JÖNKÖPING UNIVERSITY
School of Engineering

Introduction to information security

Module 1, Information Security, 7,5 ECTS

Erik Bergström
erik.bergstrom@ju.se

Overview of module 1

- Security?
- Security!
- Assets
- What is information security?
- Some basic terms

Why are you here?

What do I think/want?

- Information security is integral in society today
- CS/informatics must understand some security
- Get to know some basic concepts, principles, models, and standards
- Understand the human's role in information security
  - E.g. why we are an integral part of managing information security
  - Why we are the weak link
  - …
- Get a feel for the interdisciplinary nature of the field, and understand the relations to e.g. ethics, law…
- To get a basic sense of how information security can be applied in practice

- Make you think about security!

Scammers deepfake CEO's voice to talk underling into $243,000 transfer

05 SEP 2019 2

Machine Learning, Security threats

Previous: Firefox won't follow Chrome's anti-ad-blocke... Next: Raspberry Pi blasted into space, sends back video ...

by Lisa Vaas

Any business in its right mind should be painfully aware of how much money they could bleed via skillful Business Email Compromise (BEC) scams, where fraudsters convincingly forge emails,

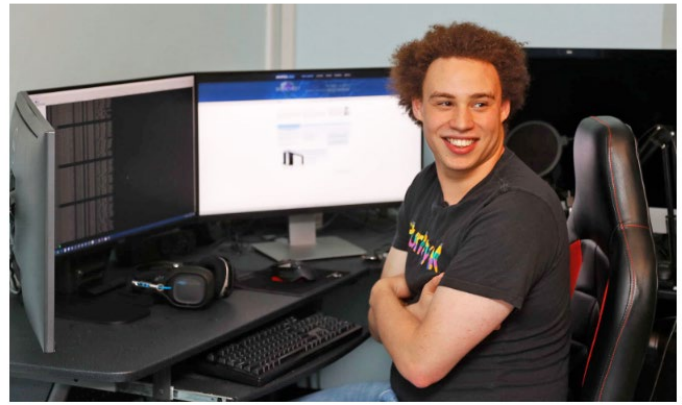
'MalwareTech' security researcher pleads guilty

Marcus Hutchins was a hero for stopping WannaCry, but created Kronos years earlier.

Richard Lawler, @Rjcc
04.19.19 in Security

36 Comments

593 Shares



ASSOCIATED PRESS

In 2017, Marcus Hutchins went from being a relatively unknown 23-year-old, to being a worldwide hero, to facing criminal charges all in a span of a few months. After he shut down the rapidly spreading WannaCry malware

Sedan id-kapningar blev olagligt har bara en person dömts för brottet. Foto: Fredrik Sandberg/ TT

Över 6.000 id-kapningar anmälda – bara en dömd

Publicerad 4 november 2016

Sedan id-kapning blev olagligt den 1 juli i år har över 6.000 fall anmälts. Bara en person har dömts för brottet.

The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC

21 January 2019

On 21 January 2019, the CNIL's restricted committee imposed a financial penalty of 50 Million euros against the company GOOGLE LLC, in accordance with the General Data Protection Regulation (GDPR), for lack of transparency, inadequate information and lack of valid consent regarding the ads personalization.

CYBER RISK SEPTEMBER 1, 2019 / 1:54 PM / 24 DAYS AGO

North Korea denies it amassed $2 billion through cyberattacks on banks

2 MIN READ

Hackers Steal $40 Million in Crypto from Binance

In May, hackers stole 7,074 bitcoins (worth US$40 million at the time (now $80M) from the world's number-one cryptocurrency exchange, Binance. From what is known by CipherTrace researchers, hackers used a multi-pronged takeover attack to obtain API keys, two-factor authentication codes, and other personal information from a large number of users, including "very high net worth accounts." API keys are unique identifiers that traders use to grant third-party programs special privileges to users' accounts, which often bypass two-factor authentication.

"The hackers used a variety of techniques, including phishing, viruses and other attacks," according to Binance CEO Zhao Changpeng who reported the theft on the same day it was discovered. "The transaction is structured in a way that passed our existing security checks." By the time Binance was able to suspend withdrawals, the hackers had already gotten away with the millions in cryptocurrency.

Zhao also announced that no customer funds would be used to cover losses, as Binance had set up a self-insurance fund, the SAFU fund, in 2018 that accrues 10% of all trading fees in a separate cold wallet.

AARIAN MARSHALL TRANSPORTATION 08.27.2019 03:30 PM

Ex-Uber Engineer Levandowski Charged With Trade-Secret Theft

Prosecutors say Anthony Levandowski took drawings and designs for self-driving technology from Google to Uber in 2016.

Nyheter

Misstänkt dataintrång mot statens lönesystem – personuppgifter i riskzonen

UPPDATERAD 2019-08-14 PUBLICERAD 2019-08-14

BUSINESS NEWS SEPTEMBER 10, 2019 / 6:07 PM / 15 DAYS AGO

Sweden's Haldex reports suspected corporate espionage to police

1 MIN READ

STOCKHOLM (Reuters) - Swedish brake systems firm Haldex (HLDX.ST) has filed a police report of suspected corporate espionage and data breaches after it discovered that a former employee had copied confidential information from its servers.

Haldex said the information, which was mainly financial, could have been passed on to at least one person in the financial industry.

"Given the large number of documents downloaded, we cannotexclude that the potential spreading of all files together may have led to the disclosure of insider information," Haldex Chairman Jorgen Durban said in a statement.

What do we have here?

What do we have here?

- Hardware
- Software
- Data/Information

Assets

- Hardware
  - Computer
  - Devices (drives, memory,…)
  - Network equipment
- Software
  - Operating system
  - Applications
  - Games
  - Individual applications

- Data/Information
  - Documents
  - Photos
  - Music
  - Videos
  - Emails
  - …

Asset values

- Off the shelf: easily replaceable
  - Hardware
    - Computer
    - Devices (drives, memory,…)
    - Network equipment
  - Software
    - Operating system
    - Applications
    - Games

- Unique: irreplaceable
  - Data/Information
    - Documents
    - Photos
    - Music
    - Videos
    - Emails
    - …
  - Software
    - Individual applications

Asset value

"The value of information goes beyond the written words, numbers and images: knowledge, concepts, ideas and brands are examples of intangible forms of information. In an interconnected world, information and related processes, systems, networks and personnel involved in their operation, handling and protection are assets that, like other important business assets, are valuable to an organization's business and consequently deserve or require protection against various hazards." (ISO/IEC 27002, 2013, p. vi)

What is security?

