BA IT-Security

Chapter 1: Introduction

Prof. Dr.-Ing. Ulrike Meyer

Overview on Chapter 1

Security goals, attacks, mechanisms and services

- Definition of security goals
- Types of attacks that threaten them
- Examples for these attacks
- Definition of security mechanisms and services
- Examples

Vulnerabilities exploited by attacks

- Levels of a system on which vulnerabilities occur
- Examples of typical vulnerabilities on each level

Attackers

- Types of attackers
- Motivation of attackers

Overview on the rest of the lecture

- Overall structure
- Connections
- Further lectures and other teaching activities

Overview

Security goals, attacks, mechanisms and services

- Definition of security goals
- Types of attacks that threaten them
- Examples for these attacks
- Definition of security mechanisms and services
- Examples

Vulnerabilities exploited by attacks

- Levels of a system on which vulnerabilities occur
- Examples of typical vulnerabilities on each level

Attackers

- Types of attackers
- Motivation of attackers

Overview on the rest of the lecture

- Overall structure
- Connections
- Further lectures and other teaching activities

Definition of IT-Security and Security Goals

IT-Security comprises all measures to

prevent, detect, mitigate, or deter attacks against confidentiality, integrity, or availability of an asset in a system, including data, software, hardware, and networks.

An attack is thus any action that compromises one of the three main security goals

Definition of IT-Security and Security Goals

Confidentiality

Only authorized entities can access assets in a system

Integrity

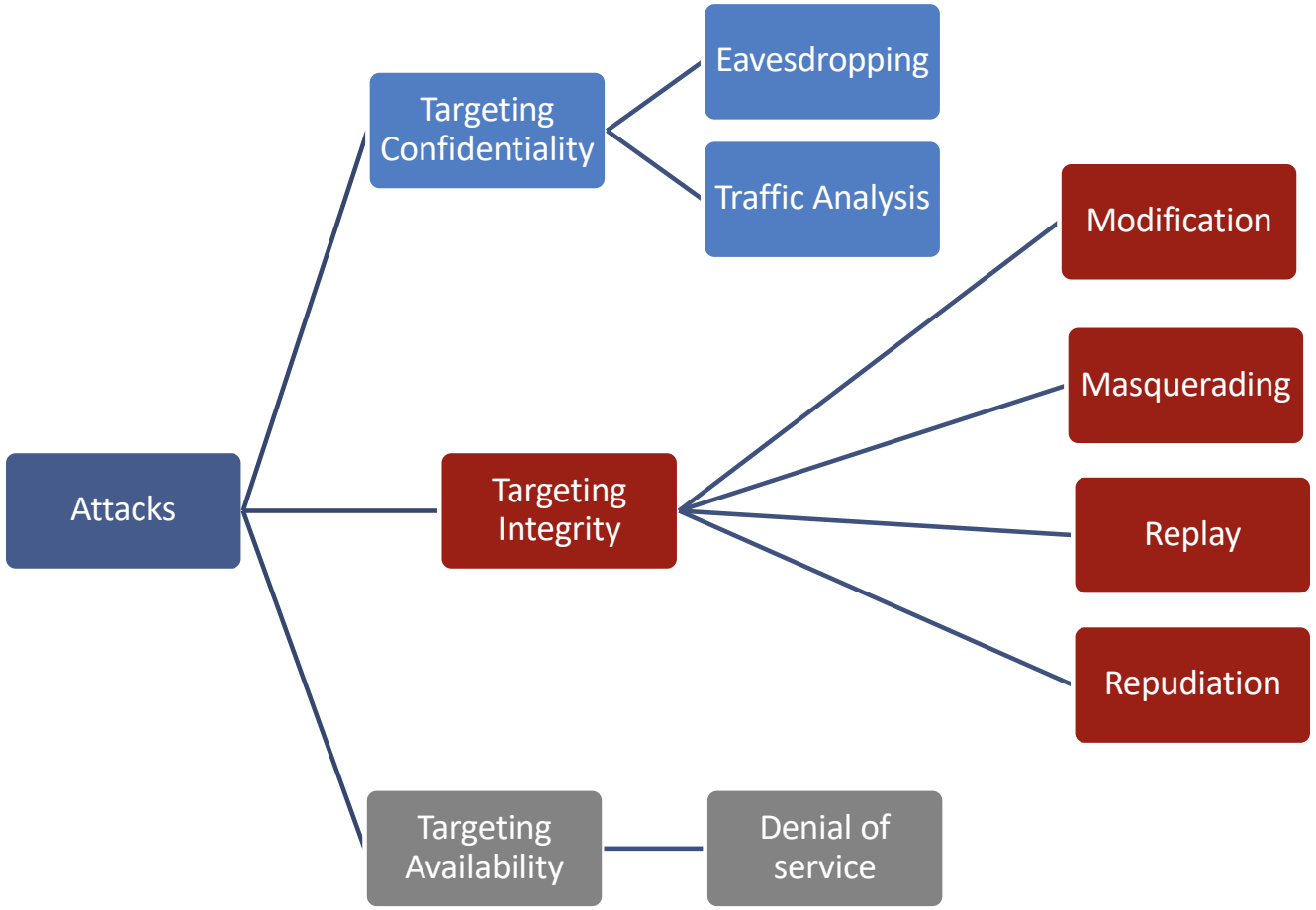
Only authorized entities can make changes assets in a system

