Stockholm University

# Basics of Information Security

Introduction to Information Security (IntroSec)

Yuhong Li

# Outline

- Significance of information security
- Information security as a subject
- Terminologies
  - C.I.A. triad
  - Threats, harm and vulnerabilities
  - Controls/countermeasures

Stockholm University

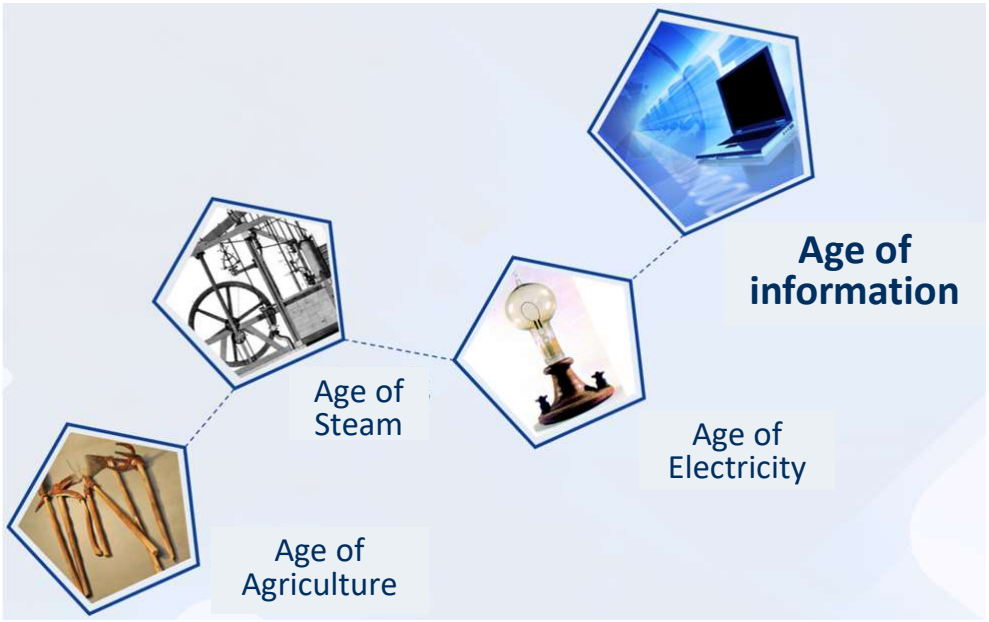
# Basics of Information Security

1.1 Significance of information security

1.2 Information security as a subject

1.3 Terminologies

# Development of Human Civilization




- Age of information
  - Information are industrial resources
  - Strategical resources, like water, electricity, oil.
  - Creating wealth for society
  - Information and information technologies are changing people's way of life, work, thinking.

# Significance of Information Security

Stockholm University

- Political, military, financial, industrial, business affairs are all managed by the information systems
- However,
  - Computer/information systems: vulnerable
  - Networks: open

⇨ Information security is a big problem and challenge

# Attack – Ukrainian Electricity System

- 2015-12-23, Ukrainian electricity system was attacked –power outage for 6 hours, 1.4 million people were affected.

**Preparing**

1. Malware generating: BlackEnergy imbedded in Office files
2. Transmission: email, phishing


**Looking for objectives**

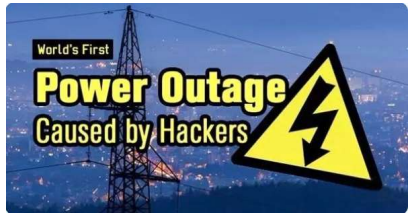
1. Judge if it is the objective (Build ID)
2. Release codes
   - KillDisk
   - SSH backdoor
3. Wait for opportunities

**Attacking**

1. Delete all the data in the disk -> cannot restart
2. Clear logs ->cannot be traced
3. Kill the sec_service.exe process -> no networking
4. Shutdown the computer, stop monitoring
5. Turn off the electricity

**Expanding the effect**

1. The system cannot restart automatically
2. DDoS the telephone system of the power station-> technical support is impossible



# Challenging – Ukrainian Electricity System

Stockholm University

- People: security awareness is weak
- The system is vulnerable:
  - BlackEnergy was known
  - The defensing system is not strong: bypass the firewall through phishing
  - The equipment can be controlled
- Organized attack:
  - Computers
  - Control electrical switch
  - DDoS: telephone system

# Other Notable Examples

Stockholm University

- Stuxnet attack: in 2010, the computer worm known as “Stuxnet” reportedly ruined almost one-fifth of Iran's nuclear centrifuges.
- Target Corporation and Home Depot breaches: "Rescator" broke into Target Corporation & Home Depot computers in 2013 & 2014, stealing roughly 40 million & between 53 to 56 million credit card numbers
- WannaCry ransomware attack in 2017: affected more than 150 countries, 300 thousands users, financial, energy, healthcare, 8 billion USD loss. Encrypting files…
- Facebook data exposure in 2018

