Vorlesung Netzsicherheit
Kapitel 1 – Einführung

PD Dr. Ingmar Baumgart, PD Dr. Roland Bless, Matthias Flittner, Prof. Dr. Martina Zitterbart
baumgart@fzi.de, [bless, flittner, zitterbart]@kit.edu

Herzlich willkommen!

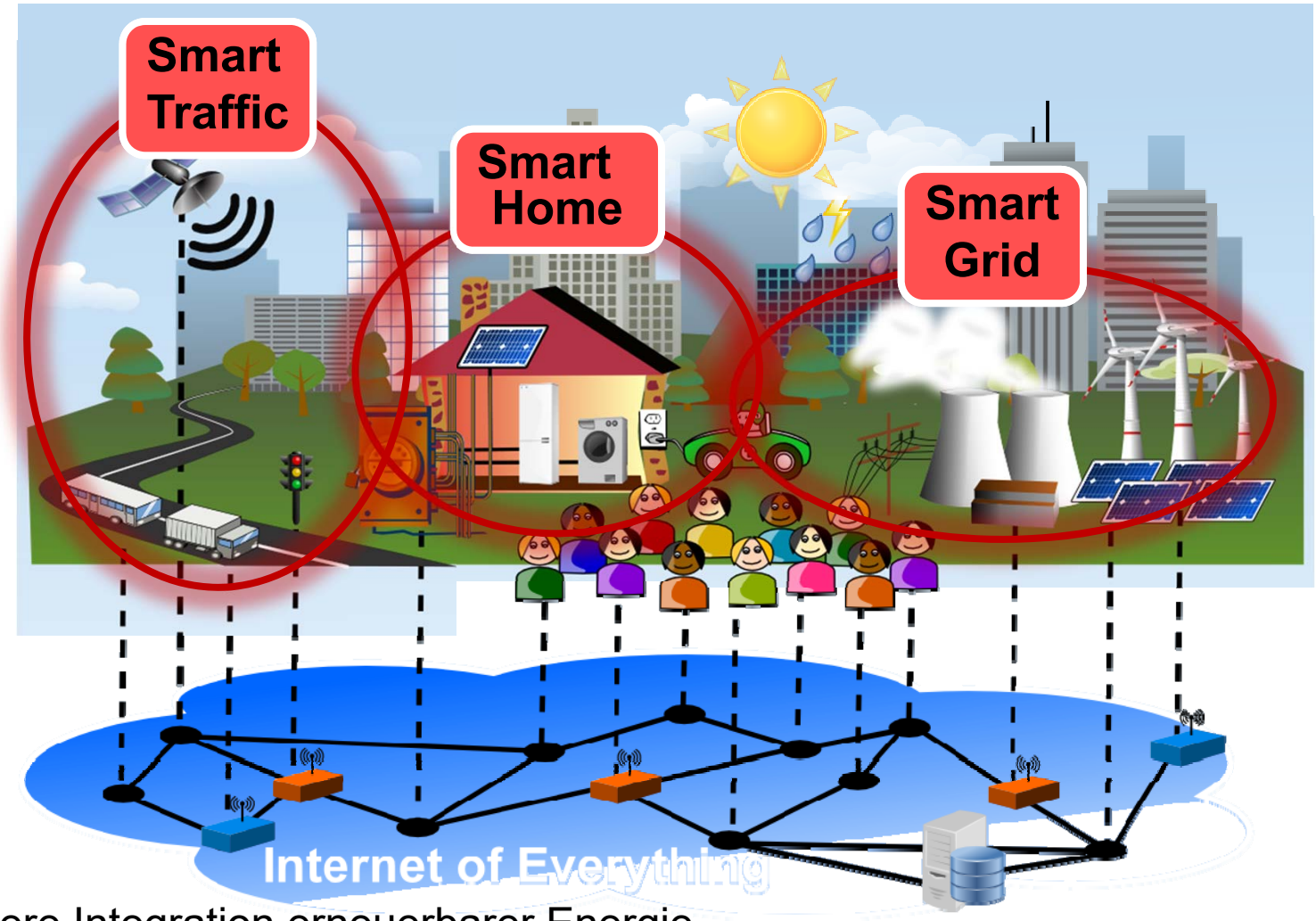
- PD Dr. Ingmar Baumgart

- PD Dr. Roland Bless

- Matthias Flittner, M.Sc.

- Prof. Dr. Martina Zitterbart

Smarte Welt – alles vernetzt



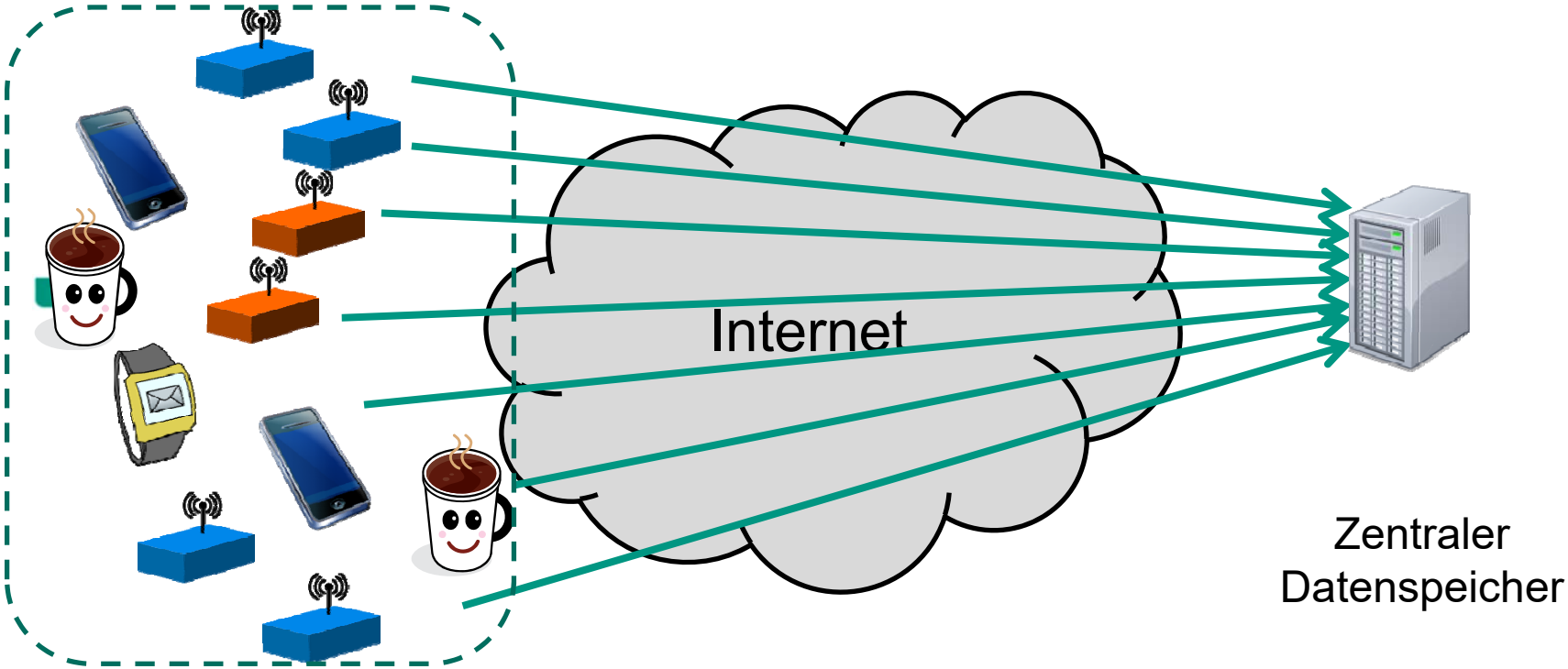
→ Bessere Integration erneuerbarer Energie

→ „Assistiertes Leben“

→ Bessere Organisation des Verkehrs

Vernetzte Daten

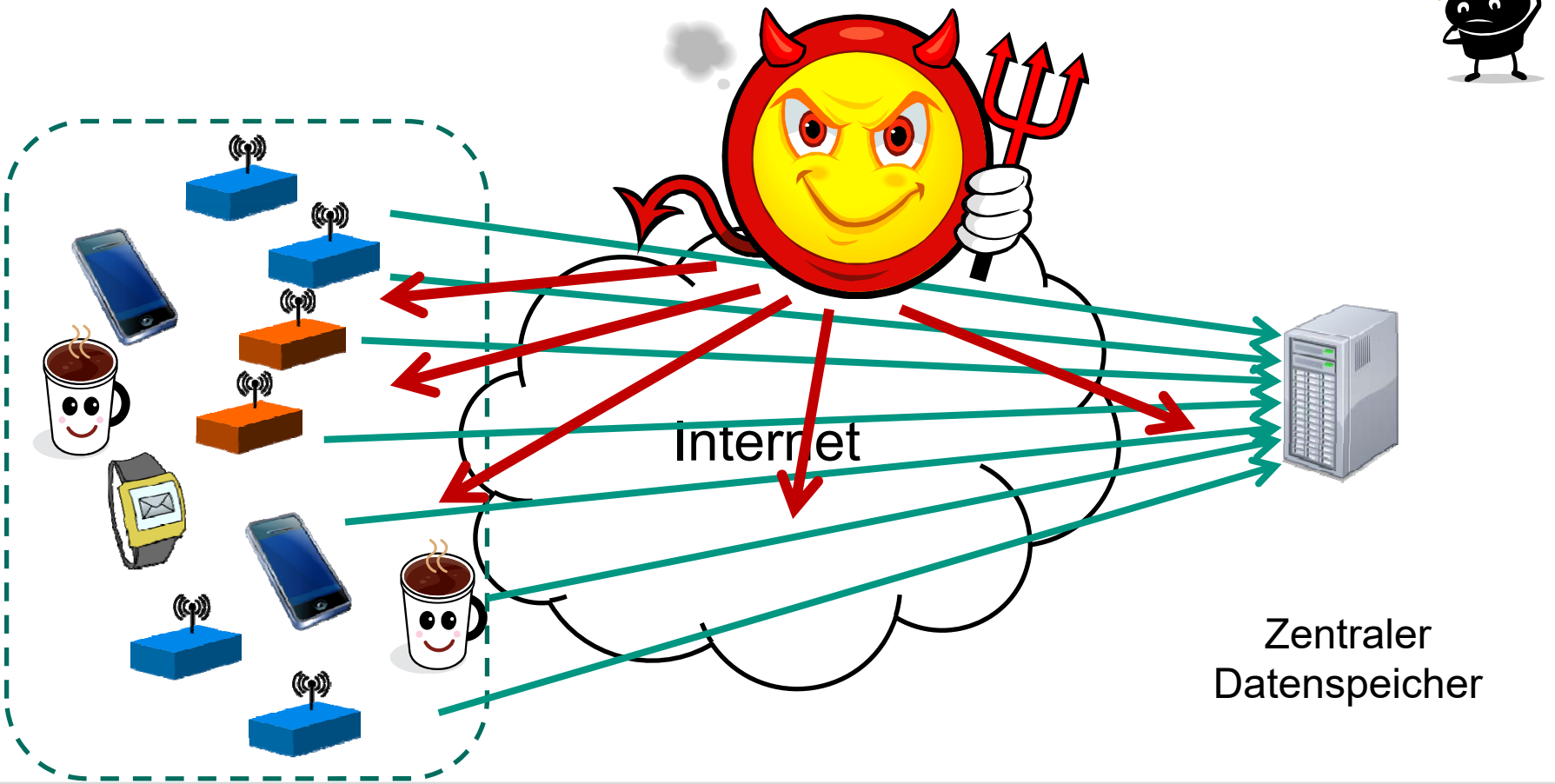
Sensoren/Geräte im Smart Home



- Kann jemand die Daten mitlesen?
- Sind die Daten dort sicher?
- Privatsphäre?
- Vertrauen?