- Cyber security? Information security? Safety? Network security? Computer security? Administrative security?...
- Well, the terms do actually mean different things!

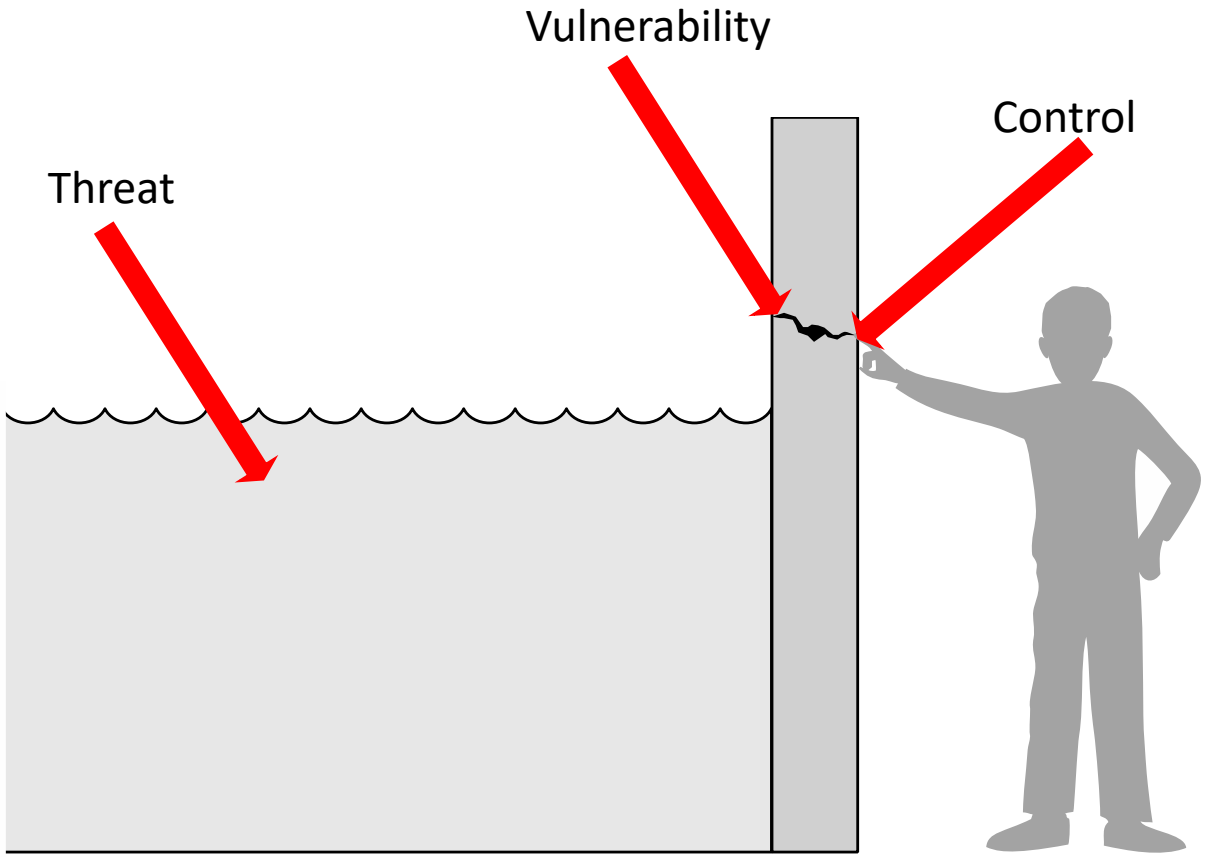
- Here, security = information security!
  - Because we want to protect information (assets)!

What is information security?

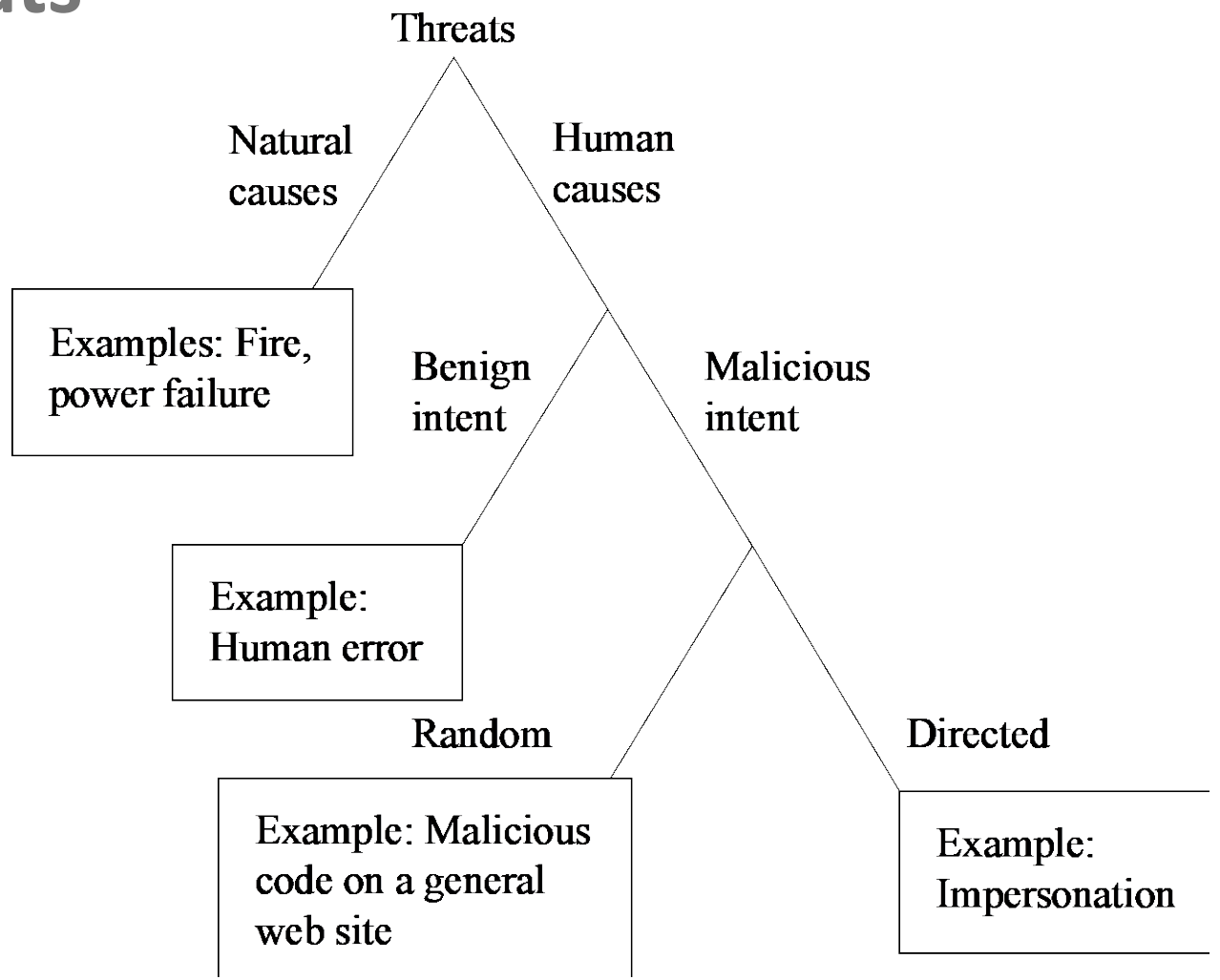
- Information security can be defined as *"means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide - (A) integrity […] (B) confidentiality […] and (C) availability"* (44 U.S. Code § 3542(b)(1), 2002).
- *"preservation of confidentiality, integrity and availability of information"* (ISO/IEC 27000, 2014).
  - (In addition: "*other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved".)*

