Chapter 16:
Security in Distributed Systems

Security in Distributed Systems

- Objectives
  - To understand why security is crucial in distributed systems
  - To learn about major security mechanisms
- Topics
  - Security statistics, IT systems, and security concerns
  - Major terminology
    - Vulnerability, trust, and risk
  - Prevention and policies in security areas
  - Attacks and damage
    - Classifications of threats and attacks
  - Major security pillars and examples
    - Authentication, authorization, en-/decryption
  - Identities and one-time passwords

Cybersecurity Statistics as of 2021

https://www.varonis.com/blog/cybersecurity-statistics/

- 2007: Hackers attack every 39 s, on average 2,244 times a day
- 2018: 62% of businesses experienced phishing and social engineering attacks
- 2019: Data breaches exposed 4.1 billion records
- 52% of breaches featured hacking, 28% involved malware, 33% included phishing or social engineering
- 2020: Estimated number of passwords used by humans/machines worldwide will be at 300 Billion
- 2022: Worldwide spending on cybersecurity countermeasures to reach $133.7 Billion USD

IT System's Status Today

- Current status on interconnection and penetration:
  (Vernetzung und Durchdringung)
  - Distributed Systems (DS) (Verteiltes System)
  - Globalization of information/communication: IT of daily life!
  - Cooperation across boundaries: e-mail, e-commerce, conferencing, data exchange, …
  - Critical dependencies of such applications!

- Current status on complexity:
  - #System components increases
  - Components interact beyond linear schemes
  - Software engineering crisis – reliability, testing, interfacing
- Current status on time:
  - Time-to-market extremely short!

IT: Information Technology

Security for Distributed Systems

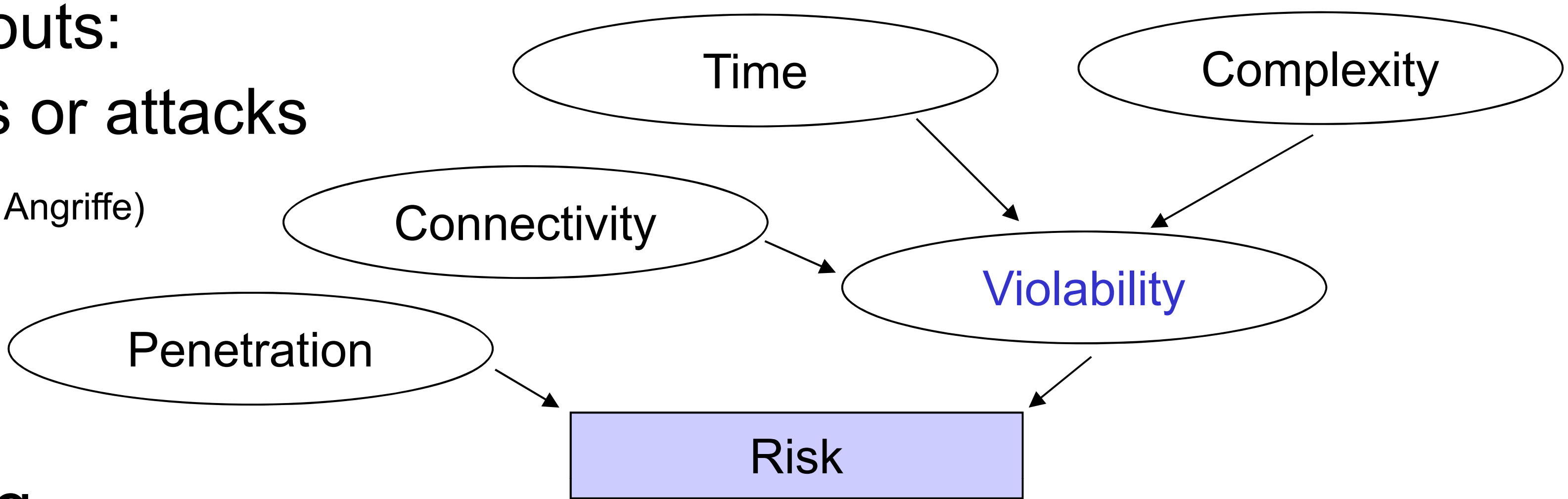
- Communication networks (enabler for distribution)
  - Telecommunication networks
    - Closed networks with open standards, but maintained centrally
  - Internet
    - Open networks maintained in a decentralized, but closed manner
- Applications
  - Stand-alone (*e.g.*, word processing, compiler, or “Tetris”)
  - Networked and distributed (*e.g.*, Web, e-mail, or banking IT)
- Concern and consequence
  - Distributed applications vulnerable due to their distribution
  - Security mechanisms are inevitable for any distributed system, including all components and communication networks

IT: Information Technology

Security – Quantification

- Quantification of security in IT systems
  - Violability (Verletzlichkeit) determines risks (Risiko) taken
    - What can go wrong will go wrong
  - Black-outs:
    failures or attacks

    (Fehler und Angriffe)



- Resulting
  - Problems: Information security, attacks, damages, …
  - Counter-measures: Cryptography, authorization, trust, …

    (Gegenmaßnahmen: Kryptographie, Authorisation, Vertrauen ...)

Vulnerability, Threat, and Risk

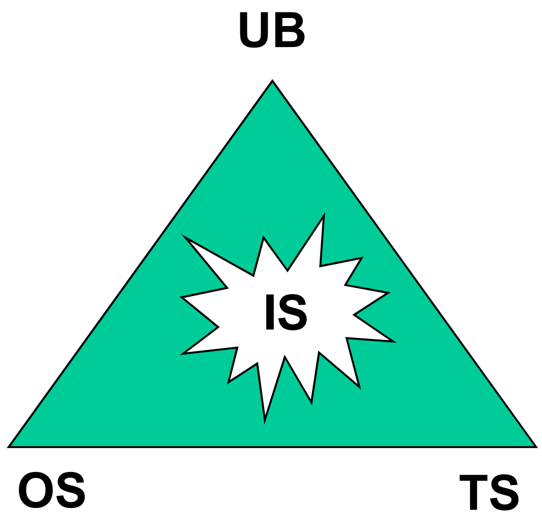
- Vulnerability
  – A quality or characteristic of a system that provides an opportunity for misuse.