Availability

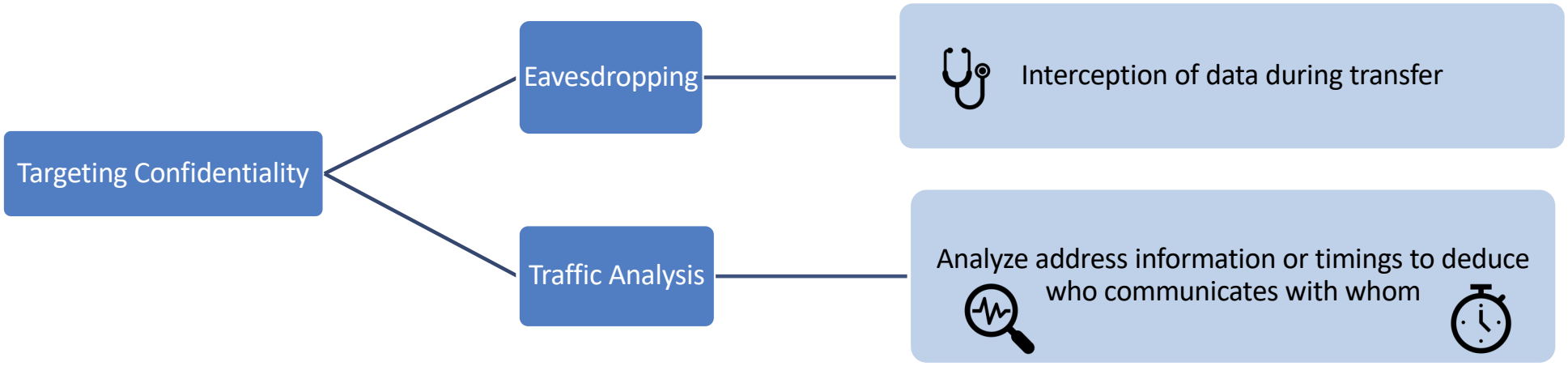
Authorized entities can access assets in a system as intended

