

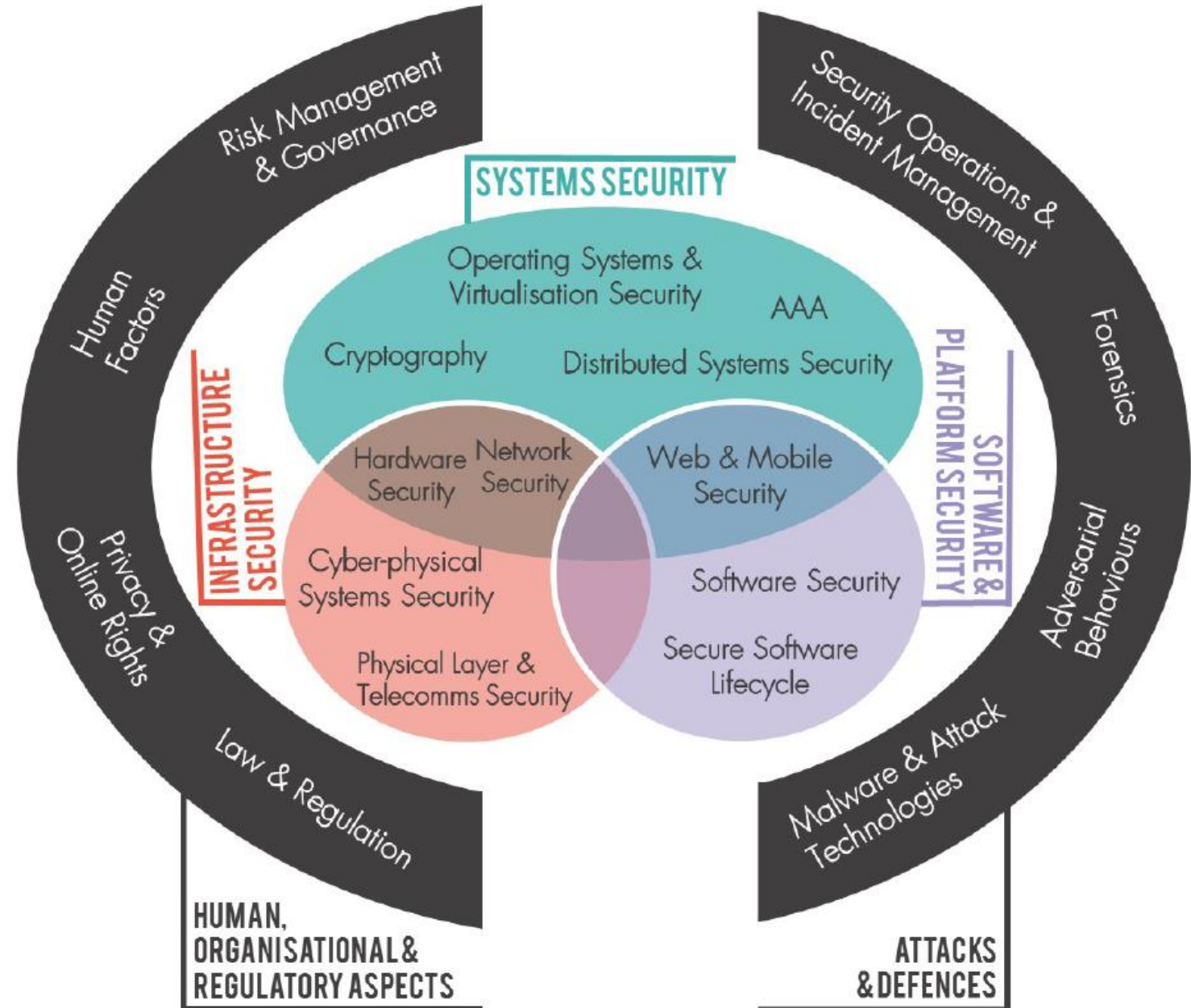
Domains of Cyber Security

Cyber security and information security

Cybersecurity refers to the **protection of information systems** (hardware, software and associated infrastructure), the data on them, and the services they provide, **from unauthorised access, harm or misuse**. This includes harm caused intentionally by the operator of the system, or accidentally, as a result of failing to follow security procedures.