- Threat
  – Any potentially malicious or otherwise occurrence that can have an undesirable effect on the assets and resources of an IT system.
- Risk
  = Threat X Vulnerabilities ***OR*** Likelihood X Impact

IT Security defines a process of risk management, supported by a set of suitable technical measures!

Security Areas (1)

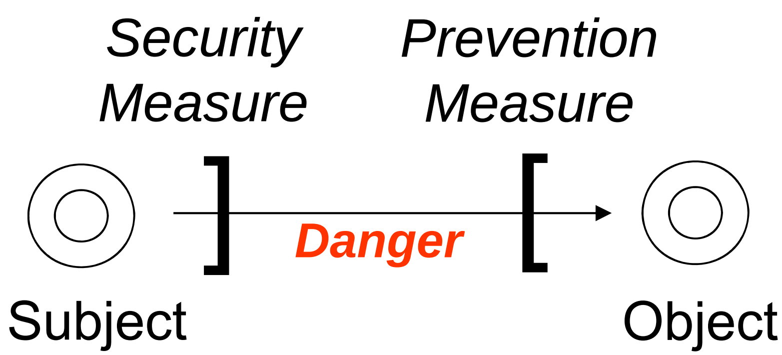
- Organizational Security (OS)
  - Trusted Third Party (TTP)
  - Certification Authority (CA)
    - Access rights (who will be enabled to do what)
    - Key management (distribution of keys)
- Technical Security (TS)
  - Security services, mechanisms, algorithms, …
- User Behavior (UB)
  - Passwords, internal- and external attacks, …
- Information Security/Information System Security (IS)
  - Effect on content, procedure, or system



Security Areas (2)

- Severe (security-concern related) issues and problems
  - How to achieve OS?
    - Whom to trust? Government, company, individual, …
    - Who certifies? Government, company, individual, …
    - Who assigns rights with which knowledge?
    - Who controls the key management? Where to store keys?
    - Are key pairs always private? Evalon and back doors …
  - How to ensure TS?
    - Cf. partly this lecture
  - How to control, check, guide UB?
    - Openness on algorithms and schemes, protocols or systems
    - Security by obscurity
    - Security models and public information

Prevention: Security and Safety



(Sicherheitsmaßnahme/
Schutzmaßnahme)

Security: Sicherheit
Safety: Schutz von Leib und Leben

Security measures address red area.
Safety measures address blue area.

	substantial (body, life)	immaterial (information)
Coincidence, law of nature, carelessness	Safety	Security
On purpose		

*Security and safety will **never** be achievable with a 100% guarantee!*

Prevention: Security Policies and Models

- Security policy
  - A statement of what is and what is not allowed
  - Axiomatic (formal) or lists of allowed/forbidden actions

  Orthogonal policies may create security vulnerabilities!

- Security models
  - The formulation of a security policy which governs all entities and which rules to constitute them
  - Representation of a particular policy or set of policies
    - Describing (if possible formally) and documenting policies
    - Testing policies for completeness and consistency
    - Supporting the concept and design phase of an implementation
    - Checking if the resulting implementation meets all requirements

Attacks and Damage

- Attacks
  - Aggressive, violent act against a person, system (component)
- Damage
  - Physical harm impairing value, usefulness, or normal function
- Cyber attacks
  - Sabotaging control of industrial security systems, causing substantial physical damage and business interruption
- IT damages
  - Utilities: telecommunications, oil, gas, energy interruptions
  - Privacy breaches
  - Consumer data losses,
  - Service, data of any industry with industrial control systems

IT Attacks and Damage Examples (1)

- Estimation of damage
  - Melissa (1999): Word 97/2000
    - 300,000,000 US$ with 150,000 systems infected for about 4 days
  - ILOVEYOU (2000): Outlook
    - 10,000,000,000 US$ with 500,000 systems infected for 24 hours
  - SQL Slammer (2003): Databases
    - Exploits“ buffer overflow of UDP Port 1434
      - 1st min: duplication of population all 8.5 s
      - From 3rd min: slower duplication due to network capacity
      - All 10 min: about 90% of all susceptible hosts infected
  - Stuxnet (2010)
    - Worm attacking Supervisory Control and Data Acquisition (SCADA)
    - Explicitly programmed for a Siemens control technology (Simatic-S7), addressing a particular industry

IT Attacks and Damage Examples (2)

- Targeted attacks (2013) at one company did cost up to $2.4 Million USD in damages per attack/incident
- WannaCry ransomware attack (2017)
  - Ransomware crypto-worm, targeting Windows machines
  - Encrypting data and demanding ransom payments
    - Infected more than 230,000 computers in over 150 countries
- DDoS attack (2018)
  - Targeted GitHub (online code management service)
  - At peaks incoming traffic at a rate of 1.3 Tbit/s
    - Sending packets at a rate of 126.9 Million/s
- DDoS attack (2019)

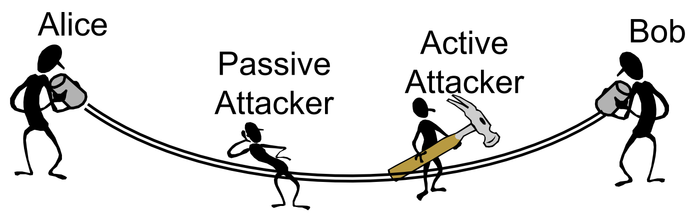
https://www.thesslstore.com/blog/largest-ddos-attack-in-history/

  - Unnamed client of Imperva experiencing 500 … 580 Million packets/s
  - Attacking network/website with packets of 800 to 900 Byte length each
    - Resulting in 3.4 Tbit/s attack traffic

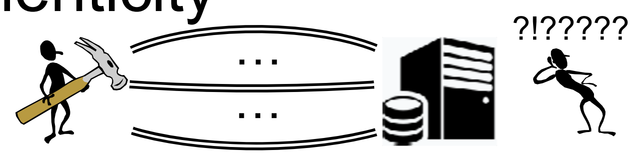
Data Transfer/Service Provisioning Attacks

TCP: Transmission Control Protocol

- One possible passive attack
  - Eavesdropping only, no change of data
  - Threat for confidentiality