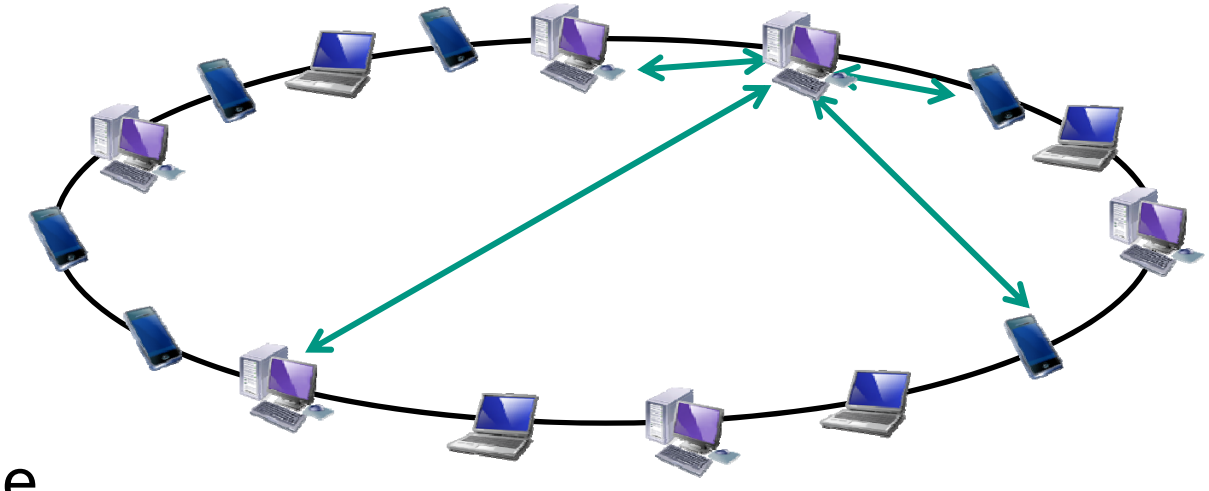
Aber …

- Systeme können (z.B. über das Internet) angegriffen werden!
- Jüngstes Beispiel: Mirai Botnet (1,1 Tbit/s und mehr)



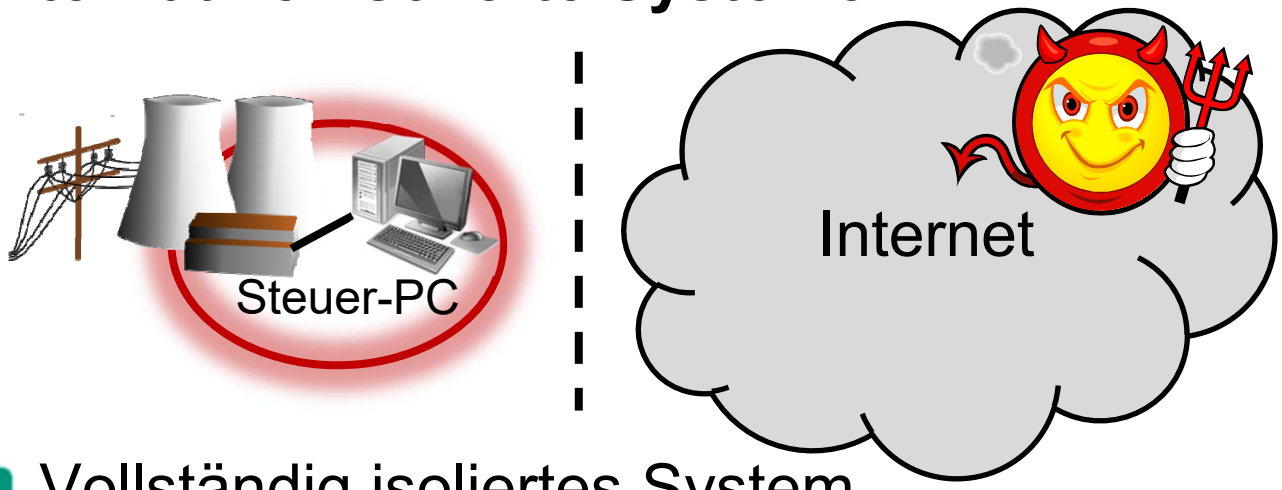
Alternative: vollständig verteiltes System?

- Verzicht auf zentralen Datenspeicher
  → „Peer-to-Peer“-Netz
  - verteilte Speicherung von Daten, Filesharing (BitTorrent)



- Probleme
  - Vertrauensbasis?
  - Kontrolle, z.B. Zugang?
  - Nachvollziehbarkeit?
  - Zuverlässigkeit?

Alternative: Isolierte Systeme?

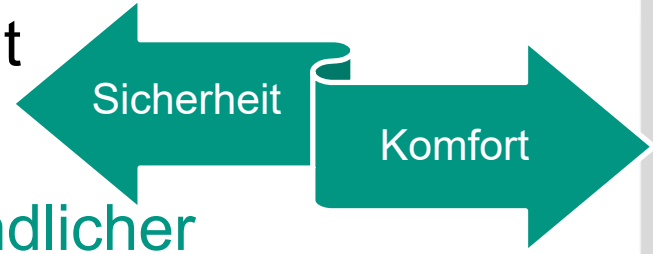


- Vollständig isoliertes System
  - Theoretisch „sicher“
    - Kein Netzwerkzugriff möglich! („Air Gap“)
    - Keine Angreifer aus der Ferne!
- Praktisch gibt es immer eine Verbindung nach außen…
  - Einspielen von System-/Sicherheitsupdates evtl. häufig notwendig
  - SneakerNet: über entfernbare Medien (z.B. USB-Flash-Laufwerk → Stuxnet)
  - über „Update“-Laptop → verwundbar

[Byre13]

Hundertprozentige Sicherheit?

- … gibt es in solchen Umgebungen nicht



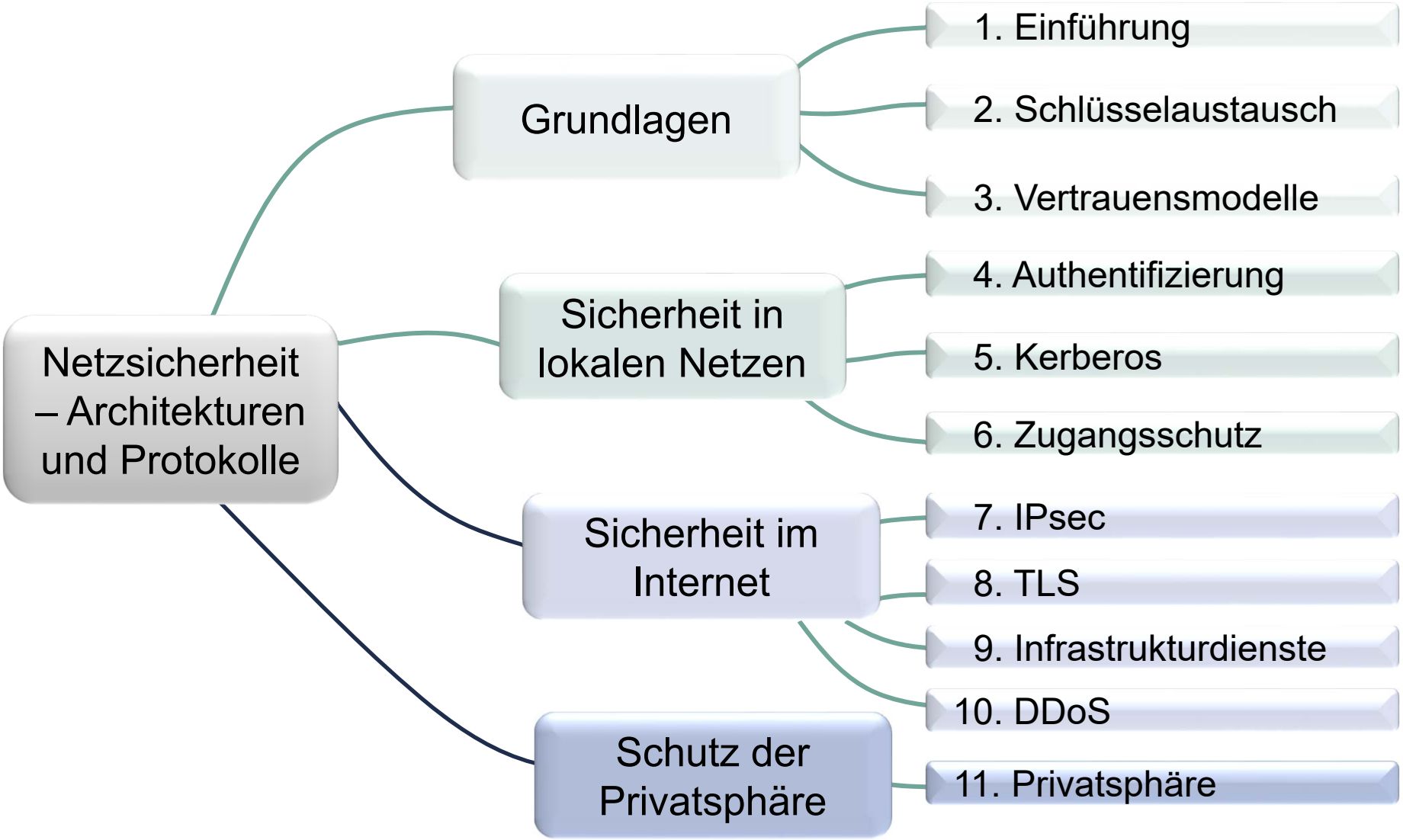
- Sicherheit macht Benutzung oft umständlicher
  - Sicherheit ist auch immer mit „Kosten“ verbunden – Abwägung, wo Zusatzaufwand gerechtfertigt ist
  - Realwelt-Beispiel: Kugelsichere Weste ist zwar sicherer, aber auch ziemlich unbequem…

→ Sicherheit auch „smart“ machen
  - Wirksam, nachvollziehbar, einfach benutzbar
  - Wir forschen an Konzepten, Algorithmen und Protokollen für sichere, effiziente und robuste Kommunikationssysteme

Ziele der Vorlesung

- Grundsätzliches Verständnis für relevante Verfahren
  - Was sind wichtige Probleme?
  - Mit welchen Konzepten können diese gelöst werden?
- Praktischer Einsatz von Protokollen
  - Welche Angriffe werden wie verhindert?
- Berücksichtigung von Randbedingungen
  - Technische Möglichkeiten
  - Kosten
  - Faktor Mensch

Inhalte der Vorlesung



Literatur zur Vorlesung

„Netzsicherheit“,
Günther Schäfer, Michael Roßberg, 2. Auflage, dpunkt Verlag, 2014, ISBN Print: 978-3-86490-115-7

„Sicherheit in Kommunikationsnetzen“,
Sorge, Gruschka, Lo Iacono, 1. Auflage, Oldenbourg-Verlag, 2013, ISBN-13: 978-3-486-72016-7

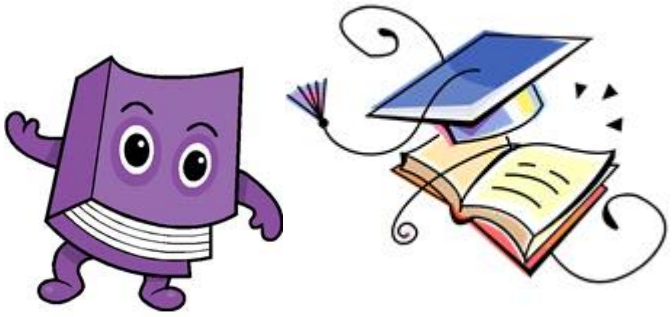
„Sichere Netzwerkkommunikation“, Bless, Blaß, Conrad, Hof, Kutzner, Mink, Schöller, Springer, 2005, ISBN 3540218459

KIT Bib: Fachgruppe: inf 2.57, Signatur: 2005 A 8165

Fakultät für Informatik: Signatur: B.Sic(47794)

Hilfreiche Literaturquellen

- Internet-Standards
  - Die Standard-Dokumente zu den Internet-Protokollen sind online frei zugänglich (https://www.ietf.org).
    - RFC-Suche (https://rfc-editor.org/rfcsearch.html)
- Allgemeines zum Internet
  - Informationen über das Internet finden Sie auch unter der folgenden Web-Adresse: http://www.isoc.org/internet/
- Artikel in Fachzeitschriften über
  - IEEE Bib (http://ieeexplore.ieee.org)
  - ACM BIB (http://portal.acm.org)
  - Frei zugänglich aus dem KIT-Netz!



… die einzelnen Kapitel enthalten dedizierte Literaturangaben

Organisatorisches

- Sprechstunde
  - Fragen am Besten in der Vorlesung klären
  - Termine für Sprechstunde nach Vereinbarung → Bitte per E-Mail Termin anfragen
- Informationen und Vorlesungsfolien im Web
  - https://telematics.tm.kit.edu/
  - https://ilias.studium.kit.edu/
  - Passwort für ILIAS Kursanmeldung: tele-matik
- Öffnungszeiten des Sekretariats
  - Montag – Donnerstag von 08:00 Uhr bis 11:45 Uhr
  - Mittwochs auch von 13:00 bis 14:00 Uhr
  - Freitags ist geschlossen
- Anmeldungen zu Praktika/Seminaren
  - Per Web unter https://telematics.tm.kit.edu
  - … oder bei Fragen und Problemen
    - im Sekretariat von Prof. Zitterbart bei Frau Natzberg oder
    - per E-Mail/Telefon an Frau Natzberg

Prüfungstermine

- Prüfung
  - Derzeit mündliche Prüfungen
- Prüfungstermine
  - Es werden mehrere Blöcke von Terminen für die Vorlesung bekannt gegeben
  - Konkrete Termine
    - Auf den Webseiten (https://tm.kit.edu/lehre/termine)
    - Im Sekretariat erfragen
- Anmeldung zu Prüfungen
  - Im Sekretariat von Prof. Zitterbart bei Frau Natzberg, Informatikgebäude am Schloss
    (Geb. 20.20), Raum 360, Tel.: 608-46411,
    Email: telematics@tm.kit.edu
  - Für die Prüfungen bitte die jeweils für Ihren Studiengang gültigen Prüfungsregelungen beachten

Forschungsthemen Lehrstuhl Zitterbart

- Future Internet: Algorithms, Protocols, Architectures

Software-defined Networking, Virtualization, Management	Network Security & Privacy Protection	High Performance Networking	Internet of Things / of Everything