Information security. Preservation of confidentiality, integrity and availability of **information**. In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Domains



Systems security

- Operating systems protection mechanisms, virtualization security
- Cryptography
- Authentication, Authorization, Accounting - AAA
- Distributed Systems Security

Systems security

- **Operating systems protection mechanisms, virtualization security**
(Manage resources, control the operation of user programs)

Areas relevant to security: process, kernel, virtual machines (VMs)
Trusted Execution Environments.

Adversarial goals: leak confidential data (e.g., crypto keys), modify data that should not be accessible (e.g., to escalation privileges) or limit the availability of the system and its services (e.g., by crashing the system)

Systems security

- **Cryptography**

algorithmic controls: protecting confidentiality (encryption), integrity (hash, MAC, digital signatures), authenticity (MAC, digital signatures), nonrepudiation (digital signatures) of data with algorithms.

Special fields: Privacy Enhancing Technologies

- Computations over encrypted data: Fully Homomorphic Encryption,
- Secure Multiparty Computation over confidential data
- Minimum data provision: zero knowledge protocols, Oblivious transfer

Systems security

- **Authentication, Authorization, Accounting - AAA)**

Access control= Authentication + Authorization

Access control is “the process of granting or denying specific requests . . .”. This process needs the following inputs

- Who issued the request? --> Identification+ Authentication
 - What is requested?
 - Which rules are applicable when deciding on the request?
- } Authorization

Accounting: Supporting processes that start after the events have occurred. E.g. regular audit, post-incident review (operating system, network devices, application log files)

Systems security

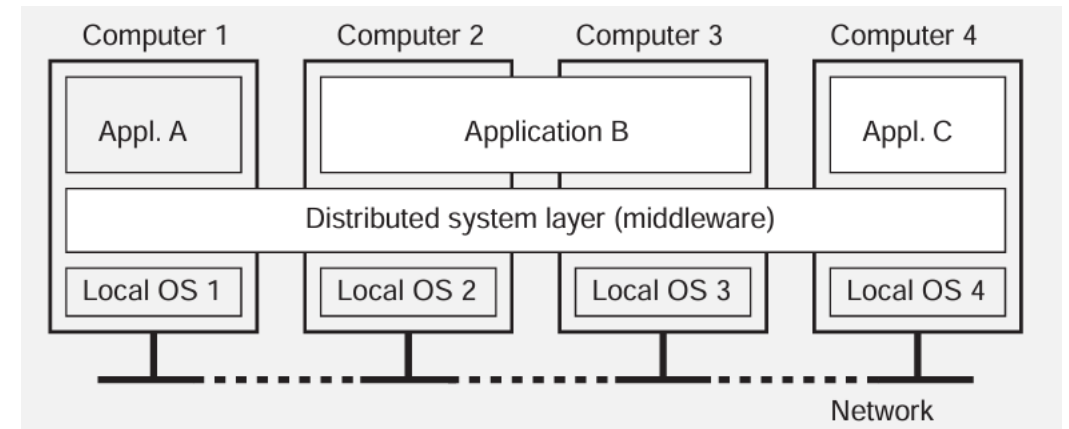
- **Distributed systems Security**

distributed system: a network of computers, often in geographically separate locations

- that provides a service by connecting data generators and users
- provides an on-demand, highly reliable, highly available and consistent resource
- appears to the operator as a single coherent system (centralised or decentralised)

security considerations:

- Data integrity protection,
- access management,
- secure data transfer,
- secure operation of middleware (e.g. replication, failure handling, data consistency (consensus mechanisms))
- secure applications