Collectively referred to as CIA

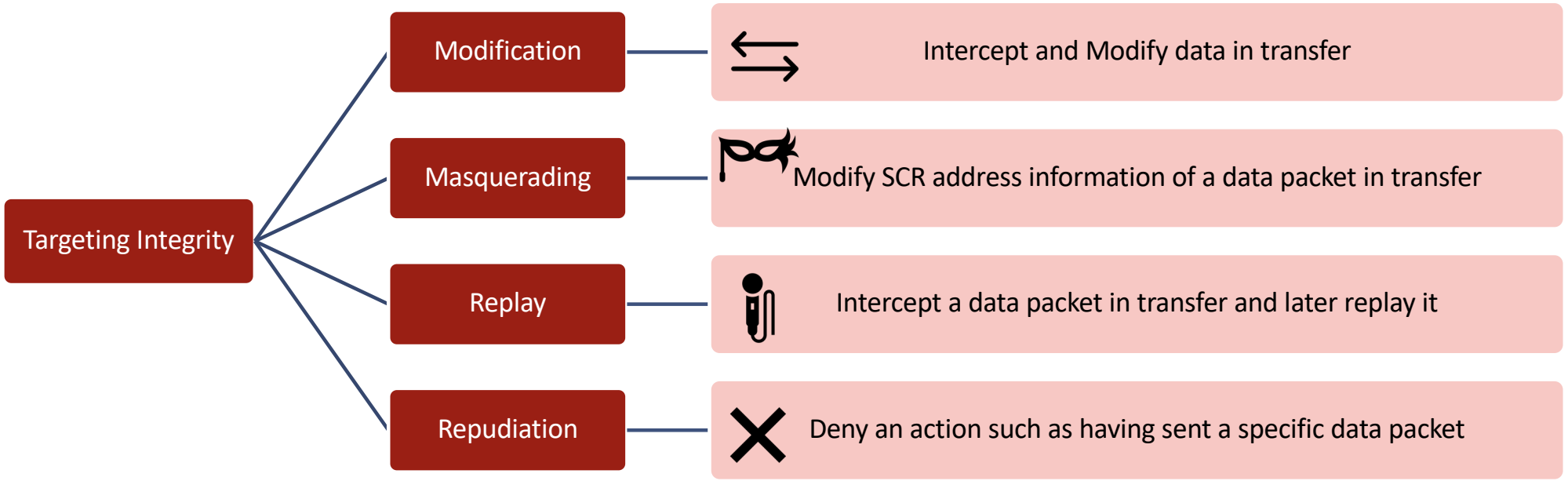
Example Types of Attacks per Goal



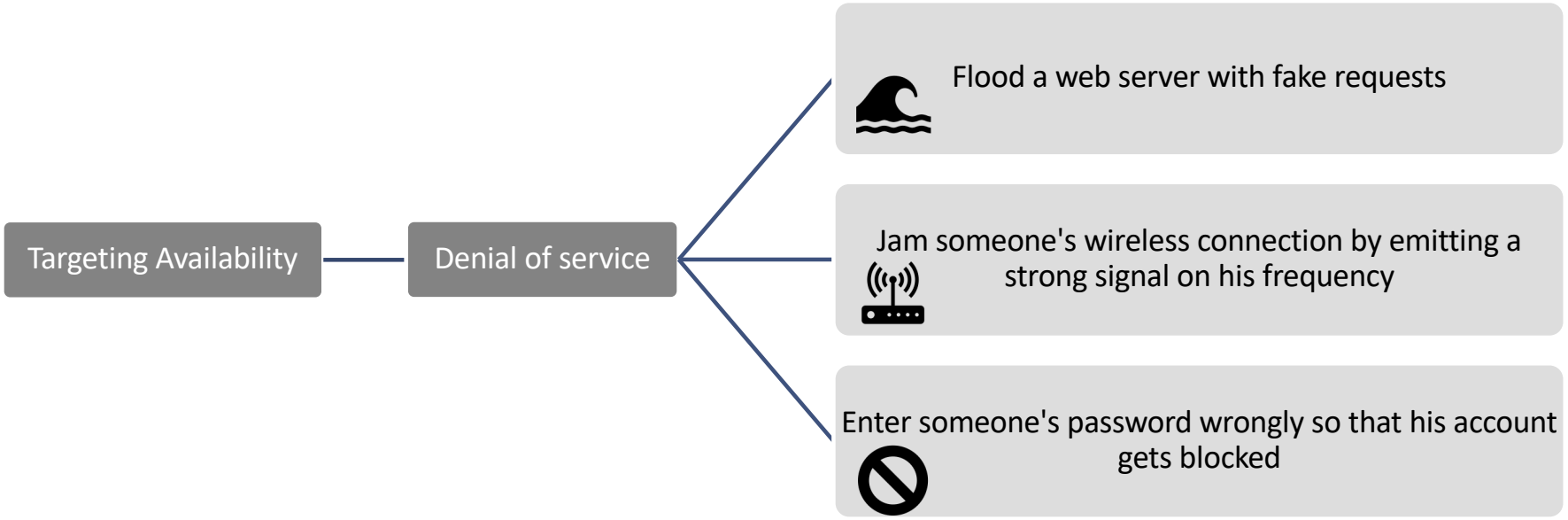
Example Attacks Against Confidentiality



Example Attacks Against Integrity



Example Attacks Against Availability



Attack Examples

Attack against Availability

Hackers Flood NPM with Bogus Packages Causing a DoS Attack

Apr 10, 2023 Software Security / JavaScript

Threat actors flooded the npm open source package repository for Node.js with bogus packages that briefly even resulted in a...

Attack against Availability

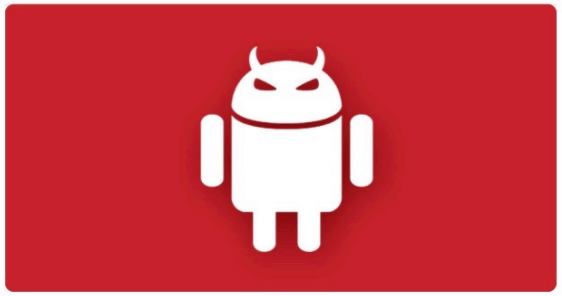
LockBit Ransomware Now Targeting Apple macOS Devices

Apr 18, 2023 Encryption / Malware

Threat actors behind the LockBit ransomware operation have developed new artifacts that can encrypt files on devices...

Examples taken from https://thehackernews.com/

Attack Examples



Attack against Integrity, Confidentiality

Goldoson Android Malware Infects Over 100 Million Google Play Store Downloads

Apr 18, 2023 Mobile Security / Hacking

The rogue component is part of a third-party software library used by the apps in question and is capable of gathering information about installed apps, Wi-Fi and Bluetooth-connected devices, and GPS locations.

Attack against Confidentiality, Integrity, Availability

New Atomic macOS Malware Steals Keychain Passwords and Crypto Wallets

Apr 28, 2023 Endpoint Security / Cryptocurrency

Threat actors are advertising a new information stealer for the Apple macOS operating system called Atomic macOS Stealer...