Some basic terms

- Threat - A set of circumstances that has the potential to cause loss or harm.
- Vulnerability - A weakness in the system, e.g., in procedures, design, or implementation, that might be exploited to cause loss or harm.
- Countermeasure or security control - Prevent threats from exercising vulnerabilities.



Types of threats



Internal and external threats

- Willis Ware's report about threats to the protection of classified data from 1970.
  - Still instructive even though it was a completely different time and environment…
  - Human and natural causes
  - Protocol issues…
- Where are we today? Tomorrow?

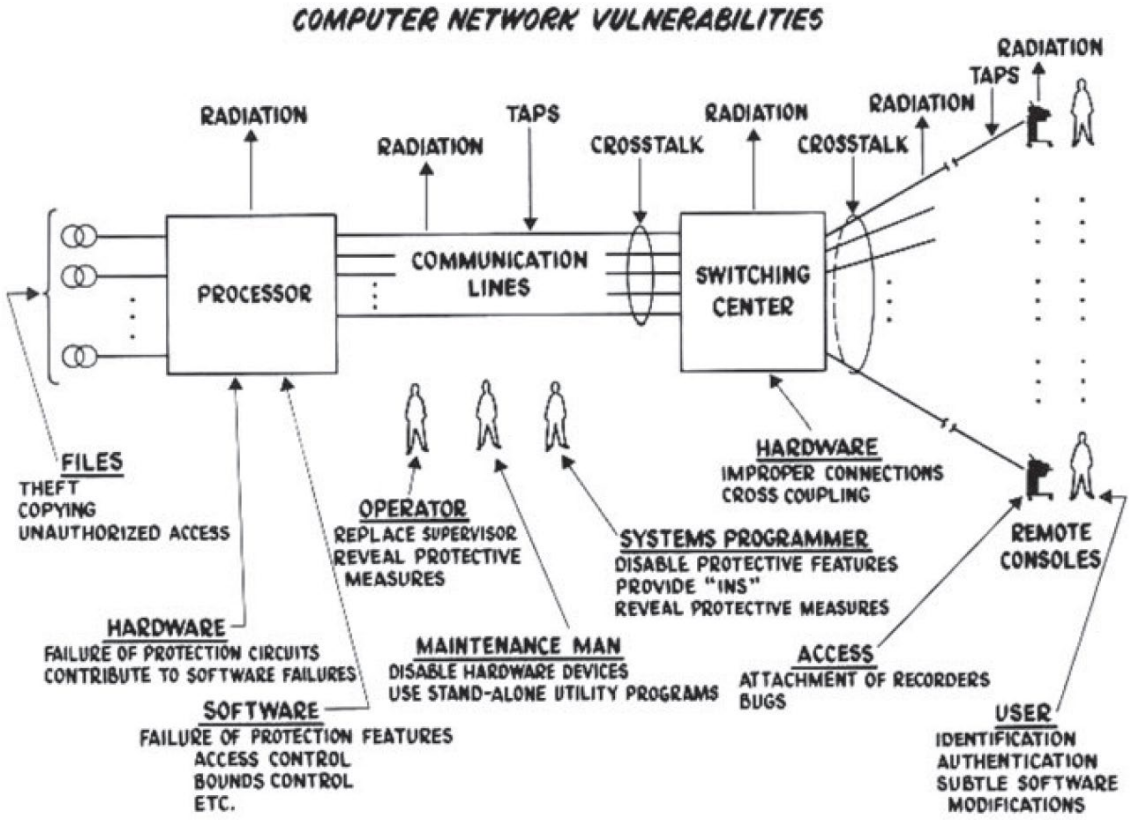
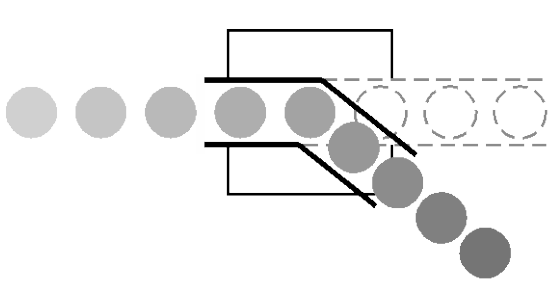


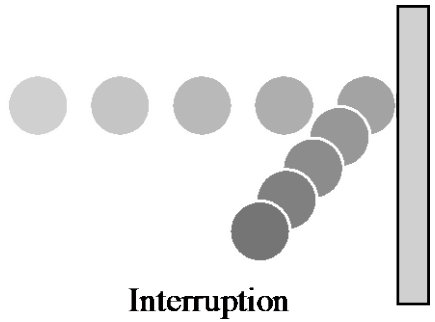
FIGURE 1-8 Computer [Network] Vulnerabilities (from [WAR70])

