Universität Zürich[UZH]

Institut für Informatik

IT-Sicherheit: Gegenmassnahmen

Vorlesung: Wirtschaftsinformatik 1, Frühjahrssemester 2020

Lerneinheit 9

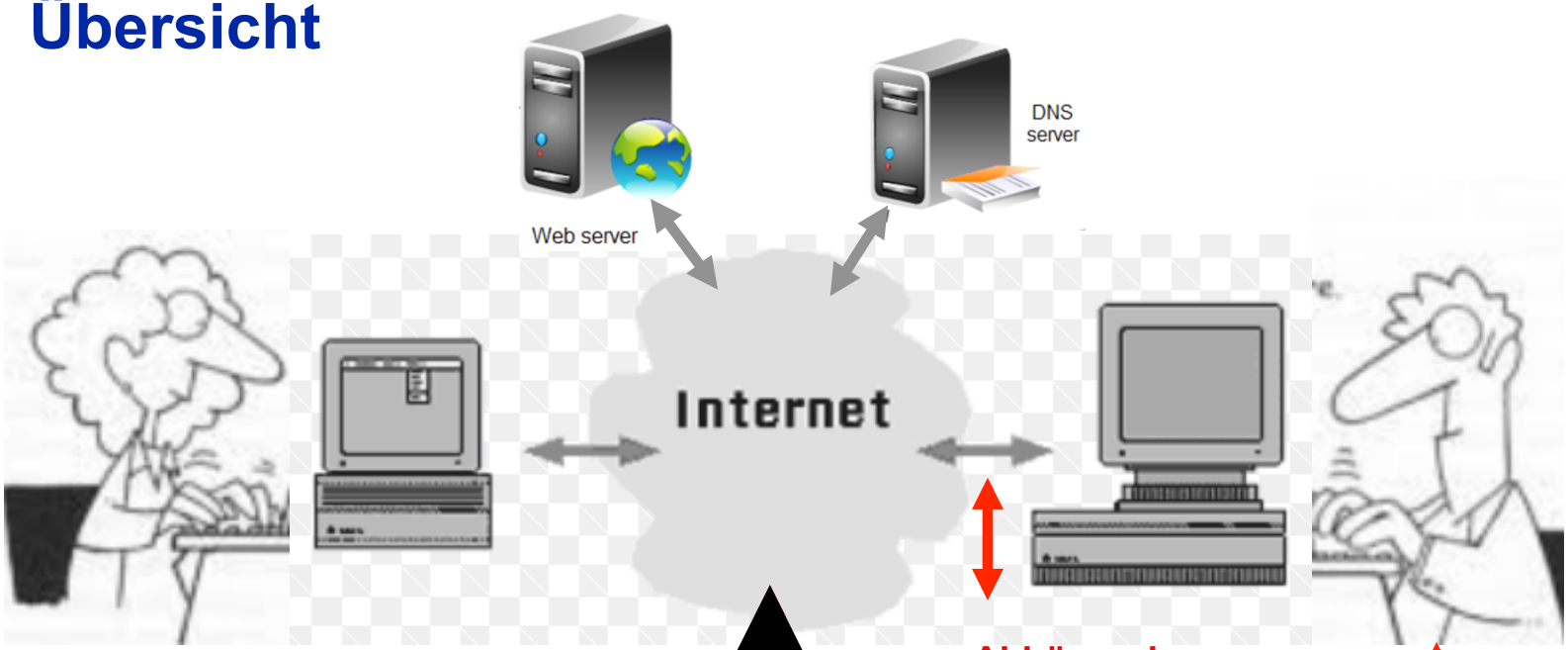
Prof. Dr. Lorenz Hilty

hilty@ifi.uzh.ch

Gliederung

1. **Übersicht**
2. Antivirensoftware
3. Kryptographische Verfahren
4. Organisatorische und ökonomische Aspekte

Übersicht



Abhören der Kommunikation:

passiv

aktiv (MITM)

Social Engineering

Phishing

Sonstiges…

Malware in Umlauf bringen:

Viren

Würmer

Trojaner

Mit Schadfunktionen:

Spyware

Backdoor

Ransom

Sabotage

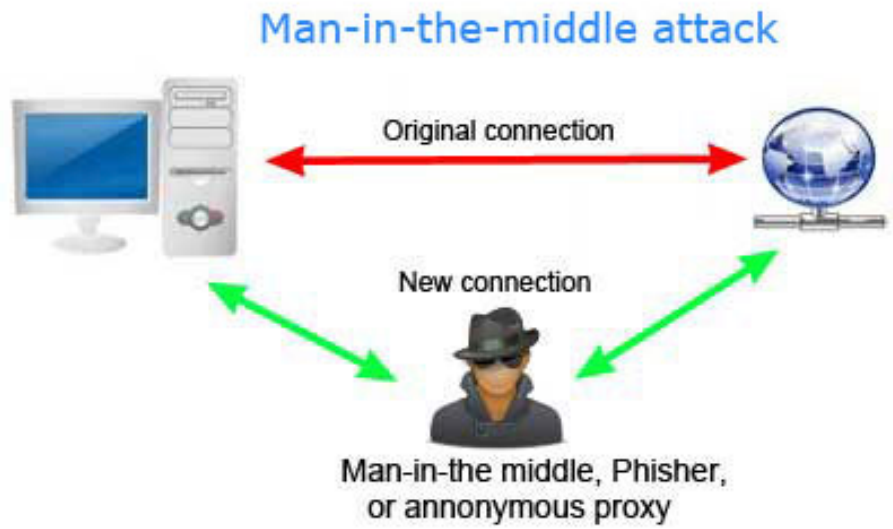
unautorisierter Zugriff auf fremde Ressourcen

