Non-repudiation)

Bewertungskriterien:

Sicherheitsniveau, Funktionalität, Betriebsmethoden, Performanz, Leichtigkeit der Implementierung

Kryptographisches System

1. Menge von Klartextnachrichten M,
2. Menge von Chiffretextnachrichten C,
3. nicht-leere Menge von Verschlüsselungs-Schlüsseln EK,
4. nicht-leere Menge von Entschlüsselungs-Schlüsseln DK

   Bijektion $f : EK \rightarrow DK$, $f(k_E) = k_D$

Kryptographisches System

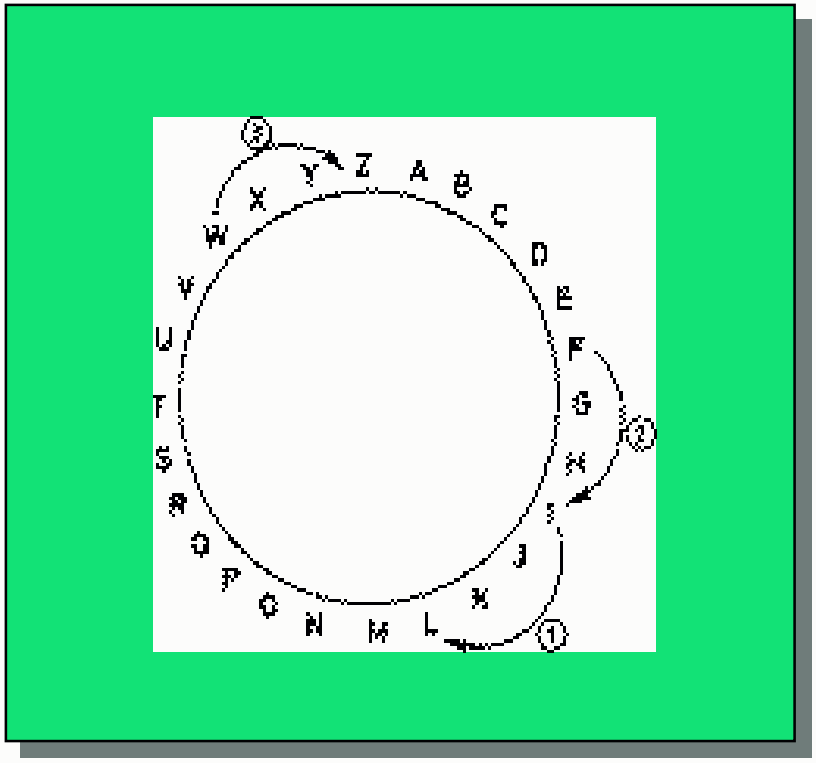
5. Verschlüsselungsverfahren
   E : M x EK → C, E(m,k) = c
   wobei E_k : M → C injektiv für jedes k∈ EK
   (auch $E_k(m)$ statt E(m,k))
6. und Entschlüsselungsverfahren
   D : C x DK → M, D(c,k) = m mit
   $D(E(m,k_E),k_D)) = m$ mit $f(k_E) = k_D$
   (auch $D_k(c)$ statt D(c,k))

Beispiel: **Caesar-Chiffrierung**
Verschieben der Buchstaben um
k Positionen nach rechts

Verschlüsselungsverfahren

Caesar-Chiffre:

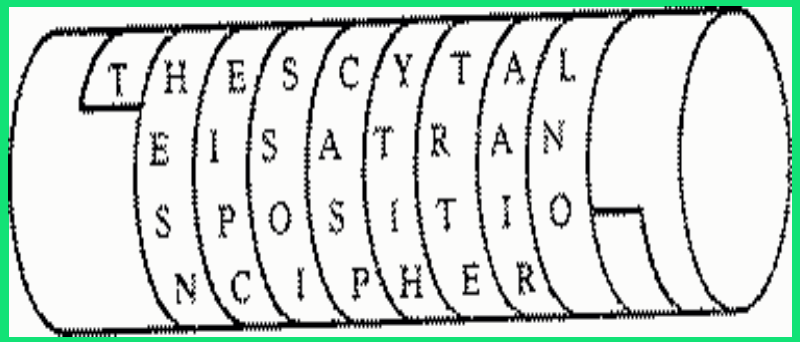
Prinzip der Substitution



Scytale Chiffre:

Prinzip der Transposition

oder Permutation



Kryptographische Systeme

- Symmetrische Verfahren (secret-key)
  - $k_E = k_D$, geheimer Schlüssel
  - Beispiele: DES (Data Encryption Standard), Blowfish, IDEA, RC2, RC4, RC5, AES (Advanced Encryption Standard, Rijndael)
- Asymmetrische Verfahren (public-key)
  - Öffentlicher (public) und privater Schlüssel (private key)
  - Bekanntestes Verfahren: RSA

Sicherheit

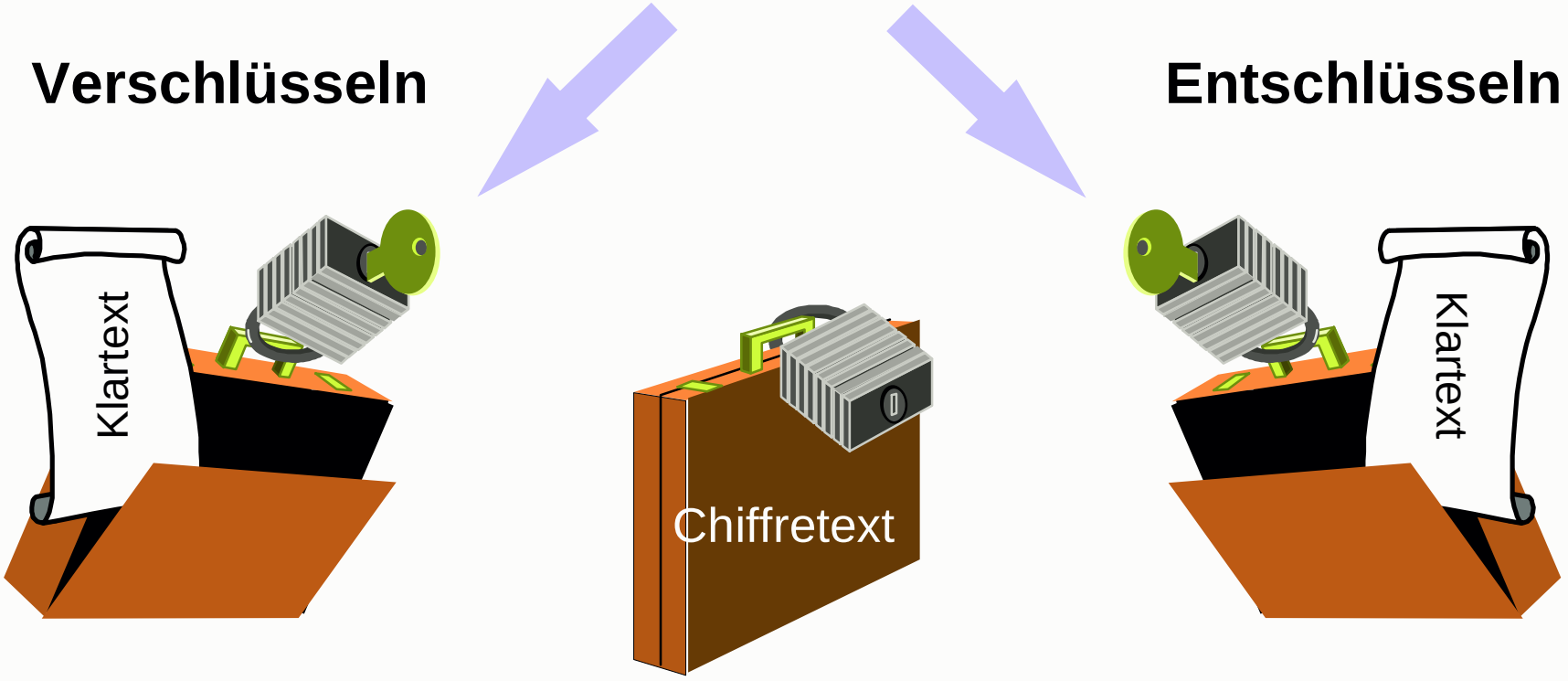
- Sicherheit darf nicht von **Geheimhaltung** der Ver- und Entschlüsselungsfunktion abhängen.
- Verschlüsselung darf ohne Kenntnis des Schlüssels nicht in einer angemessenen Zeit – abhängig von der Lebenszeit der geschützten Daten – **aufzubrechen** sein.
- Exhaustive Search: **Schlüsselraum** EK muss sehr groß sein. (Notwendig, aber nicht ausreichend!)
  - *Beispiel:* 56-Bit Schlüssel (z.B. DES): Schlüsselraum = 2^{56} unterschiedliche Schlüssel
- Anforderung an **Schlüssellänge**
  - symmetrische Schlüssellänge >= 128 Bit
  - RSA-Schlüssellänge >= 1024 Bit

Symmetrische Kryptosysteme

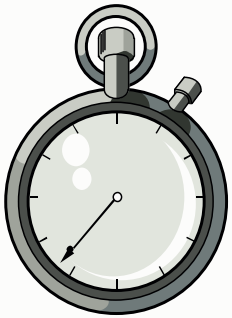
Identischer geheimer Schlüssel (secret key)

zum

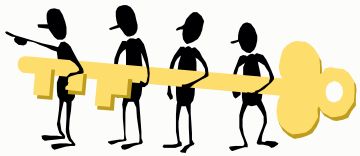
Verschlüsseln **Entschlüsseln**



Symmetrische Kryptosysteme



- **Effizient in Hard- und Software zu implementieren**
  z.B. DES, 3DES, NEU: RIJNDAEL (AES)



- **Problem der geheimen Schlüsselverteilung**
  n Partner benötigen n*(n-1)/2 Schlüssel

- **Keine Nachweisbarkeit der Herkunft einem Dritten gegenüber**

Symmetrische Kryptosysteme

- 2 Klassen symmetrischer Verfahren
  - **Blockchiffre**: Blöcke (Strings) fester Länge; jeder Block mit gleicher Funktion verschlüsselt.
  - **Stromchiffre**: (Kleine) Einheiten mit Schlüsselstrom verschlüsselt.
- One-Time Pad
  - Schlüssel gleich lang wie Klartext, zufällig und niemals wiederverwendet.
    → absolut sicher!