Some more basic terms

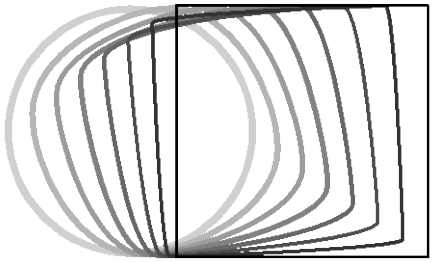
- Harm - The negative consequence of an actualized threat is harm
  - Can be characterized by four acts:
    - Interception - unauthorized access to an asset
    - Interruption - lost, unavailable, or unusable system/asset
    - Modification - unauthorized tampering with an asset
    - Fabrication - unauthorized creation of, e.g. a counterfeit object
- Attack – A vulnerability is exploited. An attack can be launched by a human or another system,… (so many different types…)



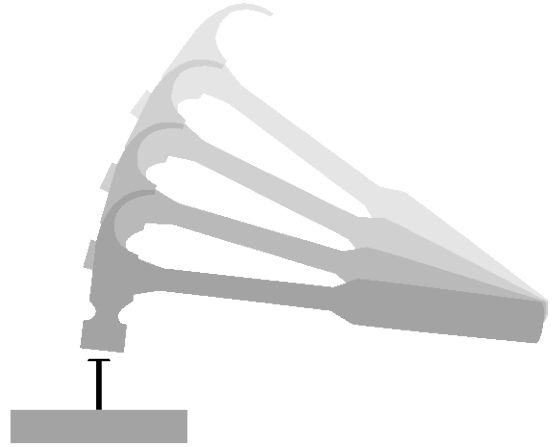
Interception



Interruption



Modification



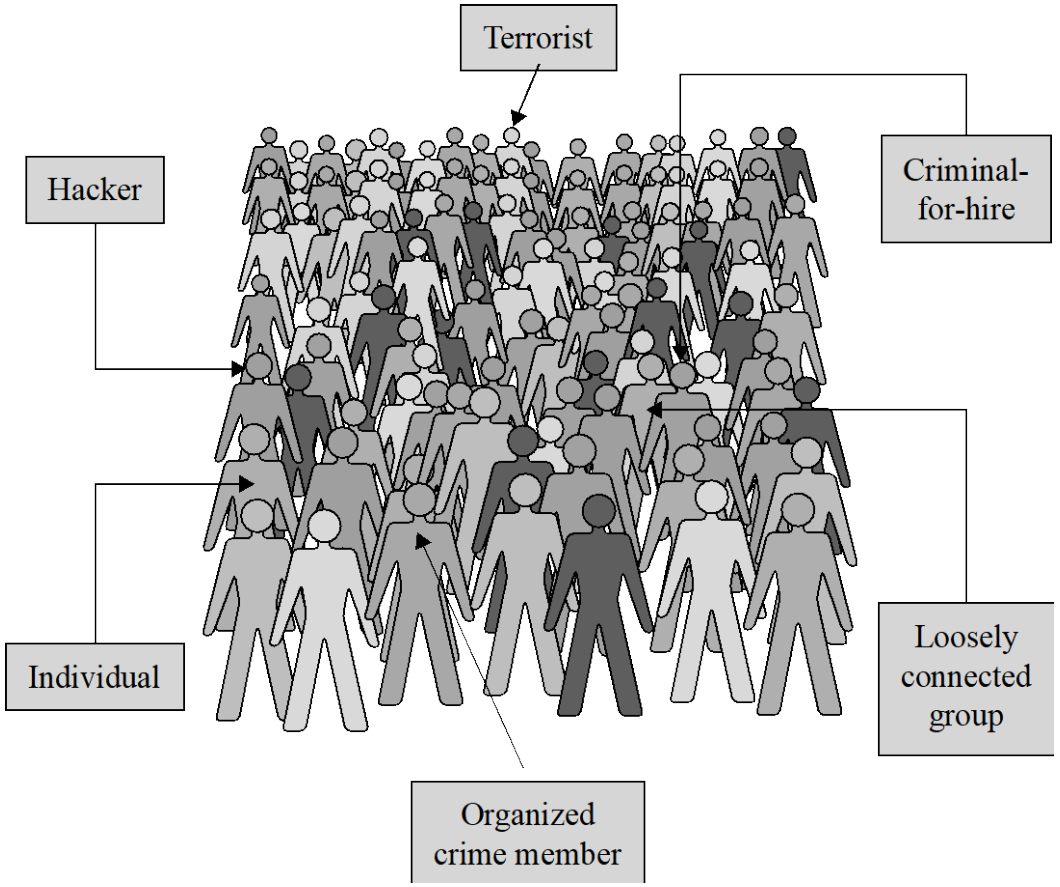
Fabrication

Method - Opportunity - Motive

- A malicious attacker must have three things (MOM):
  - Method: the skills, knowledge, tools, and other things with which to be able to pull off the attack
  - Opportunity: the time and access to accomplish the attack
  - Motive: a reason to want to perform the attack

- Deny any of the MOM, and the attack will fail!