Angreifer

DDOS Attacke:

Botnetz

Man-in-the Middle (MITM) Angriff



Beispiele:

- **ARP-Spoofing** in LANs und WLANs (Address Resolution Protocol)
- **Snarfing:** Vortäuschen eines falschen WLAN Access Points (Snarfing)
- **Pharming:** Umleiten der Zugriffe des Nutzers trotz korrekter URL auf einen falschen Webserver durch Manipulation von DNS-Anfragen

Angriffe auf IT-Systeme

- **sind möglich durch**
  - Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen (werden ausgenutzt durch Viren, Würmer, teilweise auch Trojaner)
  - Lücken in der Sicherheit der Datenübertragung, insbesondere von Kommunikationsprotokollen (werden ausgenutzt für MITM-Attacken)
  - die Beeinflussbarkeit von Benutzern (ausgenutzt durch Social Engineering, insbesondere Phishing)
- **haben das Ziel**
  - Authentifizierung zu umgehen und dem Angreifer dadurch unautorisierten Zugriff auf Ressourcen zu ermöglichen (primär betroffene Schutzziele: Vertraulichkeit, Integrität) **oder**
  - unmittelbaren Schaden anzurichten (primär betroffene Schutzziele: Verfügbarkeit, Integrität)

Gegenmassnahmen

- können folglich ansetzen
  - bei der Bekämpfung von technischen Sicherheitslücken oder der Schaffung von Resilienz (Toleranz gegenüber Störungen)
  - bei der Verschlüsselung der Kommunikation und der Authentifizierung der Kommunikationspartner
  - am Benutzerverhalten und dessen organisatorischen und ökonomischen Bedingungen

Gliederung

1. Übersicht
2. **Antivirensoftware**
3. Kryptographische Verfahren
4. Organisatorische und ökonomische Aspekte

Antivirensoftware

- Antivirenprogramme dienen zur Erkennung von Viren, Würmern und Trojanern (also nicht nur Viren).
- Auch Spyware und weitere Arten von Malware werden erkannt.
- Ursprünglich überprüften diese Programme nur ausführbaren Programmcode, scannen heute aber fast alle Dateiformate (z.B. wegen eingebetter Makros).
- Diese Programme verwenden zwar Heuristiken zur Erkennung bisher unbekannter Malware, zuverlässig kann jedoch nur *bekannte* Malware erkannt werden.
- Deshalb ist eine häufige (automatische) Aktualisierung der Antivirensoftware notwendig, was selbst auch ein Sicherheitsrisiko darstellt.

Probleme mit Antivirensoftware

- Der Echtzeitscanner, ein Hauptbestandteil eines Antivirenprogramms, kann die Funktion zeitkritischer Anwendungen und damit die Verfügbarkeit des Systems beeinträchtigen. Deshalb gibt es Ausschlusslisten für Anwendungen, die nicht gescannt werden sollen.
- Ähnliches gilt für Datenbanken, die durch Echtzeitscanner beeinträchtigt werden können.
- Mailserver können durch Antivirensoftware in ihrer Funktion gestört werden, da sie vom Antivirenprogramm entfernte Dateien vermissen.
- Der in einem Antivirenprogramm enthaltene Parser kann selbst zum Ziel von Angriffen werden.

Eine Studie ergab 2014, dass nahezu alle untersuchten Antivirenprogramme Fehler aufweisen und damit die Systeme, auf denen sie installiert sind, angreifbar machen. 40% aller IT-Sicherheitsverantwortlichen misstrauen der Antivirensoftware.

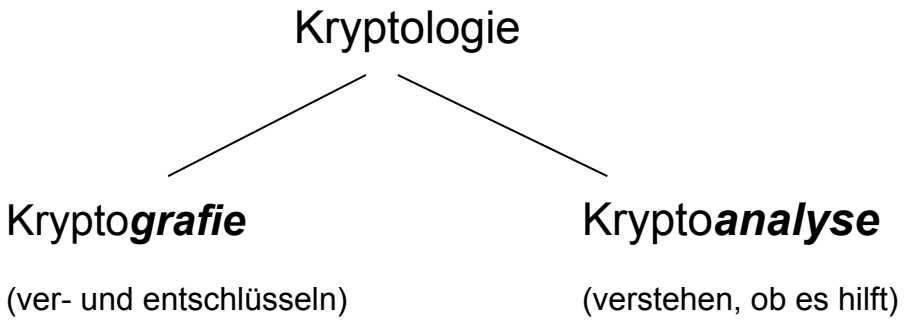
→ Die Existenz von Malware stellt für die IT-Sicherheit folglich ein Dilemma dar.

Gliederung

1. Übersicht
2. Antivirensoftware
3. **Kryptographische Verfahren**
4. Organisatorische und ökonomische Aspekte

Grundbegriffe

- Kryptografie: Die Wissenschaft von der geheimen Kommunikation. Ziel der Kryptografie ist es, zur Entwicklung von Informationssystemen beizutragen, die widerstandsfähig gegen Manipulation und unbefugten Informationszugang sind.
- Kryptoanalyse: Die Analyse der Wirksamkeit („Stärke“) von kryptografischen Verfahren.