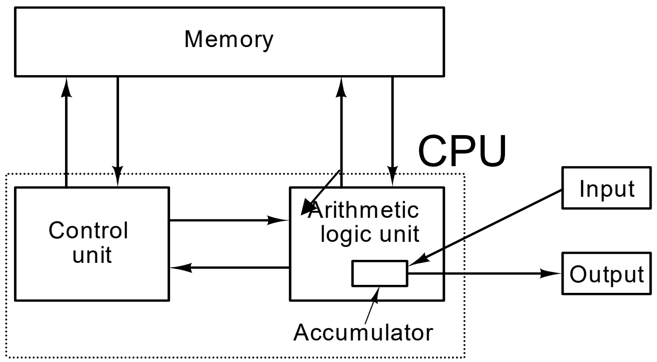
- Multiple possible active attacks
  - Changing, deletion, insertion
  - Threat for confidentiality, integrity, authenticity



- Denial-of-Service (DoS) attacks
  - Principle of generate as much as possible work for any infrastructure to prevent the processing of “normal“ tasks
    - SYN flooding by sending TCP-SYN messages to TCP Server
  - Distributed Denial-of-Service attacks (DDoS)
    - Sources of attack at millions of different nodes

Technical Leaks: Buffer Overflow (1)

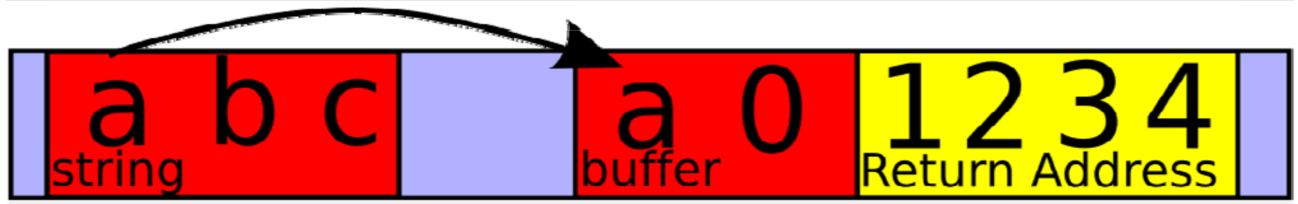
- Major security risks in current software
  - Targeted at von-Neumann Architecture
- Data are stored/written into main memory of a machine, which are too large for this memory segment
  - Effects:
    - “Wrong“ data areas are overwritten
    - Program crash
    - Corruption of application data
    - Change of run-time data



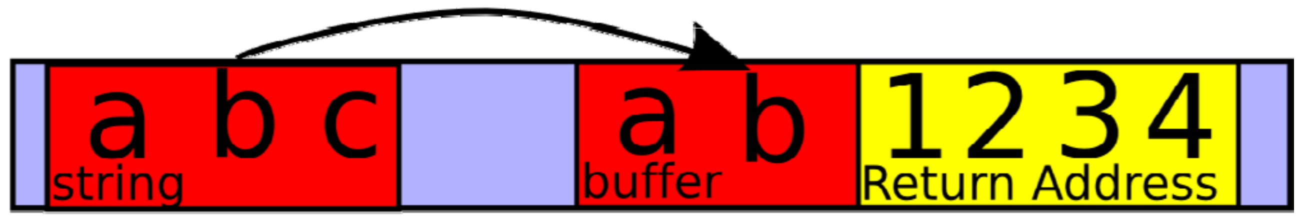
  - Exploit: run-time data contains the return address of a procedure, thus, code transferred in an attacking packet may be executed with similar privileges as the process attacked

Technical Leaks: Buffer Overflow (2)