- Methods & Tools: Evaluation, Design-Process

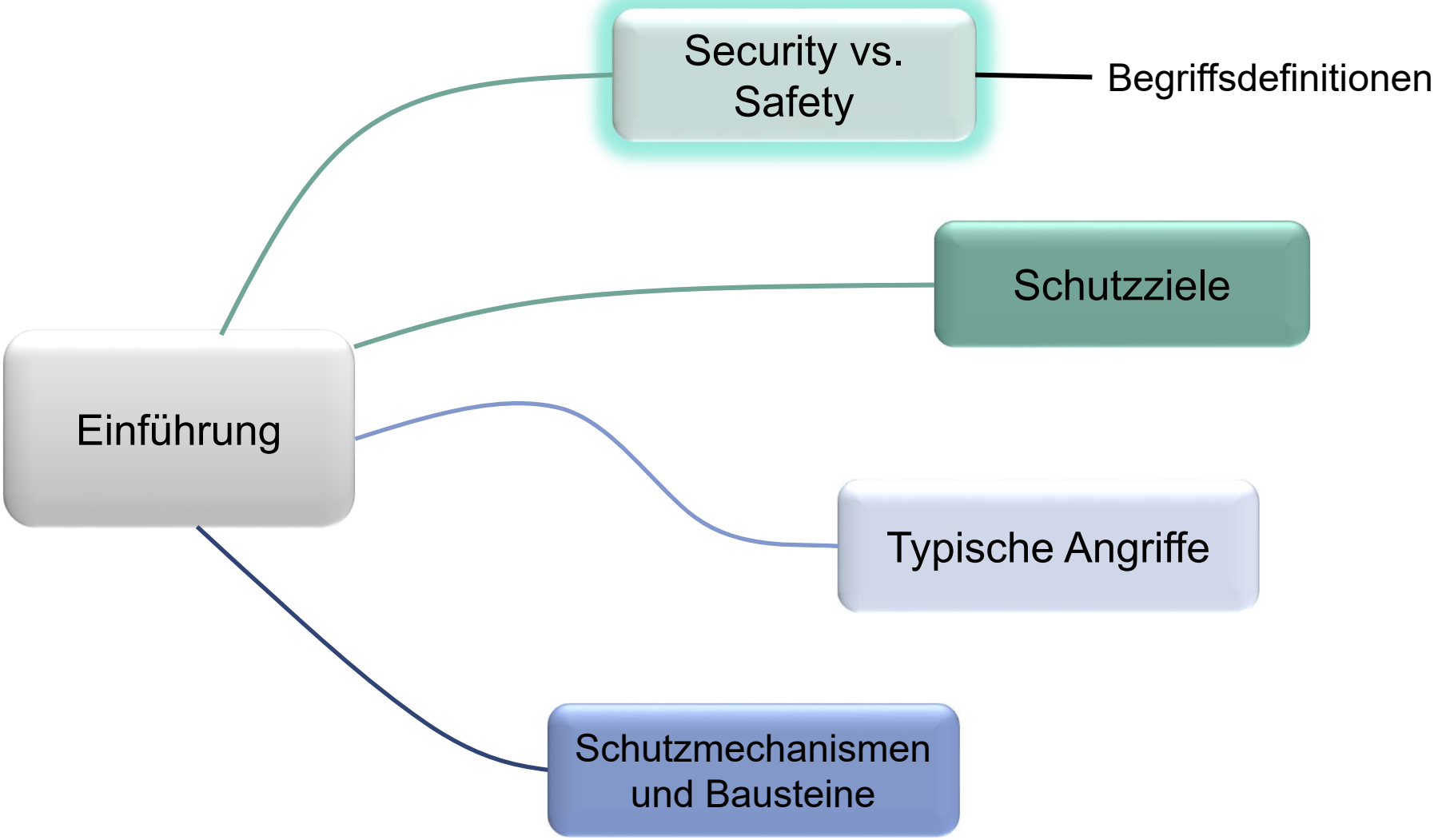
Analysis & Simulations	Prototypes, Testbed Experiments	Systematic Design Process

Selber aktiv werden?

- Interesse? Wie wäre es beispielsweise als
  - Hiwi
  - Bachelor-/Masterarbeiter
  - ... oder als aktiver Teilnehmer an einer/mehreren der Arbeitsgemeinschaften?

- Schauen Sie doch einfach mal am Institut vorbei!
  - Informatikgebäude am Schloss (Geb. 20.20), 3. Stock

Inhalte dieses Kapitels



Begriffsdefinitionen (I)

- (IT-)System
  - Gesamtheit von Komponenten, die zusammenwirken, um eine bestimmte Funktionalität zu erfüllen und Informationen zu verarbeiten
  - z.B. Internet, Auto, Smart-Home
- Komponente
  - Bestandteil eines technischen Systems, der eine abgeschlossene (Teil-)Funktion des Systems realisiert und durch explizite Schnittstellen sowohl diese Funktion anbietet als auch Funktionen anderer Komponenten erfordern kann
  - z.B. Server, Router, Firewall, Switch, WLAN Access Point

Begriffsdefinitionen (II)

- Güter
  - Ressourcen, die für mindestens einen Akteur einen (subjektiven) realen oder ideellen Wert besitzen
  - z.B. Kontaktliste im Handy, Patientendatenbank, Kreditkarteninformation, Webserver, Stromverbrauchswerte
- Schutzziel
  - Anforderungen an eine Komponente oder ein System, die erfüllt werden müssen, um Güter vor Bedrohungen zu schützen
  - z.B. übertragene Daten sollen nicht abgehört werden, übertragene Daten sollen unverändert ankommen, Laptop soll nicht gestohlen werden können

Begriffsdefinitionen (III)

- Bedrohung
  - Eine Bedrohung eines IT-Systems ist eine Möglichkeit, ein oder mehrere Schutzziele gezielt zu beeinträchtigen

- Typische Bedrohungen in vernetzten Systemen
  - Abhören von Daten
  - Einfügen, Löschen oder Verändern von Daten
  - Verzögerung und Wiedereinspielen von Daten
  - Maskerade
  - Autorisierungsverletzung
  - Sabotage
  - Offenlegung von Kommunikationsbeziehungen

Begriffsdefinitionen (IV)

- Angriff
  - Ein Angriff ist die gezielte Realisierung einer Bedrohung
- Angreifer
  - Ein Angreifer ist ein System, eine Person oder eine Personengruppe, die einen oder mehrere Angriffe durchführen
  - z.B. Hacker, Saboteur
- Angreifermodell
  - Ein Angreifermodell beschreibt die Fähigkeiten eines Angreifers, Angriffe auf ein System durchzuführen
  - z.B. Lokalität, Werkzeuge, kryptografische Fähigkeiten

Begriffsdefinitionen (V)

- Sicherheit
  - Zustand des Geschütztseins von schützenswerten Gütern vor Bedrohungen und Gefahren
  - Es gibt Gefahren, die nicht von einem Angreifer ausgehen
  - Konkret festgelegen, welche Güter und Bedrohungen betrachtet werden
  - Bedrohungen hingegen müssen immer von einem Angreifer ausgehen. Dennoch kann eine Bedrohung (durch einen Angreifer) zu einer (angreiferlosen) Gefahr führen.
  - Im Deutschen keine Unterscheidung von Safety+Security

Sicherheit: Safety vs. Security

- Safety 
  - Zustand des Geschütztseins von schützenswerten Gütern vor bestimmten Gefahren
    - Funktions- / Betriebssicherheit (Verlässlichkeit)
    - z.B. Schutz der Umgebung, Verhindern von Personenschäden
    - Gefährdung durch „wohlwollenden Angreifer“
  - Ist-Funktionalität von Komponenten stimmt mit der Soll-Funktionalität überein

- (Information-) Security 
  - Angriffssicherheit
  - Bedrohung durch „böswilligen Angreifer“
  - z.B. Schutz der Integrität von Informationen

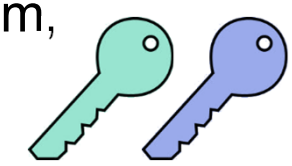
Systemsicherheit – aber wie?

- Sicherheit im Nachhinein für ein unsicheres System nachzurüsten ist manchmal praktisch unmöglich!
- Vorgehen: Sicherheitsanalyse eines Systems durchführen
- Definieren: Güter → Schutzziele → Bedrohungen
- Struktur- und Bedrohungsanalyse
  - (grober) Systementwurf muss schon existieren
  - z.B. konkrete Verortung von Angreifern und Systemen notwendig
- Sicherheitsmechanismen hinzufügen, um relevante Angriffe abzuwehren
- Analyse: welche Angriffe sind noch möglich?
- Risikobewertung

Mehr dazu in der VL
IT-Sicherheitsmanagement

Vielschichtige Sicherheit (1)

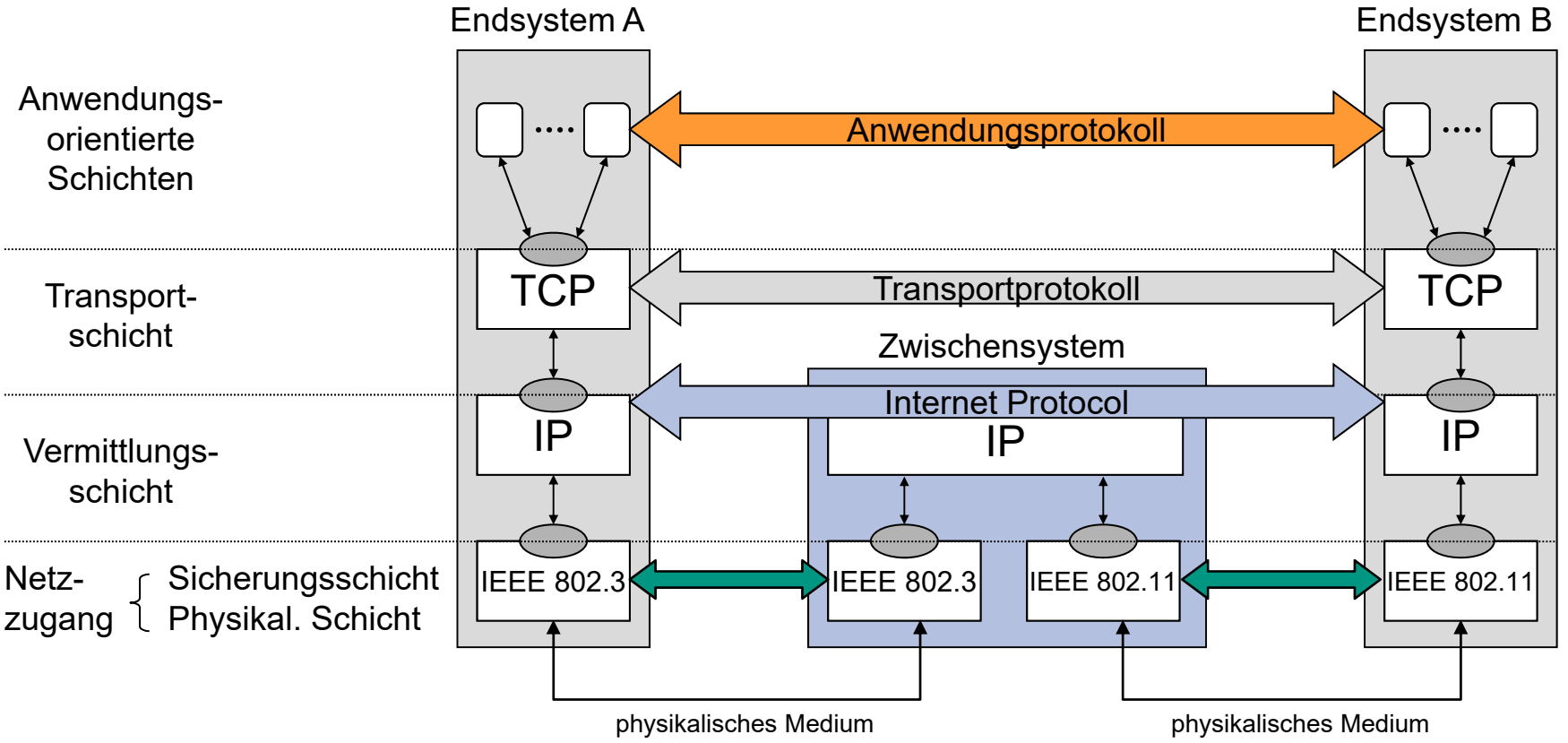
- Kryptographische Verfahren und sichere Protokolle sind nur Teilaspekt
- Richtige Umsetzung der Verfahren in der Praxis ebenso wichtig!
  - Beispiel: Einsatz eines aktuell sehr sicheren kryptographischen Verfahrens, aber Schlüsselaustauschproblem bleibt
  - Schlüsselmanagement ist häufig praktisches Problem, insbesondere auch im Internet der Dinge
    - Initiales Ausbringen von Schlüsselmaterial?
    - Wechsel der Schlüssel (z.B. nach Kompromittierung)?
    - Ist überhaupt klar, mit wem der Schlüssel getauscht wird?