Examples taken from https://thehackernews.com/

Security Mechanisms and Services

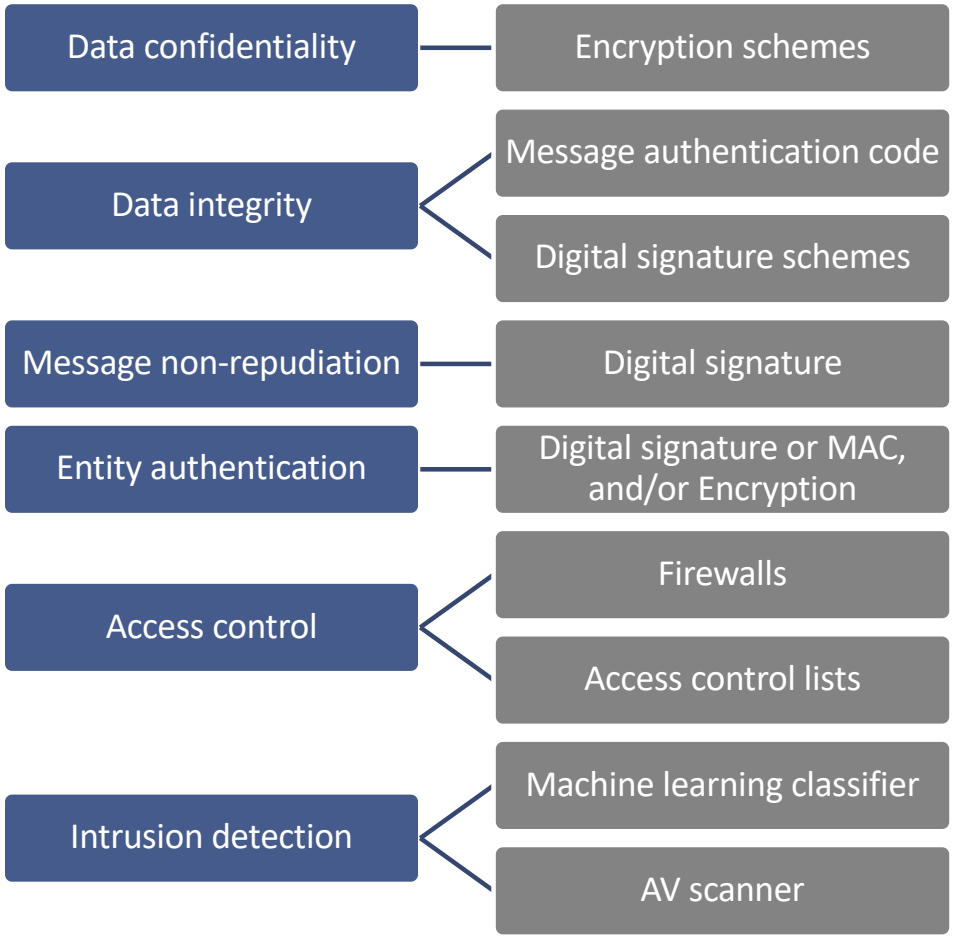
Security Mechanism

- A mechanism that is designed to detect, prevent, recover from, or deter an attack against an asset in a system

Security Service

- A service that protects the security goals of assets in a system
- A security service makes use of one or more security mechanisms

Examples for Security Services and Example Security Mechanisms



Overview

Security goals, attacks, mechanisms and services

- Definition of security goals
- Types of attacks that threaten them
- Examples for these attacks
- Definition of security mechanisms and services
- Examples

Vulnerabilities exploited by attacks

- Levels of a system on which vulnerabilities occur
- Examples of typical vulnerabilities on each level

Attackers

- Types of attackers
- Motivation of attackers

Overview on the rest of the lecture

- Overall structure
- Connections
- Further lectures and other teaching activities

Attacks make use of Vulnerabilities on all Levels of a System

Human

User / Administrators

Configuration, Password Selection, Ignoring Software Updates, Installing malicious software,…

Systems

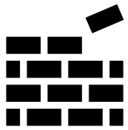
Implementations

Application software, Web servers, protocol stacks, operating systems, …

Specifications

Protocols and policies

TCP/IP, TLS, IPSec, HTTPs, access control policies,…



Building blocks

Cryptographic primitives

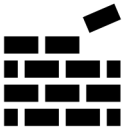
RSA, DSS, HMAC, SHA-1…

All defense mechanisms on all layers can be targeted and must interact properly

Broken Building Blocks

Classical Examples

- Encryption algorithms used in 2G mobile networks (A5/2, A5/1...)
- RC4 Encryption algorithms used in WLAN, TLS, IPSec,....
- Cryptographic hash functions MD5, SHA1
  - Used, e.g., in TLS



- **Typical Solution: Integrate multiple algorithms to choose**
  - New attacks on ciphers cannot be prevented
  - Include multiple algorithms as “mandatory“ to support in protocol specifications
  - Allow for an easy integration of additional algorithms
  - Configure your system to use secure algorithm if an algorithm is broken