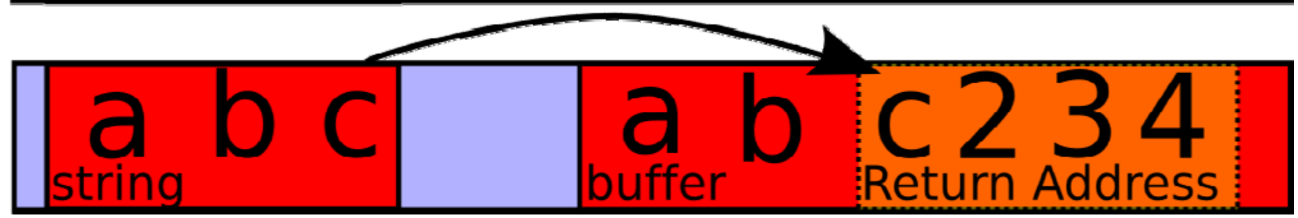
Copy 1st element



Copy 2nd element



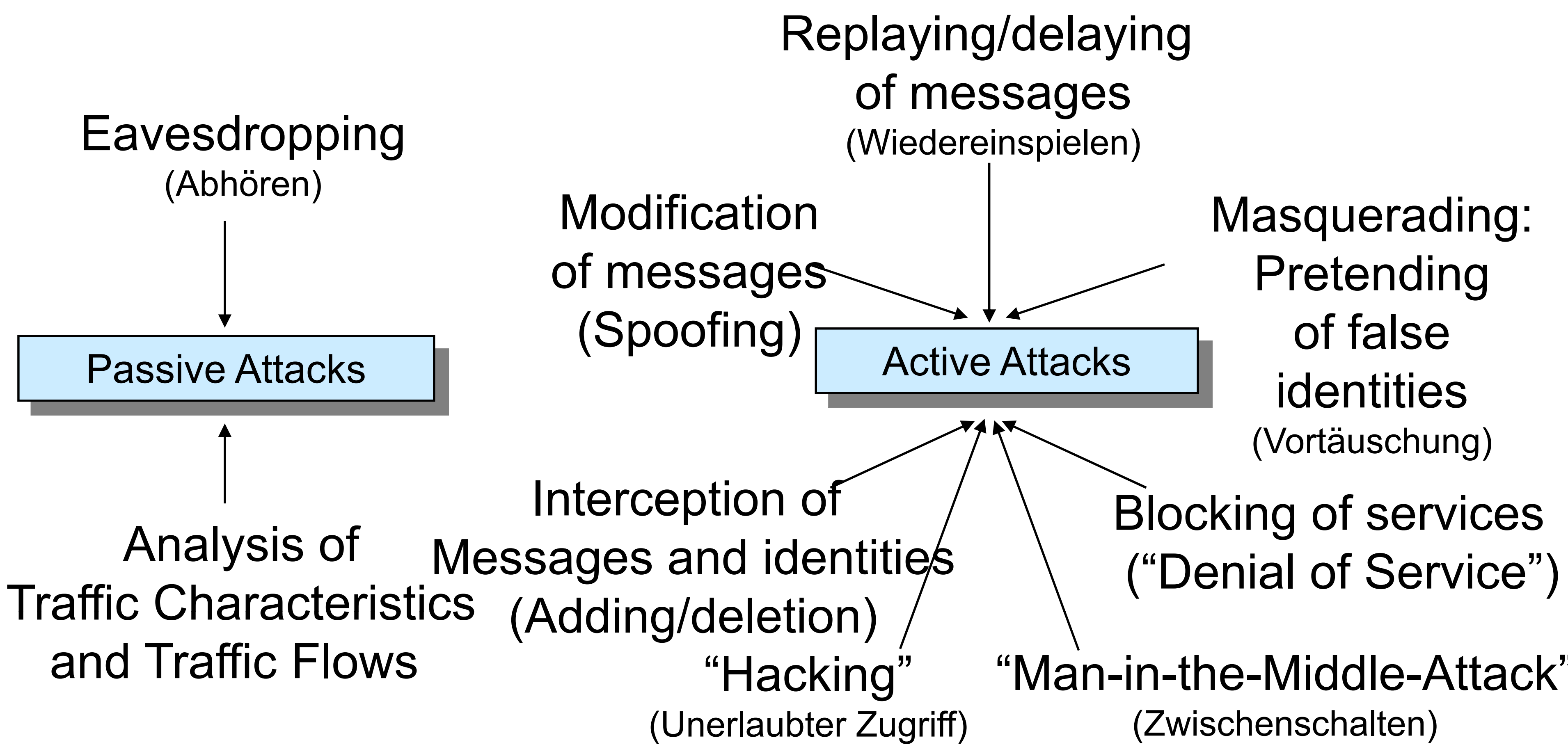
Copy 3rd element



Further Threats and Countermeasures

- Packet Snooper
  – Reading of packet content (data) → Encryption
- Packet Sniffer
  – Reading of source and destination addresses (protocol header) → Encapsulation of packet and encryption
- Session Hijacking
  – Session with multiple messages between two parties, a third party may gain control of this session → Authentication
- Data Tempering
  – Similar to session hijacking, however, only a part of the data transfer will be intercepted → Authentication and encryption

Threats and Attacks Classification



⇨ High risk!

Major 7 Security Pillars (1)

- Authentication (Authentifizierung/Authentifikation)
  – Authentication ensures that partners involved in communications can prove that the peer is that it claims to be
- Authorization (Autorisierung)
  – Authorization ensures that a partner with a known ID is enabled to utilize a service
- Integrity (Unversehrtheit, Fälschungssicherheit)
  – Integrity provides protection against the modification of a message along a transmission path
- Privacy (Privatheit)
  – Privacy defines the degree of publication of personal information and data

Major 7 Security Pillars (2)

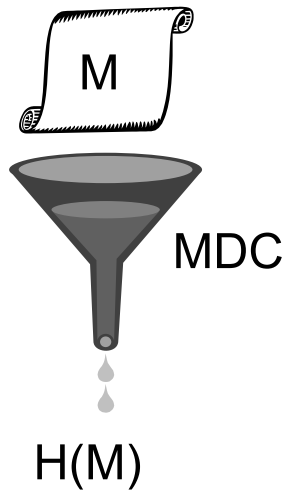
- Confidentiality (Vertraulichkeit)
  - Confidentiality protects transmitted data against eavesdroppers in a communication channel ensuring that only an authorized receiver can interpret the message received
- Non-repudiation (Nicht-Zurückweisbarkeit/Nicht-Abstreitbarkeit)
  - Non-repudiation provides that neither the sender nor the receiver can deny that a communication has taken place
- Anti-replay protection (Schutz gegen Wiedereinspielung)
  - Anti-replay protection protects a receiver from the duplicated reception of a previously obtained and already authenticated message

Authentication (1)

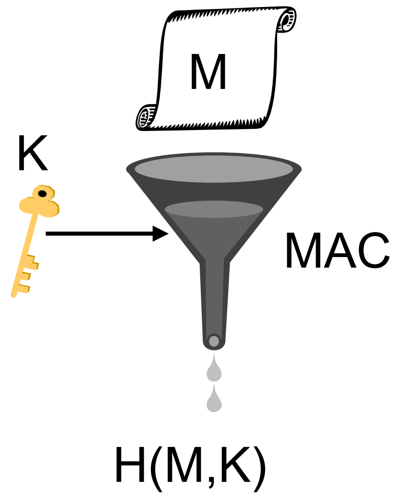
- Mechanisms to prove that the peer that it claims to be is the peer
  - Ownership (Besitz)
    - *E.g.*, smart card, physical device
  - Knowledge (Wissen)
    - *E.g.*, password, account
  - Biometrics (Körperliche Merkmale)
    - *E.g.*, finger print, iris scan
  - Location or context
    - *E.g.*, being a well-known person at a certain place for a certain reason
  - Proficiency (Können)
    - *E.g.*, signing

Authentication (2)

- Hash function (Message Digest Code, MDC)
  - Message M (arbitrarily long) → Hash H(M) (minimum of 128 bit length)
  - Note: “One-way” feature of function
    - Efficient generation
    - Very low collision possibility: M, M‘ with H(M)=H(M‘)
    - Examples: (MD5), SHA-256, RIPEMD-160



- Cryptographic hash function (Message Authentication Code, MAC)
  - Message M, key K → Hash H(M, K)
  - May be constructed out of MDC
  - HMAC (RFC 2104), *e.g.*, HMAC-MD5



Authentication (3)

- Authentication and integrity of packets
  - Adding of a Sequence Number (SN) to ensure order (re-use)
    - Securing against replay attacks by time stamps (synchronized clocks) or challenge-response mechanisms utilizing random numbers
  - Adding of MAC (Message Authentication Code) or signature, calculated from data, SN, key