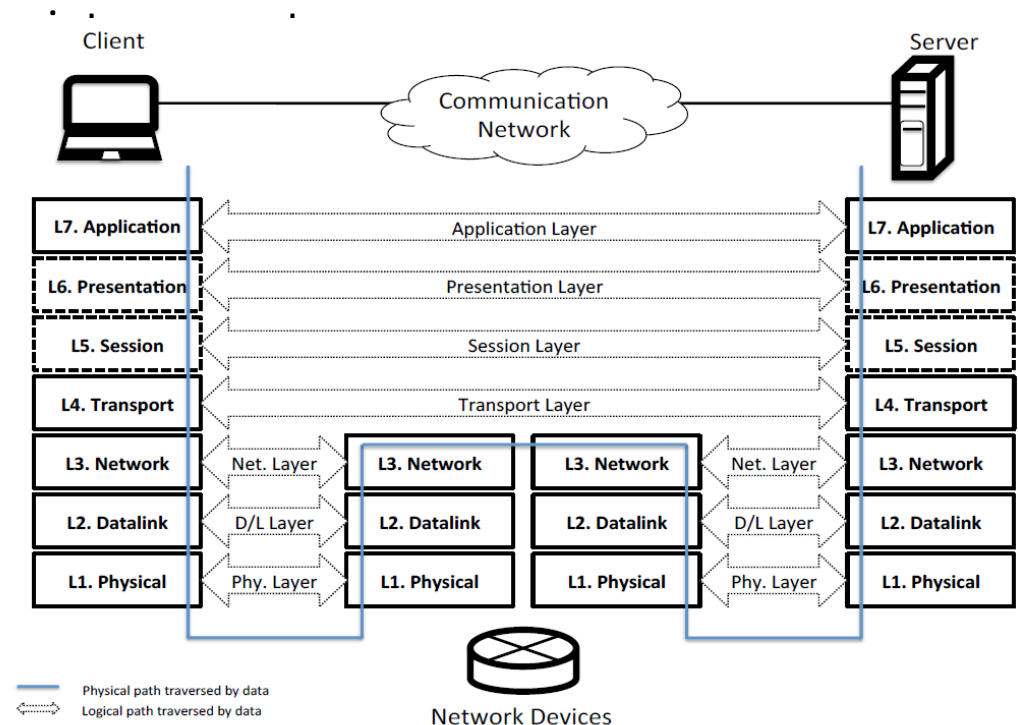


Infrastructure security

- Network security (systems security)
- Hardware security (systems security)
- Cyber-physical systems security
- Physical layer security, telecommunications

Network security

- Systems security also
- Areas covered:
 - network protocols
 - For security analysis, Dolev-Yao model: attacker has full control over the network (usually real attackers are weaker)
 - Network communication attacks must be taken into account
 - Application layer: PKI
 - Transport: TLS, QUIC (for UDP)
 - Network: IPSec
 - Data Link: IEEE 802.1X port-based authentication, switch, access point (AP) authentication
 - Security devices:
 - firewall,
 - Intrusion Detection System - IDS,
 - Intrusion Prevention System - IPS
 - Network design considerations (e.g. DMZ - demilitarized zone)



Hardware security

- Systems security also
- Areas covered :
 - „Root of Trust”: component that performs secure computation
basic requirements: secure key storage, real random number generator
 - Secure platforms: a chip or board that performs secure computing, stand-alone silicon elements with strict access rules
 - Hardware Security Modules (HSM) - vehicles
 - Trusted Platform Module (TPM) – PC
 - Trusted Execution Environment (TEE): the security area of the processor, which provides confidentiality, system integrity, authenticity, access control and end-to-end security by protecting the execution of authenticated code.
e.g. IBM 4758 Secure coprocessor,
 - Side-channel attack protection
 - PUF – Physically Uncloenable Functions: unique identifiers for hardware components

Cyber-physical systems security

- Cyber-physical systems: engineering systems, where physical devices are controlled by a computer, e.g. smart grid
- Sensors, actuators, controllers to support system operation
- Attacks at all points (8)
- Problems of SCADA systems (systems are used for controlling, monitoring, and analyzing industrial devices and processes)
- legacy systems(old technologies)

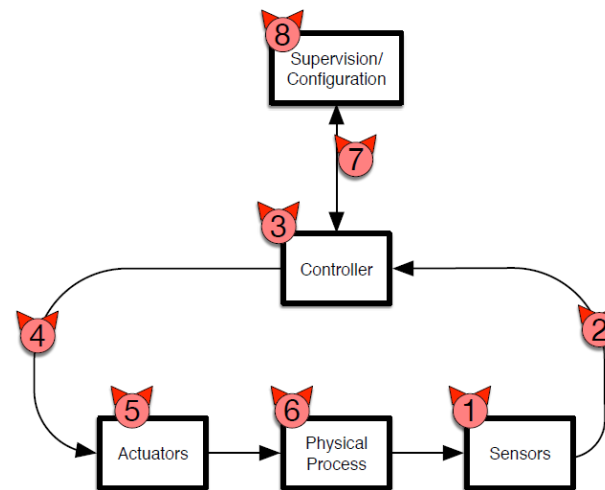


Figure 19.4: Attack Points in a CPS.