Verschlüsselungsverfahren

Grundsätzliche Arten der Verschlüsselung:

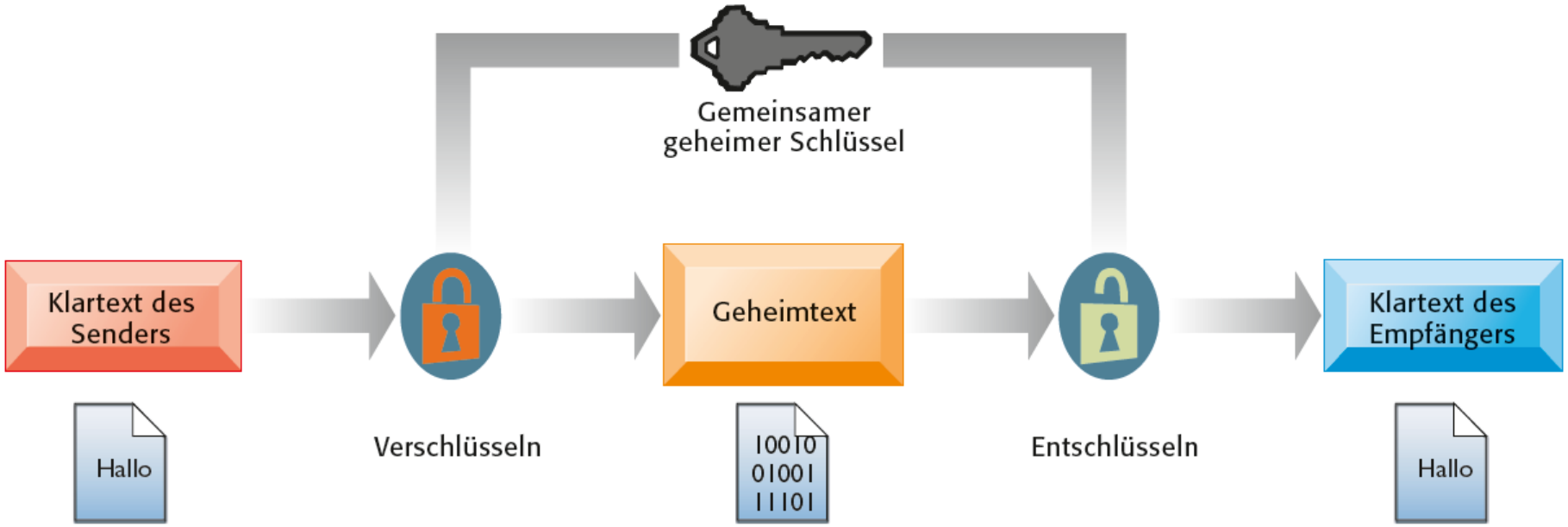
- **Symmetrisches Verfahren (Secret Key, SK):**
  Beide Kommunikationspartner besitzen den gleichen geheimen Schlüssel. Dieser dient ihnen zum Ver- und Entschlüsseln der Nachrichten.

  Beispiel: AES-Algorithmus (Advanced Encryption Standard)

- **Asymmetrisches Verfahren (Public Key, PK):**
  Jeder Kommunikationspartner besitzt ein Schlüsselpaar: einen öffentlichen und einen privaten Schlüssel. Der Sender verschlüsselt mit dem öffentlichen Schlüssel des Empfängers, der Empfänger entschlüsselt mit seinem privaten Schlüssel.

  Beispiel: RSA-Verfahren (Rivest, Shamir, Adleman)

Symmetrische Kryptografie (Secret-Key-Verschlüsselung)