Blockchiffren

- Klassische Verschlüsselungstechniken:
  - **Transposition**, Permutation: Vertauschen der Anordnung der Klartextzeichen
  - **Substitution**: Ersetzen von Zeichen (z.B. Caesar-Chiffre)
- **Produktchiffre** (z.B. DES)
  - Verknüpfungen aus Transposition und Substitution (Runden)
- Transposition fügt **Diffusion** hinzu, Substitution fügt **Konfusion** hinzu.
- Ver- und Entschlüsselung basiert auf einfachen Operationen (u.a. Shifts, XOR).
  ➔ Effizient in Hard- und Software zu implementieren.

Modi von Blockchiffren

- **Electronic Code Book** (ECB)
  - ein Klartextblock in einen Chiffretextblock verschlüsselt → Problem: Block Replay: Blöcke entfernen, wiederholen oder austauschen
- Chaining bewirkt Rückkopplung.
- **Cipher Block Chaining** (CBC)
  - XOR-Verknüpfung mit vorherigem Chiffretextblock
  - identische Anfänge → Initialisierungsvektor
- **Output Feedback** (OFB)
- **Cipher Feedback** (CFB)
- Kriterien: Sicherheitsprobleme, Fehlerfortpflanzung, Synchronisierung von Stromchiffrierungen

Data Encryption Standard

- Seit 1977 genormt, bis 1998 Standard.
- Große Akzeptanz und Verbreitung: u.a. Banken-Umfeld, DES-Chips
- 1998 lief die letzte Zertifizierungsperiode des DES aus.
- 1997: Ausschreibung für den AES (Advanced Encryption Standard)

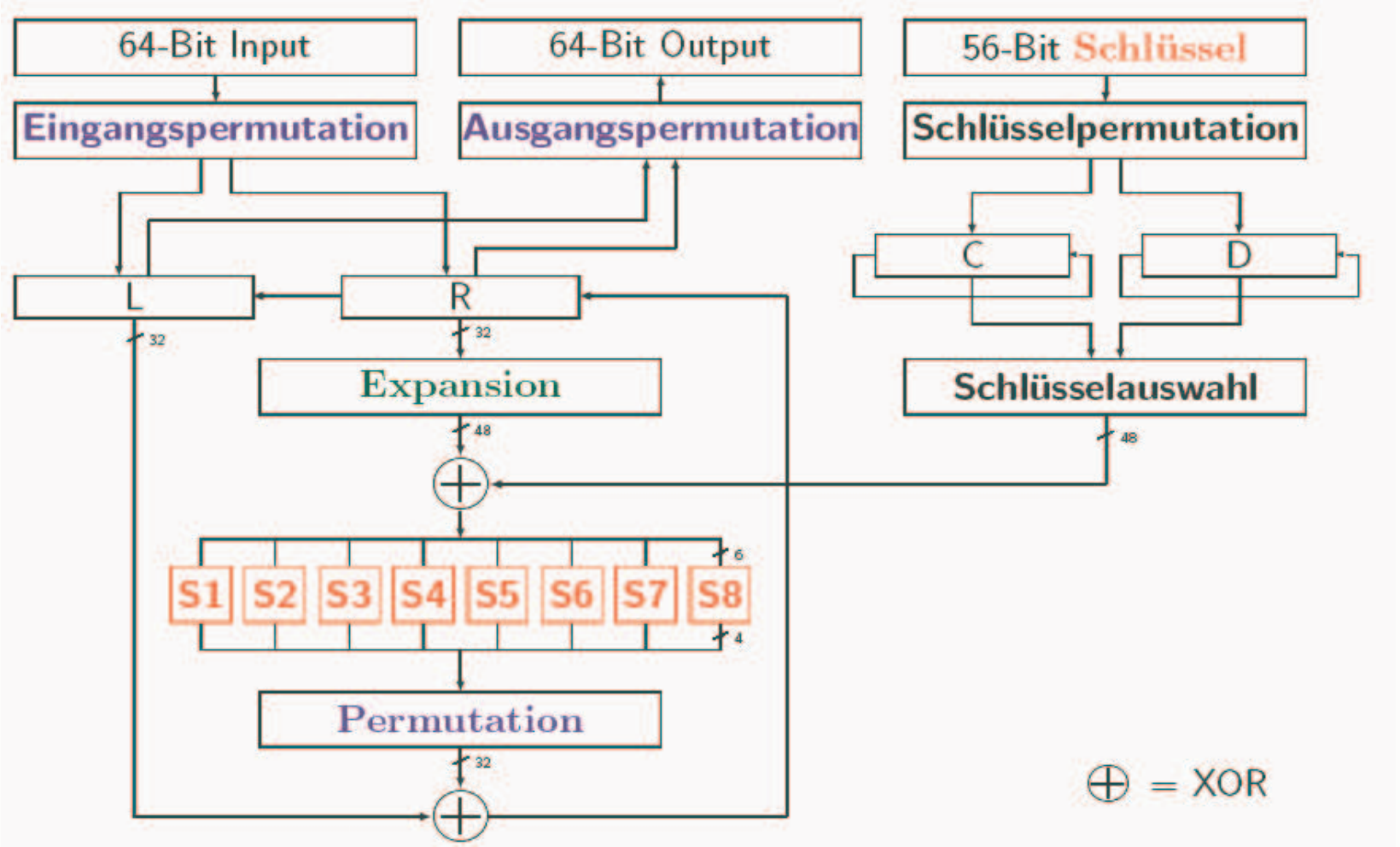
Data Encryption Standard

- Feistel-Chiffre:
  - Blockchiffre: Eingabeblock wird in zwei Hälften aufgeteilt.
  - Die Blöcke werden in mehreren Runden verarbeitet.
  - Die Rundenfunktion wird auf eine der beiden Hälften angewandt
  - und das Ergebnis mit der anderen Hälfte mittels XOR verknüpft.
  - Danach werden die beiden Hälften vertauscht und die nächste Runde wird ausgeführt.

Data Encryption Standard

- Diffusion und Konfusion durch Verknüpfung von Transpositionen und Substitutionen
- Blockchiffre mit 64 Bit Blocklänge
- Schlüssel von 64 Bit, 56 Bit frei wählbar
  → zu kurz!
- DES sowohl zum Verschlüsseln als auch zum Entschlüsseln: E = D
- Substitutionsboxen

Data Encryption Standard



Data Encryption Standard

Sicherheit des DES

- Gezielt entworfen, um differentielle Kryptoanalyse abzuwehren.
- Problem: kurze Schlüssel!
- Dreifachverschlüsselung mit zwei oder drei verschiedenen Schlüsseln: Triple DES (EDE)
- Effektive Schlüssellänge < 112 bit

Kryptoanalyse

Klassifikation von Angriffen (bei bekanntem Verschlüsselungsverfahren):

- Ciphertext-only attack
  - Häufigkeit des Auftretens von bestimmten Buchstaben
- Known-plaintext attack
  - Standardbriefanfänge; Präambeln bei Programmen bzw. Kommunikationsprotokollen ...
- Chosen-plaintext attack
  - Z.B. Passwort-Cracking
- Chosen-ciphertext attack
  - Z. B. Angriff auf asymmetrische Verfahren

Methoden der Kryptoanalyse

- Brute force, Exhaustive Search
  - Durchprobieren aller Schlüssel
- Differentielle Kryptoanalyse (Biham, Shamir 1991)
  - Ermittlung von Unterschieden in den Chiffretexten abhängig von gezielt festgelegten Unterschieden in den Klartexten
- Lineare Kryptoanalyse (Matsui 1993)
  - basiert auf linearen Zusammenhängen zwischen Klartext, Chiffretext und Schlüssel

Hash-Funktionen

- Hash-Funktion
  - Recheneffiziente Funktion, die beliebig lange Binärstrings auf Binärstrings einer festen Länge, sogenannte Hash-Werte, abbildet.
- Kryptographische oder Einweg-Hash-Funktionen (one-way hash function)
  - Es ist rechnerisch unmöglich, zwei verschiedene Eingaben mit gleichem Hash-Wert zu finden (kollisionsfrei).
  - Es ist rechnerisch unmöglich, eine Eingabe zu einem gegebenen Hash-Wert zu finden.

Hash-Funktionen

- Kryptographische Verwendung bei
  - digitalen Signaturen (Hash-Wert der Nachricht wird signiert),
  - Datenintegrität (Virenschutz, Software-Verteilung),
  - Protokollen (z.B. Authentifizierung, digitale Signatur).
- A.k.a.: Fingerprint, kryptographische Prüfsumme, Message Integrity Check (MIC), Modification Detection Code (MDC), ...
  - Öffentlich bekannt
  - Kein geheimer Schlüssel
- Message Authentication Codes (MACs)
  - Geheimer Schlüssel
  - Datenintegrität und -authentizität
- Beipiele: MD2, MD5, RIPE-MD (128bit), SHA (160bit)

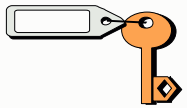
Kryptographische Systeme

- Symmetrische Verfahren (secret-key)
  - Identischer geheimer Schlüssel zur Ver- und Entschlüsselung
- Asymmetrische Verfahren (public-key)
  - Theoretisch beschrieben von Diffie und Hellman 1976.
  - Jeder Teilnehmer besitzt ein Schlüsselpaar (privater und öffentlicher Schlüssel).
  - Basis: Einweg-Funktionen (Funktionswertberechnung ist einfach, Umkehrung nur mit sehr großem Aufwand)

Public Key-Kryptographie

Teilnehmer (A und B)...

...und je Teilnehmer einen privaten....