Types of attackers

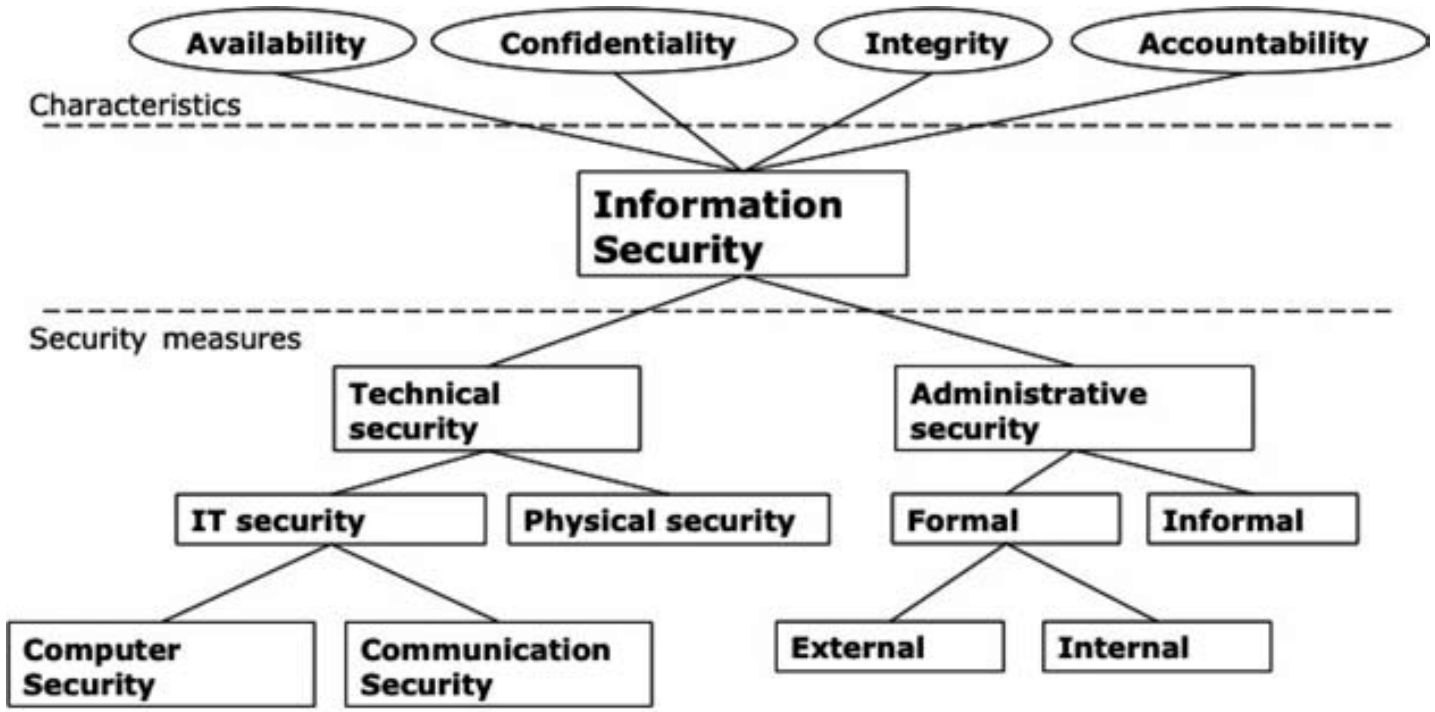


- Advanced Persistent Threat (APT) is increasingly problematic:
  - Organized
  - Directed
  - Well financed
  - Patient
  - Silent

Computer vs. attack

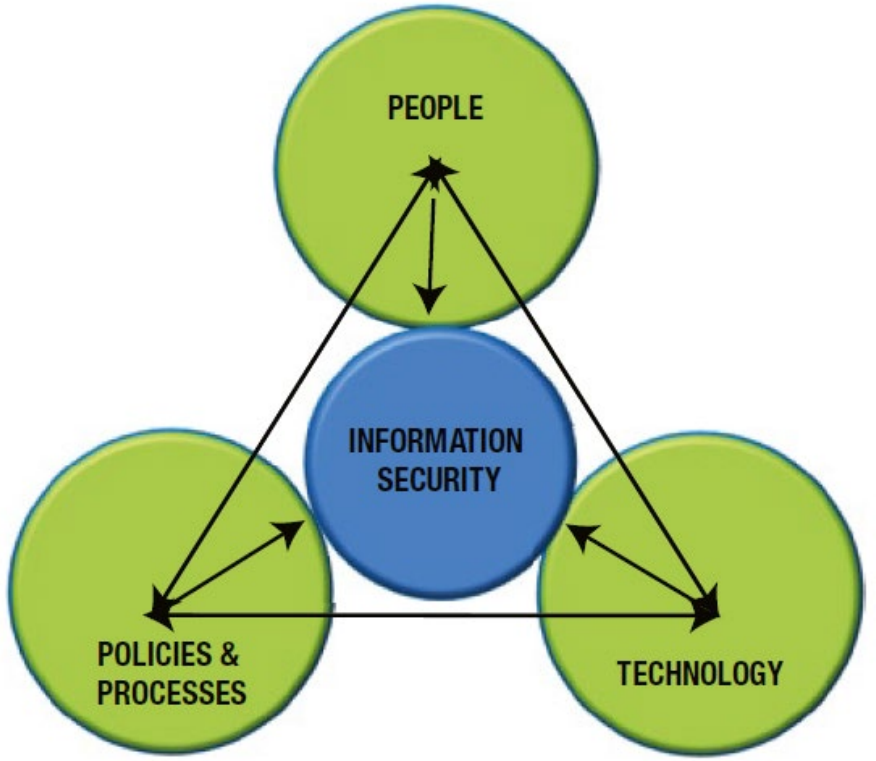
- Computer as the target of an attack
  - Denial-of-service attacks, website defacements, targeting e.g. political organizations.
- Computer as a method of attack
  - Launching offensive attacks requires the use of computers, e.g. Stuxnet.
- Computer as an enabler of attack
  - Websites, email lists, messaging apps… are effective, fast, and inexpensive ways to allow many people to coordinate, e.g. the 2008 Mumbai attacks.
- Computer as an enhancer of attack
  - The Internet has proved to be an invaluable means for terrorists to spread propaganda and recruit agents, e.g. JihadJane waged “violent jihad” online.

The information security model and pillars of security



Source: Åhlfeldt, 2008

Also SIS-TR 50:2015



Rao (2014)

Terms in the information security model

- C-I-A Triad
  - Confidentiality - The ability of a system to ensure that an asset is viewed only by authorized parties
  - Integrity - The ability of a system to ensure that an asset is modified only by authorized parties
  - Availability - the ability of a system to ensure that an asset can be used by any authorized parties
- Sometimes two other characteristics (security aspects) are considered:
  - Authentication - The ability of a system to confirm the identity of a sender
  - Non-repudiation - The ability of a system to confirm that a sender cannot convincingly deny having sent something
- Or even more, e.g., accountability, auditability, authenticity/trustworthiness, privacy (Cherdantseva & Hilton, 2013), and reliability (ISO/IEC 27000, 2014)

Confidentiality

- Only authorized people or systems should be able to access protected data
- It is the ”classical” security aspect
- Some examples that could mean a failure of confidentiality:
  - An unauthorized person accesses a data item
  - An unauthorized process or program accesses a data item
  - A person authorized to access certain data accesses other data not authorized
  - An unauthorized person accesses an approximate data value
  - An unauthorized person learns the existence of a piece of data