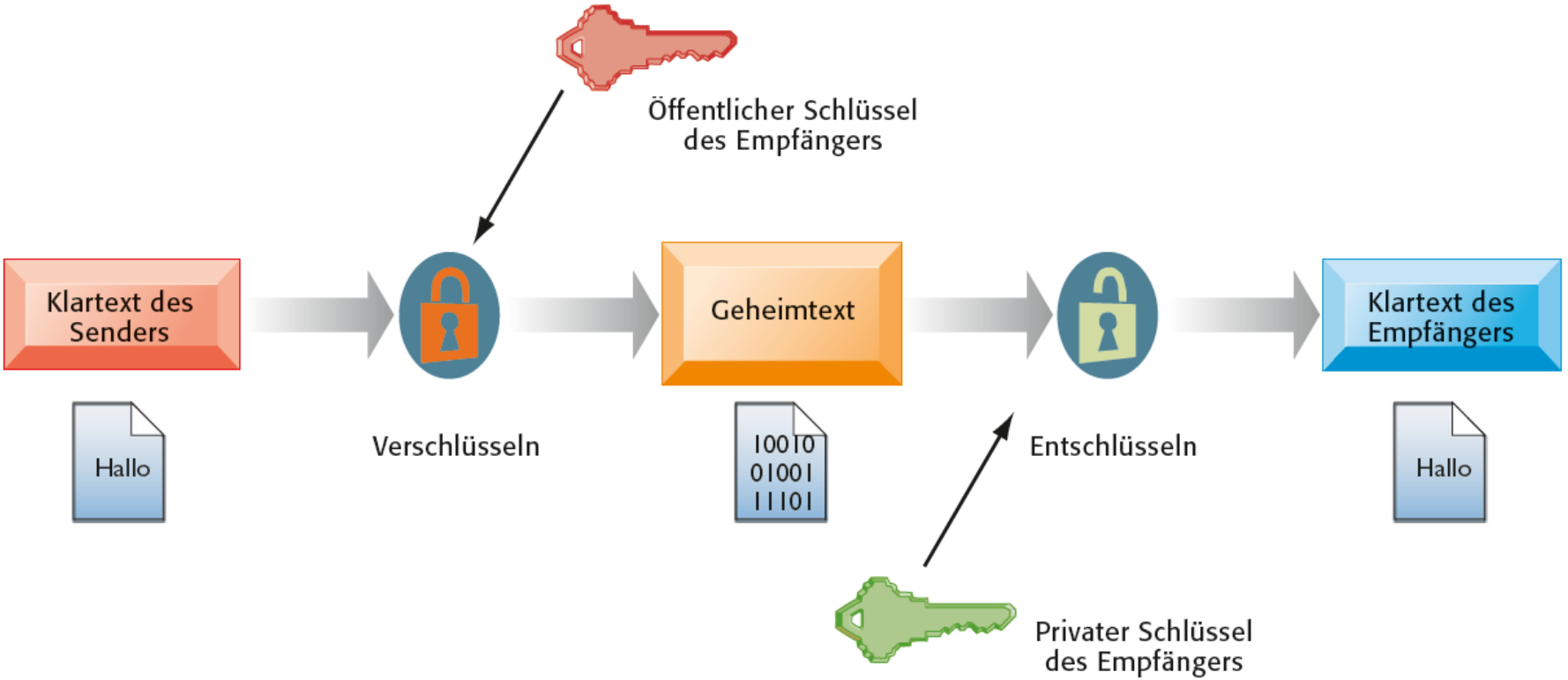


Vorteil: hohe Geschwindigkeit beim Ver- und Entschlüsseln

Nachteil: aufwändige Verteilung des Schlüssels unter allen Kommunikationspartnern

Adäquates Verfahren, wenn Daten nur für eine Person verschlüsselt werden.

Asymmetrische Kryptografie (Public-Key-Verschlüsselung)



Vorteil: einfacheres Schlüsselmanagement

Nachteil: Ausführung deutlich langsamer als bei SK-Verfahren

Wird nicht nur zur Verschlüsselung von Nachrichten, sondern auch zur Erstellung und Verifizierung digitaler Signaturen verwendet.

Verschlüsselung allein genügt nicht

Durch Verschlüsselung allein ist Kommunikation noch nicht sicher. Zusätzlich muss sichergestellt sein,

- dass eine Nachricht tatsächlich von dem Absender stammt, von dem sie zu kommen scheint **(Authentizität des Senders)**,
- dass eine Nachricht nicht verfälscht wurde **(Integrität)**,
- dass der Sender das Senden der Nachricht nicht im Nachhinein abstreiten kann **(Nicht-Abstreitbarkeit)**.

Hierfür gibt es elektronische Signaturen (juristischer Begriff), die technisch als digitale Signaturen umgesetzt werden.

- Eine **elektronische Signatur** ist digitaler Code, der einer elektronisch übertragenen Nachricht hinzugefügt wird, um ihren Inhalt und den Sender eindeutig zu identifizieren.
- Eine **digitale Signatur** ist das Verfahren (und das Ergebnis) der Erzeugung einer elektronischen Signatur mit Hilfe eines asymmetrischen Kryptosystems.

Verschlüsselung und digitale Signatur (1/2)

Achtung:

Verschlüsselung und digitale Signatur sind im Prinzip voneinander unabhängig:

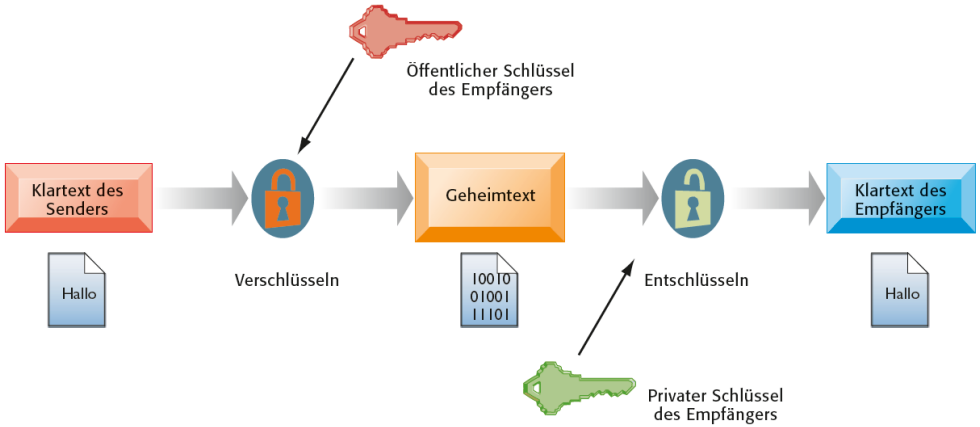
- Man kann eine Nachricht verschlüsseln, ohne sie zu signieren.
- Man kann eine Nachricht signieren, ohne sie zu verschlüsseln.