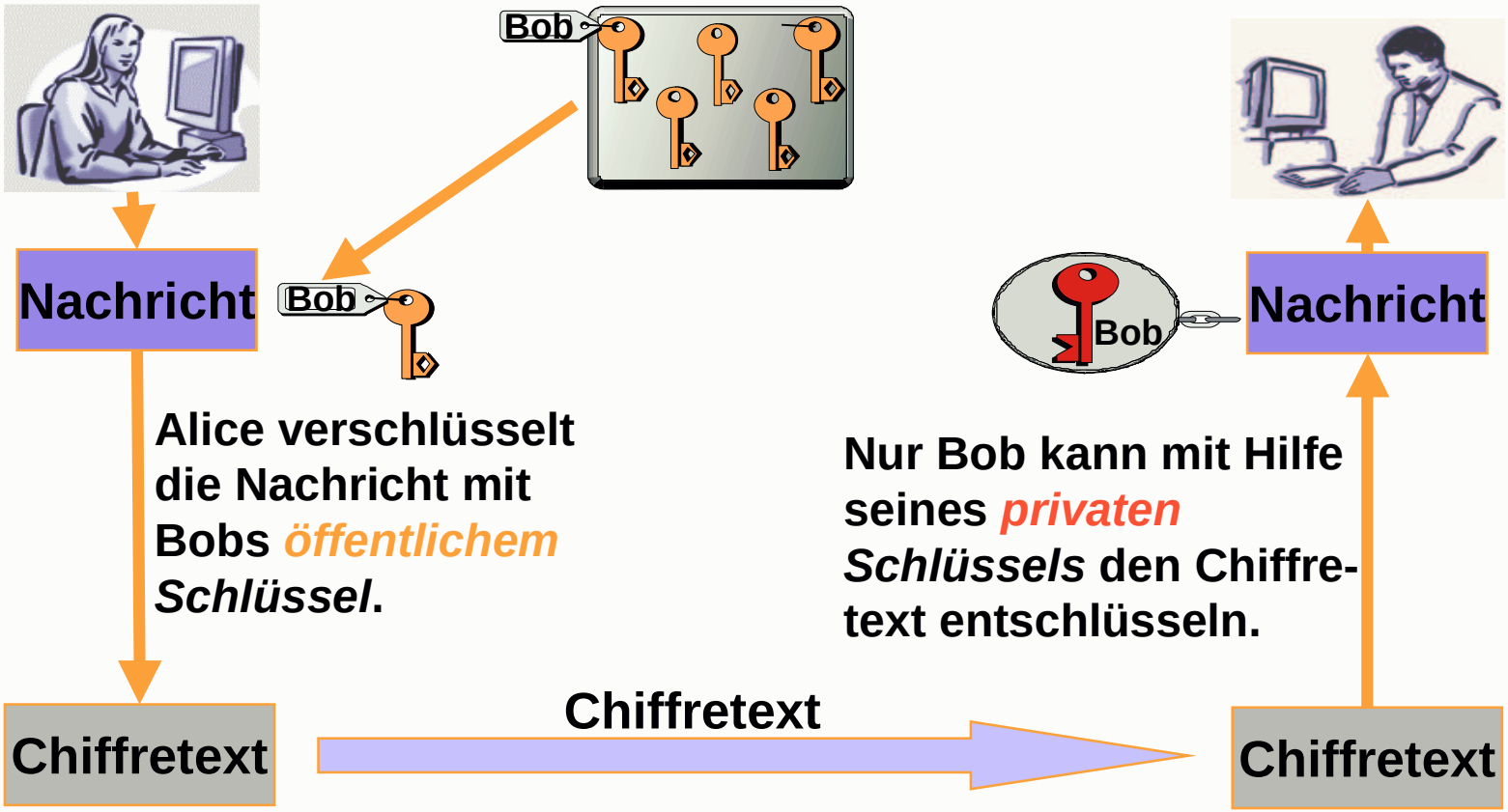
... und einen öffentlichen Schlüssel

Allgemeine Eigenschaften

- Die Schlüsselpaare (k_E, k_D) müssen folgende Eigenschaft erfüllen: Für alle Klartexte m muss gelten $D(E(m, k_E),k_D)) = m$, k_E öffentlich, k_D geheim.
- E und D sind einfach zu berechnen.
- k_D aus k_E nicht mit vertretbarem Aufwand berechenbar.
  - Einweg-Funktion mit Falltür
- Optional: $E(D(m,k_D),k_E)) = D(E(m,k_E),k_D)) = m$

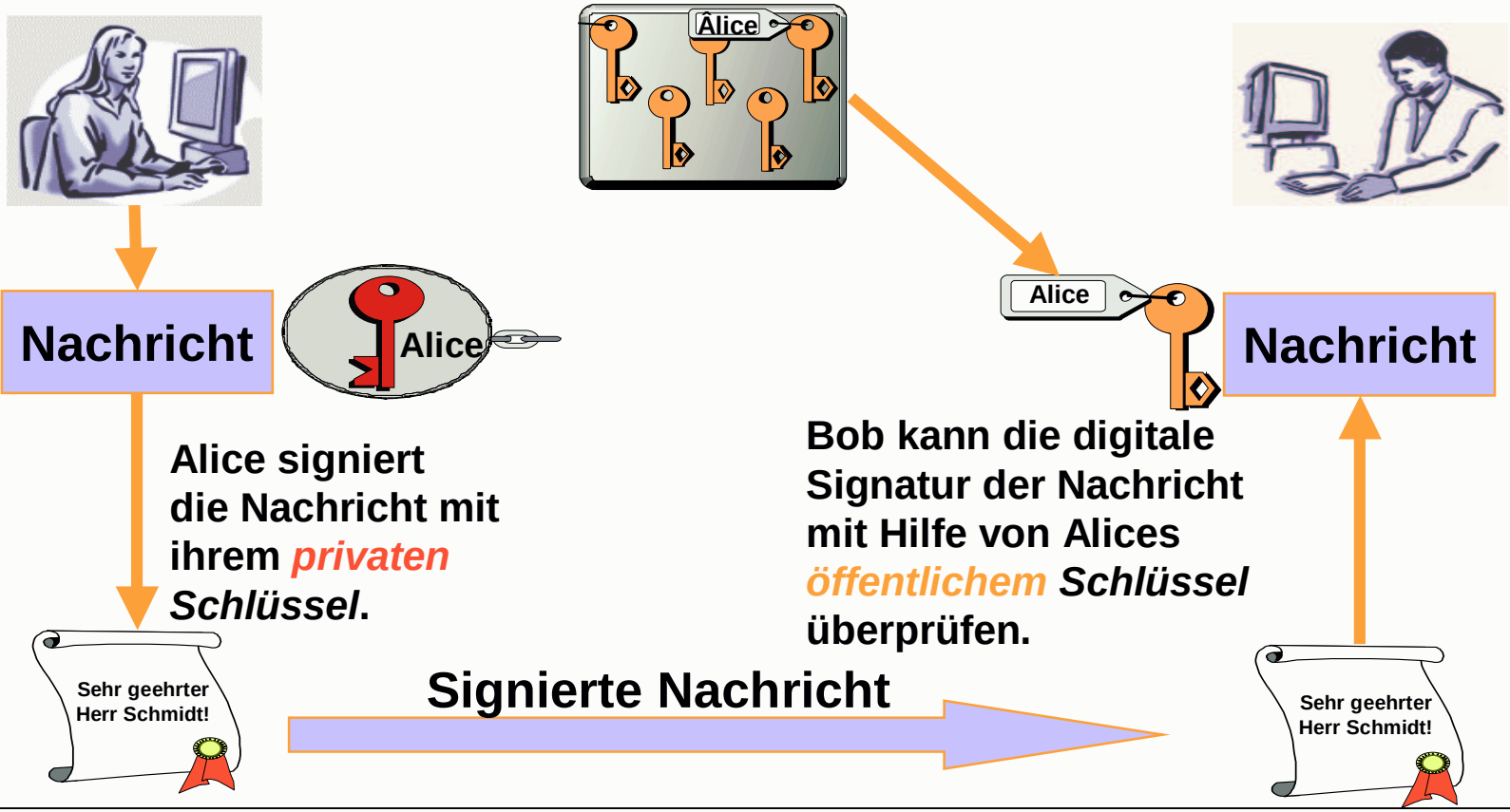
Verschlüsselung einer Nachricht

- Alice möchte Bob eine Nachricht senden.



Digitale Signatur

- Alice möchte eine Nachricht signieren und sicherstellen, dass die Nachricht an Bob nicht unbemerkt verändert werden kann.



Asymmetrische Kryptographie

- Verschlüsselung bewirkt Vertraulichkeit der Kommunikation.
- Digitale Signatur bewirkt Integrität und Authentizität der Nachricht.
- Mit Hilfe der Public Key-Kryptographie lässt sich auch eine Authentifizierung beim Logon erreichen.

Asymmetrische Systeme

- RSA (Signatur und Verschlüsselung)
  - Faktorisierung großer Zahlen
- Diffie-Hellman Schlüsselaustauschprotokoll
  - Diskrete Logarithmen ($y=a^x \bmod n$, y,a,n bekannt, was ist x?)
- DSA Signaturalgorithmus
  - Diskrete Logarithmen
- El Gamal Verschlüsselungsalgorithmus
  - Diskrete Logarithmen
- Algorithmen auf Elliptischen Kurven
  - Diskrete Logarithmen über elliptischen Kurven

RSA-Verfahren

- 1978 von Ronald Rivest, Adi Shamir und Leonard Adleman entwickelt.
- Mathematische Basis: Primfaktorzerlegung
- Einsatz: Verschlüsseln, Signieren, Schlüsselaustausch
- Standard-Verfahren (Andere Systeme nicht weit verbreitet.)
- Falls der Algorithmus mathematisch gebrochen werden sollte, sind viele Verschlüsselungssysteme gebrochen.

RSA-Verfahren

Mathematik:

- Restklassendivision: $x \bmod y = z \Leftrightarrow x = ky + z$, wobei x,y,z ganzzahlig
- Eulersche Zahl: $\varphi(m) = |\{a|ggt(a,m)=1 \wedge a<m\}|$
- Primzahl p: $\varphi(p) = p-1$
- Kleiner Satz von Fermat:
  - Falls ggt(M,n)=1, dann $M^{\varphi(n)} = 1 \bmod n$.