- Authentication of systems or users
  - Application of non-cryptographic mechanisms
    - Username and password, biometric approaches (finger print, iris)
  - Application of cryptographic mechanisms
    - Login messages with MAC and signature or PKI, use-only-once passwords

PKI: Public Key Infrastructure

Multi-factor Authentication

- 2-factor case
  - Increasing the level of security
  - Combination of two different authentication schemes
    - Bank card and PIN (Personal Identification Number)
    - Credit card and signature
    - PIN and fingerprint
    - (Weak example: username and password)

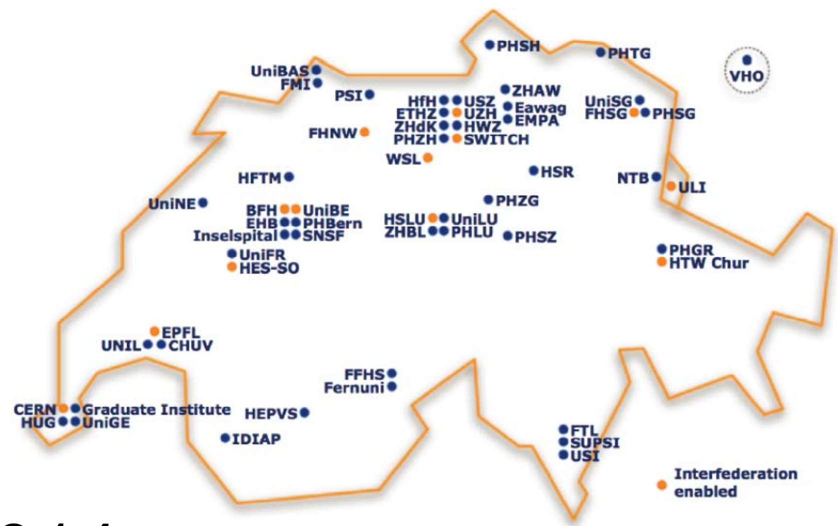
- 3-factor case
  - Achieves "highest" degree of security
    - Username and password and fingerprint
    - Username and password and SecureID token (SmartCard)

AAA

- AAA (Authentication, Authorization, and Accounting) important for effective network management/security
  - Access of network via Network Access Server (NAS), Communication, Remote Access, or Terminal Servers
  - Provisioning at the point of network entry, *e.g.*, dial-in users
  - Control who is allowed to connect to the network (“First A”)
  - Control what users are allowed to do (“Second A”)
  - Accounting of utilized resources (“Third A”) for monitoring, charging (monetary/incentives), and billing
    - At the access point (NAS: Network Access Server)
    - Within the network
    - Along communication paths

Example – SWITCH's AAI Federation

- Authentication and Authorization Infrastructure (AAI)
  - To simplify inter-organizational access to Web resources
  - AAI applies the concept of Federated Identity Management
    - Shibboleth-based
  - Deployed by most Swiss universities
  - Single login

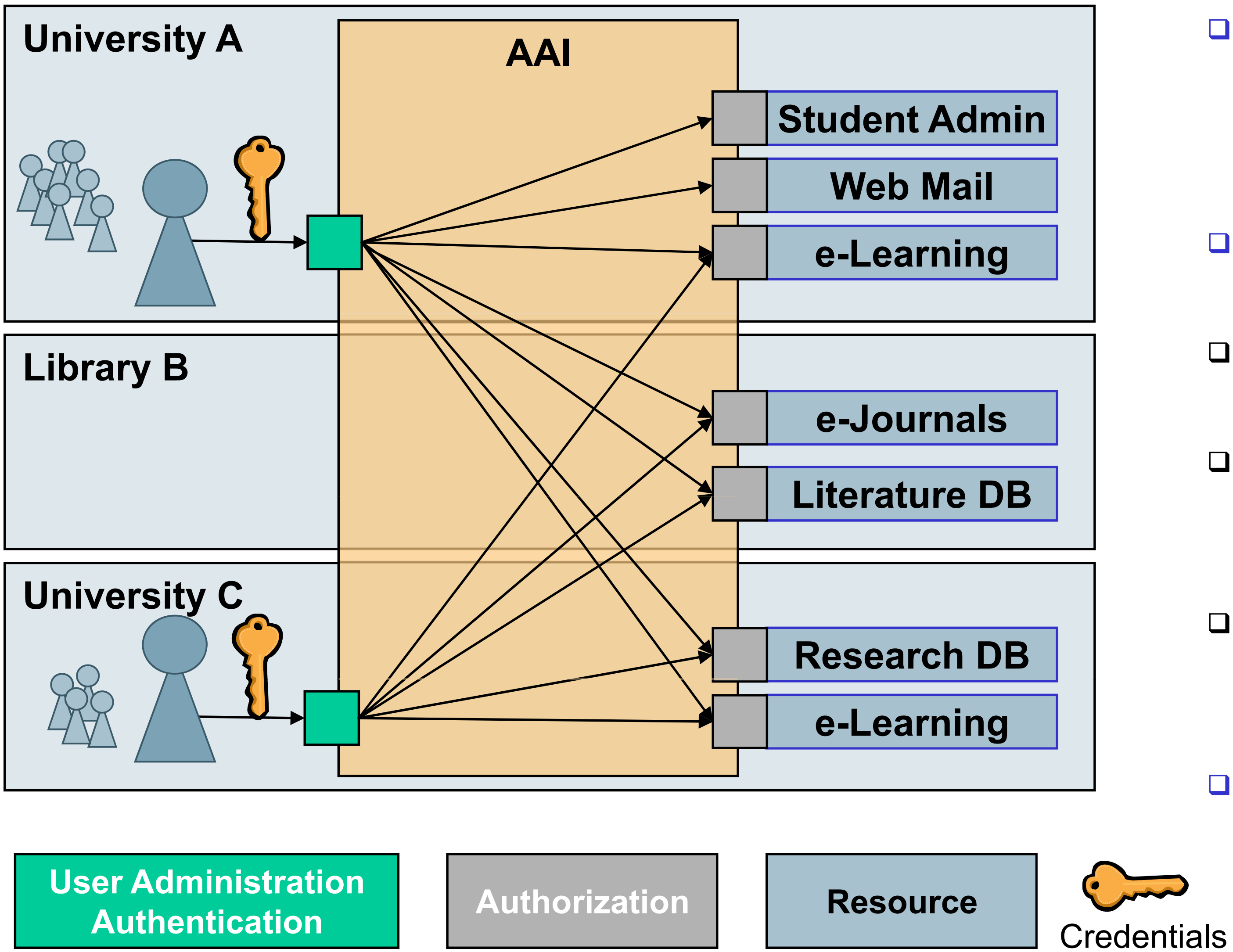


- Characteristics as of August 2014:
  - Close to 400.000 AAI-enabled accounts
  - More than 55 Home Organizations
  - More than 800 Web resources handled