Ein Zusammenhang ist jedoch gegeben,

- weil die Kombination der beiden Verfahren sinnvoll ist, denn nur auf diese Weise können die Ziele der IT-Sicherheit erreicht werden;
- weil beide Verfahren auf asymmetrischen Schlüsseln beruhen können. Sie verwenden die Schlüssel **jedoch auf unterschiedliche Weise.**

Verschlüsselung und digitale Signatur (2/2)

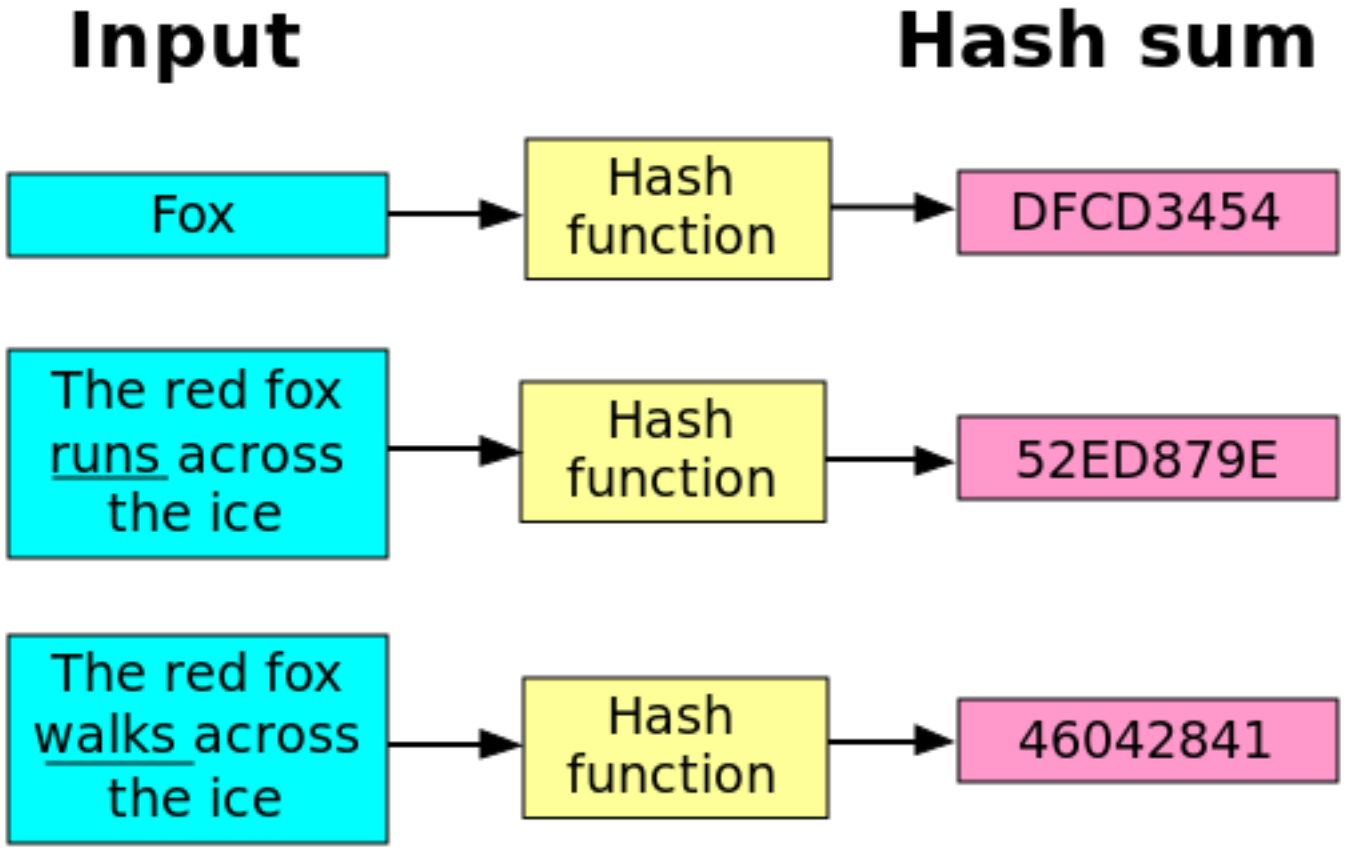
- Asymmetrische Verschlüsselung verwendet den **öffentlichen** Schlüssel des **Empfängers** zum **Verschlüsseln**, seinen **privaten** zum **Entschlüsseln**.