RSA-Verfahren

Vorbereitung:

- Generiere zwei große (und verschiedene) Primzahlen p und q und berechne das Modul n = pq.
- Es gilt: $\varphi(n) = (p-1)(q-1)$.
- Wähle d, $1 < d < \varphi(n)$, so dass $ggt(\varphi(n),d) = 1$.
- Berechne e, $1 < e < \varphi(n)$, mit $ed = 1 \bmod \varphi(n)$, d.h. e ist multiplikatives Inverses modulo $\varphi(n)$ zu d.
- (e,n) ist der öffentliche Schlüssel, (d,n) der private Schlüssel.
- d, p, q, $\varphi(n)$ sind geheim zu halten.

RSA-Verfahren

Verschlüsseln und Entschlüsseln:

- Transformation der Nachricht M in binäre Darstellung $M = M_1,...,M_m$, so dass für Blockgröße r gilt: $k = 2^r$ mit $k \leq n$.
- Blockweises Verschlüsseln mit Verschlüsselungsfunktion E: $E(M_i)=(M_i)^e \bmod n = C_i$
- Entschlüsselungsfunktion D: $D(C_i) = (C_i)^d \bmod n = M_i$

Beweis für Entschlüsselung

- Da $ed = 1 \bmod \varphi(n)$, gib es k ganz mit $ed = 1 + k\varphi(n)$.
- Falls ggT(M,p) = 1, gilt nach kleinem Satz von Fermat $M^{p-1} = 1 \bmod p$.
- Somit $M^{1+k(p-1)(q-1)} = M \bmod p$.
- Dies gilt auch, falls ggT(M,p) = p.
- D.h. es gilt in jedem Fall $M^{ed} = M \bmod p$.
- Genauso: $M^{ed} = M \bmod q$.
- Da p und q verschiedene Primzahlen sind, folgt $M^{ed} = M \bmod n$.
- D.h. $D(C_i) = (C_i)^d \bmod n = (M_i)^{ed} \bmod n = M_i$

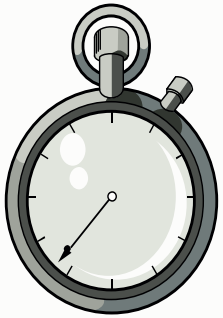
Beispiel

- $p = 47$, $q = 59$, $n = pq = 2773$, $\varphi(n) = 2668$
- $d = 157$, $e = 17$, dann ist $ed = 1 \bmod 2668$
- Verschlüsseln von $M = 920$:
  $C = E(M) = E(920) = 920^{17} \bmod 2773 = 948$
- Entschlüsseln von $C = 948$:
  $D(C) = D(948) = 948^{157} \bmod 2773 = 920$
- Bem.: Die Berechnung der Inversen e erfolgt mit dem erweiterten Euklidischen Algorithmus. Für die Berechnung der modularen Exponentialfunktionen gibt es ebenfalls effektive Algorithmen.

Sicherheit asymm. Verfahren

- Annahme: Ziehen von e-ten Wurzeln ist so schwer wie Faktorisierung des Moduls n (kein Beweis).
- Aufwand für Faktorisierung des Moduls nimmt stark mit der Größe des Moduls zu (kein Beweis, nur Erfahrung).
- Empfehlung zur Zeit: n mindestens 1024-stellige Binärzahl, p,q mind. 512-stellig.
- Für langfristige Verträge etc. n ca. 2048-stellig.
- Schlüssellänge bei El Gamal, DSA ähnlich.
- Elliptische Kurven bieten deutlich kürzere Schlüssellängen.

Asymmetrische Kryptosysteme



- **Problem: Relativ rechenzeitintensiv**
  z.B. RSA, elliptische Kurven

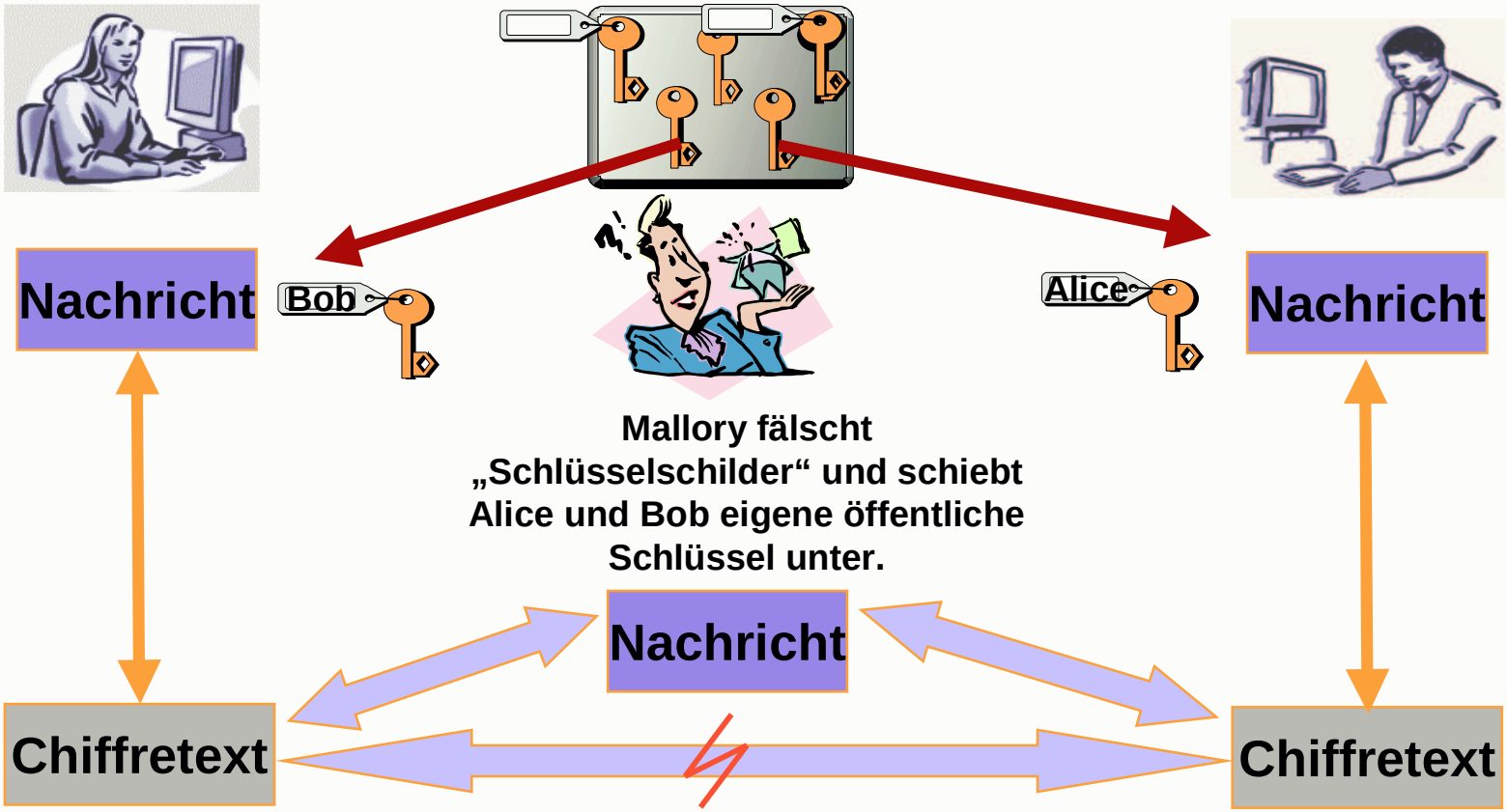
- **Keine geheime Schlüsselverteilung nötig!**
- **n Kommunikationspartner benötigen nur n Schlüsselpaare!**
- **Problem: Wer garantiert für Authentizität des öffentlichen Schlüssels?**

- **Digitale Signatur garantiert Authentizität und Integrität z.B. für Vertragsabschluss.**

Hybridverfahren

- Verbindung der Vorteile symmetrischer Verfahren (Schnelligkeit) mit den Vorteilen asymmetrischer Verfahren (Schlüsselverteilung)
- Konkret:
  - Alice und Bob tauschen zunächst ihre asymmetrischen Schlüssel aus.
  - Die asymmetrischen Schlüssel verschlüsseln und signieren nur einen zufällig bei Alice (oder Bob) erzeugten symmetrischen Sitzungsschlüssel.
  - Die tatsächliche Kommunikation wird dann mit dem Sitzungsschlüssel verschlüsselt.
- Alle heute auf asymmetrischen Protokollen aufsetzenden Anwendungen verschlüsseln in dieser Weise.

Man-in-the-Middle Attack

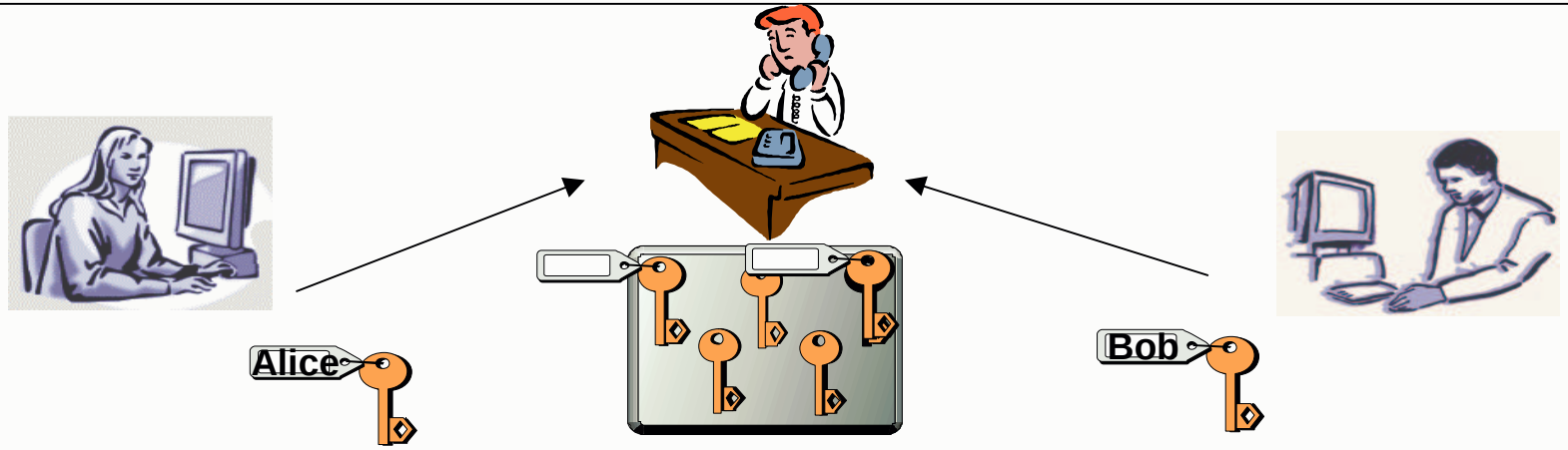


Folge: Mallory liest alle Nachrichten mit, ohne dass Alice und Bob dies bemerken!