VHO: Virtual Home Organization

SWITCH
The Swiss Education & Research Network

Situation with an AAI



- No user registration and user data maintenance at resource needed
- Single login process for the users
- Many new resources available for the users
- Enlarged user communities for resources
- Authorization independent of location
- Efficient implementation of inter-institutional access

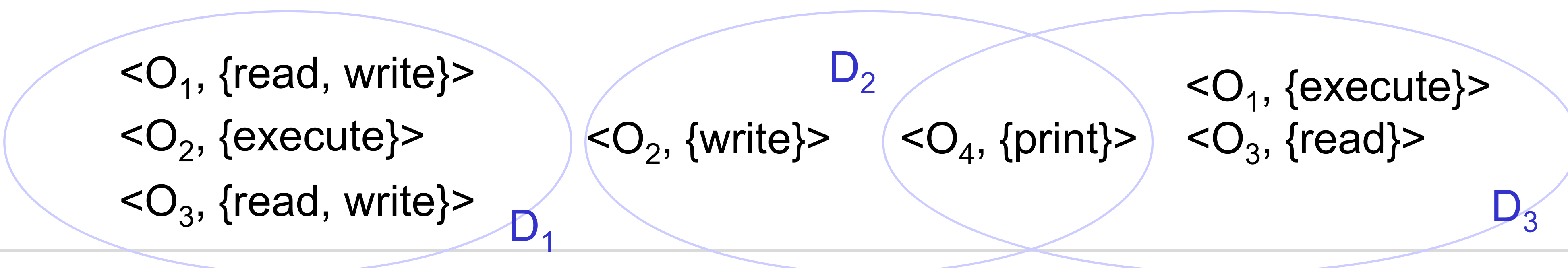
Authorization (1)

- Exact definition of
  - Access to services
  - Access to resources
  - Possibility to view database entries
  - Option to change files
  - …
- Authorization is highly application-dependent
  - Network: *e.g.*, access to a WLAN-based Internet connectivity
  - System: *e.g.*, access to files in an operating system
- Means and mechanisms vary
  - Access control matrices

WLAN: Wireless Local Area Network

Authorization (2) and Protection

- Protection (Zugriffsschutz)
  - Mechanisms to ensure the access rights onto resources by programs, processes, and users
- Definition of access rules by policies
- Protection Domains (D) define a set of objects (O) and its access rights (in”{ }“)
  - Domain may be equaling a user, a process, a procedure, …
- Examples
  - Process in D_2 is able to access O_2 in write mode
  - <O_4, {print}> is separately accessible by D_2 and D_3



Protection Domains in Operating Systems

- Operating systems: Unix, Windows, MacOS X, …
  - Protections required for multiple users, processes, threads

- Domain = User
- Change of the domain
  - Temporal change of the userID

- Support by a file system
  - ID of owner and domain bit (setuid bit) are associated with the file.
  - setuid bit = off: Execute the file with the userID
  - setuid bit = on: Execute the file with the ID of the file owner

Authorization (3) and Access Control Matrix

- Owner is allowed to change access rights (column) for other domains
- Change of a domain controlled by “switch”, *e.g.*, process executed in D_2 may change to D_3 or D_4
- ”control“ allows for the administration of access rights within a domain, *e.g.*, process in D_2 may change D_4
- A single column defines an Access Control List (ACL)
- Support of user groups highly useful

F: File

D: Domain

P: Printer

	F_1	F_2	F_3	P	D_1	D_2	D_3	D_4
D_1	r		r			s		
D_2				p			s	s c
D_3		r o	r	e				
D_4	rw o		rw o		s			

r: read

w: write

o: owner

s: switch

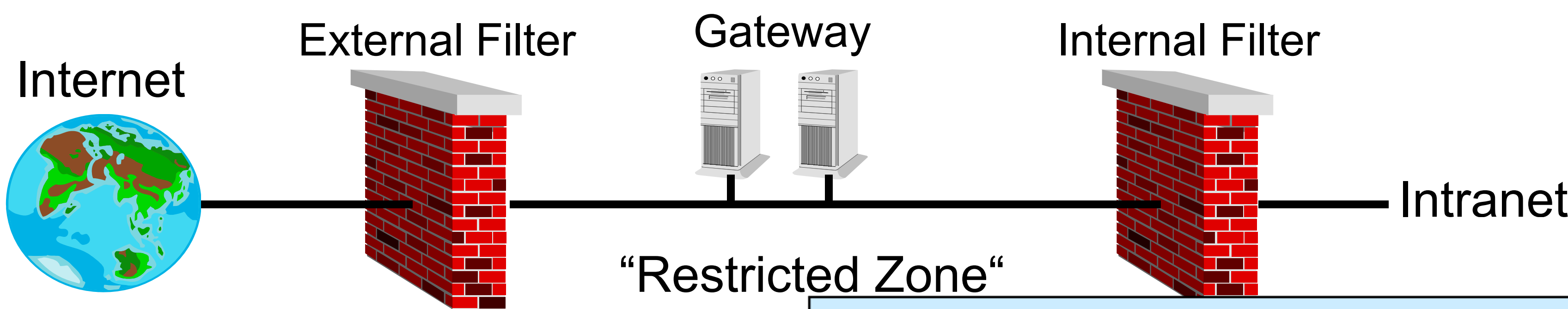
p: print

c: control

e: execute

Authorization (4) – Access Control

- Based on applications: Model of access rights (AR)
  - Examples: Unix/NT file system AR, SNMP objects AR
- Based on network/transport layer: Firewalls
  - Packet filter based on source/destination address and ports (TCP/UDP)
  - Topology-driven ingress/egress filtering
  - Gateways with access control and logging
  - Use of private IP addresses and address translations (NAT)



