Programming of Distributed Systems

Topic VIII – Security

Dr.-Ing. Dipl.-Inf. Erik Schaffernicht

Security objectives in distributed systems

Goals

- **Integrity** – protection from unauthorized alterations of hardware, software or data
  (by non-authorized users or in non-authorized ways)
- **Confidentiality** – dissemination of data only to authorized users
- **Authenticity** – sources of messages must be verifiable
- **Availibility** – services should be available and function correcly

Threats in distributed systems

- **Interception** – eavesdropping, access to storage, listening in the network
- **Interruption** – data or services become unusable (denial of service) or destroyed (intentional file corruption)
- **Modification** – changing data or software (changing data entries, worms, etc.), repudiation of communication
- **Fabrication** – replaying recorded messages, inventing users, etc.
- **Masquerade** – entities claiming to be a different entity

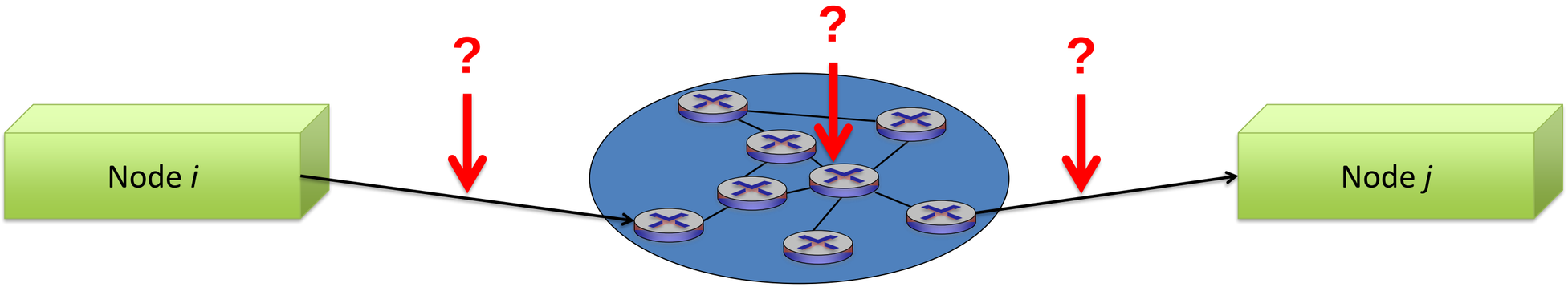
Network Security Analysis

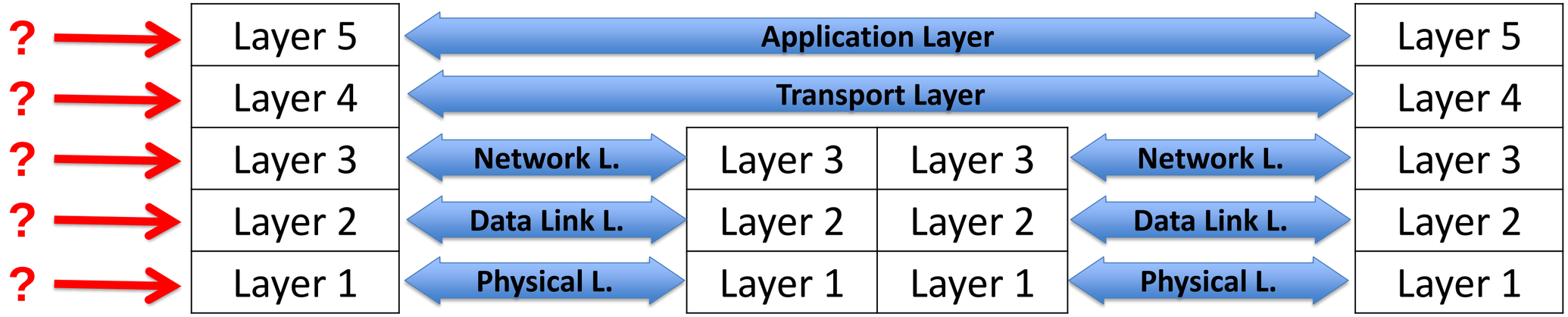
Countermeasures against threats have to be evaluated for a given network configuration

- evaluate the risk potential of the general threats to the entities using a network
- estimate the expenditure (resources, time, etc.) needed to perform known attacks

Cave-at: It is generally impossible to assess unknown attacks!

Possible points of attack





Attacks on the Message Level

Passive attacks:

- eavesdropping

Active attacks:

- delay of messages
- replay of messages
- deletion of messages
- modification of messages
- insertion of messages

Security aspects in distributed systems

Security policies

- What actions are allowed for which entity and which ones are prohibited for whom.

Means

- *Cryptography*
- Secure channels
- Access control
- Security management

Cryptography

Purpose:

- *encryption* of data: plaintext → ciphertext to conceal meaning
- *signing* of data: generate check value or signature to a given (plain or cipher) text, verifiable by some or all communication parterns

Categories:

- symmetric cryptography (1 key for en-/decryption, sign/verify)
- asymmetric cryptography (2 different keys for the two operations)
- cryptographic hashing (0 keys, part of the data)

Cryptography

- **Symmetric encryption**
  - Use of a single (secret) key for both encrypting/signing and decrypting/verifying a message
  - AES, RC6, Blowfish, KASUMI, ...