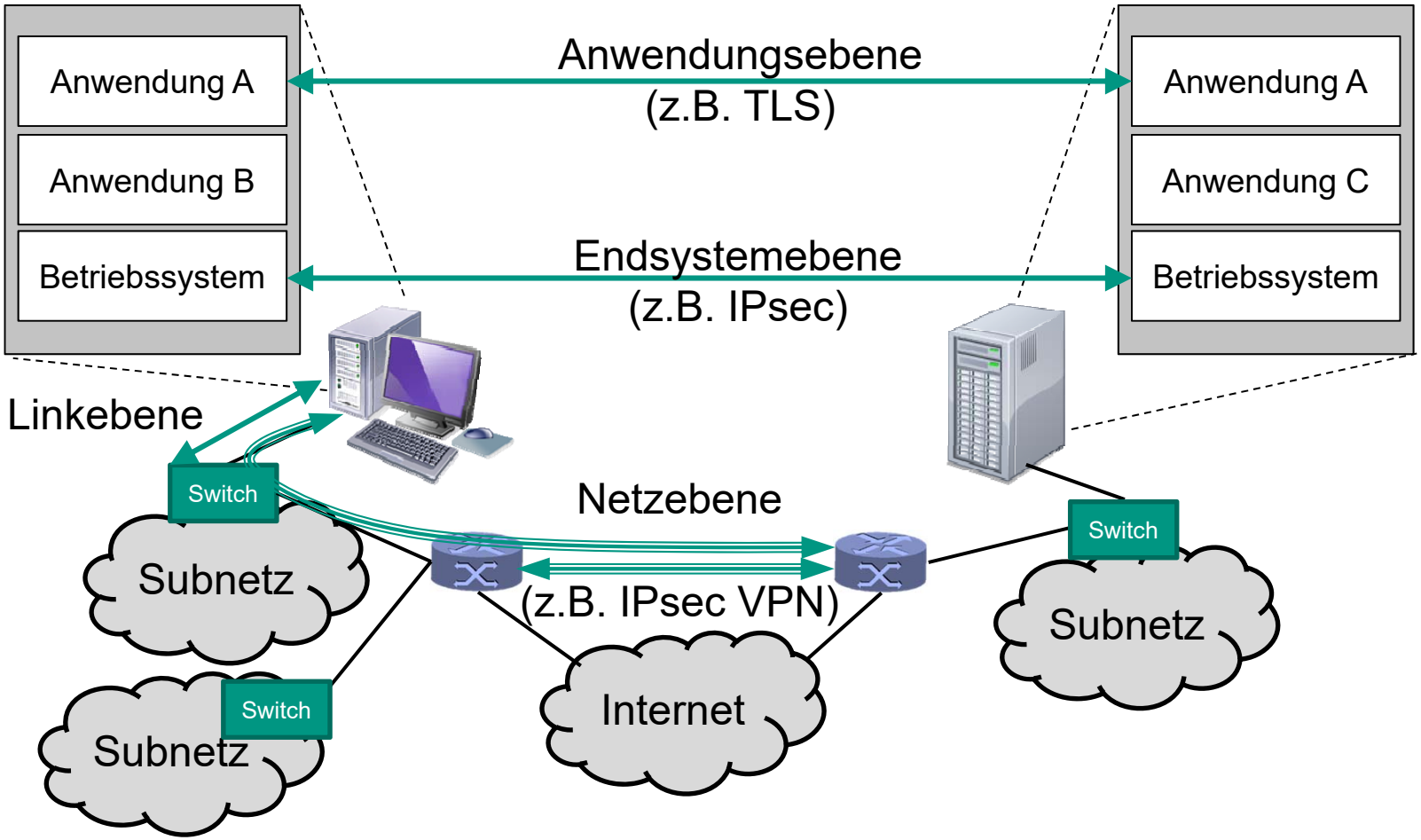
- Kontrollebene und Metadaten?
  - z.B. Verkehrsanalyse häufig wichtiger als Kenntnis des Inhalts

Vielschichtige Sicherheit (2)

- Reichweite und Abdeckung von Sicherheitsmechanismen
  - Übertragungsabschnitt gegenüber „Ende-zu-Ende“
  - Inhalte gegenüber Meta-Daten



Vielschichtige Sicherheit (3)



Vielschichtige Sicherheit (4)

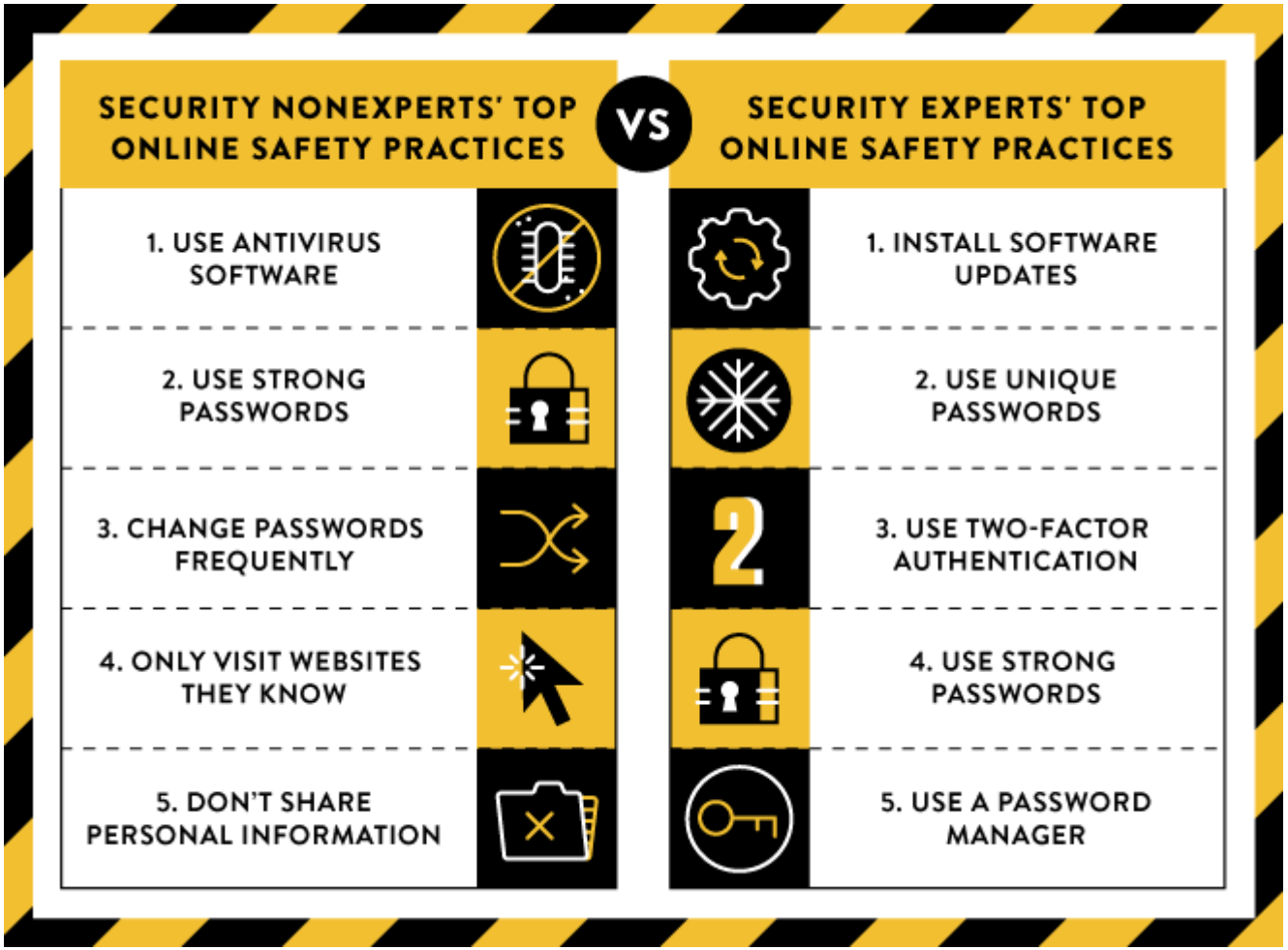
- Einordnung existierender Lösungen wichtig
  - „Reichweite“ der Sicherheitsmechanismen
    - Je höher in den Schichten desto besser
    - „Endsystem zu Endsystem“ besser als Hop-by-Hop
    - In welchen Netzbereichen wirksam?
  - Welchen Systemen bzw. Protokollen muss vertraut werden?
    - Oft spielen mehrere Protokolle zusammen
    - Datenebene und Kontrollebene (z.B. Signalisierung, Routing, Netzmanagement) berücksichtigen
  - Welche Schutzziele können erreicht werden?
    - Gibt es Zwischensysteme für Man-in-the-Middle-Angriffe?
    - Wo sind kritische Ziele für (D)DoS-Angriffe?
  - Was bleibt unberücksichtigt?
    - Beispiel: Mit TLS werden Vertraulichkeit und Integrität der Inhalte gesichert, aber mit welchem Server kommuniziert wird, bleibt sichtbar, u.a. durch IP und DNS

Netzsicherheit

- Fokus der Vorlesung auf Kommunikationssicherheit:

  Sicherheit bei Übermittlung von Daten über ein Kommunikationsnetz
- Gesamtsicherheit eines Systems immer nur so gut wie schwächstes Glied in der Kette
- Relevant, aber oft nur am Rande betrachtet
  - Kryptographische Verfahren
  - Software-Sicherheit bzw. Endsystemsicherheit

Praktische Tipps



[IuRC15]

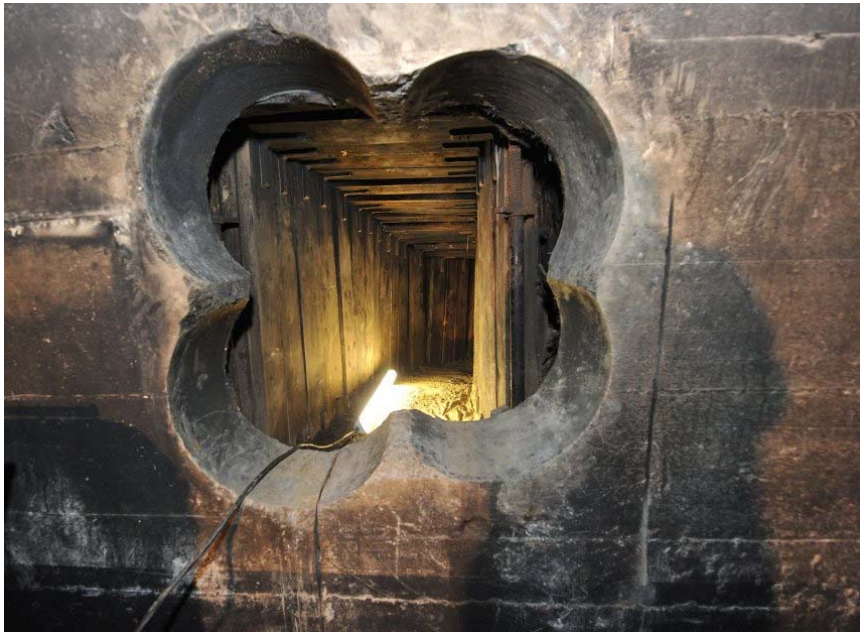
Wie sicher ist „sicher“?

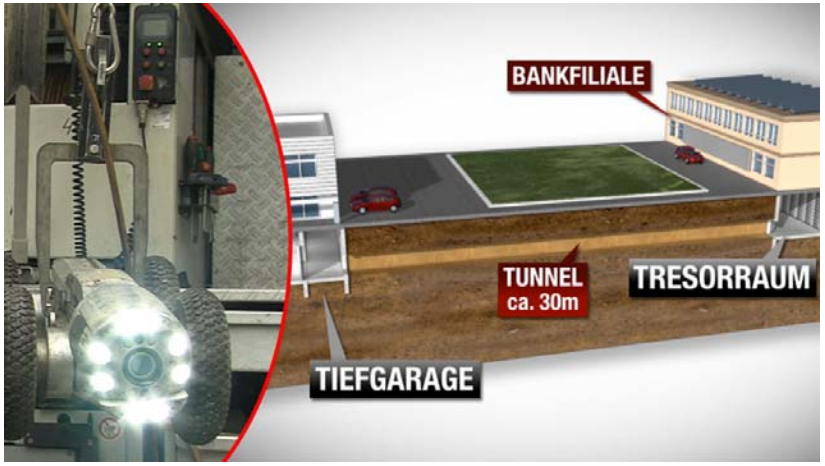
- Sicherheit ist relativ
  - … gegenüber einem bestimmten Angreifer definiert
    - Festlegung von Zielen und Fähigkeiten des Angreifers bei initialer Sicherheitsanalyse
    - Vollständigkeit schwierig
      - alle Angriffsmöglichkeiten berücksichtigt?

- Probleme
  - Unvollständige Analyse ist inhärentes Problem
    - Mögliche Fehleinschätzung der Angreifer-Ziele/-Fähigkeiten
    - Fähigkeiten und Ziele des Angreifers ändern sich über die Zeit
  - Kryptoanalytischer Fortschritt → Schwächung von Bausteinen
  - Fehlerhafte Implementierung von Protokollen und Verfahren
    - Beispiel: Doppeltes Goto bei Überprüfung der SSL-Zertifikate

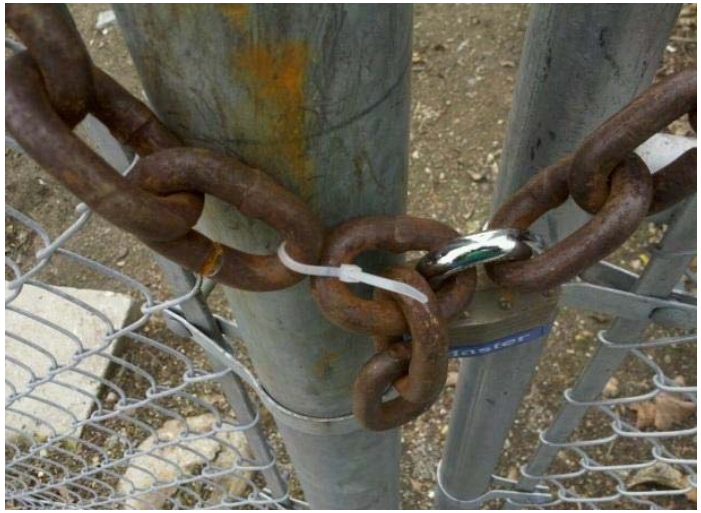
Hundertprozentige Sicherheit ?