# Trend of Attacks

Stockholm University

- Seek for the economical and political benefits. E.g.,
  - Contract fraud
  - Bank account, credit cards
    - 2016.2, attackers obtained the SWIFT password of Bangladesh Central Bank, transferred successful 0.101billion USD (tried 0.951 USD)
  - Illegal business activities
  - Infringement of intellectual property rights
- Organized attacks
- Attacks to mobile phones
- Hardware viruses
  - Algorithms can be implemented by using hardware
  - Even more  difficult to detect and clear
- Privacy exposure: big data + AI
- Information warfare, cyber warfare


TRAINING DOYENS
26468 E Walker Dr,Aurora, Colorado 80016-6104
Email: support@trainingdoyens.com | Toll Free:+1-888-300-8494 | Tel: +1-720-996-1616 | Fax: +1-888-909-1882

Stockholm University

**The Latest Australian News and Statistics in Cyber Crime and Cyber Security**

Stockholm University

# Basics of Information Security

1.1 Significance of information securitiy

1.2 Information security as a subject

- Connotation of information security
- Research fields and contents
- Theoretical foundations

1.3 Terminologies

# Information Theory's Viewpoint

Stockholm University

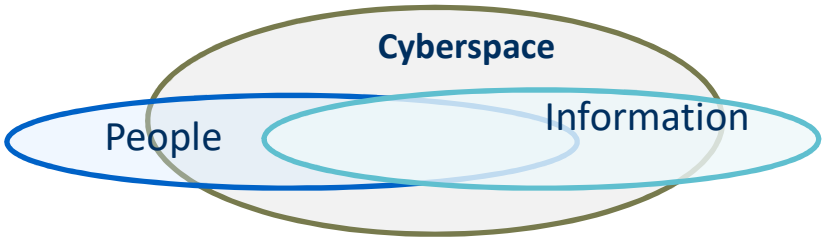
- Information: one of the three pillars of modern society: energy, material, information

- Information is the connotation, system is the carrier
  - Information cannot exist independently without the system;
  - Information has only three states: being stored, transmitted, processed

# Information Security in Cyberspace

Stockholm University

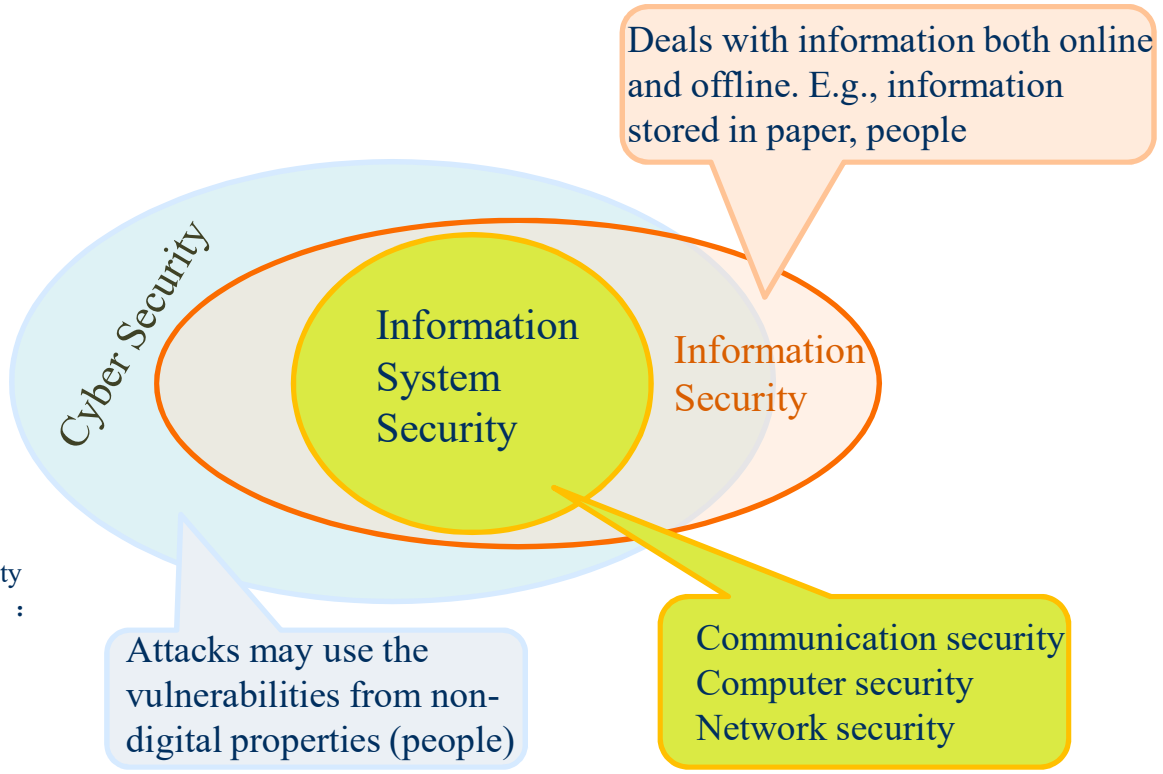
- Personal security is the basic requirement of human beings to their living environment
- Information security is the basic requirement of information to its living environment: to ensure that the information will not be disrupted or destructed by its environment
  - Where there is information, there is problems of information security.
- Cyberspace is human being's living environment, it is also the living environment of information.
  - Cyberspace security is the basic requirement of both human beings and information to their common environment.
  - Information security is the biggest problem for cyberspace security
    - System is the carrier, information is the connotation
    - Without information security, there is no cyberspace security.