- **Asymmetic encryption**
  - Keys for encryption (public) are different than those for decryption (private)
  - RSA, ElGamal, Elliptic curve cryptography, ...

Modification Check Values

Known from computer communication

- error detection codes
  (e.g. to detect bit errors during transmission)
  - Parity bits, cyclic redundancy check, ...

Idea

- use a similar mechanism to detect message modifications

Problem

- difference between random errors and deliberate modifications

Cryptographic Hash Functions

A hash function h is a function that maps input x of arbitrary finite length to an output $h(x)$ of fixed bit length n.

- the above property is also called compression

- Often assumed:
  Given h and x it is easy to compute $h(x)$
  (ease of computation)

Cryptographic Hash Functions

A cryptographic hash function h is a function that additionally satisfies the following properties:

- *pre-image resistance*: for all pre-specified outputs y it is computationally infeasible to find an x such that $h(x)=y$
- *2nd pre-image resistance*: given x it is computationally infeasible to find any second input x' with $x \neq x'$ such that $h(x) = h(x')$
- *collision resistance*: it is computationally infeasible to find any pair (x,x') with $x \neq x'$ such that $h(x) = h(x')$

Ensuring integrity of messages

Option 1

- digital fingerprint of a message computed with a cryptographic hash function
  (MDC – modification detection code)
- fingerprint is then digitally signed (e.g. using public key cryptography)

Option 2

- parametrize the cryptographic hash function with a secret key (e.g. symmetric cryptography)
  (MAC – message authentification codes)

Security aspects in distributed systems

Secure channels

- authentification of communicating parties
- ensure data integrity & confidentiality

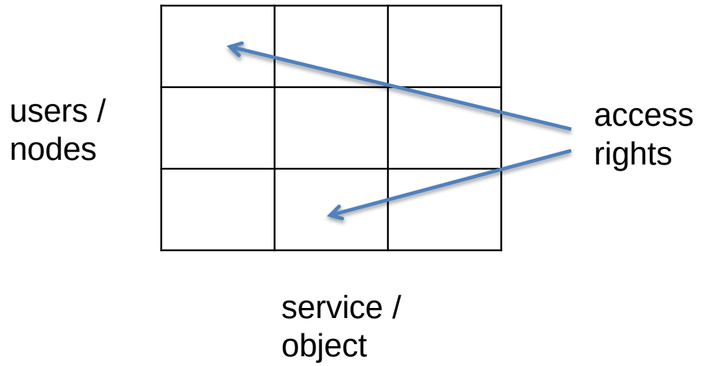
Authentification = Identification + Verification

- user login authentification
- authentification of communicating entities
- hashing of data to ensure integrity

Security aspects in distributed systems

Access control schemes

- Access Control Lists / Matrix



- Firewalls
  - packet-filtering based on source and destination address in packet header (network layer)
  - application gateway, looks at the content of incoming and outgoing messages (application layer)
  - often a combination of the two above

Security aspects in distributed systems

Security management

- Key management / exchange for symmetric cryptography
- Key distribution centers / Certification Authorities for asymmetric cryptography