“Keep the good bits in and the bad bits out.“

Firewalling Mechanisms

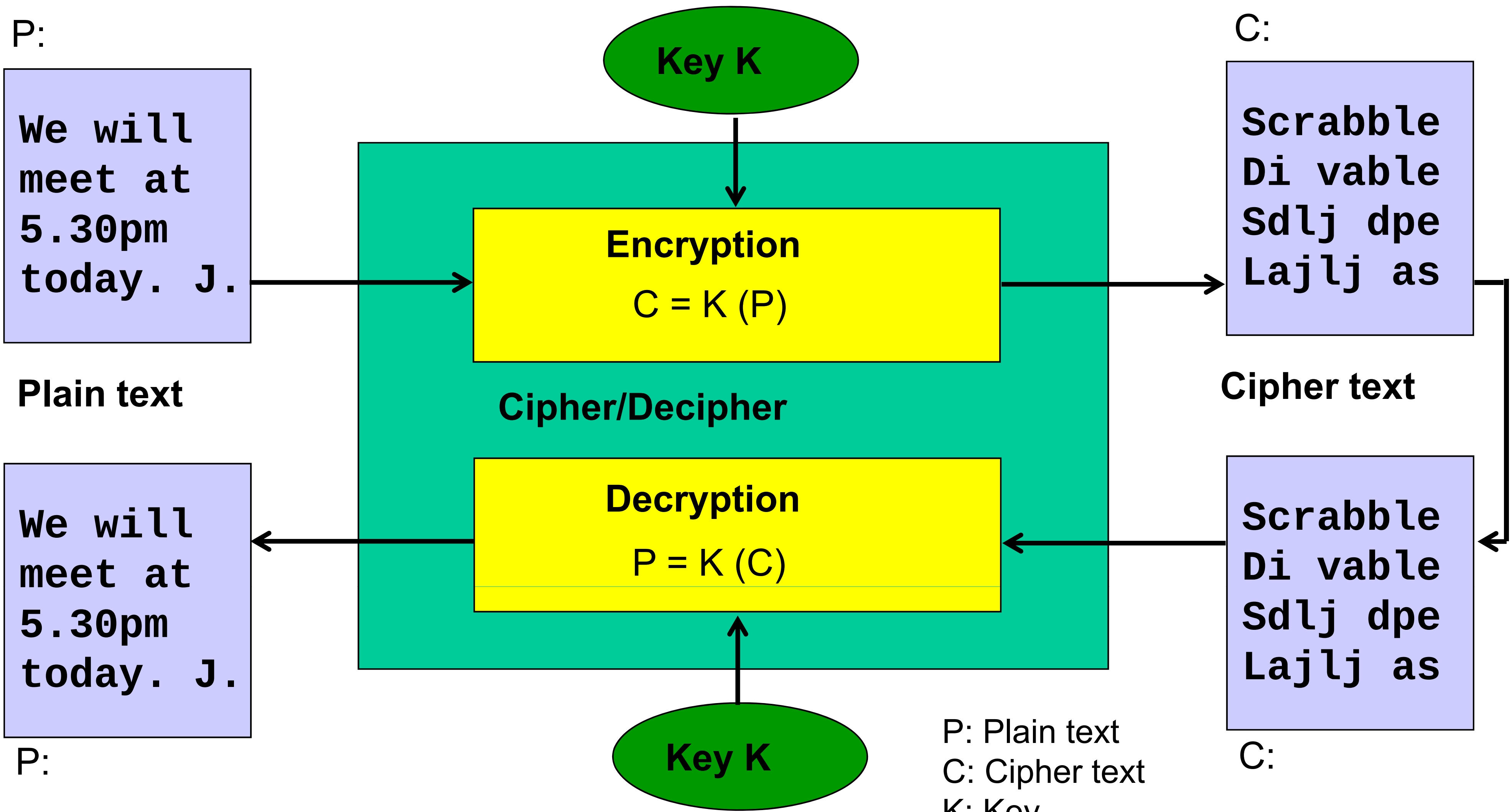
IP: Internet Protocol
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
WWW: World-wide Web

- Based on network/transport layer
  - Packet filter based on
    - Analysis of incoming and outgoing packets
    - Source/destination address and ports (TCP/UDP)
  - Valid and fire-walled data maintained in an access list
    - Incoming: `deny *.*.*.*, 23` blocks telnet
    - Outgoing: `permit 137.193.*.*, 80` enables http for hosts IP=137.193.x.y
  - Example: Firewalls located in routers
    - Filtering based on IP address and port number: *e.g.*, port 80 packets will stop the access to a WWW server hidden behind the firewall
- Most secure solution
  - Physical separation of internal and external hosts

Encryption and Decryption

- En-/Decoding (En-/Decryption) (Verschlüsselung/Entschlüsselung) of data to ensure confidentiality and privacy
  - Encoding of plain text
    - Only possible with the knowledge of a key (the “secret”)
    - Easy to do and fast to process
  - Decoding of cipher text (encrypted data)
    - Only successful with the right key
    - Extremely large, dedicated, and specific calculation effort, iff the key is not known (attack situation only), otherwise easy and fast to process
  - Respective algorithms
    - In the past, based on alphabet shifts (Cesar’s Shiffre)
    - More elaborate schemes applied today
  - Provides for confidentiality, integrity, and partially privacy

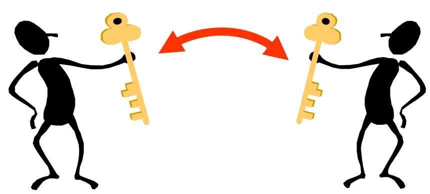
Cryptography



P: Plain text
C: Cipher text
K: Key

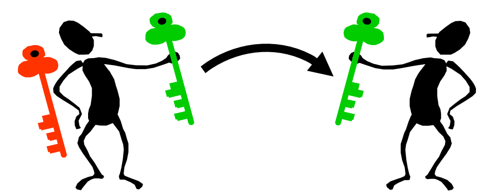
Cryptographic Variants

- Symmetric cryptography
  - Entities own a shared, secret key



- Advantages
  - Small overhead/calculation
  - Short keys
- Drawbacks
  - Key exchange complicated