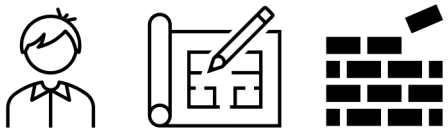
New Problem: Secure Algorithm Selection

Need to agree on the algorithm to be used on specific connection

- Algorithm negotiation must be protected

Typical Approach

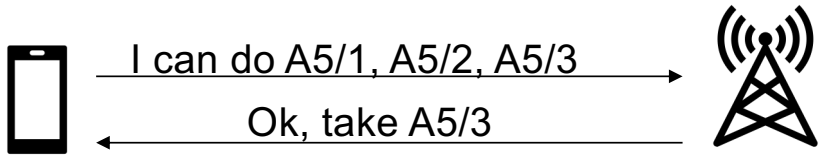
- Parties exchange information on which algorithms they support
- One of the algorithms both support is selected
- Information exchanged needs to be protected against manipulation
  - Problem: algorithms, e.g., for integrity protection have not been selected yet



Example for Insecure Algorithm Negotiation

Insecure negotiation leads to downgrading attacks

- Attacker can downgrade the negotiation to a broken algorithm



Broken!

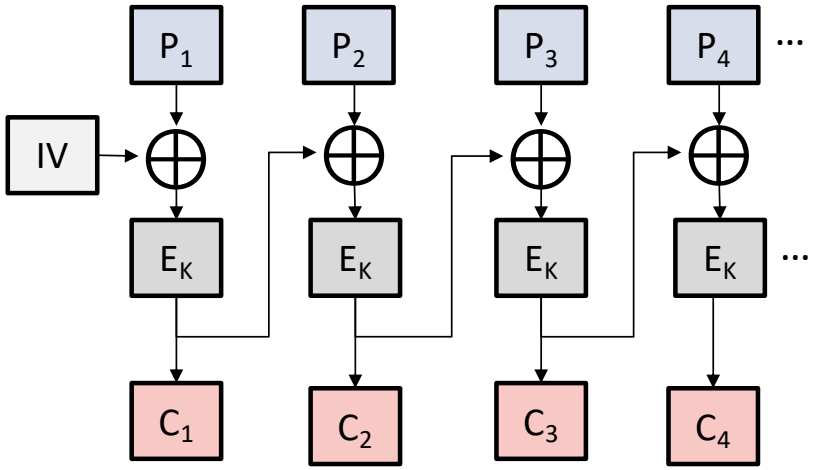
A5/1, A5/2, A5/3

- encryption algorithms supported in 2G mobile networks
- A5/2 totally broken since 2001

- Works because integrity of messages indicating the supported algorithms is not protected
- Broken algorithm often still supported to service old devices that only support old mechanisms
  - Backward Compatibility

Problem: ALL Building Blocks Need to be Negotiable

Broken CBC Mode of Encryption for Symmetric Ciphers



$IV := C_0$

Encryption: $C_i = E_k(P_i \oplus C_{i-1})$

Decryption: $P_i = D_k(C_i) \oplus C_{i-1}$

- If CBC Mode is used, then in some application settings it is possible to decrypt messages even if the underlying encryption algorithm E_K is secure
- All **mandatory TLS 1.2** ciphers used CBC-Mode

Typical Sources for Vulnerabilities in Protocols and Specifications

- **Design Flaws**
  - E.g. WEP: wired equivalent privacy problem in Wireless LAN (2001)
    - Authentication breaks after simple eavesdropping on one authentication protocol run
    - Weak encryption, no integrity protection
    - …
- **Backward Compatibility Problems**
  - If devices support different versions of a protocol, downgrading to an older version is often possible
    - Attack pretends that one of the communicating endpoints does not support newer version
- **Incomplete Specifications**
  - Krack-attack against WLAN (2017)
    - Problem in the protocol design: unspecified how to handle unexpected messages

Typical Sources for Vulnerabilities in Implementations

- **Software vulnerabilities**
  - Buffer overflows, Format string vulnerabilities, XSScripting,…
  - Bugs like the OpenSSL bug: implementation problem on Debian-based systems (2006)
    - Lead to only 32,767 $(= 2^{15} - 1)$ different SSH-keys
    - Not a vulnerability in the protocol design
    - "Just" a problem in the implementation of the pseudo-random function
  - Using malicious libraries or insecure code fragments of others
- **Update life cycles**
  - Software vulnerabilities can typically not be entirely avoided
  - Updates that patch vulnerabilities need to be published and deployed
- **Insecure default settings**
  - E.g., if IoT device ships with a default admin password and does not require changing it

Examples for Users and Administrators as Vulnerabilities

- **Failing to update available software patches**
  - More and more automated but still many software vulnerabilities exploited although patches are available
- **Deliberately installing malicious software**
  - Typically, unintended
    - Trojans: malicious software masquerading as benign application
    - Clicking on a malicious attachment
    - Installing free software from dubious sources
- **Social Engineering**
  - Talking someone into revealing their password
  - Luring someone on a fake website and making them enter their login data

Example Social Engineering

13 FEB 2018 OPINION

Never Mind Malware - Social Engineering Will Be Your Biggest Threat This Year

Called to an urgent Zoom meeting with HR? It might be a phishing attack

Graham Cluley • @gcluley
10:15 am, April 26, 2020

Coronavirus phishing attack disguises as a message from the Center for Disease Control