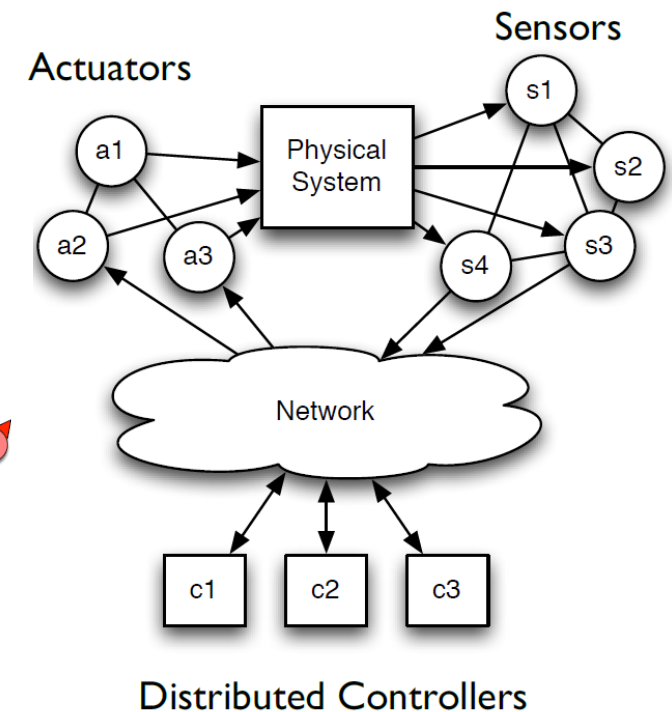


Figure 19.1: General architecture of cyber-physical systems

Software security

Goal: CIA protection of software data and functionality

Bug: programming errors that allow an attacker to compromise a security objective (CIA). Typically, the result of insecure programming.

Categories:

- Web security (systems security)
- Mobile security (systems security)
- Secure software lifecycle
- Secure software development

Web and mobile security

- Web security (systems security)
 - Web applications have both server-side and client-side code that must be protected
 - Web browser support (e.g. Javascript), plugins etc. increases the attack surface
 - Webification: process data on the web platform
- Mobile security (systems security)
 - Smartphones equipped with sensors (GPS), cameras, significant computing and storage capacity and internet connectivity
 - Mobile applications can request access to the device's resources and access users' personal information.
 - Mobile applications with feature-rich network connectivity and capacity are an attractive target for attackers.
 - Appification: „There is an app for everything.“

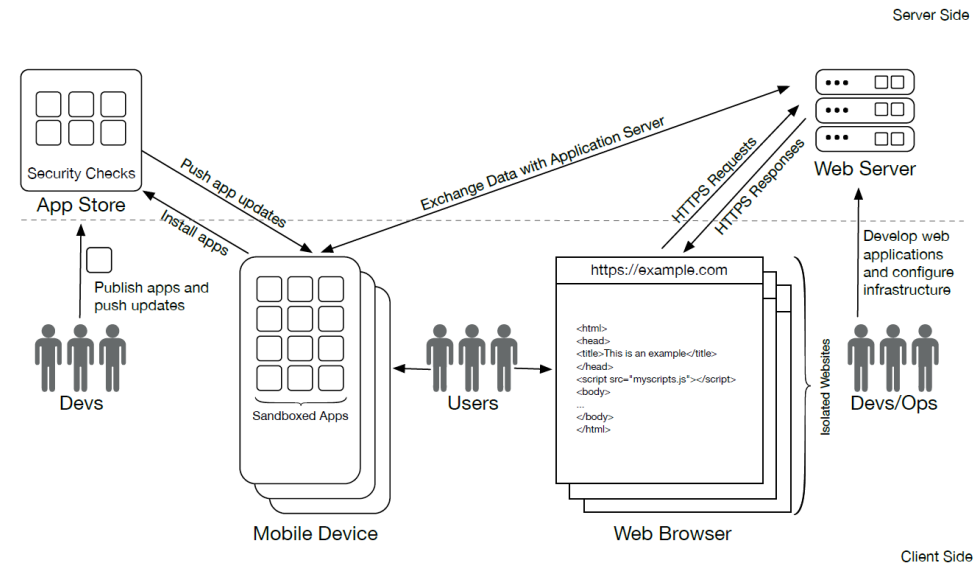


Figure 15.1: Web and Mobile Ecosystem

Secure software lifecycle

The software development process from design to operational use.