Zertifikate

- Problem
  - Wer gibt die Sicherheit, dass die zum öffentlichen Schlüssel gehörenden Angaben zur Person vertrauenswürdig sind?
- Lösung
  - Eine Zertifizierungsstelle (Certification Authority, CA) verbürgt in einem Zertifikat mit der eigenen digitalen Signatur die Zusammengehörigkeit von personen-bezogenen Daten und öffentlichem Schlüssel.
  - Entscheidend für das Vertrauen in eine PKI sind die Certification Policies und deren Umsetzung in der Praxis.

Zertifizierungsinstanz (CA)



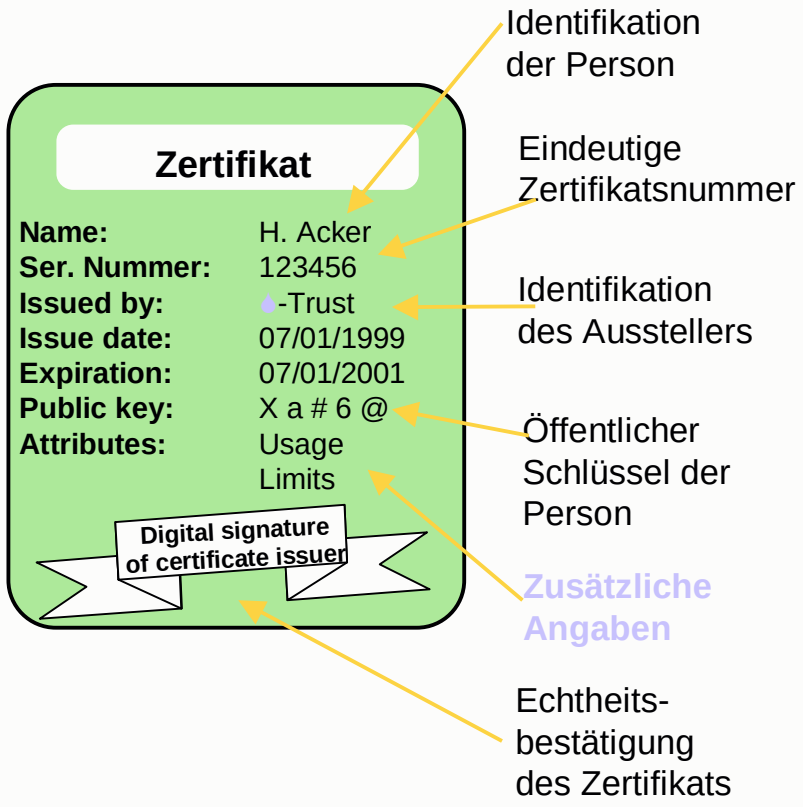
- Alice und Bob wenden sich mit ihren öffentlichen Schlüsseln an eine vertrauenswürdige dritte Instanz (CA), die die Schlüsselschilder mit ihrer eigenen Unterschrift signiert, d.h ein „Zertifikat“ erzeugt.
- Beide können dann anhand der Unterschrift der CA überprüfen, ob die Schlüssel authentisch ihrem Kommunikationspartner gehören.

Was enthält ein Zertifikat?

- Angaben zur Person (Inhaber)
- Öffentlicher Schlüssel
- Seriennummer des Zertifikats
- Gültigkeitsdauer
- Angaben zum Aussteller (CA)
- Digitale Signatur der CA
- Erweiterungen

Zertifikate

- **Zertifikate**
  - verknüpfen natürliche/juristische Personen mit kryptographischen Schlüsseln,
  - sind zeitlich begrenzt,
  - können zusätzlich persönliche Angaben der Zertifikatsinhaber enthalten.
- Zertifikate werden von **vertrauens-würdigen Stellen** ausgegeben: (Trusted Third Party, Certification Authorities)
  - Spezifische Zertifikatsangaben und proprietäre Erweiterungen
  - Unterschiedliche Praxis der Vergabe von Zertifikaten (Certification Policies)
  - Kooperationen zwischen eigenständigen Certification Authorities
- Nutzung digitaler Signaturen setzt zwingend *Zertifikate* voraus.



Public Key-Infrastruktur (PKI)

- **Die für eine Kommunikation mit asymmetrischen Schlüsseln nötige Infrastruktur wird “PKI” genannt, z.B. zertifikatsbasiert:**
- Certification Authority (CA) stellt Zertifikate aus.
- Registration Authority (RA) verwaltet Zertifikate.
- End Entity: der Zertifikatsinhaber (Person, Server, Organisation).
- Verzeichnisdienst (Directory Service) veröffentlicht Zertifikate.
- Kartenproduzent stellt sichere Schlüsselspeicher bereit (Smartcards, USB-Token, etc.).

Public Key-Infrastruktur (PKI)

- Anforderungen an eine CA:
  - Interoperabilität (Standards)
  - Dezentrale Verwaltung (online)
  - Revozierungssystem
  - Verlängerung von Zertifikaten
  - Anbindung an Anwendungssysteme
  - Support für unterschiedliche Zertifikatstypen
  - Kommunikation mit Partner-CAs
- Alternative zur CA: Web of Trust
  - Bekannte Kommunikationspartner vertrauen sich gegenseitig und unterschreiben Zertifikate ohne eine zentrale Stelle.
  - Realisiert im sicheren Email-Standard PGP (Pretty Good Privacy).

Public Key-Infrastruktur (PKI)

- Zertifikatstypen: X.509, PGP, WTLS
- Überprüfung von Revozierungen
- Sperrlisten (Certificate Revocation List, CRL)
- Online-Abfrage (Online Certificate Status Protocol, OCSP)
- Schutz des privaten Schlüssels:
  - Passwort-geschützte Datei, SmartCard, USB-Token, ...

Anwendungen

- E-Mail
- E-Commerce
- Elektronische Bankgeschäfte (HBCI, Elko)
- Verbindliche Verträge (Signaturgesetz)
- Online-Behördengänge (Signaturgesetz)
- Signatur von Software (z.B. Java-Applets)
- Virtual Private Networks (VPN)
- Mobile Dienste

Netzwerksicherheit

- Kapitel 3: Netzwerksicherheit
  - Überblick über TCP/IP
  - Sichere elektronische Kommunikation (Email, IP, Web)
  - Firewalls

Netzwerksicherheit

Sicherheitsziele:

- Integrität und Authentizität der übertragenen Daten
- Vertraulichkeit der übertragenen Daten
- Verbindlichkeit
- Verfügbarkeit

Netzwerksicherheit

Schwachstellen, Bedrohungen

- Netzwerkprotokolle meist nicht für offene Netze mit Blick auf Sicherheit entwickelt.
  → auch Internet-Protokollsuite IPv4
- Bieten vielfältige Möglichkeiten für
  - Abhören (Sniffing, Snooping) und
  - Manipulation der übertragenen Daten,
  - Vortäuschen falscher Identität (IP-, DNS-, Web-Spoofing, Email),
  - Man-in-the-Middle-, Replay-Attacken,
  - Denial-of-Service-Attacken,
  - anwendungsspezifische Angriffe, z.B. auf Web-Anwendungen (SQL-Injection, Cookie-poisoning, Buffer-overflow, Manipulation von Parametern, ...).

Netzwerksicherheit

Sicherheitsmaßnahmen:

- Physikalische Zugangskontrolle
- Netzwerkzugangskontrolle
- Netztrennung, Firewall-Gateways (Paketfilter, Proxy)
- Virenschutz
- Kryptographische Schutzfunktionen
  - S/MIME, PGP, PEM, ...
  - TLS/SSL
  - IPsec
- Authentifizierungssyteme
  - Passwort-basiert, kryptografisch, Tokens, Biometrie
  - Kerberos

Überblick über TCP/IP

- Suite von Kommunikationsprotokollen
- Namesgeber sind dabei
  - TCP = Transmission Control Protocol
  - IP = Internet Protocol
- Entwickelt von U.S. Defense Advanced Research Projects Agency
- ARPANET seit 1983
- Information über TCP/IP-Protokolle ist als Requests for Comments (RFC) veröffentlicht.

Eigenschaften von TCP/IP

- Offene Protokollstandards, frei erhältlich, hardware- und betriebssystem-unabhängig.
- Unabhängig von spezifischer physikalischer Netzwerk-Hardware (Ethernet, Token Ring, Wählleitung, X.25-Netz, ...).
- Gemeinsames Adressschema.
- Standardisierte High-level-Protokolle für weit verbreitete Anwenderdienste.

OSI Referenzmodell

- Architekturmodell für Beschreibung von Struktur und Funktion von Datenkommunikationsprotokollen
- ISO/OSI (International Standards Organization/Open Systems Interconnect)
- Sieben Schichten (layers) mit definierten Datenkommunikationsfunktionen
- Stack oder Protocol Stack

OSI Referenzmodell

7 Application Layer	Besteht aus Anwendungsprogrammen, die das Netzwerk benutzen.
6 Presentation Layer	Standardisiert Datendarstellung für die Anwendungen.
5 Session Layer	Verwaltet Sitzungen zwischen Anwendungen.
4 Transport Layer	Liefert Ende-zu-Ende-Fehler-erkennung und -behebung.
3 Network Layer	Verwaltet Verbindungen über das Netzwerk für höherliegende Schichten.
2 Data Link Layer	Bietet verlässliche Datenauslieferung über die physikalische Verbindung.
1 Physical Layer	Definiert die physikalischen Eigenschaften des Netzwerkmediums.