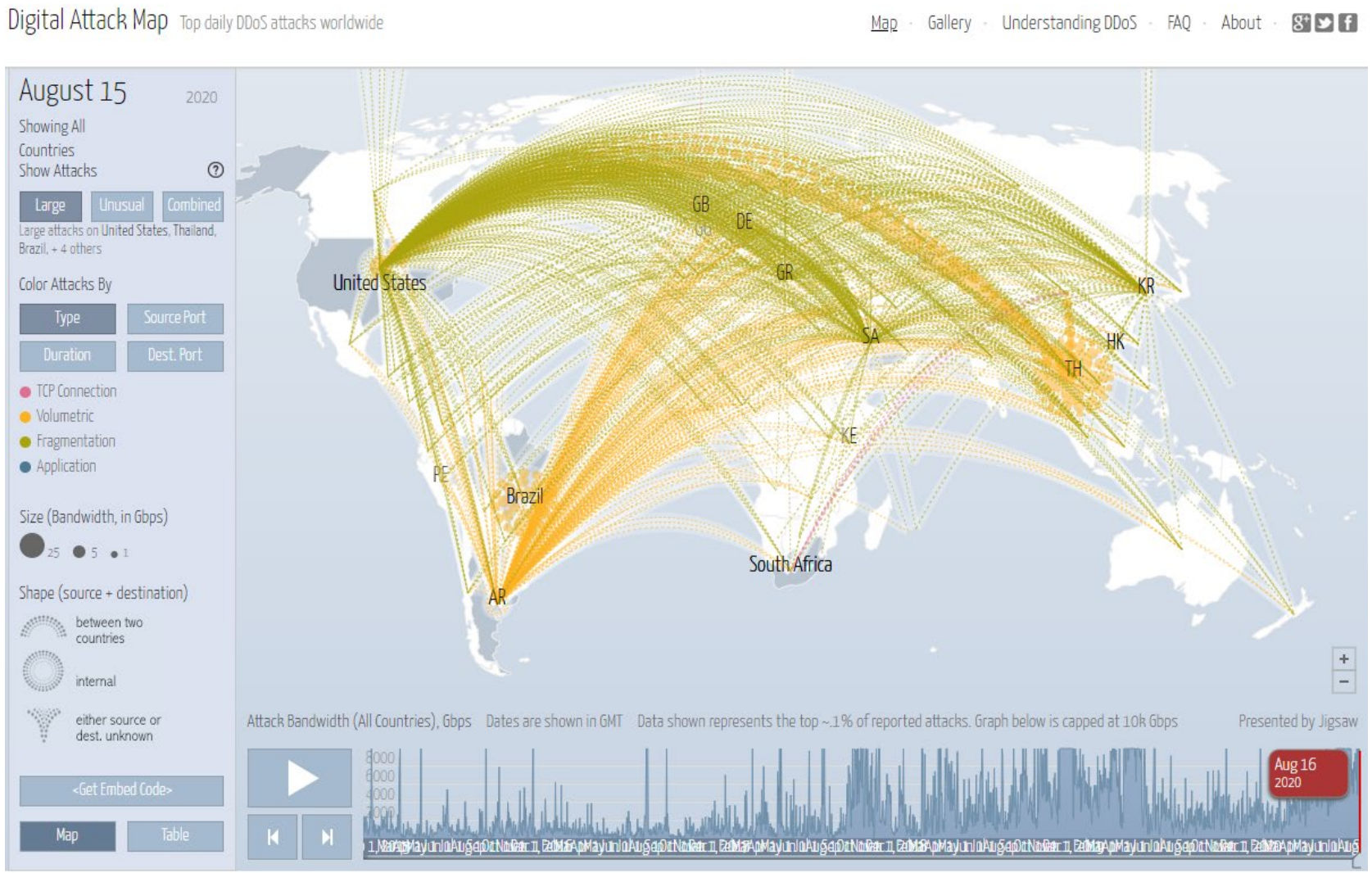
Integrity

- Integrity is harder to pin down than confidentiality because it means different things in different contexts
  - A correct email addressed to the wrong recipient
  - A processor producing incorrect results
- Integrity is not binary!
- If integrity is preserved, we may mean that the item is:
  - Precise, accurate, unmodified, modified only in acceptable ways, modified only by authorized people, modified only by authorized processes, consistent, internally consistent, meaningful and usable
- Integrity can be enforced similarly as confidentiality: by rigorous control of who or what can access which resources in what ways!

Availability

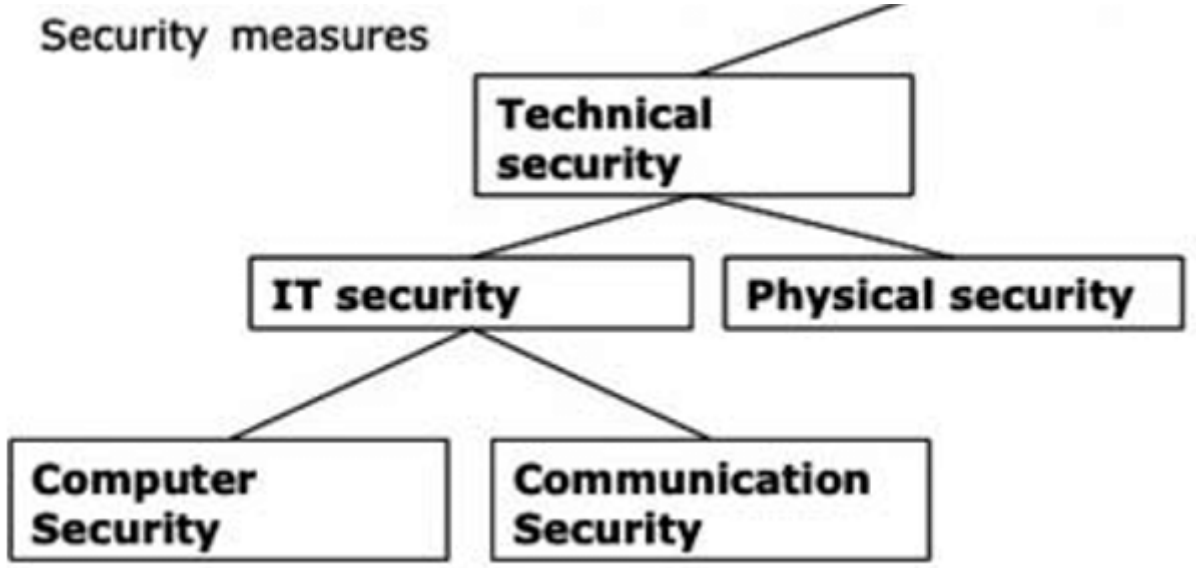
- Availability applies both to data/information and to services
- Availability could be real-time, but not necessary
- Closely related to fault tolerance
- Service or information is available if:
  - It is present in a usable form
  - It has enough capacity to meet the service's needs
  - It is making clear progress, and, if in wait mode, it has a bounded waiting time
  - The service is completed in an acceptable period of time
- Distributed Denial-of-Service is the most common availability threat