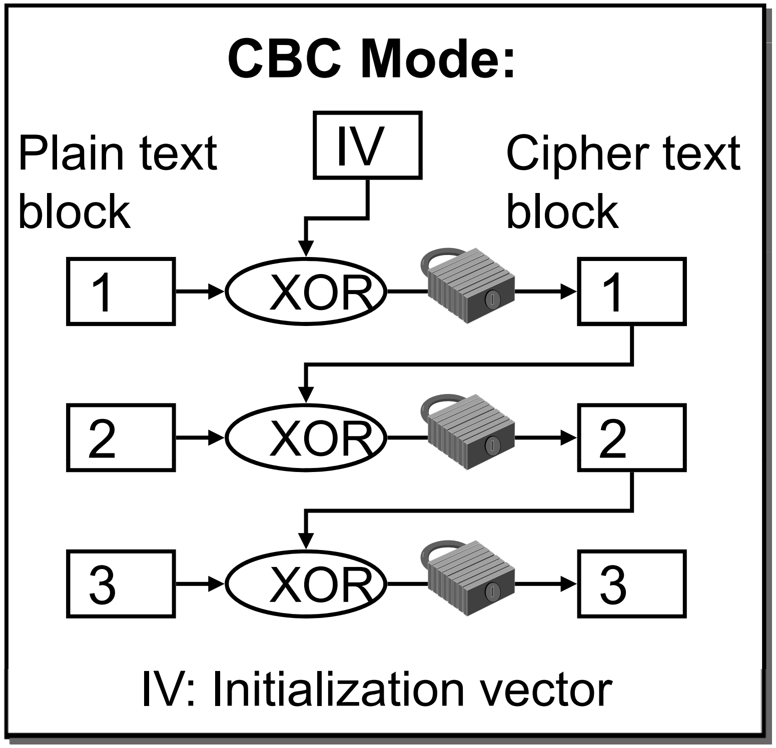
- Asymmetric cryptography (public key cryptography)
  - Key pair of private/public parts



- Advantages
  - Public keys easy to publish
- Drawbacks
  - Longer keys
  - Larger overhead/calculation

Symmetric Encryption

- Symmetric encryption
  - Current minimum key length 80 or better 128 bit
  - Secure algorithms: 3DES (Digital Encryption Standard), IDEA
- Operation
  - Block cipher with 64 bit blocks
  - Electronic Code-book (ECB)
    - Block-wise encryption
    - Attacker may interchange blocks
  - Cipher Block Chaining (CBC)
    - “More” secure: every block is dependent on preceding block
  - Byte-wise encryption



Asymmetric Encryption

- Asymmetric encryption (Public Key Encryption)
  - Encryption easy and publicly accessible to everyone
  - Decryption difficult for everyone except the intended recipient
  - Current minimum key length 1024 bit (309 decimal digits)
  - Secure algorithms: RSA (Rivest-Shamir-Adelman), ElGamal
- Practical encryption: Hybrid approaches
  - First: User authentication and exchange of a session key, public-key-based (in a non hybrid version: symmetric)
  - Second: Symmetric encryption of user data by session key and further authentication required with session key
  - Note: Longer sessions should change session key on a periodical basis, *e.g.*, once per 30 min or 1 hour

Asymmetric Schemes and Signatures

- *Cf.* CECN class as of Fall Term 2019
  - Public key encryption
    - Examples
    - RSA principle with trap door function
    - Example calculation based on prime numbers
      - Principle of prime number factorization
        - Theory vs. practice
  - Application of asymmetric schemes
    - Signatures and Certificates
      - Digital signature
      - Certification of the association between public key and “individual”

Identities in an Electronic World

- Host identity
  - Related to a network: per-layer naming conventions
  - Hostname, Internet Protocol (IP) address, Medium Access Control (MAC) address (“Ethernet Address“)
  - Uniform Resource Locator (URL) for web pages
  - Maintained in distributed data bases with respective mappings
  - Spoofing possible, mapping mechanisms are not secure
  - Identifiers (ID) represent a formal description:
    - IDs may be dynamic (DHCP) or static (fixed IP address)
    - IDs may be local (MAC address) or global (IP address, URL)
- How to identify an “individual” uniquely, non-reputably?

One-time Passwords – Example (1)

- One-time passwords (OTP) are generated by a continuous hashing of an initial password
  - Remember: A cryptographic hash function H is a “one way” function!
- Alice starts with s = “hello“ and applies H = “SHA-1”
  - f(s)=f572d396fae9206628714fb2ce00f72e94f2258f
  - f(f(s))=532879bf0a70126eb698cc6aeab1792be32b9270
  - f(f(f(s)))=dec69a5f76bbe15a2fc574d0ae7edabcc5cb4ab9
  - f(f(f(f(s))))=d128cbe9c3f1370f93f005b81ebcfeb2bc9806c6
- Finally, Alice and Bob share f(f(f(f(s))))
  - 1st password f(f(f(s))), 2nd password f(f(s)), 3rd password ...

One-time Passwords – Example (2)

- Alice

has f(f(f(f(s)))),f(f(f(s))),f(f(s)),f(s),s

sends f(f(f(s)))

dec69a5f76bbe15a2fc574d0ae7edabcc5cb4ab9

- Next time she

sends f(f(s))

532879bf0a70126eb698cc6aeab1792be32b9270

Bob

has y=f(f(f(f(s))))

d128cbe9c3f1370f93f005b81ebcfeb2bc9806c6

receives x=f(f(f(s)))

dec69a5f76bbe15a2fc574d0ae7edabcc5cb4ab9

Bob checks if f(x) ↔ y, password OK: y=f(f(f(s)))

Bob receives x=f(f(s))

532879bf0a70126eb698cc6aeab1792be32b9270

Bob checks if f(x) ↔ y, password OK: y=f(f(s))

One-time Passwords – Example (3)

- Bob easily checks, if the next password has been used
  - A cryptographic has function has been applied!
  - f(s) → f(f(s)) simple calculation
  - f(f(s)) → f(s) very, very difficult calculation.
  - Eavesdropping on f(f(s)) does not help, since he/she cannot derive the next password from this information!

- Holding a OTP leads to a possible authentication, which can lead to a verification of a certificate, thus, an identification of an “individual” (a person or machine)
  - Only an “indirect” identification, possibly reputable