- Tunnelraub Berlin 2013
  - 45m langer unterirdischer fachmännischer Tunnel von Parkhaus in eine Bank
  - Bauzeit mehrere Monate
  - Team von Tätern
  - Diebstahl von 10 Millionen €

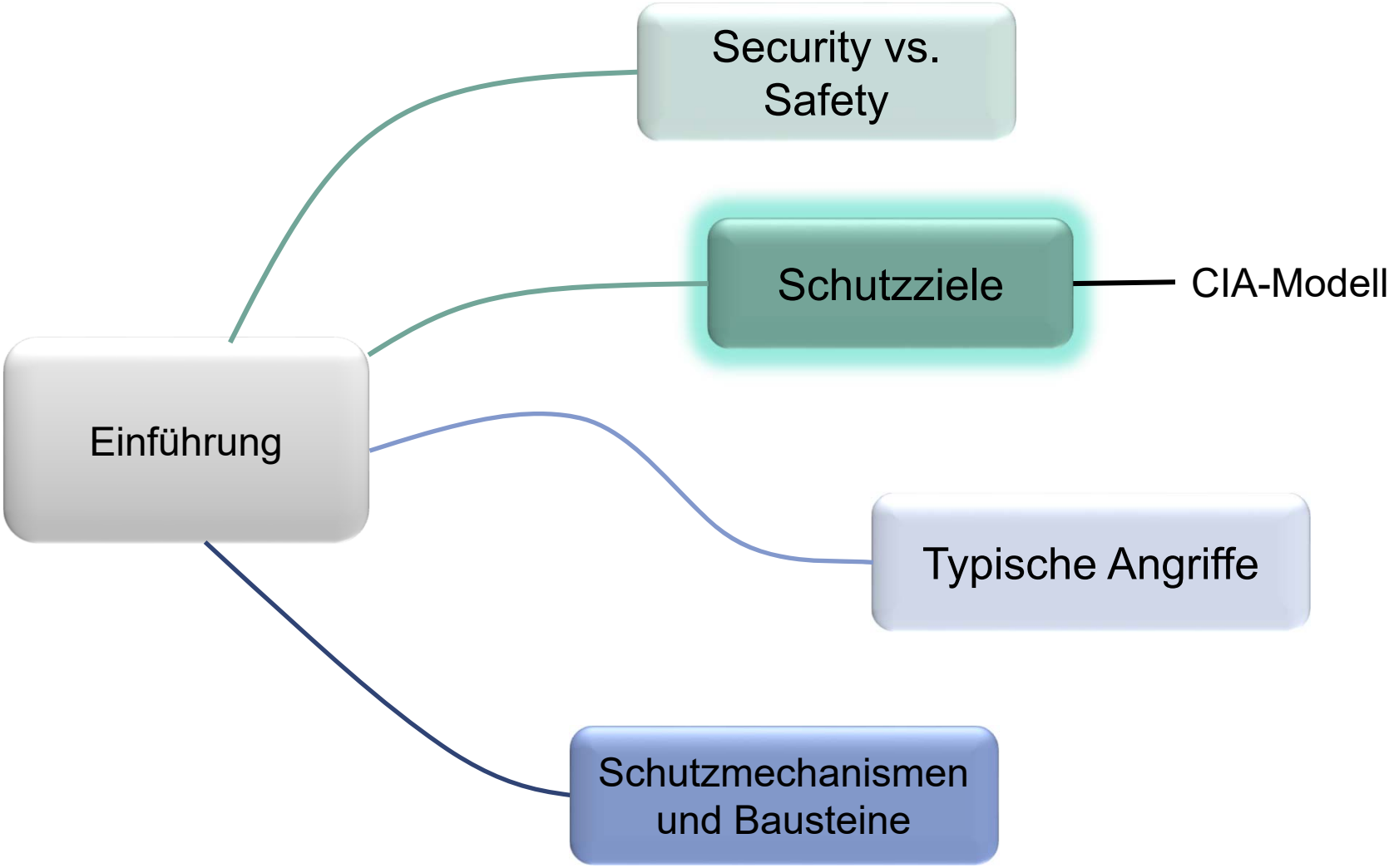




Fake Security ?!



Inhalte des Kapitels



Schutzziele (Wiederholung)

- Schutzziel
  - Anforderungen an eine Komponente oder ein System, die erfüllt werden müssen, um schützenswerte Güter vor Bedrohungen zu schützen

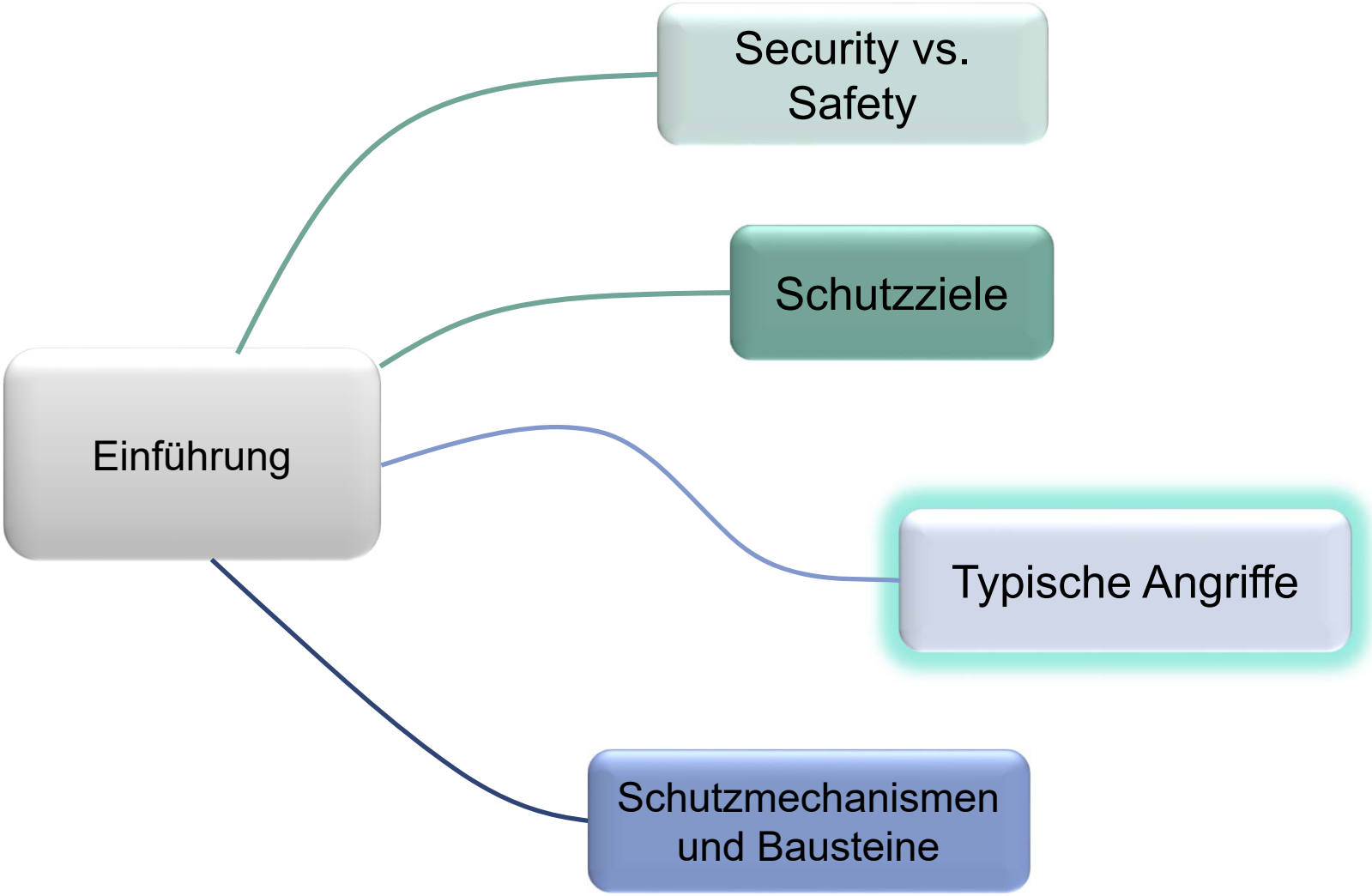
- Häufige Kategorisierung in
  - **C**onfidentiality (Vertraulichkeit)
  - **I**ntegrity (Integrität)
  - **A**vailability (Verfügbarkeit)

- Weitere Schutzziele
  - Authentizität
  - Privatsphäre
  - (Nicht-)Abstreitbarkeit

Definitionen Schutzziele (Wiederholung)

- Vertraulichkeit
  - Ein System bewahrt Vertraulichkeit, wenn es keine unautorisierte Informationsgewinnung ermöglicht
- Integrität
  - Ein System bewahrt *starke* Integrität, wenn es nicht möglich ist, Daten unautorisiert zu manipulieren
  - Ein System bewahrt *schwache* Integrität, wenn unautorisierte Manipulationen an Daten nicht unbemerkt möglich sind
- Verfügbarkeit
  - Beschreibt, in welchem Maße die Funktionalität des Systems von berechtigten Subjekten unabhängig von Einflüssen in Anspruch genommen werden kann
- Authentizität
  - Angegebene Quelle von Daten entspricht tatsächlicher Quelle + Datenintegrität (Echtheit von *Subjekten / Daten)*

Inhalt des Kapitels



Warum ein Angreifermodell?

- Wichtig für (sicheren) Sicherheitsarchitektur
  - Was will ich schützen → Güter und Schutzziele
  - Welche Motivation und Fähigkeiten setzt ein Angreifer ein?

  → Angreifermodell
  - Hands-on Beispiel:
    - Es macht einen Unterschied, das Haus gegen Vandalismus oder gegen einen professionellen Einbrecher abzusichern

- Bewertung einer Sicherheitsarchitektur ohne Nennung des angenommenen Angreifermodells (fast) nicht möglich

„Klassisches“ Angreifermodell: Dolev-Yao

- Bei Protokollen wie TLS oder IPsec oft nicht explizit genannt
  - Implizit geht man häufig von einem Angreifer aus, den man „Dolev-Yao“-Angreifer nennt

- Merkmale:
  - Angreifer ist omnipräsent im Netz, kann sämtliche Kommunikation abhören
  - Kann eigene Dateneinheiten erzeugen und versenden
  - Kann fremde Dateneinheiten modifizieren
  - Kann allerdings nicht Entschlüsseln oder Verschlüsseln, ohne den Schlüssel zu kennen

Angreifer = „Outsider“

Alternative Angreifermodelle

- Angreifer kann Systeme korrumpieren
  - Diese Systeme arbeiten zusammen
  - Können sich ggf. – über Out-Of-Band-Mechanismen – synchronisieren
- Adaptives Korrumpieren vs. statisches Korrumpieren
  - Angreifer analysiert Protokollabläufe und korrumpiert dann nach und nach gezielt Systeme oder einmalig und zufällig
- Global vs. lokal korrumpierte Systeme
  - Korrumpierte Systeme entweder im ganzen Netz verstreut oder beschränkt auf Teile des Netzes

Angreifer = „Insider“

Systematische Einordnung von Angriffen

- Unterscheidung von aktiven und passiven Angriffen
  - Passiv: Unautorisierte Informationsgewinnung → Vertraulichkeit
  - Aktiv: Unautorisierte Manipulation → Integrität und Verfügbarkeit

- Typische Angriffstechniken
  - Abhören
  - Zwischenschalten („Man in the Middle“)
  - Manipulieren
  - Unterdrücken
  - Einfügen
  - Wiedereinspielen (Replay)
  - Sabotage/Denial-of-Service