DigitalAttackMap.com



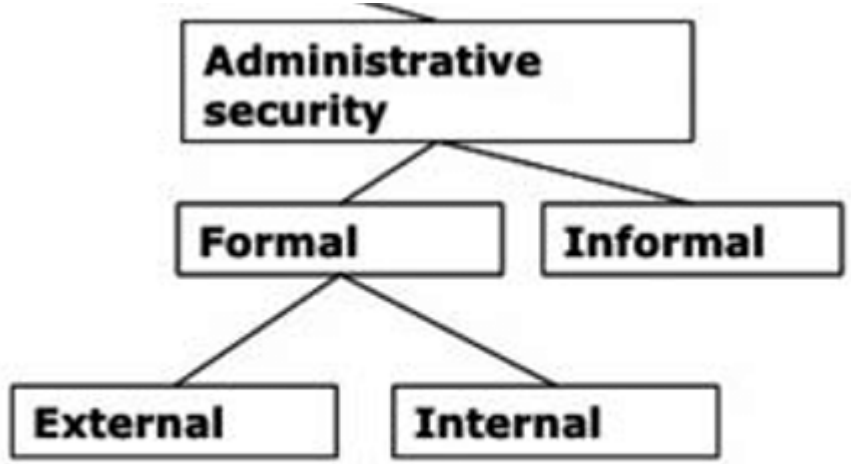
Terms in the information security model

- Technical security – security controls related to:
  - IT security
    - Computer security – data, information systems,… e.g. secure storage
    - Communication security (network security) – Security controls for secure transmission
  - Physical security – staff, fire alarm, door locks,…



Terms in the information security model

- Administrative security – security controls related to:
  - Formal
    - External - regulations concerning security issues, e.g., laws, regulations and agreements with other organizations
    - Internal - internal formalism for information security management, such as IT-strategies, security polices, educational programs,…
  - Informal
    - E.g. behavioral issues like values, attitude, beliefs, norms,…



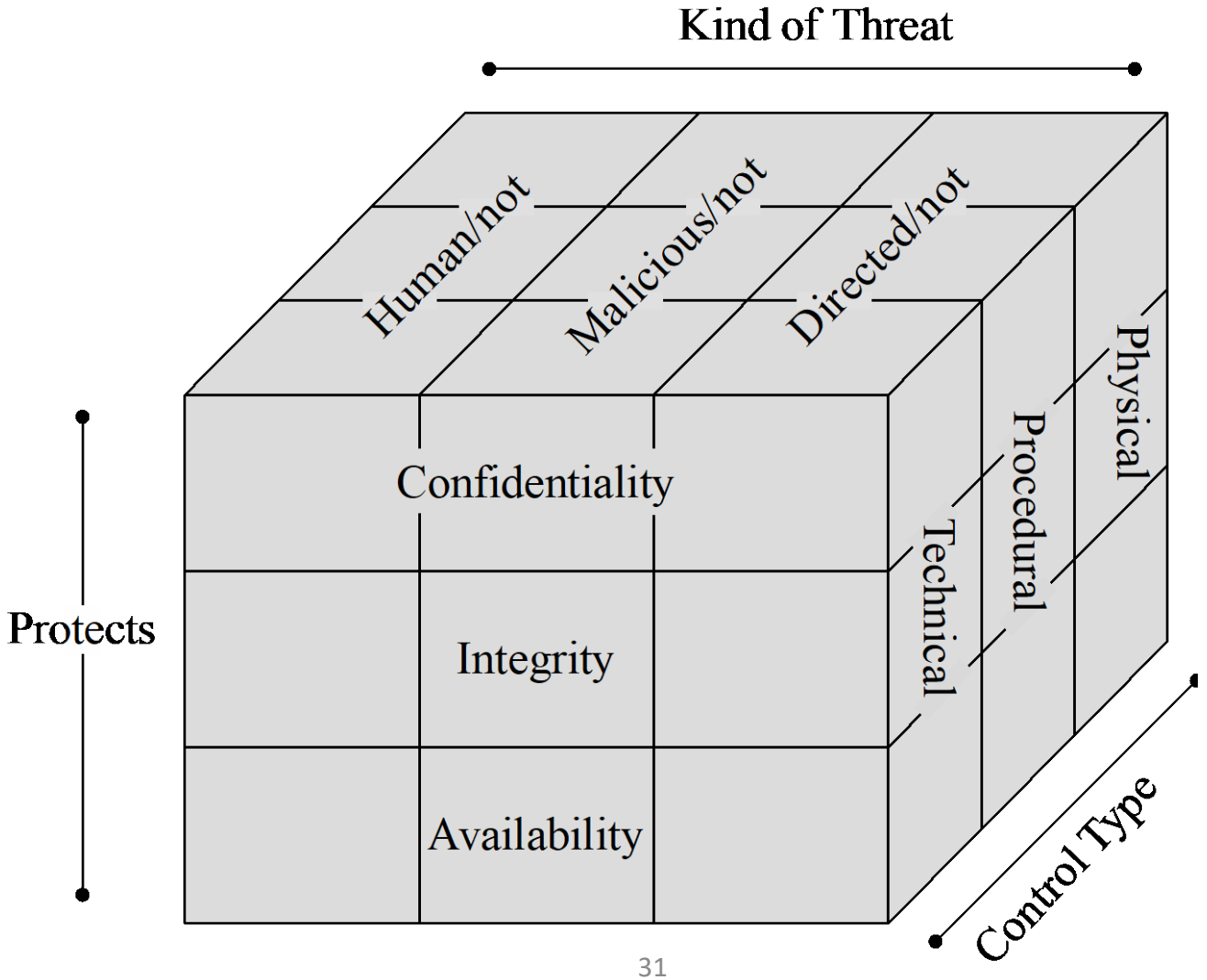
Risk

- The possibility for harm to occur is called risk
- Often risk = impact x likelihood
- We can deal with harm in several ways:
  - Prevent it, by blocking the attack or closing the vulnerability
  - Deter it, by making the attack harder but not impossible
  - Deflect it, by making another target more attractive (or this one less so)
  - Mitigate it, by making its impact less severe
  - Detect it, either as it happens or some time after the fact
  - Recover from its effects
- The risk that remains uncovered by controls is called residual risk