Graham Cluley • @gcluley
12:36 pm, February 10, 2020

Example: Malware delivered with Social Engineering

Hackers disguise malware attack as new details on Donald Trump's COVID-19 illness

GRAHAM CLULEY Follow @gcluley

OCT 8, 2020 | IT SECURITY AND DATA PROTECTION

Overview

Security goals, attacks, mechanisms and services

- Definition of security goals
- Types of attacks that threaten them
- Examples for these attacks
- Definition of security mechanisms and services
- Examples

Vulnerabilities exploited by attacks

- Levels of a system on which vulnerabilities occur
- Examples of typical vulnerabilities on each level

Attackers

- Types of attackers
- Motivation of attackers

Overview on the rest of the lecture

- Overall structure
- Connections
- Further lectures and other teaching activities

Types and motivation of attackers

All of them can be insiders or outsider attacker

- **Criminals and Hackers-for-hire**

  - Making money as main motivation
    - Stealing and selling login credentials, trade secrets, personal data, …
    - Extortion, e.g., by threatening to publish stolen data or to stage a denial-of-service attack,…
    - Spreading spam
    - Get paid for exploits, malware, bots,…

- **Crackers and Hacktivists**

  - Achieve Fame and glory in the blackhat community
  - Claim to crack for the greater good

- **Secret service and military personal**
  - Cyber attacks and defenses

- **End users**

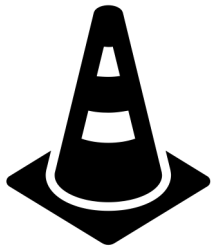
  - That do not adequately protect their computers

- **Pentesters**

  - Try to break into systems on demand
    - with explicit consent of system operator
  - Reveal and help to fix exposed vulnerabilities

Summary

- **Attacks typically threaten one or more of the CIA security goals**
  - Confidentiality, Integrity, Availability
- **Attacks can exploit vulnerabilities on all levels of a system**
  - Security mechanisms required on each level
  - Mechanisms on different levels must interact properly
- **Security mechanisms and services aim at protecting against attacks by**
  - prevention, detection, mitigation, or deterrence
- **Attackers vary greatly with respect to**
  - Their motivation
  - Their power w.r.t. their skills, knowledge on / access to the target, and their computational resources,…



Overview

Security goals, attacks, mechanisms and services

- Definition of security goals
- Types of attacks that threaten them
- Examples for these attacks
- Definition of security mechanisms and services
- Examples

Vulnerabilities exploited by attacks

- Levels of a system on which vulnerabilities occur
- Examples of typical vulnerabilities on each level