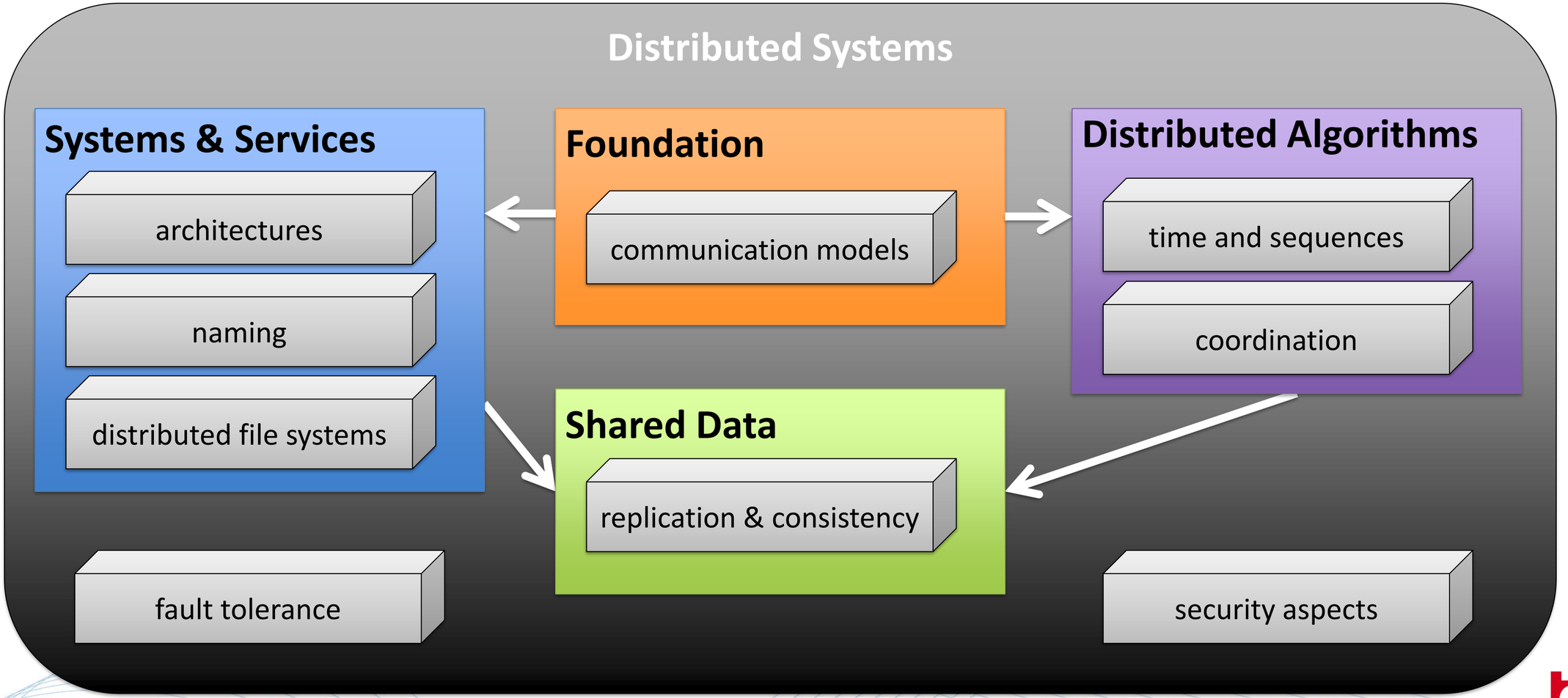
- → Life-cycle of crypto keys

Programming of Distributed Systems

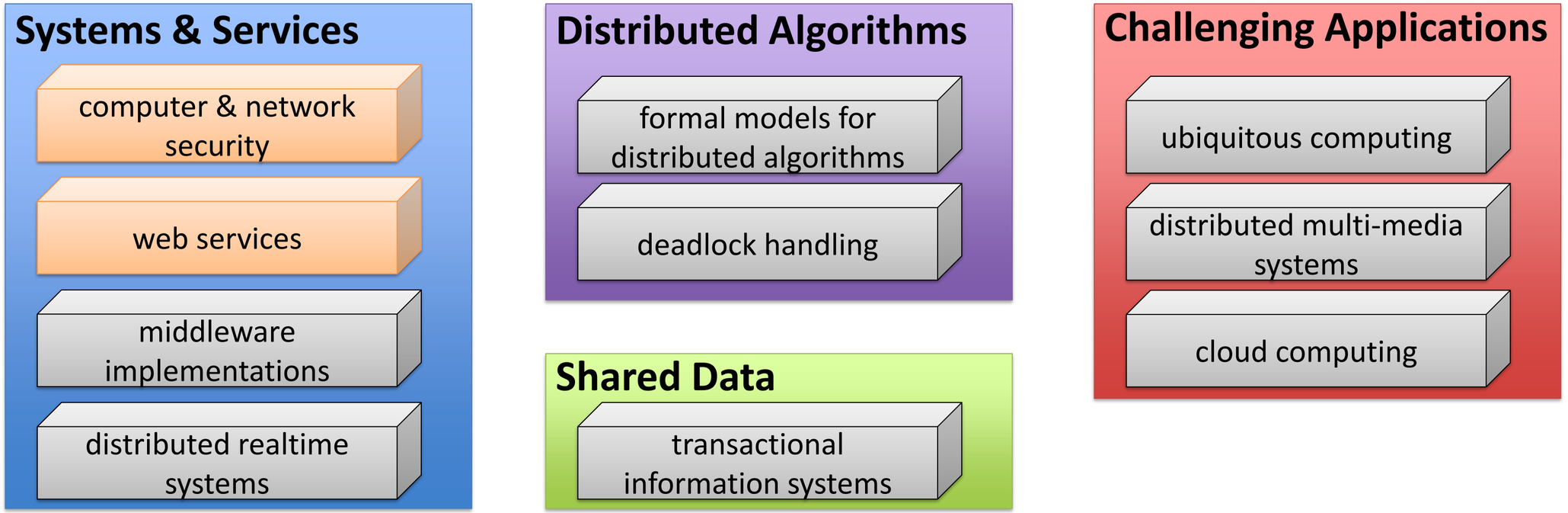
Summary

Dr.-Ing. Dipl.-Inf. Erik Schaffernicht

Overview of the topics covered



Topics not (sufficienly) covered



Learning Goals Revisited

- Ability to describe and explain important aspects of distributed systems
- Understand and use distributed resources
- Chose an appropriate design for problems involving distributed components
- Be aware of the pitfalls and challenges inherent to designing and operating distributed systems

Common pitfalls revisited

- The network is reliable
- The network is secure
- The network is homogeneous
- The topology does not change
- Latency is zero
- Bandwidth is infinite
- Transport cost is zero
- There is one administrator