(Security) controls/countermeasures

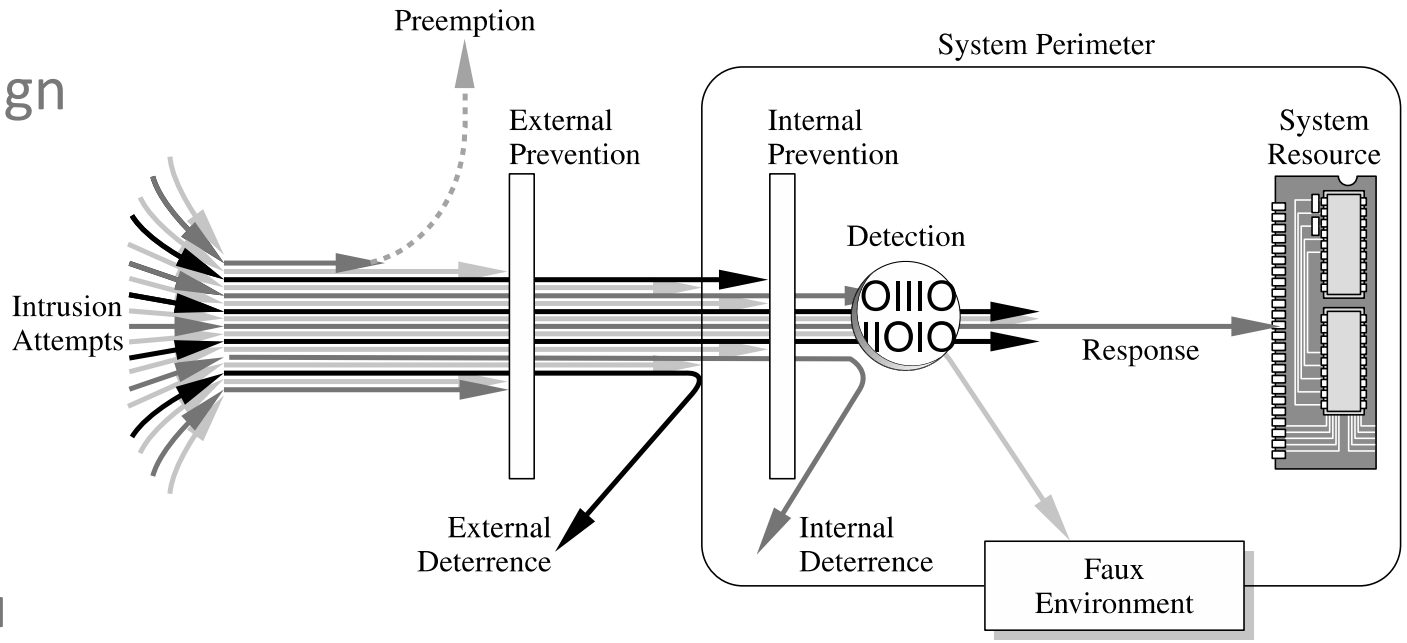
- A control or countermeasure is a means to counter threats.
  - Physical controls: Stop or block an attack by using something tangible, e.g.:
    - Walls, fences, locks, fire extinguishers…
  - Procedural or administrative controls use a command or agreement that requires or advises people how to act, e.g.:
    - Laws, regulation, policies, copyright, patents, contracts…
  - Technical controls counter threats with technology (hardware or software), e.g.:
    - Passwords, access controls, firewalls, encryption…

Controls/countermeasures



Prevention – Detection - Response

- Prevention
  - Prevent breaches by system design and incorporating security technologies and defenses.
- Detection
  - If a breach occurs, detect it.
- Response
  - Have a recovery plan so that you can make a fast response, restore data, handle media, law enforcement…



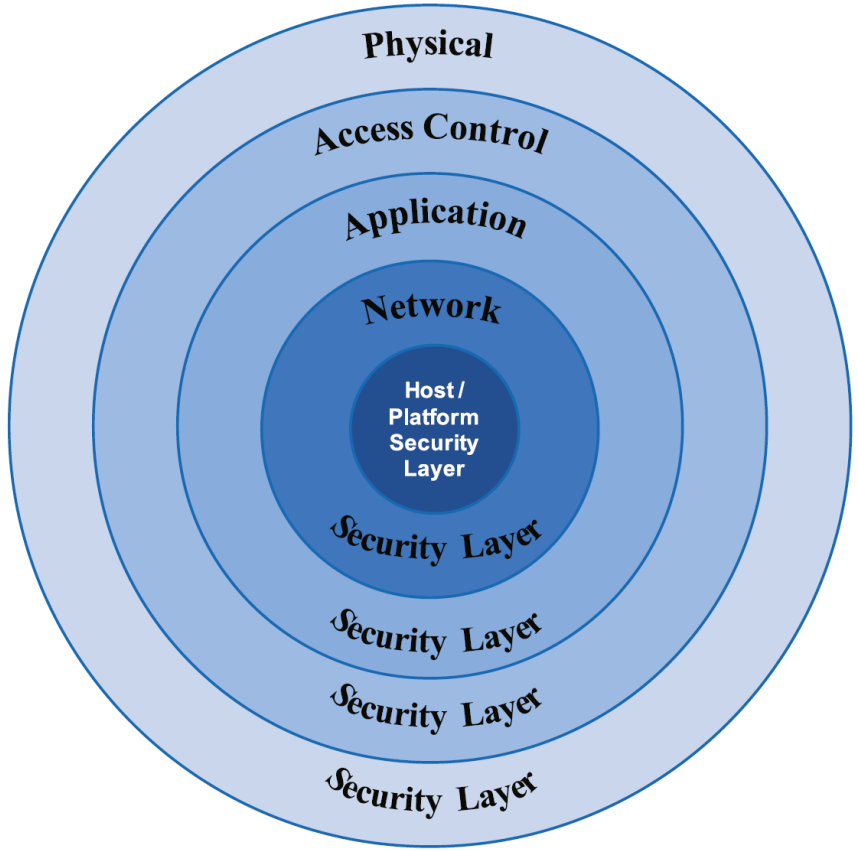
A typical breach…

1. An email with a link to an internal system is received by an employee
2. The employee clicks on the link and ”log in”
3. Username and password is collected and sent to the attacker
4. The attacker uses credentials to access internal information

- Prevention – E.g. to detect spam, filter suspicious links, train users, use tight access controls…
- Detection – E.g. to detect suspicious behaviour,
- Response – E.g. block user, check logs, start recovery plan…

Layers of protection

- The layers complement each other
  - Physical
    - Locks…
  - Access control
    - Authorization, authentication
  - Application
    - Security controls securing web servers, databases… e.g. encryption and identity management
  - Network
    - IDS/IPS, hardening, secure protocols…
  - Host/platform
    - Hardening, password management, anti-virus…



JÖNKÖPING UNIVERSITY

School of Engineering