OSI Referenzmodell

- Daten werden den Stack hinunter durchgereicht, bis sie von den Physical Layer Protokollen über das Netzwerk übertragen werden.
- Kommunikationspartner (peer) muss gleichen Stack implementiert haben.
- Daten werden am anderen Ende wieder den Stack hochgereicht zur empfangenden Anwendung.
- Schichtenmodell minimiert Auswirkungen von technologischen Änderungen auf die gesamte Protokollsuite.

TCP/IP Protokollarchitektur

4 Application Layer (SMTP, Telnet, FTP etc.)	Besteht aus Anwendungen und Prozessen, die das Netzwerk benutzen.
3 Host-to-Host Transport Layer (TCP, UDP, ICMP)	Leistet Ende-zu-Ende-Datenauslieferung.
2 Internet Layer (IP)	Definiert die Datagramme und handhabt das Routing der Daten.
1 Network Access Layer (Ethernet, FDDI, ATM etc.)	Besteht aus Routinen für den physikalischen Netzwerkzugang.

TCP/IP Protokollarchitektur

- **Encapsulation**
  - Jede Schicht im Stack fügt den zu sendenden Daten Kontrollinformationen hinzu, sogenannte **Header**.
  - Umgekehrt werden beim Empfang Header entfernt.
- **Network Access Layer**
  - Encapsulation of IP datagrams into the frames transmitted by the network.
  - Mapping of IP addresses to the physical addresses used by the network.
  - Address Resolution Protocol (ARP)

IP

- **Internet Layer**

  Internet Protocol (RFC 791)

  – Datagramm: Grundeinheit für Übertragung im Internet

  – Internet Adressschema (32-bit IP-Adresse)

  – Routing von Datagrammen zu entfernten Hosts über Gateways

  – Fragmentierung und Reassemblierung von Datagrammen

  – Verbindungsloses Protokoll

  – Nicht-verlässliches Protokoll (keine Fehlererkennung und -behebung)

ICMP

- **Internet Layer**

  Internet Control Message Protocol (ICMP), RFC 792

  – Flusskontrolle
  – Erkennung unerreichbarer Ziele
  – Umleitung von Routen (ICMP Redirect Message)
  – ICMP Echo Message (UNIX ping)

UDP

- **Transport Layer**

  User Datagram Protocol (UDP)

  - Verbindungslose Datagramm-Auslieferung
  - Nicht-verlässlich
  - Minimaler Protokoll-Overhead
  - 16-bit Quell- und Zielport
    - Identifizieren zuständige Anwendung auf beiden Hosts

TCP

- **Transport Layer**

  Transmission Control Protocol (TCP)

  – Verlässliche Datenauslieferung
    - Segmente mit Sequenznummern
    - Positive Acknowledgment with Retransmission
    - Ende-zu-Ende Fehlererkennung und -behebung
  – Verbindungsorientiert
    - Three-way handshake
    - SYN, ACK und FIN flags
    - ACK-Segment liefert auch Flusskontrolle
  – Byte-stream
  – 16-bit Quell- und Zielport

Anwendungsprotokolle

- **Application Layer**

Weit verbreitete Anwendungsprotokolle:

- **Telnet** (Network Terminal Protocol)
- **FTP** (File Transfer Protocol)
- **SMTP** (Simple Mail Transfer Protocol)
- **DNS** (Domain Name System)
  - Ordnet IP-Adressen Namen zu.
- **NFS** (Network File System)
- **HTTP** (Hypertext Transfer Protocol)
  - World Wide Web
- Routing Protokolle (RIP, OSPF, BGP-4, ...)

TCP/IP Protokollarchitektur

- Adressierung
  - IP-Adressen identifizieren Hosts im Internet.
  - Bsp.: 192.178.16.1
  - Netzwerk- und Host-Adressteil
    - Class A, B, C, D, E
    - Default route, loopback address
    - Broadcast address
    - Multicast
    - Subnets
- Routing
  - Gateways liefern Daten an das korrekte Netzwerk ab.
- Multiplexing
  - Protokoll- und Port-Nummern liefern Daten an das korrekte Software-Modul im Host ab.

Sichere elektronische Kommunikation

- Beispiele: Email, WWW und IP
- Exemplarisches Aufzeigen der oben genannten Schwachstellen und Bedrohungen für diese Protokolle/Anwendungen
- Kryptographische Schutzfunktionen
  - **Digitale Signatur** für Integrität und Authentizität der Kommunikation
  - **Verschlüsselung** für Vertraulichkeit der Kommunikation
  - Einsatz in den verschiedenen Schichten: Anwendung, Transport, Internet
- Firewalls und Authentifizierungssysteme: später

SMTP

- Beispielablauf

```
220 fwd05.sul.t-online.com T-Online ESMTP receiver fsmtpd ready.
HELO me.foo.bogus
250 Ok.
MAIL FROM:<george@whitehouse.gov>
250 Ok.
RCPT TO:<fricke@uni.bogus>
250 Ok.
DATA
354 Ok, start with data.
From: george@whitehouse.gov
To: fricke@uni.bogus
Subject: Mail spoofing

Wie geht das?
.
250 Message accepted.
```

Sichere Email?

- Schwachstellen, Bedrohungen
  - Absenderadresse und Nachricht leicht fälschbar
  - Nachricht abhörbar und manipulierbar
  - Store-and-Forward-Prinzip
  - Denial-of-Service-Angriffe (auf empfangende Mailsysteme)
  - Spam
  - Mail relaying
  - ...
- Sicherheitsanforderungen
  - Vertraulichkeit der Nachricht
  - Authentizität der Herkunft
  - Integrität der Nachricht
  - Non-repudiation
  - Einwurfbestätigung
  - Empfangsbestätigung
  - ...

Sichere Email

- **Kryptographische** Sicherheitsdienste für elektronische Nachrichten
  - Authentizität, Integrität und Verbindlichkeit durch **digitale Signaturen**
  - Ende-zu-Ende-Vertraulichkeit und Datensicherheit durch **Verschlüsselung**
- Standards/Produkte
  - S/MIME
  - PGP
  - PEM (veraltet)
  - Lotus Notes
  - ...

Sichere Email

- Probleme, Randbedingungen
  - Welches Produkt, welchen Standard nutzt der Kommunikationspartner? (Interoperabilität)
  - Anforderungen an Schlüssel-, Zertifikatsmanagement; PKI
  - Message Recovery
    - Firmeninteresse vs. Vertraulichkeit
  - Die Anforderungen, insbesondere an „Interoperabilität“ und „PKI“, hängen stark vom Anwendungsszenario ab:
    - Unternehmensinterne Kommunikation
    - Kommunikation mit Partnern (Lieferanten, Dienstleister,...), B2B
    - Kommunikation mit (bekannten/spontanen) Kunden (E-commerce), B2C
  - Verteilerlisten
  - Vertretungen (insbesondere in Firmen)
  - ...

S/MIME

- **Secure/Multipurpose Internet Mail Extensions**
  S/MIME Version 3 (Proposed Standard)
  - Message Specification (RFC 2633)
  - Certificate Handling (RFC 2632)
- Senden und Empfangen von sicheren MIME-Daten
  - I.d.R. durch MUAs (mail user agents), wie Netscape Messenger, MS Outlook u.a.
  - Aber nicht auf Mail beschränkt.
- Basiert auf „Cryptographic Message Syntax“ (RFC 2630, abgeleitet von PKCS #7) und MIME-Specs
  - Benutzt die Content Types Data, SignedData und EnvelopedData.
  - Benutzt X.509-Zertifikate (PKIX).

Enveloped-only Message

Content-Type: application/pkcs7-mime; smime-type=enveloped-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

rfvbnj756tbBghyHhHUujhJhjH77n8HHGT9HG4VQpfyF467GhIGfHfYT6
7n8HHGghyHhHUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H
f8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
0GhIGfHfQbnj756YT64V

Signed-only Message (1)

Content-Type: application/pkcs7-mime; smime-type=signed-data;
name=smime.p7m
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7m

567GhIGfHfYT6ghyHhHUujpfyF4f8HHGTrfvhJhjH776tbB9HG4VQbnj7
77n8HHGT9HG4VQpfyF467GhIGfHfYT6rfvbnj756tbBghyHhHUujhJhjH
HUujhJh4VQpfyF467GhIGfHfYGTrfvbnjT6jH7756tbB9H7n8HHGghyHh
6YT64V0GhIGfHfQbnj75

Signed-only Message (2)


```
Content-Type: multipart/signed;
        protocol="application/pkcs7-signature";
        micalg=sha1; boundary=boundary42

--boundary42
Content-Type: text/plain

This is a clear-signed message.

--boundary42
Content-Type: application/pkcs7-signature; name=smime.p7s
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename=smime.p7s

ghyHhHUujhJhjH77n8HHGTrfvbnj756tbB9HG4VQpfyF467GhIGfHfYT6
4VQpfyF467GhIGfHfYT6jH77n8HHGghyHhHUujhJh756tbB9HGTrfvbnj
n8HHGTrfvhJhjH776tbB9HG4VQbnj7567GhIGfHfYT6ghyHhHUujpfyF4
7GhIGfHfYT64VQbnj756

--boundary42--
```

S/MIME

- Signatur und Verschlüsselung gleichzeitig möglich.
- Absender-Zertifikat kann signierter Nachricht beigepackt werden.
- ➢ Empfänger kann dann an Absender verschlüsselte Nachrichten senden.
- ➢ Gängige MUAs, wie Netscape Messenger, MS Outlook, haben dies benutzerfreundlich implementiert.
- ➢ Statt Peer-to-peer-Zertifikatsaustausch auch Einsatz eines Verzeichnisdiensts möglich.