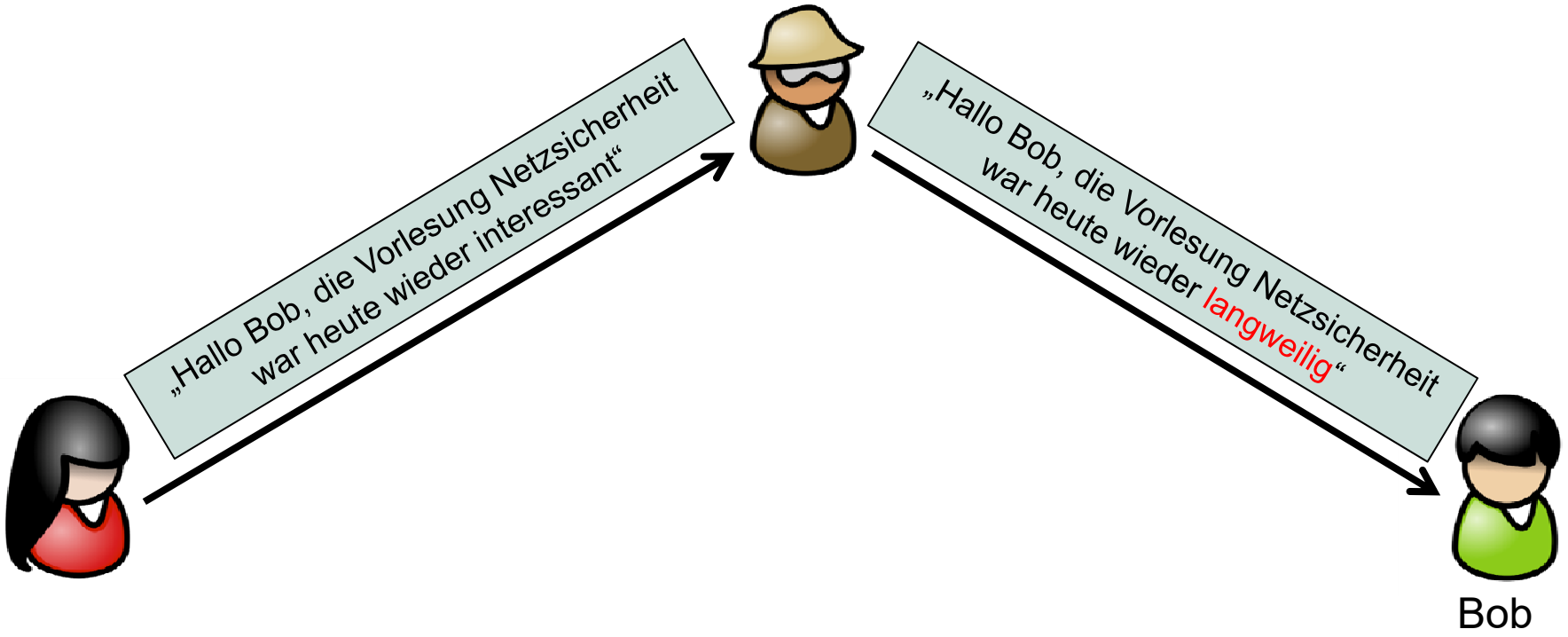
Abhören

- Passiver Angriff auf die Vertraulichkeit
- Beispiel: NSA-Skandal

Man in the middle

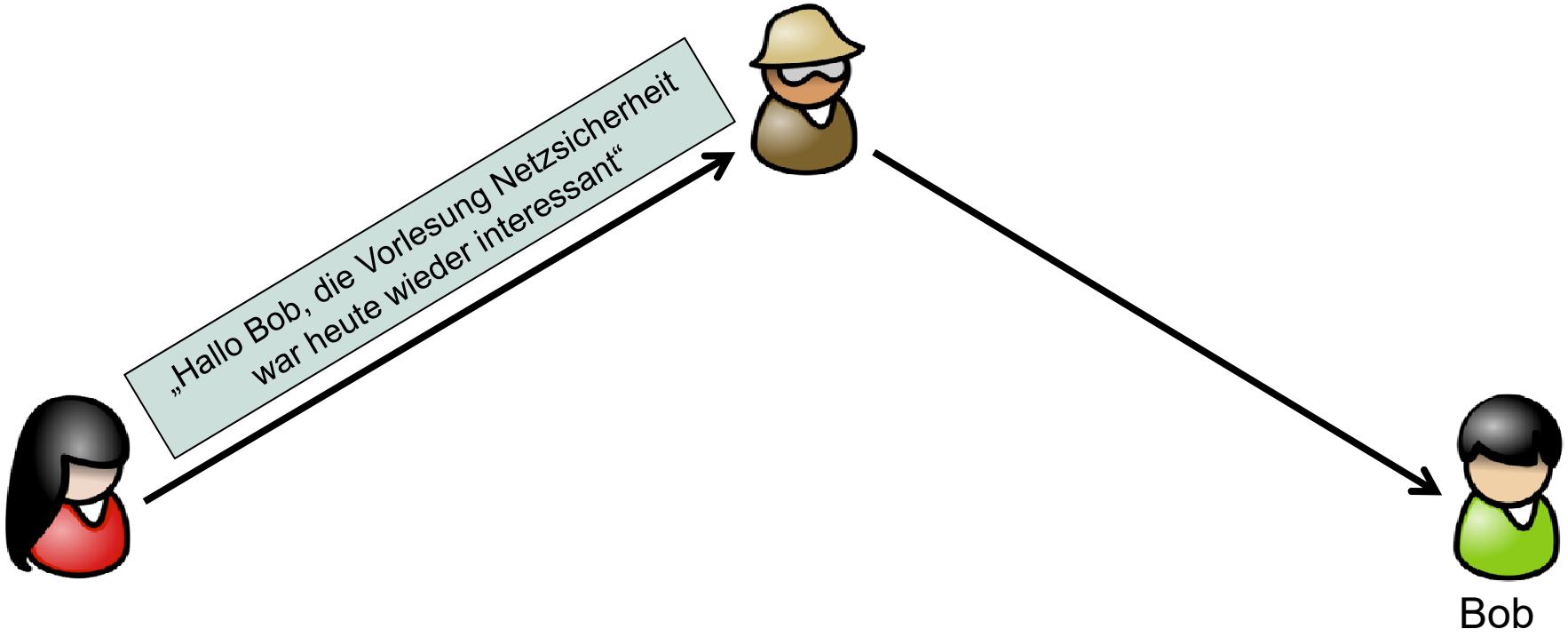
- Aktiver Angriff
  - Kann genutzt werden, um weitere Angriffe auszuführen
- Beispiel: Apples „goto fail“-Bug kann ausgenutzt werden, um „Man in the middle“-Angriff auf TLS auszuführen

Manipulieren



- Aktiver Angriff auf die Integrität
- Beispiel: Ändern des Betrages einer Überweisung

Unterdrücken

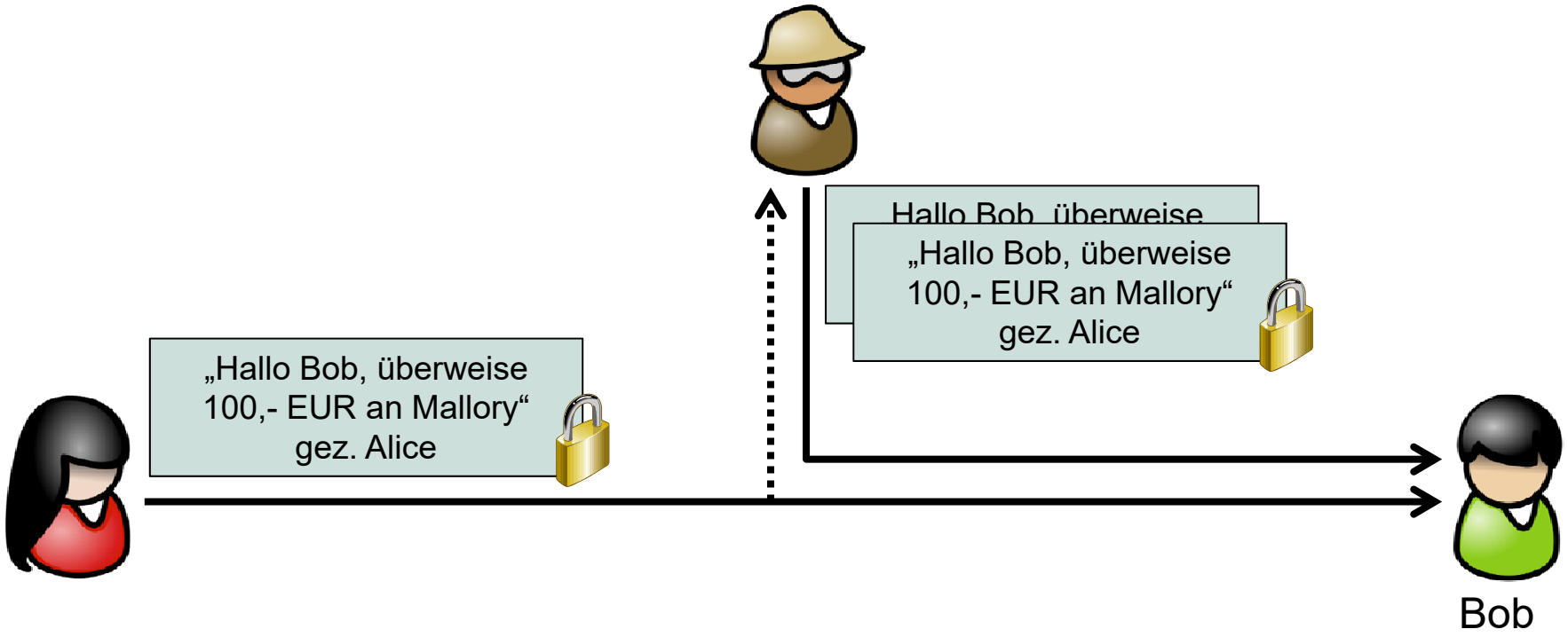


- Aktiver Angriff auf die Integrität und die Verfügbarkeit
- Beispiel: Zurückhalten wichtiger Nachrichten

Einfügen

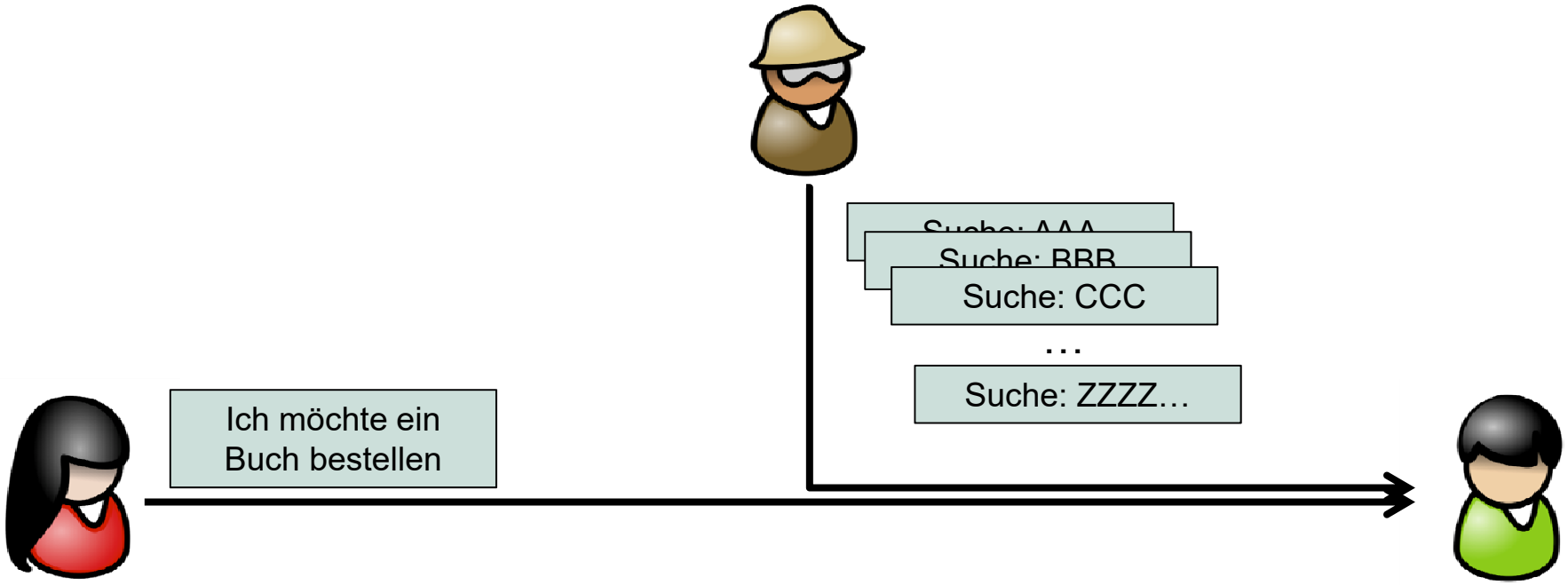
- Aktiver Angriff auf die Authentizität
- Beispiel: gezielte Desinformation

Wiedereinspielen (Replay)



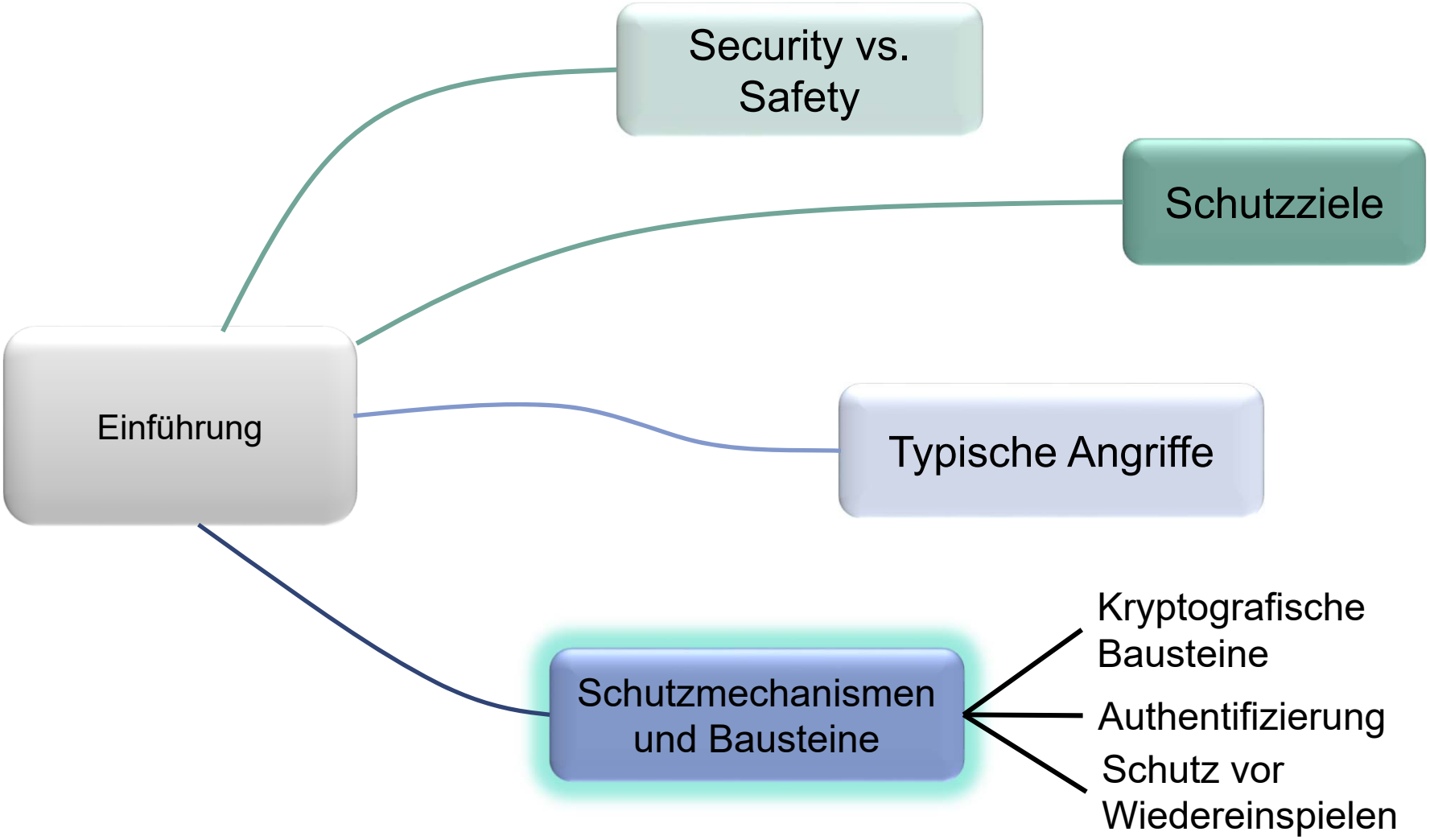
- Erneutes Einspielen einer authentischen Nachricht (kann z.B. signiert sein)
- Aktiver Angriff
- Beispiel: Wiedereinspielen einer Überweisungstransaktion