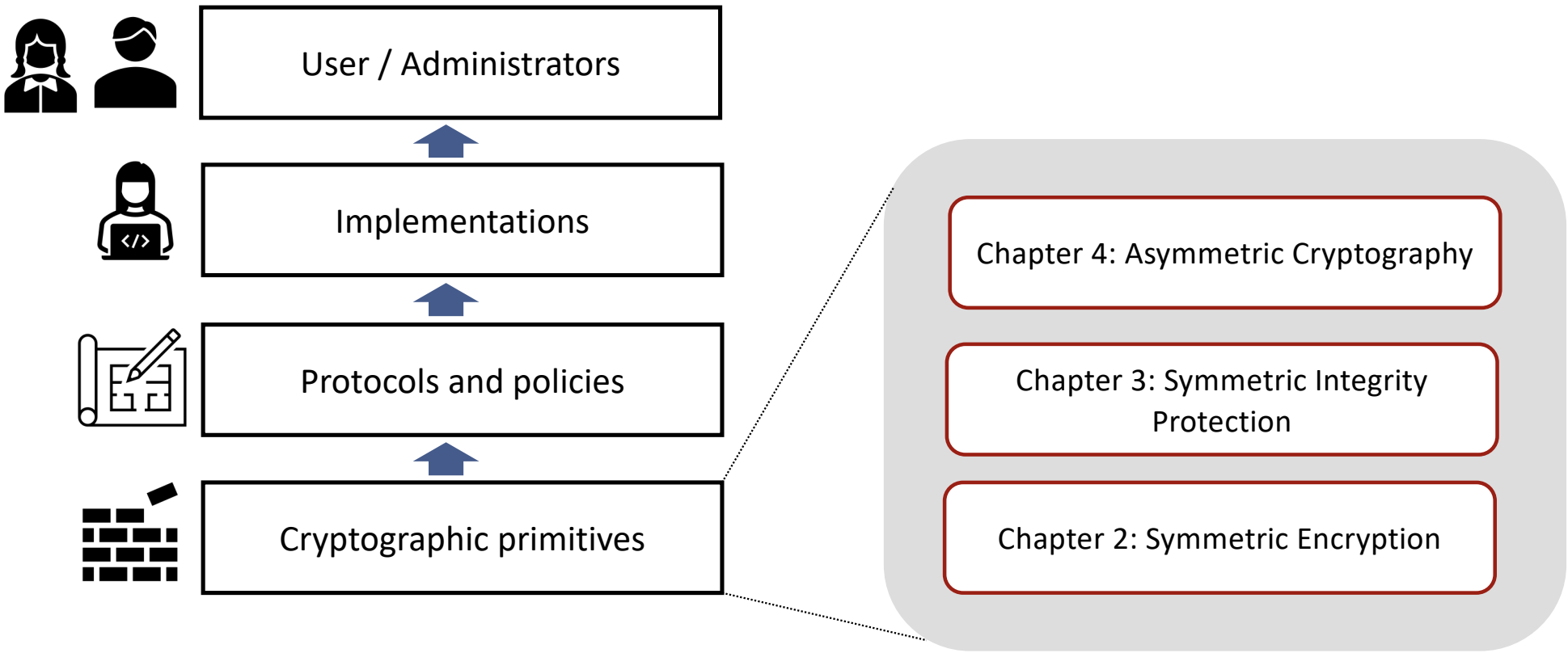
Attackers

- Types of attackers
- Motivation of attackers

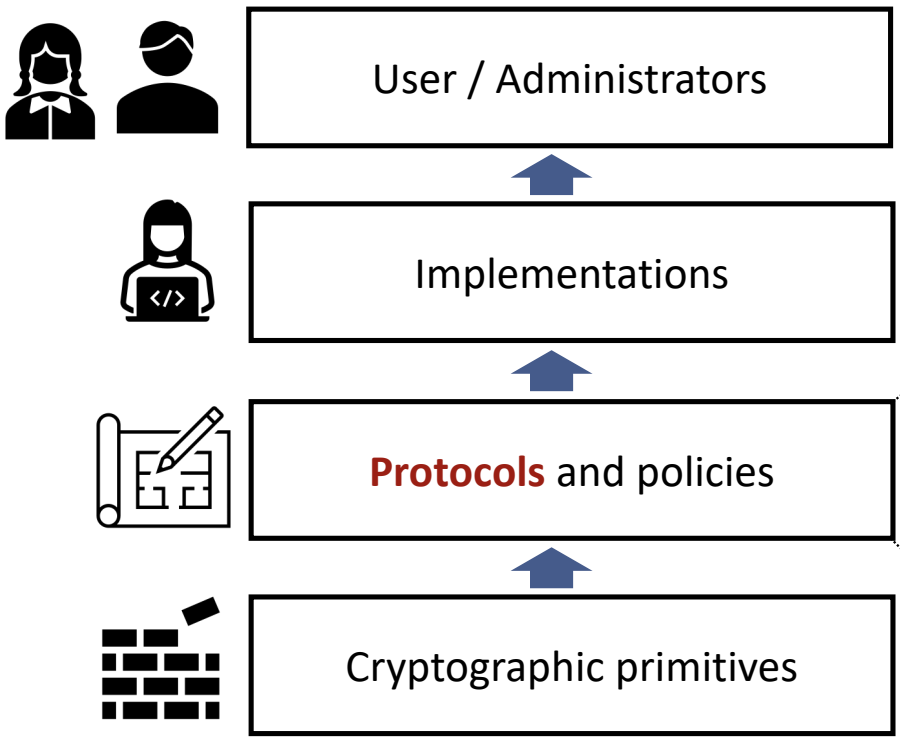
Overview on the rest of the lecture

- Overall structure
- Connections
- Further lectures and other teaching activities