HTTP

- Beispielablauf

```
GET / HTTP/1.1
Host: www.uni-hildesheim.de

HTTP/1.1 200 OK
Date: Wed, 18 Dec 2002 20:00:34 GMT
Server: Apache
Last-Modified: Wed, 18 Dec 2002 08:58:56 GMT
ETag: "edf9b-3425-3e0038d0"
Accept-Ranges: bytes
Content-Length: 13349
Content-Type: text/html


<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN">
<html><!-- #BeginTemplate "/Templates/generic.template.dwt" -->
...
```

HTTP

- Anwendungsprotokoll über TCP (RFC 2068)
- **Zustandsloses Klartextprotokoll**
- HTTP **Header** enthält alle wichtigen Informationen.
  - Was, Wie, Wer, von Wo
- Wichtigste Methoden: **PUT** und **GET**
- **GET:** Daten als URL-Argumente versendet.
- **PUT**: Daten als Inhalt versendet.
- Alle Variablen und Werte sind **manipulierbar** (Formularfelder, Cookies, URL)
- **Session-Id** beseitigt Zustandslosigkeit für Web-Anwendungen.
  - Cookies
  - URL rewriting

World Wide Web (WWW)

- Schwachstellen, Bedrohungen
  - **Abhören** der übertragenen Daten
    - Passwörter, Kreditkartennummern, persönliche Daten, Session-Id, ...
  - **Manipulation** der übertragenen Daten
  - **Proxies** (z.B. für Caching)
  - **Vortäuschen**/Fälschen einer Web-Site
  - Aktive Inhalte (JavaScript, ActiveX, Java, ...)
    - **Malicious Code**

World Wide Web (WWW)

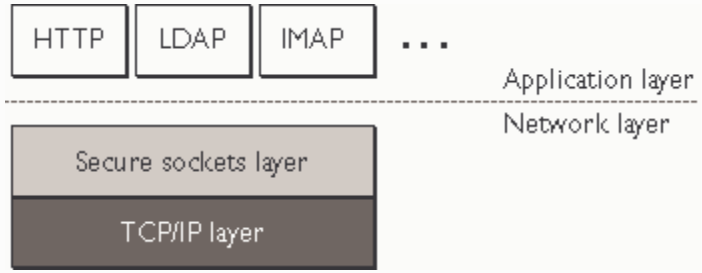
- Schwachstellen, Bedrohungen (cont.)
  - Spezifische **Angriffe auf Web-Anwendungen**:
    - Manipulation von Eingabe-Parametern (z.B. hidden fields, cookies, vorbereitete Links)
    - Directory Traversal
    - Encoding-Attacken (Unicode Exploit)
    - Cross-site-scripting (XSS)
    - Buffer-overflows, Format-String-Attacken
    - Command-Injection, z.B. SQL-Injection

Sicherheitsprotokoll TLS/SSL

- SSL/TLS (Transport Layer Security) sichert die **Vertraulichkeit** der Kommunikation von Client/Server-Applikationen durch kryptographische Methoden.
  - Kein Abhören, Manipulieren oder Fälschen von Nachrichten möglich (**Verschlüsselung**, **Integritätsprüfung** der übertragenen Daten).
  - **Authentifizierung** des Servers und (optional) des Clients möglich mittels Public Key-Kryptographie (**X.509-Zertifikate**).
- **Transport Layer Security** Protokoll (TLS version 1.0), proposed Internet Standard (RFC 2246)
- Weiterentwickelt von Netscape **Secure Sockets Layer** (SSL) Protokoll Version 3.0

Sicherheitsprotokoll TLS/SSL

- Läuft über einem verlässlichen Transportprotokoll: z.B. über TCP.
- Bietet Kommunikationssicherheit unabhängig vom Anwendungsprotokoll.
- Jedes (verbindungsorientierte) higher-level Protokoll kann transparent über TLS gesichert werden: HTTP, LDAP, IMAP, ...



Sicherheitsprotokoll TLS/SSL

- Zwei Subprotokolle: **TLS Record Protocol** und **TLS Handshake Protocol**
  - **TLS Handshake Protocol** etabliert Sicherheits-kontext zwischen Kommunikationspartnern:
    - Authentifizierung des Servers gegenüber dem Client
    - (optional) Authentifizierung des Clients gegenüber dem Server
    - Aushandlung von Sicherheitsparametern (kryptographische Algorithmen etc.)
    - Benutzt Public-key-Kryptografie um shared secrets zu generieren.

TLS Handshake Protocol

Client		**Server**
ClientHello	-------->	
		ServerHello
		Certificate*
		ServerKeyExchange*
		CertificateRequest*
	<--------	ServerHelloDone
Certificate*		
ClientKeyExchange		
CertificateVerify*		
[ChangeCipherSpec]		
Finished	-------->	
		[ChangeCipherSpec]
	<--------	Finished
Application Data	<------->	Application Data

Sicheres WWW

- **HTTPS** = HTTP über SSL/TLS
- Server-Zertifikat bewirkt Verschlüsselung und Authentifizierung des Web-Servers.
- Optional auch Authentifizierung des Clients (Browser) durch Zertifikat.
  - Ersatz für schwächere Authentifizierung durch Passwort.
- Untersützt von den meisten Browsern (Netscape Navigator, MSIE, ...) und Web-Servern.
- Weiterhin:
  - Angriffe auf Web-Anwendungen möglich.
  - Kein erhöhter Schutz vor Angriffen auf Client.

IP-Sicherheit

- Schwachstellen, Bedrohungen
  - Abhören der übertragenen Daten
  - Manipulation der übertragenen Daten
  - Vortäuschen falscher Identität durch Spoofing der IP-Adresse (oder des DNS-Namens)
  - Denial-of-Service-Angriffe
  - ...
- Protokolle höherer Schichten (TCP/UDP, Anwendungen) implementieren oft keine eigenen, weitergehenden Sicherheitsmechanismen.
  - Vertrauen auf IP-Adresse zur Client-Authentifizierung (Rechner, nicht Benutzer)
    - Z.B. r-Befehle mit rhosts-Sicherheit, NFS
  - Fehlende kryptographische Maßnahmen für Vertraulichkeit und Integrität der Kommunikation.
  - ...

IPsec

- Sicherheitsprotokoll in der Netzwerkschicht (Internetschicht) für IPv4 und IPv6
- Kryptographische Sicherheitsdienste unterstützen
  - Authentifizierung
  - Integrität
  - Zugangskontrolle
  - Vertraulichkeit
- Security Architecture for the Internet Protocol (RFC 2401)
  - Host-to-Host, Gateway-to-Gateway, Host-to-Gateway
- IP Encapsulating Security Payload (ESP) (RFC 2406)
  - Vertraulichkeit, Data Origin Authentication, Integrität, ...
  - Transport-Modus, Tunnel-Modus
- IP Authentication Header (AH) (RFC 2402)
  - Keine Vertraulichkeit
- Protokolle für Schlüsselmanagement (IKE, ISAKMP, ...)

Virtual Private Network

- Sichere Verbindung über unsichere Netze (z.B. Internet) mittels kryptographischer Sicherheitsdienste in den unteren Protokollschichten.
- IPsec im Tunnelmodus zwischen mehreren Security Gateways
  - Verbinden mehrerer privater Netze (Firmenlokationen) über öffentliche Netze (z.B. Internet)
- bzw. zwischen Host und Security Gateway
  - Remote-Access zum Unternehmensnetz von mobilen Rechnern/Heimarbeitsplätzen über öffentliche Netze (z.B. Internet)

Firewalls

- Generelles Konzept zur Absicherung von **Übergängen zwischen Netzwerken** mit unterschiedlichen Sicherheitsniveaus
- Gateways als **ein** Teil eines Sicherheits-konzepts
- In der Regel **mehrstufige** Firewall-Strukturen
- Weitere wichtige Komponenten
  - **Content Security** (Virenschutz, URL Blocking, ...)
  - Starke **Authentifizierung** für Remote Access
  - Schutz von Web-Servern und **E-Business-Systemen**

Firewalls

- **Anwendungsbereiche**
  - Internetzugang
  - Verbindungen zwischen unabhängigen Firmen
  - Anbindung von Heimarbeitsplätzen oder externen Vertriebsmitarbeitern an das Unternehmensnetz
    - Authentifizierung, Verschlüsselung, ggfs. Protokollierung
  - Verbindung von Filialnetzen über das Internet
    - Virtual Private Network (Verschlüsselung)
  - Trennung sensibler Netzbereiche vom restlichen Unternehmensnetz
    - Z.B. Forschung und Entwicklung, Personal, ...

Firewalls

- Zusammenspiel mit **internen Servern**
  - Nameserver
    - internes und externes DNS
  - Management-Systeme, Log-Hosts
  - Mail-Server
  - WWW-Proxies (Caching, Virenscanning, ...)
  - News-Server
  - E-Business-Systeme
    - Extern erreichbarer Web-Server
    - Interne Anwendungen und Datenbanken
  - ...

Firewalls

- **Grundkomponenten**
  - IP-Filter
  - Dynamische Filter
  - TCP-/UDP-Relays
  - Application Gateways/Proxies

IP-Filter

- Filtern jedes einzelnen Pakets
  - unabhängig von vorherigen Paketen
- In der Regel auf Basis der IP-Header-Felder
  - Protokoll (ICMP, TCP, UDP, ...)
  - Quell-IP-Adresse
  - Ziel-IP-Adresse
  - Quell-Port (bei TCP-/UDP-Paketen)
  - Ziel-Port (bei TCP-/UDP-Paketen)
  - Flags im TCP-Header
- Keine Pakete mit Source-Routing akzeptieren!
- Kein dynamisches Routing, keine ICMP-Redirects akzeptieren!

IP-Filter

- Meist in Hardware-Routern implementiert.
- Probleme:
  - Z.B. FTP (im aktiven Modus) benötigt weitere TCP-Verbindung für Datenübertragung von Server zu Client. → Großer Portrange für eingehende Verbindungen muss geöffnet werden.
  - Durch Manipulation von IP-Fragmenten können einige IP-Filter umgangen werden.
  - Fehlende Kenntnis der Anwendungsprotokolle, insbesondere des Status. → Kein Schutz vor anwendungsgetriebenen Angriffen.