Einfügen → Denial-of-Service (DoS)



- Aktiver Angriff auf die Verfügbarkeit eines Dienstes
  - DoS = „Dienstverweigerung“ → gezielte Sabotage durch Angreifer
  - Angreifer versucht das Opfer von „sinnvoller Arbeit“ abzuhalten
- Beispiele
  - Überlastung der Verarbeitungsleistung durch viele Suchanfragen
  - Überlastung des Endsystems durch viele Verbindungsanfragen (z.B. TCP-Syn-Flood)

Schwerpunkte des Kapitels



Schutzmechanismen und Bausteine

- Mechanismen und Bausteine, um Schutzziele zu gewährleisten
  - Vertraulichkeit → Verschlüsselung
  - Integrität bzw. Authentizität
    → Digitale Signaturen und Message Authentication Codes (MAC)
    → Schutz vor Wiedereinspielungsangriffen
  - Authentifizierung → Passwörter und Zertifikate
  - Verfügbarkeit → Schutz durch Cookie-Mechanismen
- Notwendige zusätzliche Mechanismen
  - Schlüsselaustauschverfahren

Kryptografische Bausteine

- Verschlüsselung
  - Symmetrische Verschlüsselung (z.B. AES, ChaCha20)
    - Kommunikationspartner verfügen über denselben Schlüssel zum Ver- und Entschlüsseln
    - Hohe Effizienz, da meist einfache Operationen (Bit-Shift, XOR)
  - Asymmetrische Verschlüsselung (z.B. RSA, ECDSA, DH, ECDH)
    - Kommunikationspartner verfügen über öffentliche und private Schlüssel
    - Basis: Faktorisierung von Zahlen gilt als schwer
- Integritätssicherung
  - Kryptografische Hashfunktion
    - Verwendet symmetrische Kryptografie
  - Digitale Signatur
    - Verwendet asymmetrische Kryptografie
  - Kombination: Authenticated Encryption with Associated Data (AEAD)
- Schlüsselaustausch (s. nächstes Kapitel)

Verschlüsselung

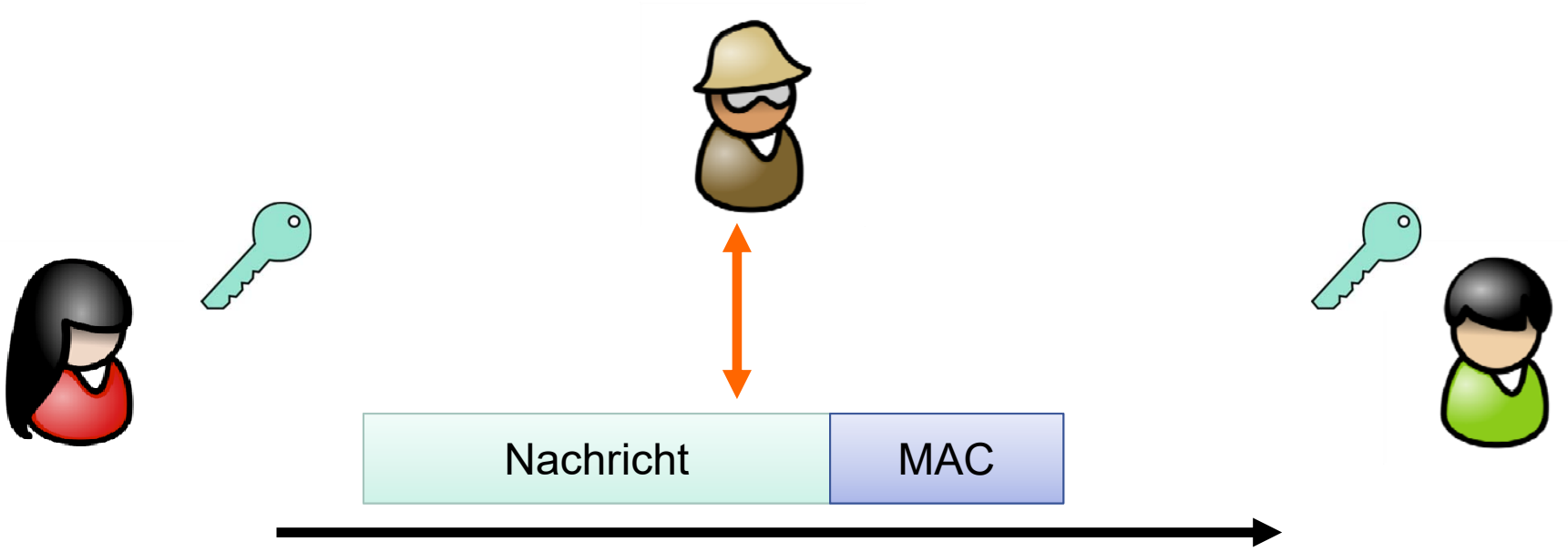
- Internet: unzuverlässiger Transport
  - Paketverluste
  - Reihenfolgevertauschungen
- Verschiedene Betriebsmodi für Blockchiffre
  - Cipher Block Chaining (selbstsynchronisierend)
  - Cipher Feedback (selbstsynchronisierend)
  - Output Feedback (nicht selbstsynchronisierend)
  - Counter (nicht selbstsynchronisierend)
- Reine Verschlüsselung schützt nicht vor Modifikation!
  - Nur in Kombination mit Integritätssicherung sinnvoll

Kryptografische Hashfunktion

- Eigenschaften kryptografischer Hashfunktionen
  - Bildet Nachrichten a beliebiger Länge auf Hashwert $\mathrm{H}(\mathrm{a}) = b$ fester Länge ab
  - Einwegfunktion/Urbildresistenz: zu gegebenem b ist es (praktisch) nicht möglich ein a zu finden, so dass gilt $H(a) = b$
    - Anschauliches Beispiel: Telefonbuch
      - Nummer zu Name leicht
      - Name zu Nummer nicht leicht
  - Schwache Kollisionsresistenz
    - Für gegebenes a ist es schwierig, ein $\bar{a} \neq a$ zu finden, so dass gilt $H(a) = H(\bar{a})$
  - Starke Kollisionsresistenz
    - Es ist schwierig, zwei verschiedene Werte a und $\bar{a}$ aus der Urbildmenge A zu finden, so dass gilt $\mathrm{H}(a) = H(\bar{a})$
- Beispiele für kryptographische Hashfunktionen
  - MD5, SHA-1 (gelten beide als nicht mehr sicher),
    SHA-2 (SHA-224, SHA-256, SHA-384, SHA-512),
    SHA-3 (Keccak)

Message Authentication Code (MAC)

- Ziel
  - Erkennung von Manipulationen an den gesendeten Daten
- Vorgehensweise
  - Alice erstellt Nachricht m und berechnet Hash $H(m)$
  - Alice hängt Hash an Nachricht an
- Voraussetzung
  - Alice und Bob besitzen gemeinsamen symmetrischen Schlüssel

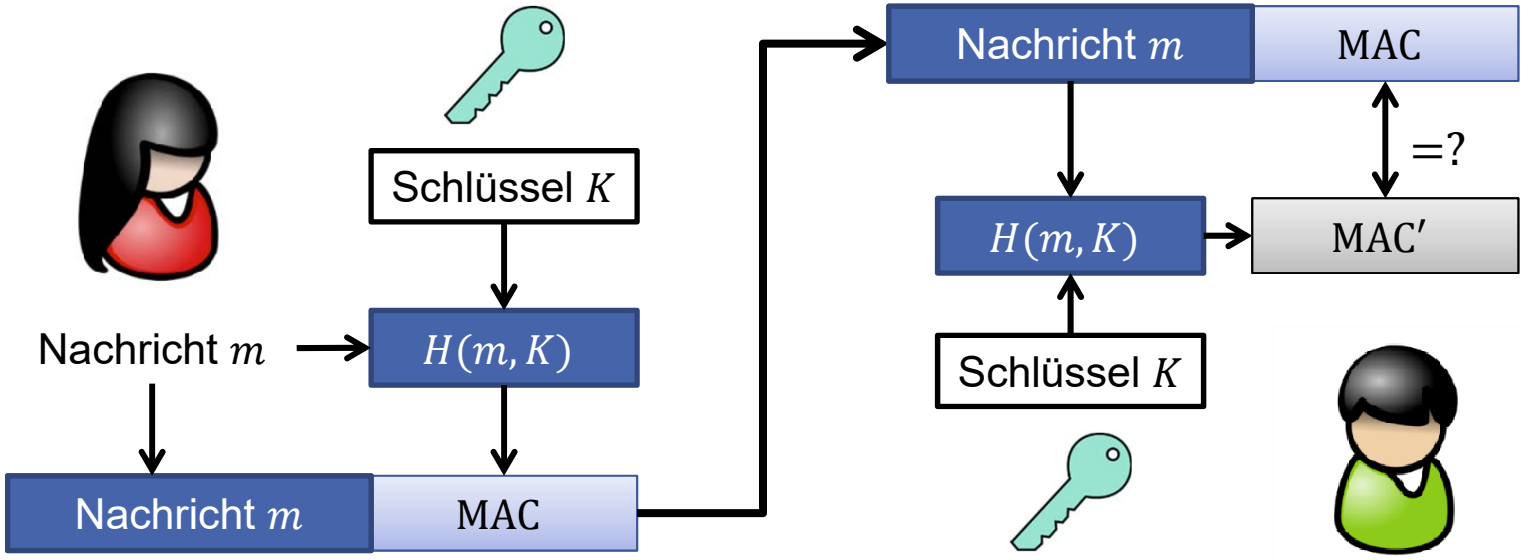


Message Authentication Code

C I A

- Berechne Message Authentication Code auf Basis einer Hashfunktion H()
  - über zu sichernde Daten und
  - über geheimen Schlüssel
  - *Keyed-Hashing for Message Authentication*

→ Angreifer kann gültigen Hashwert nach Veränderung der Daten nicht neu berechnen



Beispiel: HMAC

- Gegeben
  - Nachricht m
  - Kryptografische Hashfunktion H, z.B. SHA-256, SHA-3
  - Schlüssel K bzw. $\overline{K}$ (auf Blocklänge aufgefüllter Schlüssel)
  - Zwei Zeichenketten ipad und opad der Länge des Eingangsblocks
- Berechnung beim Sender

$$\mathrm{HMAC}_K(m) = H(\overline{K} \oplus \mathrm{opad} \mid H(\overline{K} \oplus \mathrm{ipad} \mid m))$$

- Überprüfung beim Empfänger

$$\mathrm{HMAC}_K(m) == H(\overline{K} \oplus \mathrm{opad} \mid H(\overline{K} \oplus \mathrm{ipad} \mid m))\ ?$$

- Konstruktion macht schwächere Annahmen über Sicherheit von $H()$
- Naiver Ansatz $H(K|m)$ ermöglicht Angreifer einfache Berechnung von $H(K|m|x)$ bei Kenntnis von $H(K|m)$, d.h. Anhängen von Daten einfach möglich

[KrBC96] [RFC 2104]

Beispiel: HMAC

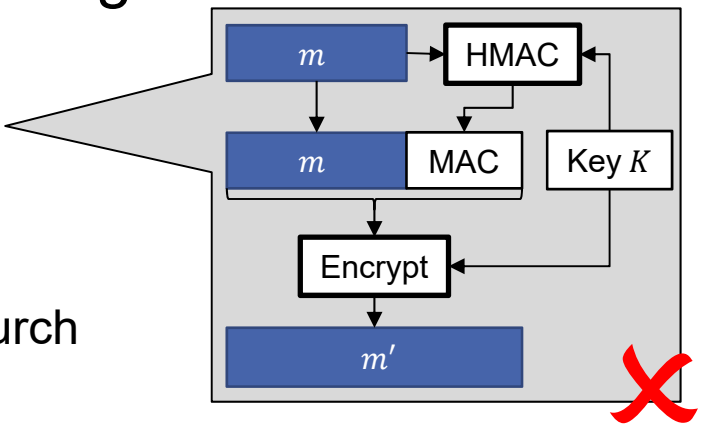
- Eigenschaften
  - Unabhängigkeit von verwendeter Hashfunktion
  - Schlüssel K zum Erzeugen einer authentischen Nachricht nötig
  - Schlüssel K nötig, um Authentizität einer Nachricht zu überprüfen
  - Keine einfache Verlängerung von m möglich bei Kenntnis von m und $\mathrm{HMAC}_K(m)$
  - Effiziente Implementierung möglich

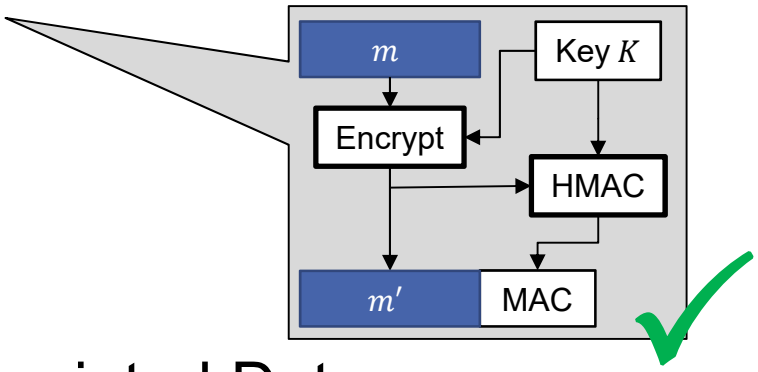
- Aber … *wie wird der gemeinsame Schlüssel verteilt?*

→ Kommt im nächsten Kapitel!