Cryptographic Primitives



Cryptographic Primitives

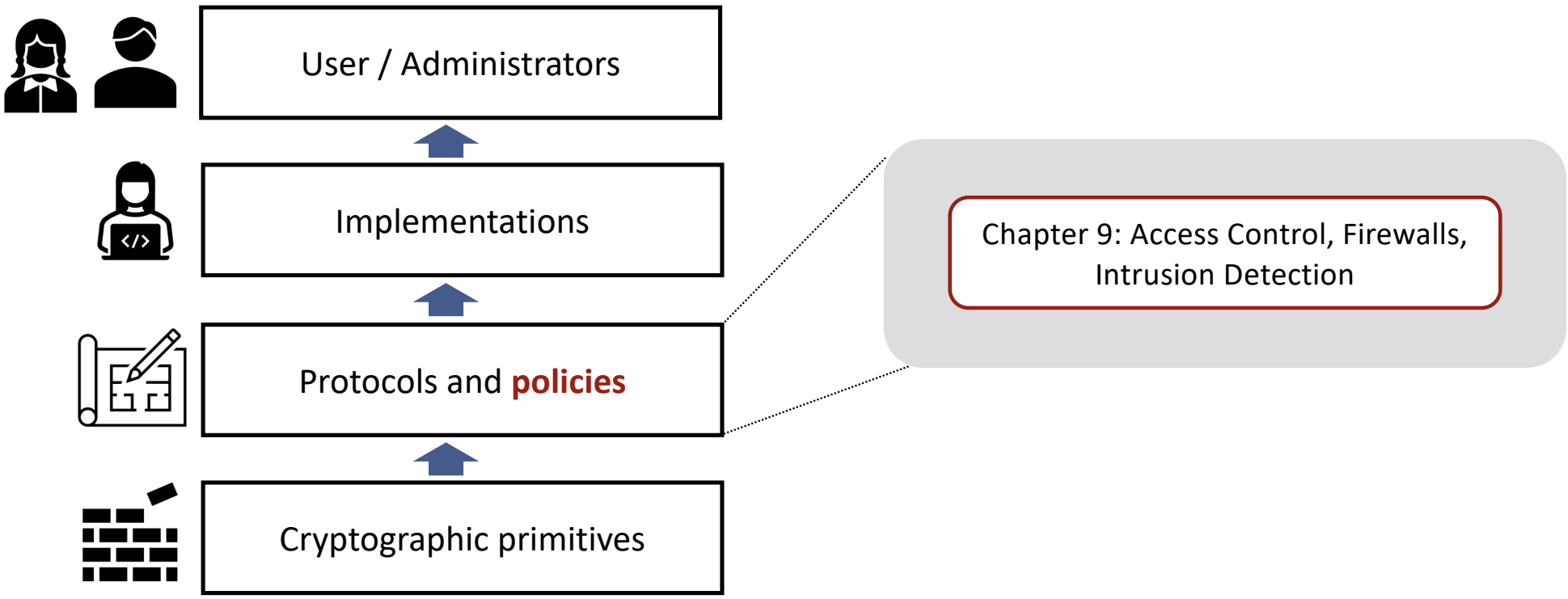


Chapter 7: Securing Applications

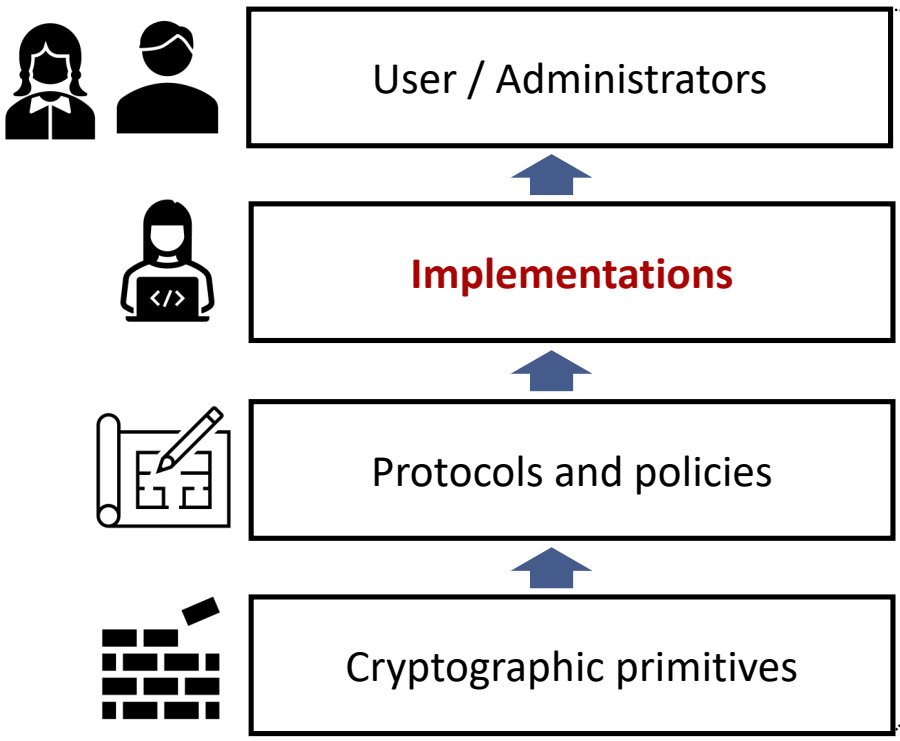
Chapter 6: Network Security Protocols

Chapter 5: Authentication and Key Agreement

Cryptographic Primitives



Cryptographic Primitives



Chapter 8: Denial of Service Attacks

Chapter 10: Malware and Software Vulnerabilities

Cryptographic vs. Non-Cryptographic Protection

Cryptographic Protection against Attacks on Confidentiality and Integrity

- Chapter 4: Asymmetric Cryptography
- Chapter 3: Symmetric Integrity Protection
- Chapter 2: Symmetric Encryption
- Chapter 5: Authentication and Key Agreement
- Chapter 6: Network Security Protocols
- Chapter 7: Securing Applications

Most Prominent Example Attacks that cannot be prevented / detected by cryptographic means alone

- Chapter 8: Denial of Service Attacks
- Chapter 10: Malware and Software Vulnerabilities

Non-Cryptographic Protection against Attacks on Confidentiality, Integrity, and Availability

- Chapter 9: Access Control, Firewalls, Intrusion Detection

References

- **IETF RFC 4949: Security Glossary**
- **W. Stallings, Cryptography and Network Security: Principles and Practice, 8th edition, Pearson 2022**
  - Chapter 1: Information and Network Security Concepts