IP-Filter

- Beispiel einer Access Control List eines Cisco-Routers

```
! HTTP proxy outbound
access-list 101 permit tcp host proxy1 any eq www
access-list 101 permit tcp host proxy1 any eq ftp
access-list 101 permit tcp host proxy1 any eq ftp-data
access-list 101 permit tcp host proxy1 any gt 1023
! default rule
access-list 101 deny ip any any log
! Interface bindings
interface ethernet 0
ip access-group 101 in
```

Dynamische Filter

- Status jeder Verbindung wird in einer Tabelle gespeichert („Stateful Inspection“).
- Antwortpakete werden der Verbindung zugeordnet.
- Z.B. FireWall-1 von CheckPoint

TCP-/UDP-Relays

- Verbindungsweiterleitung über ein dual-homed Gateway (ohne IP-Forwarding)
- Flexibler: Socks Version 5
- In der Regel Änderungen am Client nötig.

Application Gateways/Proxies

- Arbeiten vollständig auf **Anwendungsebene**.
- Nehmen Verbindungen für ein spezielles Protokoll entgegen, verarbeiten Daten auf Anwendungsebene und leiten diese weiter.
- Z.B. für Email (SMTP), WWW (HTTP), FTP
- Vollständige Trennung der Kommunikations-verbindungen zwischen internem und externem Netz.
- Semantik des Applikationsprotokolls bekannt.

→ Filterung auf Applikationsebene möglich.

  → Z.B. nur Download, kein Upload via FTP aus internem Netz.

- Hoher Aufwand, hohe Performance-Anforderungen.

Authentifizierung

- Kapitel 4: Authentifizierung
  - Passwörter
  - Token
  - Biometrische Verfahren
  - Kerberos

Authentifikationsverfahren

- Wissen
  - Passworte, PINs
- Besitz
  - SmartCard, EC-Card, SIM-Card
- Biometrische Merkmale
  - Fingerabdruck, Iris (Augenhintergrund), Gesicht
- Sicherheitskritische Anwendungen werden durch eine **Kombination** von Verfahren abgesichert:
- Z.B. Besitz und Wissen:
  - Geldautomat, Handy

Begriffe

- Identifizierung
  - Wer ist mein Kommunikationspartner?
- Authentifizierung
  - Ist mein Kommunikationspartner tatsächlich der, der er zu sein vorgibt?
- Autorisierung
  - Welche Berechtigungen räume ich meinem Kommunikationspartner auf meinem System ein?

Passwortverfahren (1)

- Benutzer oder System gibt Passwort mit einer bestimmten Gültigkeitsdauer vor.
- Vorteile:
  - Weit verbreitet.
  - Einfach und kostengünstig zu realisieren.
- Probleme:
  - Wahl der Passworte durch Benutzer sehr schlecht, durchschnittlich mehr als 80% leicht zu knacken.
  - Systemgenerierte Passwörter: Schwer zu merken.
  - Speicherung, Verwaltung:
  - Social Engineering: „Gib mir mal kurz dein Passwort.“
  - Speicherung in zwar verschlüsselter, aber allgemein lesbarer Datei: z.B. /etc/passwd.
  - Ungeschützte Übertragung über Netze zum Server.

Passwortverfahren (2)

- Einmal-Passwörter
- Sehr sicher, da Passwort nur einmal verwendet.
  - 1. Möglichkeit: Vor der Übertragung werden lange Passwortlisten vereinbart (z.B. TAN-Liste).
  - 2. Möglichkeit: Benutzer und System können Passwörter berechnen (z.B. S/Key).
- Z.B. S/Key-Funktionsweise
  - Anfangswert a (Seed), geheimer Schlüssel K, Länge der Passwortliste l, Hashfunktion H
  - $P_1 = H(a, k)$, $P_2 = H(P_1,k)$, ... , $P_l = (P_{l-1},k)$
  - Benutzer und System müssen a, K, l am Anfang vereinbaren und natürlich geheim halten.

Challenge Response (1)

- Challenge-Response-Verfahren (symmetr.)
  - Benutzer und Server vereinbaren geheimen Schlüssel K und Funktion F (z.B. Hash-Funktion).
  - Server übermittelt eine Zufallszahl z an Benutzer und berechnet F(z,K).
  - Benutzer berechnet F(z,K) und übermittelt Ergebnis an den Server, der Gleichheit überprüfen kann.
- Vorteile:
  - Passwort wird nie übertragen.
  - K kann z.B. in einem Token (Chipkarte o.ä.) gespeichert werden.

Challenge Response (2)

- Challenge-Response-Verfahren (asymmetr.)
  - Server kennt öffentlichen Schlüssel P des Benutzers.
  - Server übermittelt Zufallswert z an Benutzer.
  - Benutzer signiert z und übermittelt Signatur.
  - Server kann mit öffentlichem Schlüssel Signatur überprüfen.
- Vorteil:
  - Passwort wird nie übertragen.
  - Existierende PKI kann von vielen Anwendungen zur Authentifizierung genutzt werden.
  - Ebenfalls Benutzung von Token möglich.

Token (1)

- Kryptographische Schlüssel sind für Benutzer einfacher zu handhaben, wenn sie in abgeschlossener, kleiner Hardware transportiert werden können.
- Besitz (Token) und Wissen (PIN zum Bedienen des Token) können zur 2-Faktor-Authentisierung kombiniert werden.
- Z.B. Challenge Response Verfahren mit taschenrechnerähnlichem Token:
  - Benutzer schaltet mit PIN Token ein.
  - Benutzer gibt Server-Challenge in Token ein.
  - Token berechnet mit gespeichertem Schlüssel Antwort.
  - Benutzer schickt Antwort zum Server.

Token (2)

- Token ohne Challenge-Response:
- Z.B. SecureID-Cards:
  - Berechnung eines Einmal-Passworts aus einem geheimen Schlüssel, der aktuellen Zeit und der Benutzer-PIN.
  - Server kennt geheimen Schlüssel und kann Rechnung nachvollziehen.
  - Änderung des Passworts z.B. alle 60 sec.
  - Begrenzte Lebensdauer der Karten: Abschaltung nach 3 Jahren.

Token (3)

- Chip-Karten:
  - Speicher-Karte:
    - Nicht flüchtiger Speicher, keine CPU, sehr billig.
    - Z.B. Telefonkarte, Krankenversicherungskarte
  - SmartCard:
    - Chip mit CPU, ROM, RAM und EEPROM
    - ROM speichert Betriebssystem, Kryptoverfahren, PIN-Prüfungsalgorithmus etc.
    - EEPROM speichert Schlüssel, PIN, Kontonummer etc.
    - Z.B. Geldkarte, SIM-Karte für Handy
- USB-Token
  - Gleiche Funktionen, andere Anschlüsse

SmartCard-Sicherheitsdienste

- Authentifizierung
  - Benutzer authentifiziert sich mit PIN gegenüber Karte.
  - Karte authentifiziert sich mit Challenge-Response gegenüber Kartenleser.
- Vertraulichkeit
  - Verschlüsselung zwischen Kartenleser und SmartCard
- Integrität
  - MAC Berechnung zwischen Kartenleser und SmartCard
- Verbindlichkeit
  - Erstellen digitaler Signaturen

Beispiel GSM: SIM-Karte

- SIM-Karte enthält u.a.
  - Teilnehmerkennung,
  - Authentifizierungsschlüssel,
  - PIN.
- Benutzer authentifiziert sich gegenüber Karte mit PIN.
- SIM-Karte authentifiziert sich mit symmetr. Challenge-Response gegenüber Netz.
- Aushandlung eines Sitzungsschlüssels zur vertraulichen Kommunikation.
- Problem: Das Netz authentifiziert sich nicht!

Biometrische Verfahren

- Authentifizierung anhand der Wiedererkennung unverwechselbarer und unveräußerlicher Merkmale
  - Z.B. Iris-Erkennung, Gesichtserkennung, Fingerabdruck
- Notwendig: Speicherung von Referenzmustern
  - Abweichung vom Original unvermeidlich.
  - Bei der Überprüfung müssen Toleranzwerte festgelegt werden.
- Fehlertypen
  - Abweisung berechtigter Benutzer, Akzeptanzproblem.
  - Unberechtigter wird authentifiziert, Sicherheitsproblem.
- Bisher noch kein Erfolg auf breiter Front, Zukunft fraglich.
  - Unausgereifte Technik, keine Akzeptanz, inakzeptable Fehlerraten, Eingriff in Persönlichkeitsrechte, ...

Einwahlauth.: PAP vs. CHAP

- PAP = Password Authentication protocol
- Verwendet bei Einwahl via PPP.
- Kennung und Passwort im Klartext.
- Keine Unterbindung bei Missbrauch möglich.
- Initiative ergreift der Client.

- CHAP = Challenge Handshake Authentication Protocol
- Verwendet bei Einwahl via PPP.
- Server sendet Challenge.
- Keine Passwortübertragung.

Einwahl: RADIUS / TACACS

- PAP und CHAP dienen nur der Authentifizierung der PPP-Verbindung.
- Eine Datenbank mit Kennung/Passwort ist vorzuhalten.
- Authentifizierungsdatenbanken sind aber in Netzwerken normalerweise bereits vorhanden.
- Abhilfe: RADIUS(Remote Dial-In User Service)-Protokoll oder TACACS-Protokoll bietet Verbindung zwischen Authentifizierungsserver und Einwahlauthentifizierung.

Kerberos

- Netzwerkauthentifizierungsprotokoll
- Keine Schlüssel übers Netzwerk.
- Kerberos-Server hält alle Schlüssel aller angeschlossenen User, Geräte und Dienste (Principals) im Netzwerk.
- Wenn ein Principal einen Dienst nutzen will, authentifiziert er sich mit Passwort gegenüber dem Kerberos-Server, der ein zeitlich begrenztes „Ticket“ zur Nutzung des Dienstes für den Principal ausstellt.
- Möglichkeit für Single-Sign-On.
- In vielen Betriebssystemen implementiert (Unix, Windows).