Secure software development

- Memory management
- Protection against injection attacks (SQL, command, script injection)
- API (Application Programming Interface), protection of communication between software components (software libraries, operating system, etc.)
- Protection against software-based side channel attacks
- Software testing (writing test cases, analysing outputs for specific inputs)

Human, organisational and regulatory aspects

Administrative control

- Consideration of human factors (e.g. usable security)
- General laws, regulations, directives (e.g. NIS2)
- Data protection regulations, directives (e.g. GDPR)
- Risk assessment, risk management

Human Factors

- **Usable security**

It is the practice of preventing threats that arise from the interaction between people (users) and computer systems. Unlike traditional systems and network security, it focuses on users, analyses their behaviour, mental models and decision-making processes, and determines protective measures.

„fitting the task to the human”

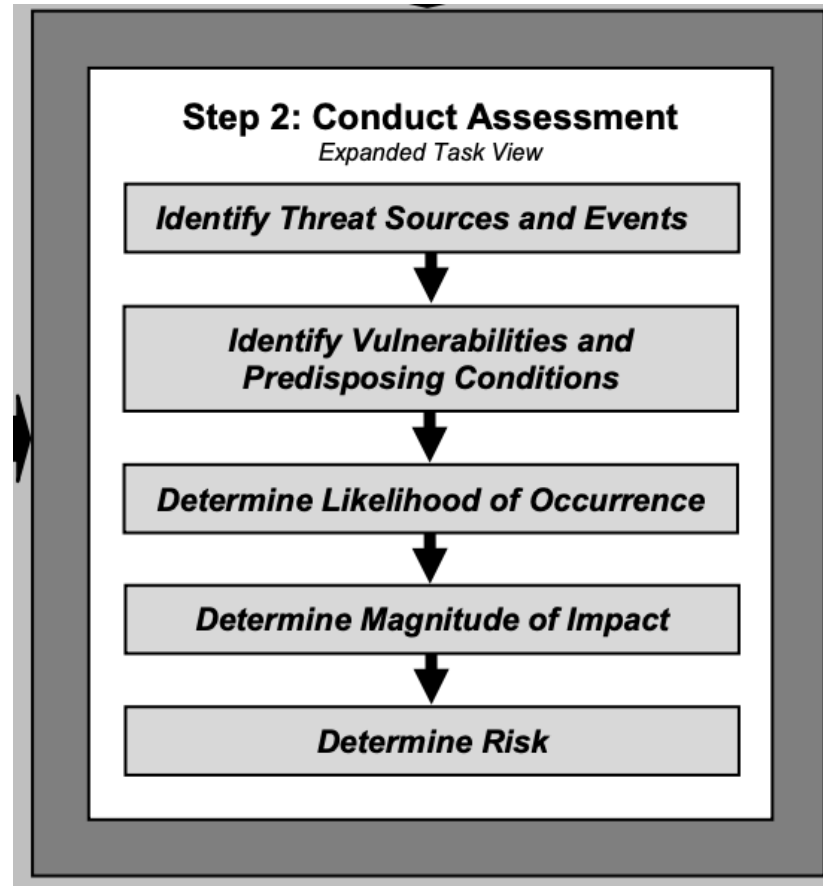
instead of

„fitting the human to the task”

e.g. one time password length is max. 6 characters (short-term memory)

- **Developing user behaviour (e.g. training)**
- **Defining conditions of use of IT systems and user obligations**
- **Disciplinary sanctions in case of security breaches**

Risk assessment, risk management



Risk assessment:

- Threat Analysis
- Vulnerability Assessment
- Determining the probability of threats occurring
- Determining the impact of threats
- Determination of risk

Risk management:

- additional countermeasures to reduce the impact or likelihood of a threat occurring
- acceptance of the risk
- transfer to a third party (e.g. insurance)

Digital forensic

- A digital (forensic) trace is an explicit or implicit record of a specific event, the execution of a computation, or the communication and/or storage of specific data.
- Digital forensics is the process of identifying and reconstructing a sequence of events that lead to the current observable state of an IT system.
- Explicit traces: timestamped event logs,
- Implicit traces: a remnant of a file (proves it was present)
- Domains: data storage, memory, application, cloud