# Information Security, Computer Security, Cyber Security …

- The terms comes from different understandings at different periods
- Different realms, focuses
- Different classifications from different organizations
- One opinion:

Von Solms R, Van Niekerk J. From Information Security to Cyber Security[J]. Computer & Security. 2013（38）: 97-102.



# Information System Security

Stockholm University

- Information security is the basic requirements to its living environment -> information system security
  - Protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
- Information system security
  - Device security
  - Data security
  - Content security
  - Behavior security

# Device Security

- Devices are the physical foundation of information system
- Device security is the primary problem of information system security

- Stability
  - The probability that devices won't fail in a certain time.
- Reliability
  - The probability that devices can execute tasks properly in a certain time.
- Availability
  - The probability that devices are ready for  work.

# Data Security

- To protect data from being disclosed, tampered, destroyed.

- Confidentiality
  - Only authorized people or system can access the protected data
- Integrity
  - Precise, accurate, authentic, unmodified or modified only by authorized people/processes
- Availability
  - Can be used easily and in the way it was intended to be.

# Behavior Security

- The processes and results of subjects' behaviours won't harm information security, or can guarantee the security of information.

- Confidentiality
  - The process and results of behaviours should not harm the confidentiality of data; in some cases, the processes and results of behavious should be confidential.
- Integrity
  - The process and results of behaviours should not harm the integrity of data; in some cases, the processes and results of behavious should be able to be predicted.
- Controllability
  - The deviation of the process can be detected, controlled or corrected.

# Content Security

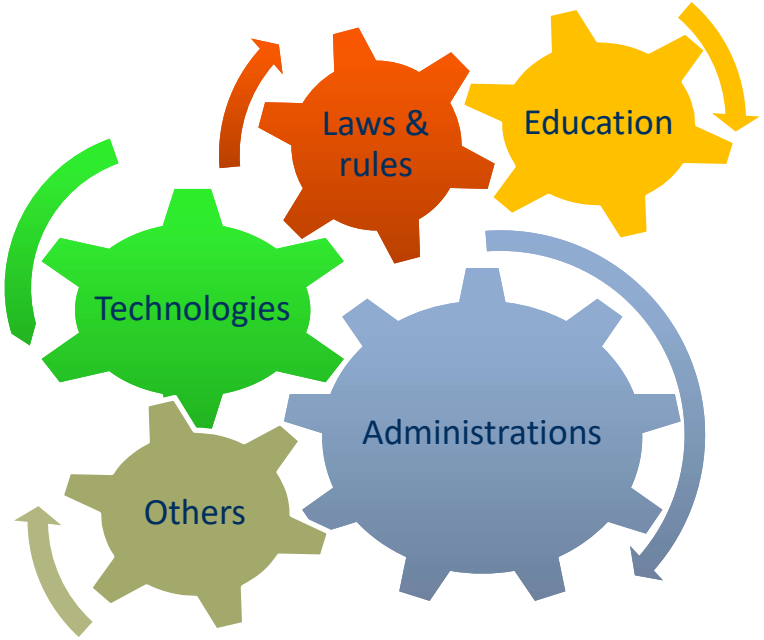
- Requirements in terms of politics, laws and moral.

- Meet the requirements of laws and regulations.

# Measures to Achieve Information Security

Stockholm University

- Laws, education, administration, technology, …




- Laws, education, administration should not be neglected;
- Complex engineering system: comprehensive measures are needed.