Authenticated Encryption with Associated Data

- Verschlüsselung und Integritätssicherung sollten immer zusammen ausgeführt werden, aber:
  - Zuerst die Prüfsumme berechnen, dann verschlüsseln?
    - Problem mit “MAC-then-encrypt”: Chosen Ciphertext Attack, → Angriffe durch Padding Orakel (BEAST, LUCKY 13)
  - Verschlüsseln und dann Prüfsumme berechnen?
  - Verschlüsseln und Prüfsumme berechnen?

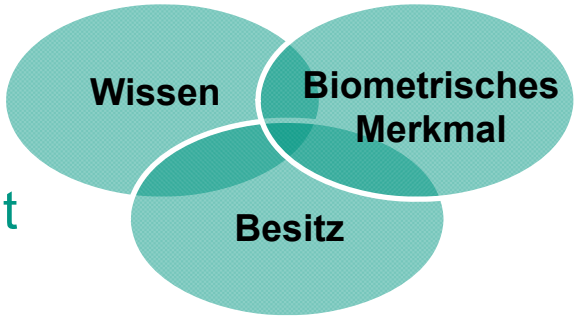




- State of the Art: Authenticated Encryption with Associated Data
  - AES GCM (Galois Counter Mode)
  - ChaCha20+Poly1305

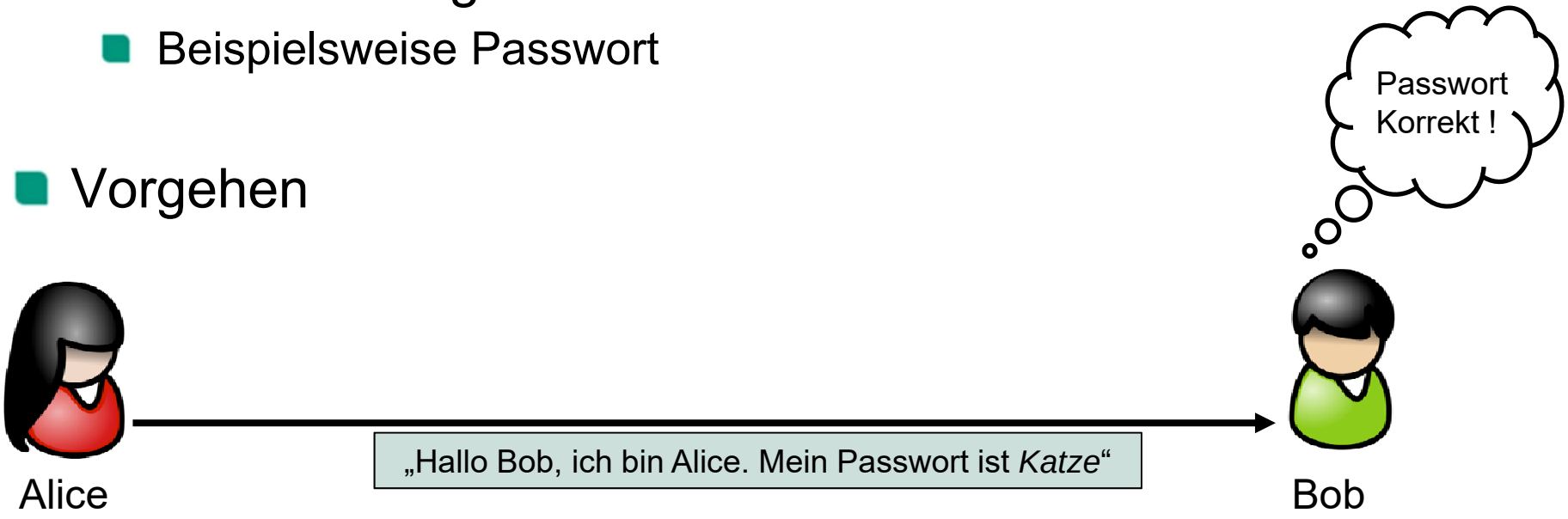
Authentifizierung

- Überprüfung, ob Kommunikationspartner tatsächlich derjenige ist, der er vorgibt
- Unterschiedliche Möglichkeiten
  - Besitz, Wissen, Biometrisches Merkmal
  - Kombination erhöht den Grad der Sicherheit (Zwei-Faktor-Authentifizierung)
- Aber meist nur in Form von Wissen
  - Benutzername und Passwort (Credentials)
- Mechanismen und Bausteine
  - Passwörter
  - Challenge-Response
  - Zero-Knowledge
  - Digitale Zertifikate



Passwörter

- Authentifizierung durch Nachweis eines Geheimnisses
  - Beispielsweise Passwort
- Vorgehen



- Nachteile
  - Liste von Passwörtern notwendig → Ziel für Angreifer
  - Passwort muss übertragen werden → Vertraulichkeit gefährdet
  - Oft schlechte Wahl der Passwörter

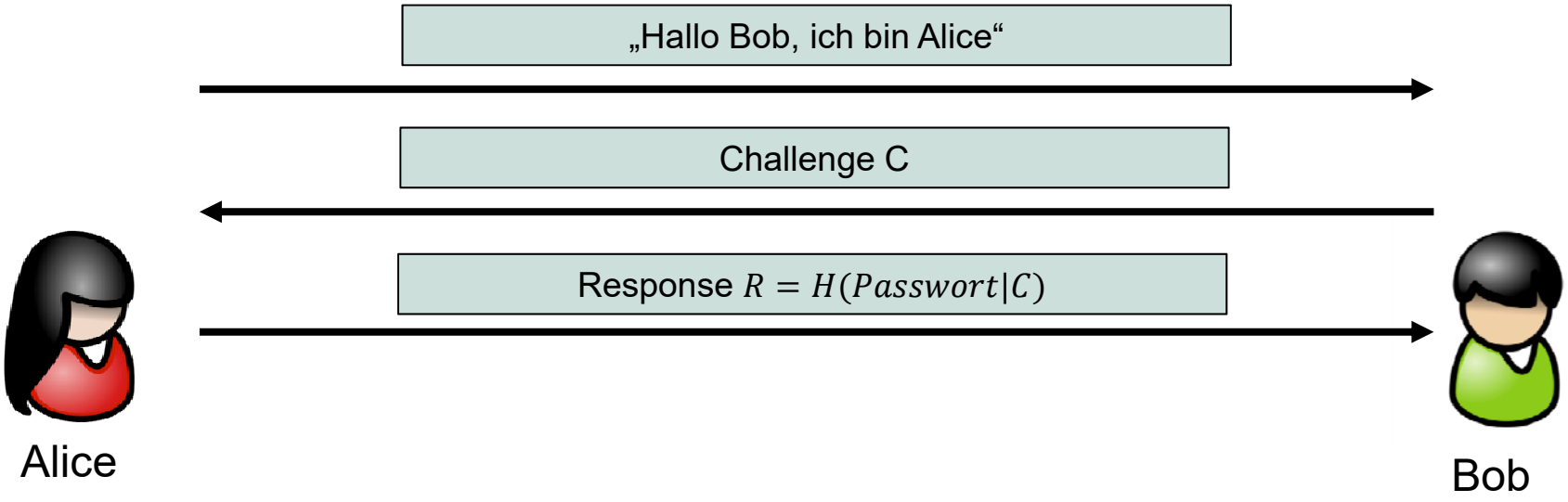
Passwort-Hashes

- Statt Klartext-Passwort Nutzung eines Passwort-Hashes
  - → Muss immer noch übertragen werden
    → ggf. Offline-Angriff möglich (Aufzeichnen + systematisches Durchprobieren, z.B. Wörterbuch)
  - → Muss immer noch gespeichert werden

- Authentifizierung ohne Übertragung des Passworts?
  - Frage-und-Antwort Spiel → Challenge-Response-Authentifizierung

Challenge-Response-Authentifizierung

- Voraussetzungen
  - Alice und Bob haben Passwörter ausgetauscht und gespeichert



- Bob kann durch Kenntnis von Alices Passwort die Response R und somit die Authentizität von Alice überprüfen
- Offline-Angriff ebenfalls möglich ($\mathrm{R}, H()$ und C bekannt)!

Digitale Zertifikate

- Problemstellung
  - Authentifizierung eines Sachverhaltes, den man nicht selbst überprüfen kann
  - man verlässt sich auf vertrauenswürdige Dritte, die ihn schon kontrolliert haben
- Zertifikat ist digitales Dokument, in dem eine Instanz einen bestimmten Sachverhalt mittels digitaler Signatur bestätigt
  - erzeugt Vertrauen in den Sachverhalt
- Zertifikate werden von vertrauenswürdiger Instanz erstellt
  - Certification Authority (CA)
- ID-Zertifikate
  - öffentlicher Schlüssel → eindeutiger Name (*Identität*)
  - Authentifizierung von öffentlichen Schlüsseln
- Authentifizierung: Nachweis, dass Zertifikatsinhaber in Besitz des passenden privaten Schlüssels ist

Schutz vor Wiedereinspielungsangriffen

- Neben Integrität und Authentizität von Nachrichten häufig wichtig zu erkennen, ob Nachricht bereits früher versendet wurde
  - Sonst Wiedereinspielungsangriffe möglich
  - z.B. Wiedereinspielen erfolgreicher Legitimation
- Umsetzung mit Hilfe von
  - Zeitstempeln → synchronisierte Uhren notwendig
  - Sequenznummern → Einigung auf Sequenznummernbereich notwendig
- Idee: Sender führt Integritätssicherung über Nachricht und Zeitstempel bzw. Sequenznummer durch

  → Wiedereinspielen der Nachricht kann erkannt werden

Zusammenfassung

- Sicherheit wird zunehmend wichtiger
  - Sicherheitsmaßnahmen bringen Zusatzaufwand mit sich
- Es existieren zahlreiche Bedrohungen für vernetzte Systeme – heutzutage praktisch alles immer vernetzt
  - Relevante Bedrohungen durch Angreifer identifizieren ist nicht immer einfach
  - Vorherrschende Angriffsform DDoS
- Es gibt zahlreiche Bausteine zur Sicherung
  - Geschickte Kombination notwendig
  - Smarte Sicherheit wünschenswert – einfache Handhabung wichtig

Literatur

[JoBu10] Johannes Buchmann: *Einführung in die Kryptographie,* 5. Aufl., Springer, 2010

[Byre13] Eric Byres: *The Air Gap: SCADA's Enduring Security Myth*, Communications of the ACM, Vol. 56 No. 8, Pages 29-31, 2013 URL: http://cacm.acm.org/magazines/2013/8/166309-the-air-gap/fulltext

[DiHe76] W. Diffie, M. E. Hellman: *New Directions in Cryptography*. In: IEEE Transactions on Information Theory. 22, Nr. 6, 1976, S. 644–654

[KrBC96] H. Krawczyk, M. Bellare, R. Canetti: *Keying Hash Functions for Message Authentication*, Juni 1996, (extended version of paper in Advances in Cryptology Crypto 96 Proceedings, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed., Springer-Verlag, http://cseweb.ucsd.edu/~mihir/papers/kmd5.pdf

[RFC2104] H. Krawczyk, M. Bellare, R. Canetti: *HMAC: Keyed-Hashing for Message Authentication*; RFC 2104, Internet Engineering Task Force, Februar 1997

Literatur

[RFC2827] P. Ferguson und D. Senie. Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice), Mai 2000. Updated by RFC 3704. URL: http://www.ietf.org/rfc/rfc2827.txt

[RFC4732] M. Handley, E. Rescorla und IAB. Internet Denial-of-Service Considerations. RFC 4732 (Informational), Dezember 2006. URL: http://www.ietf.org/rfc/rfc4732.txt

[IuRC15] I. Iulia, R. Reeder, S. Consolvo: “...no one can hack my mind”: Comparing Expert and Non-Expert Security Practices, Symposium on Usable Privacy and Security (SOUPS) 2015, July 22–24, 2015, Ottawa, Canada. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf