Cybersecurity Fundamentals

Dominik Herrmann, University of Bamberg

What will you learn in this video?

Why is cybersecurity **challenging**?

What are common **threats** to data and systems?

Who is attacking and what are their motives?

What approaches are available for **defenders**?

Why is cybersecurity **challenging**?

What are common **threats** to data and systems?

Who is attacking and what are their motives?

What approaches are available for **defenders**?

Why is cybersecurity challenging?

Cyberspace

virtual world consisting of networked systems that affect our lives

Complexity

quantity and diversity

Asymmetry

attacking versus defending

Why is cybersecurity **challenging**?

Who is attacking and what are their motives?

What are common **threats** to data and systems?

What approaches are available for **defenders**?

Goal of cybersecurity: protecting assets

(hardware, software, data)

Information Security

Objective:

protect data and any information derived from its interpretation

data at rest vs. **data in transit**

Systems Security

Objective:

ensure that (computer) systems operate as designed

Information Security

Objective:

protect data and any information derived from its interpretation

data at rest vs. **data in transit**

Systems Security

Objective:

ensure that (computer) systems operate as designed

Protection Goals in Information Security

confidentiality	integrity	availability
prevent unauthorized **information gain**	prevent or detect unauthorized **modification**	prevent unauthorized **deletion or disruption**
encryption	verification codes (e.g., in online banking)	backup

Who is *authorized*?

confidentiality | **integrity** | **availability**

one authorized party

multipe authorized parties
e.g., sender and receiver

Sometimes security is about protecting the *identity*.

confidentiality | **integrity** | availability

authenticity

detect when the identity of a party (e.g., in a message) has been **forged**

non-repudiation

prevent parties from **denying** that they carried out an act, e.g., sending a message

Information Security

Objective:

protect data and any information derived from its interpretation

Systems Security

Objective:

ensure that (computer) systems operate as designed

Systems Security: How to *design* secure systems?

confidentiality

encrypting data

OR

authentication in combination with **access control**

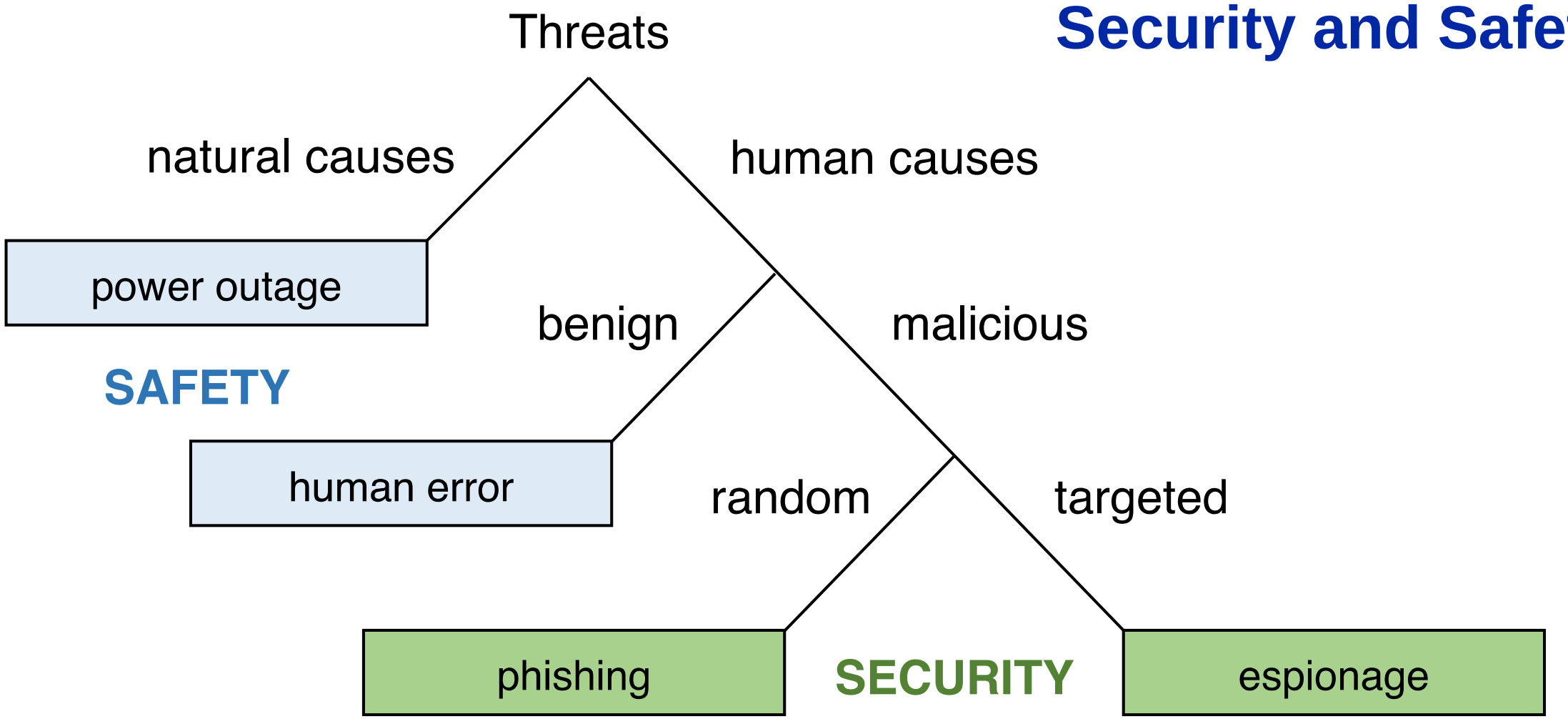
integrity | **availability**

We rely on systems to operate properly.

Attackers may **disable** them or **manipulate** their operation.

Especially relevant for **cyber-physical systems**, i.e., critical infrastructures that society relies on.

Security and Safety



Source of many threats: bugs in software and hardware

weakness → **vulnerability**

e.g., buffer overflow

e.g., CVE-2018-8392

MS JET Database Engine Remote Code Execution Vulnerability (possible due to a buffer overflow)

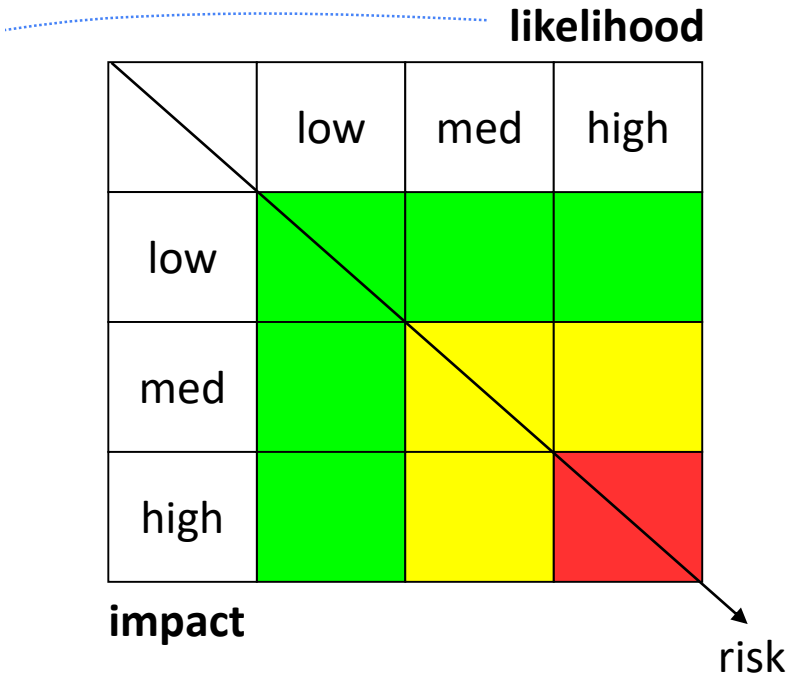
Common Weakness Enumeration
https://cwe.mitre.org

Common Vulnerabilities and Exposures
https://cve.mitre.org

Time of creation:
design, implementation, configuration, operation

Risk Management Perspective

Risk: Possibility that an attack causes damage.
Severity is the product of likelihood and impact.



Why is cybersecurity **challenging**?

What are common **threats** to data and systems?

Who is attacking and what are their motives?

What approaches are available for **defenders**?

When does an attack happen?

opportunity

exposure

working method

exploitability

motive

Different kinds of attackers and their motives

professionals

corporate spies

cyber criminals

nation states

insiders (including the supply chain)

financial and political benefit

hobbyists

(script kiddies)

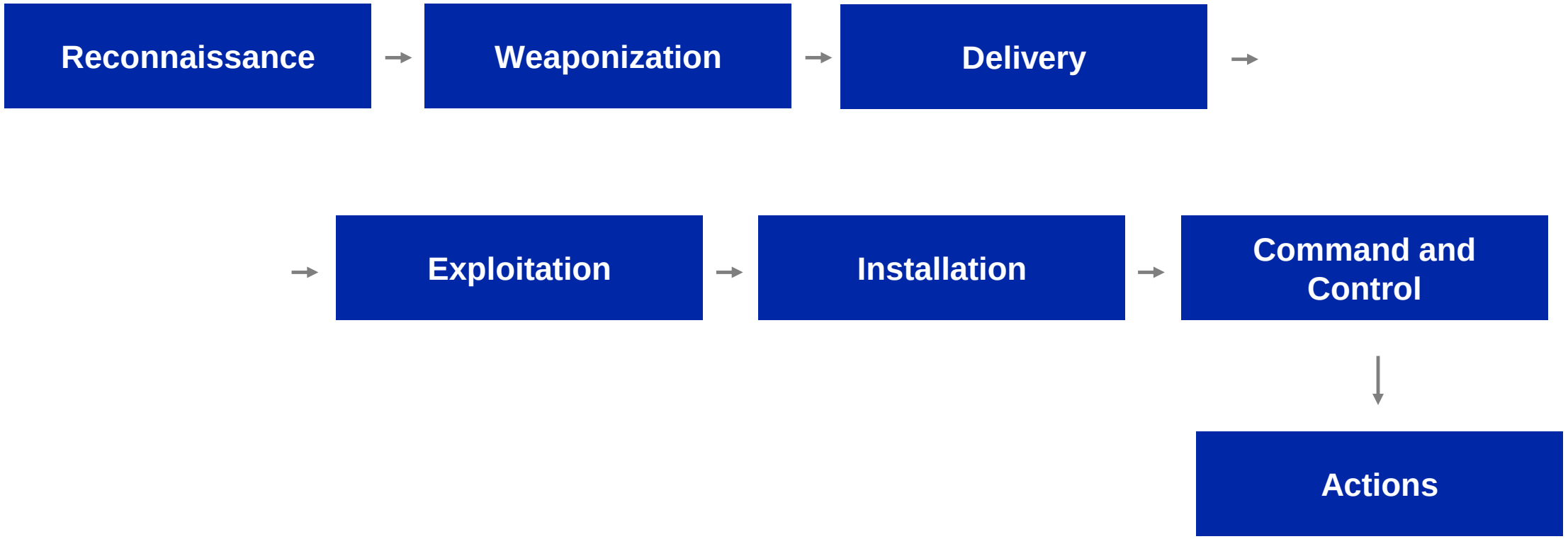
hacktivists

rogue hackers

money, fun, to further a cause

whitehats

Typical stages of an intrusion: the Cyber Kill Chain



Hutchins EM et al. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns […]. Leading Issues in Information Warfare & Security Research 1:8.

Why is cybersecurity **challenging**?

Who is attacking and what are their motives?

What are common **threats** to data and systems?

What approaches are available for **defenders**?

Defensive measures come in two flavors

proactive measures

Prevention: ensure that attack is not possible by minimizing exposure and exploitability

Deterrence: increase the effort for the adversary to become unattractive

Deflection: redirect effort of attacker towards another target, e.g., by deploying honeypots

reactive measures

Detection: either in real time or post mortem (via intrusion detection systems or logs)

Mitigation: reduce the impact of an attack, e.g., via network segmentation

Recovery: fast recovery from attack, e.g., via offsite backups and emergency playbooks to navigate a crisis

We have known fundamental security design principles

… since 1975!

Continuous Improvement because security is a process.

Least privilege, i.e., not more access rights than necessary.

Defense in depth instead of single points of failures.

Open design instead of security by obscurity.

A **chain of control** limited to trustworthy code and inputs.

Deny by default, i.e., access has to be granted explicitly as needed.

Transitive trust: If A trusts B and B trusts C, A effectively also trusts C.

Trust but verify the identity of other users and components.

Separation of duty: Split up critical tasks to reduce their complexity.

Least Astonishment: comprehensi-ble measures, intuitive consequences

Saltzer JH, Schroeder MD (1975). The protection of information in computer systems. Proc. IEEE 63(9):1278–1308.

Why is cybersecurity challenging?

Complexity
quantity and diversity

unawareness, incompetence, and neglicence

Asymmetry
attacking vs. defending

missing incentives because risks transferred to users **(externality)**

What was covered in this video?

Why is cybersecurity **challenging**?

What are common **threats** to data and systems?

Who is attacking and what are their motives?

What approaches are available for **defenders**?

Cybersecurity Fundamentals

Dominik Herrmann, University of Bamberg