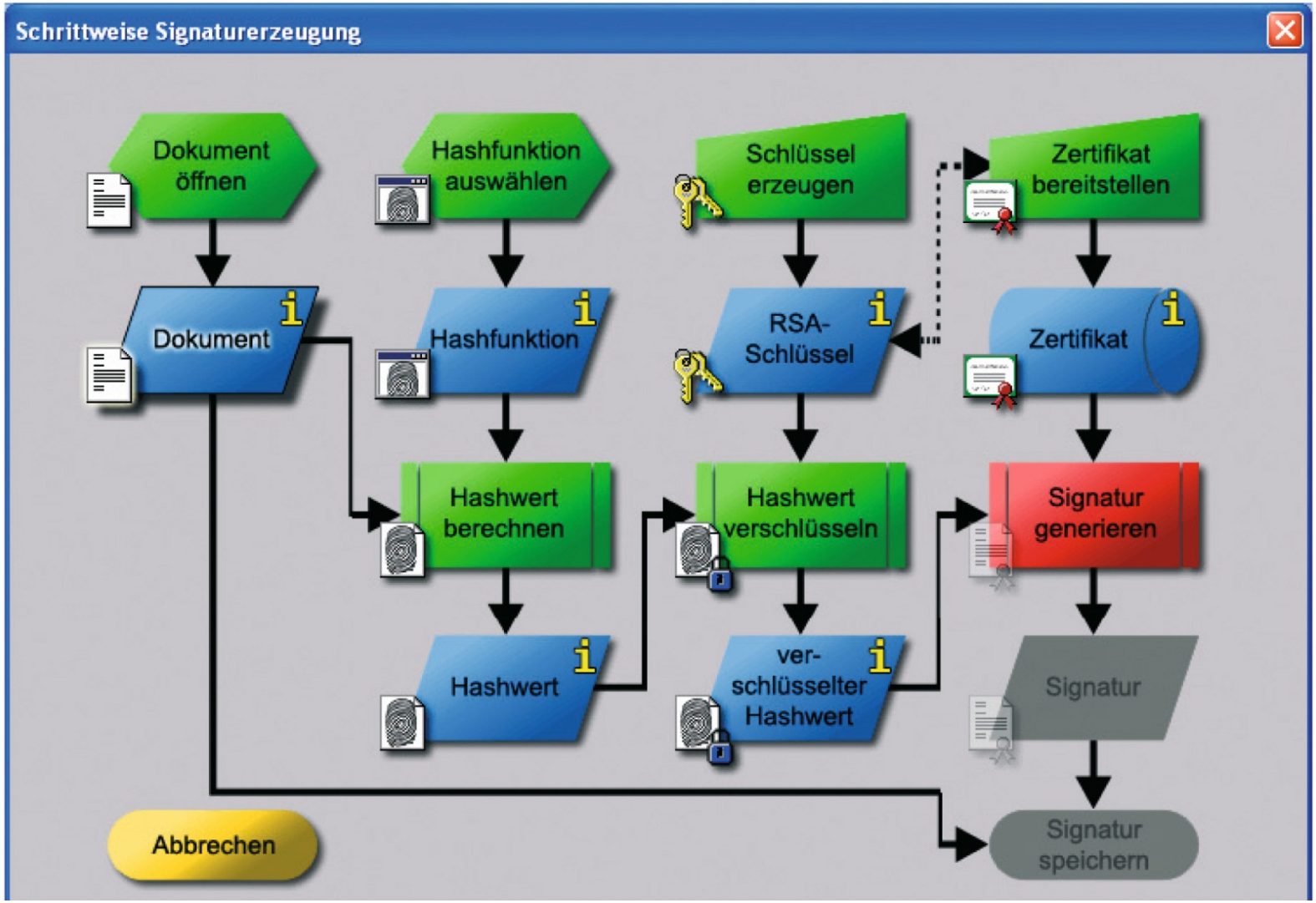
- Digitale Signatur verwendet
  - den **privaten** Schlüssel des **Senders** zum **Signieren** (durch den Sender)
  - den **öffentlichen** Schlüssel des **Senders** zum **Verifizieren** der Signatur (durch den Empfänger)
  - Zusätzlich ist ein **Zertifikat** aus vertrauenswürdiger Quelle nötig, das dem Sender seinen öffentlichen Schlüssel zuordnet.

Exkurs: Hashfunktion

Eine Hashfunktion wird u.a. benötigt, um bei der digitalen Signatur die Integrität der Nachricht sicherzustellen, siehe nächste Folie.
(Es gibt zahlreiche andere Anwendungen von Hashfunktionen.)



Erstellung einer elektronischen Signatur



Digitale Zertifikate

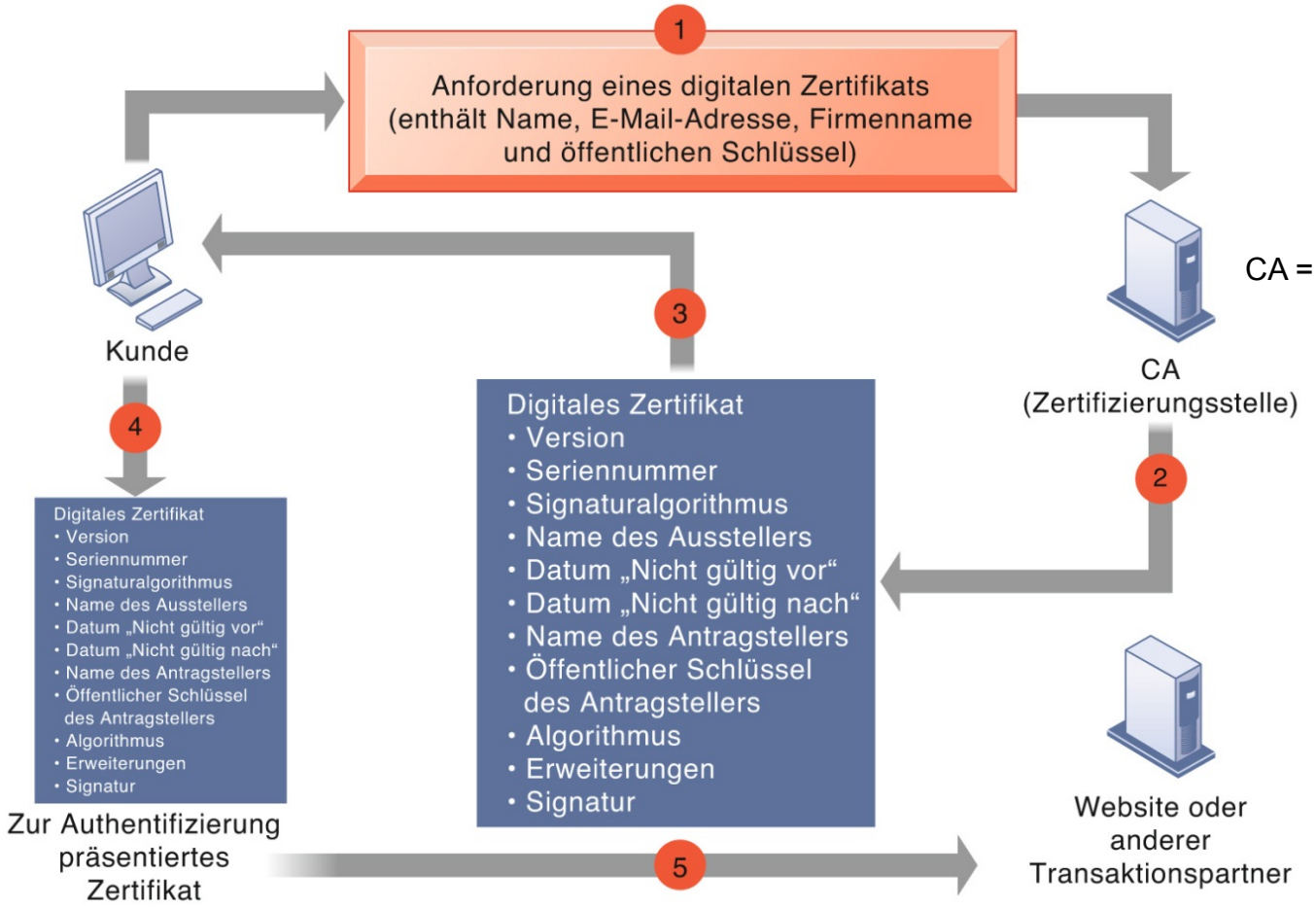


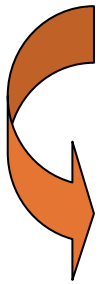
Abbildung 15.12: Digitale Zertifikate
Digitale Zertifikate können genutzt werden, um die Identität von Menschen oder elektronischen Daten sicherzustellen. Sie schützen Online-Transaktionen durch die Bereitstellung einer authentischen und verschlüsselten Kommunikation.

Rolle der Schlüssel bei Verschlüsseln und Signieren (Beispiel RSA)

(n, e): öffentlicher Schlüssel, (n, d): privater Schlüssel

M: Klartext, C: chiffrierter Text

Die Nachricht wird in Portionen i=1,2,3,… zerlegt.

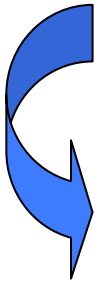


Nachricht verschlüsseln

$$C_i = M_i^e \bmod n \quad \text{für } i=1,2,3,\ldots$$

Nachricht entschlüsseln

$$M_i = C_i^d \bmod n \quad \text{für } i=1,2,3,\ldots$$



Signatur erzeugen

$$C = M^d \bmod n$$

Signatur verifizieren

$$M = C^e \bmod n$$

Gliederung

1. Übersicht
2. Antivirensoftware
3. Kryptographische Verfahren
4. **Organisatorische und ökonomische Aspekte**

Wahl des optimalen Sicherheitslevels

Das Gesetz vom abnehmenden Grenznutzen gilt auch für IT-Sicherheitsmassnahmen.

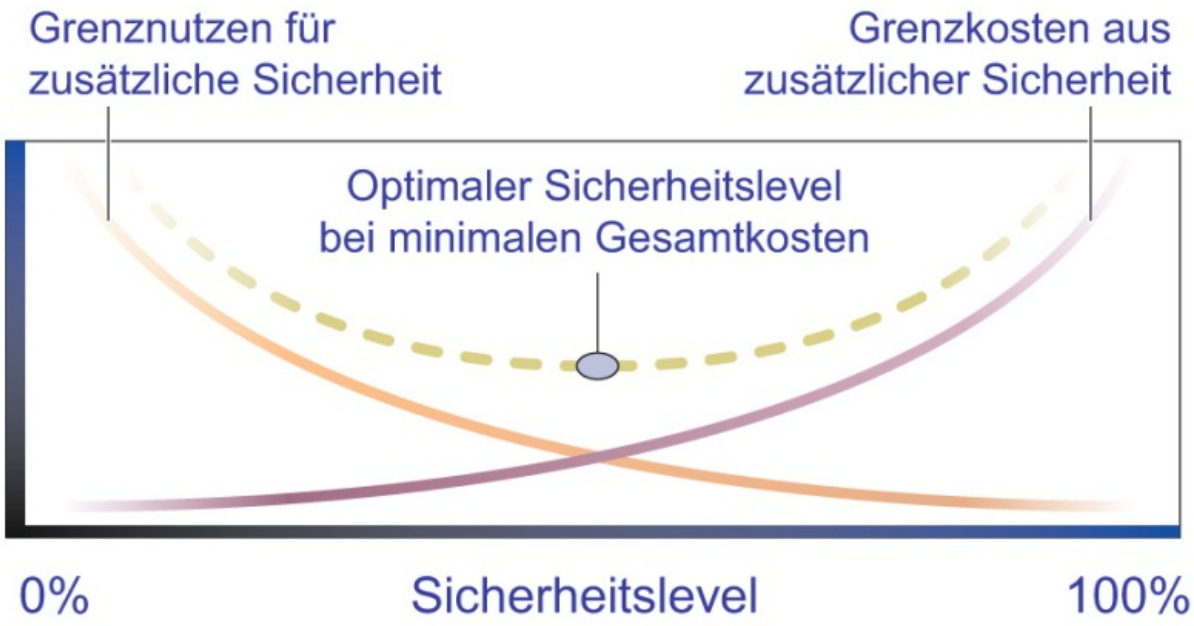


Abbildung 15.6: Optimaler Sicherheitslevel: Balance zwischen Kosten und Nutzen. Die Gesamtkosten setzen sich aus den Sicherheitskosten und den erwarteten Risikokosten zusammen.

Fiktives Beispiel

Tabelle 15.11

Beispiel für eine einfache Risikoabschätzung

Risiko	Wahrscheinlichkeit des Auftretens (%)	Verlustbereich/Durchschnitt (Euro)	Erwarteter jährlicher Verlust (Euro)
Stromausfall	30	5.000 bis 200.000 (102.500)	30.750
Veruntreuung	5	1.000 bis 50.000 (25.500)	1.275
Benutzerfehler	98	200 bis 40.000 (20.100)	19.698

Diese Aufstellung zeigt die Ergebnisse einer sehr vereinfachten Risikoabschätzung von drei ausgewählten Bereichen. Die Wahrscheinlichkeit, dass eines dieser Risiken innerhalb eines Jahres auftritt, ist als Prozentwert angegeben. Die nächste Spalte zeigt den geschätzten Verlustbereich, der bei jedem Auftreten stattfinden könnte, sowie einen durchschnittlichen Verlust, der als arithmetisches Mittel aus dem höchsten und dem niedrigsten Wert berechnet wird. Der erwartete jährliche Verlust kann ermittelt werden, indem man den durchschnittlichen Verlust mit der Wahrscheinlichkeit seines Auftretens multipliziert.

Schutz des vernetzten Unternehmens (1/3)

- Fehlertoleranz durch redundante Hardware- Software- und Stromversorgungskomponenten
  (letztere: Uninterruptible Power Supply, UPS)
- Redundante Festplatten (RAID, Redundant Array of Independant Disks)
- Load Balancing (Lastausgleich): Zugriffe auf mehrere Server verteilen, um DOSAttacken vorzubeugen
- Spiegelung: Alle Prozesse und Transaktionen werden auf eine zweiten System dupliziuert; sofern das primäre System ausfällt, kann das zweite System unmittelbar übernehmen

Schutz des vernetzten Unternehmens (2/3)

- **Disaster Recovery Planning (DRP):**
  Pläne für die Wiederherstellung von IT-Systemen nach einem Unterbruch durch ein schwerwiegendes Ereignis

technische Ebene

- **Business Continuity Planning (BCP):**
  Pläne für die Weiterführung des Geschäftsbetriebs nach einem Unterbruch durch ein schwerwiegendes Ereignis

Geschäftsprozess-ebene

Sicherheitsfunktionen können auch an Managed Security Provider (MSSP) ausgelagert werden, z.B. Überwachung der Netzwerkaktivität (Monitoring).

Schutz des vernetzten Unternehmens (3/3)

Sensibilisierung der Benutzer

- Wahl starker Passwörter
- Möglichst einheitliche Anforderungen an Passwörter über alle Systeme
- Wachsamkeit gegenüber Phishing und andere Formen des Social Engineering fördern.
- Aufmerksamkeit für Malware fördern.

Jedoch können strukturelle Probleme, insbesondere **falsche Anreizzstrukturen**, nur begrenzt durch Appelle an individuelles Verhalten gelöst werden.

Eine spieltheoretische, d.h. ökonomische Betrachtung ist notwendig.
→ **Ökonomie der Informationssicherheit** (siehe nächste Folien)

Ökonomische Aspekte der IT-Sicherheit (1/2)

Für alle Beteiligten gibt es den Tradeoff zwischen Aufwand und Nutzen der Sicherheit und – daraus resultierend – ein subjektives Optimum.

- **Anbieter von Softwareprodukten und Dienstleistungen:**
  Wenn die Kunden die Sicherheit der Produkte nicht einschätzen können (Informations-Asymmetrie), sind sie nur bereit, wenig für Sicherheit zu bezahlen. Dadurch gibt es für den Anbieter keinen Anreiz, hohe Sicherheit zu bieten. (= Zitronenproblem)

- **Nutzer von Netzwerken**
  Sie tragen nicht die vollen Konsequenzen eines Schadens, zu dem sie beitragen. Z.B. kann ein einzelner Nutzer wenig zu verlieren haben, als schwächstes Glied in einer Sicherheitskette aber für die Allgemeinheit einen hohen Schaden verursachen.
  (= Allmend-Problem)

Ökonomische Aspekte der IT-Sicherheit (2/2)

- Die Haftung für Sicherheitsprobleme sollte jenen Akteuren übertragen werden, die am besten in der Lage sind, das entstehende Sicherheitsrisiko zu beherrschen.
- Den Unternehmen müssen Anreize gegeben werden, z.B. durch Gesetze und Überprüfung ihrer Datenschutzrichtlinien, die Privatsphäre ihrer Kunden zu achten.

Laudon/Laudon/Schoder
Wirtschaftsinformatik
3., vollständig überarbeitete Auflage

Grundlage für diese LE:
Abschnitt 15.2

Zum Prüfungsstoff gehören neben den Folien:

Laudon/Laudon/Schoder 2016, **Abschnitte 15.2.5 bis 15.2.8, S. 1015-1033**

Fehlerhinweis: S. 1025, Exkurs Zahlenbeispiel RSA-Verfahren, rechte Spalte, Punkt 5 muss korrekt lauten:

"Verschlüsselung: $C = 2^7 \bmod 55 = 18$"

Die *Ent*schlüsselung ist im Beispiel nicht gezeigt.