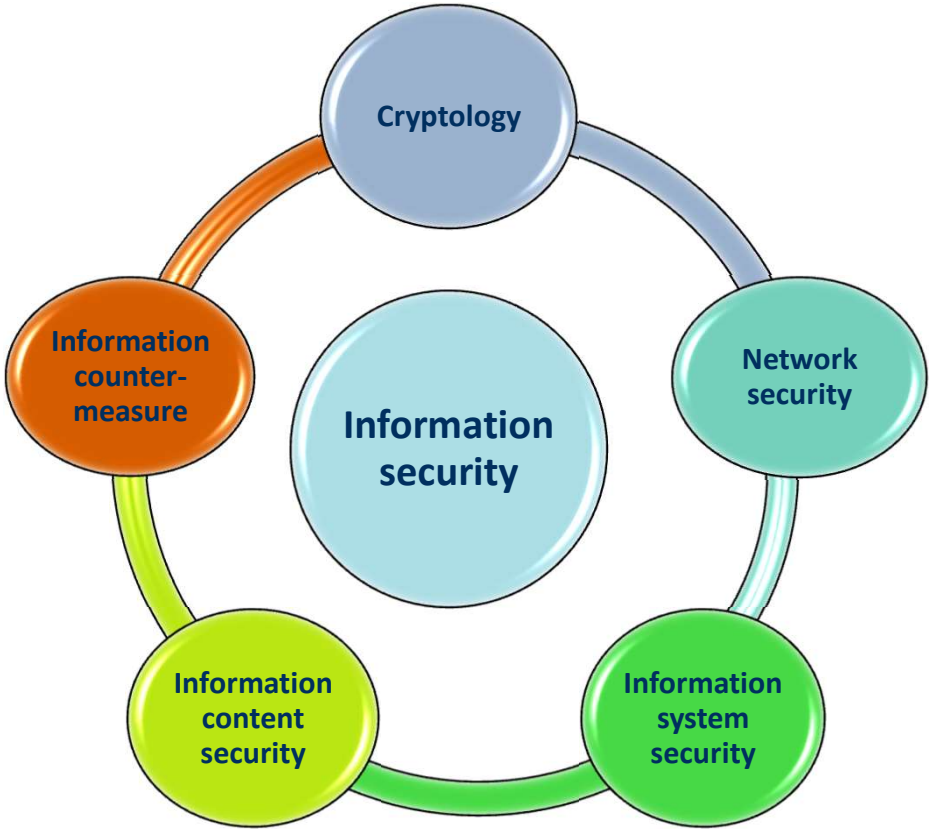
# Information Security as a Subject

Stockholm University

- Three states of information: storage, transmission, processing -> to ensure security
- Information security: study the security problems in information
  - Storage
  - Transmission (retrieval)
  - Processing
- A subject with its own connotation, theory, technologies and applications

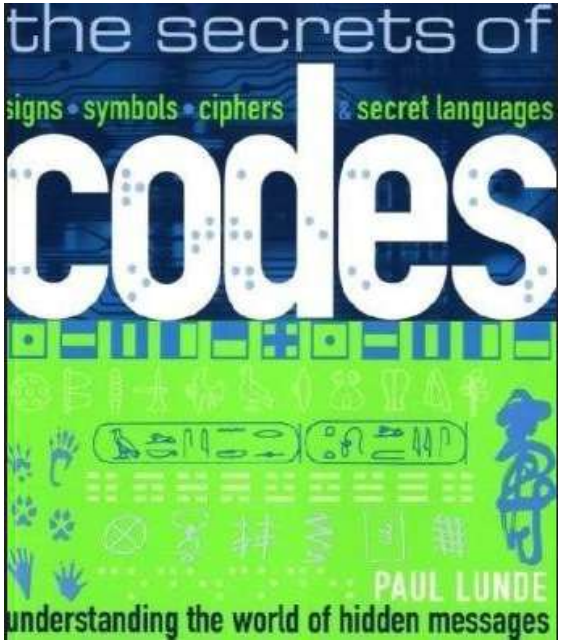
# Research Fields and Contents

- Information security as a subject has its own research fields.



# Cryptology

- Cryptography
  - Making secret codes. Secret writing that enables an entity to store and transmit data in a form that is available only to the intended entities
- Cryptoanalysis
  - Read a ciphertext without having the correct key, to crack cipher
- Major research areas:
  - Symmetric encryption
  - Asymmetric encryption (public key encryption)
  - Hash functions
  - Cryptographical protocols
  - New cryptographies: quantum cryptography, chaotic cryptography, biocryptography
  - Management of cryptography
  - Applications of cryptography



# Network Security

Stockholm University

- Protections at each layer of the OSI model and the scope of the networks
- Major research areas
  - Threats to network security
  - Communication security
  - Protocol security
  - Network defense
  - Intrusion detection and awareness
  - Emergency response and recover
  - Trusted networks
  - Management of network security

# System Security

- Threats and countermeasures from the whole system point of view.
- Research areas:
  - Security threats of systems
  - Device security
  - Hardware subsystem security
  - Software subsystem security
  - Access control
  - Trustworthy computing
  - Evaluation and verification of system security
  - System security level protection
  - Application system security

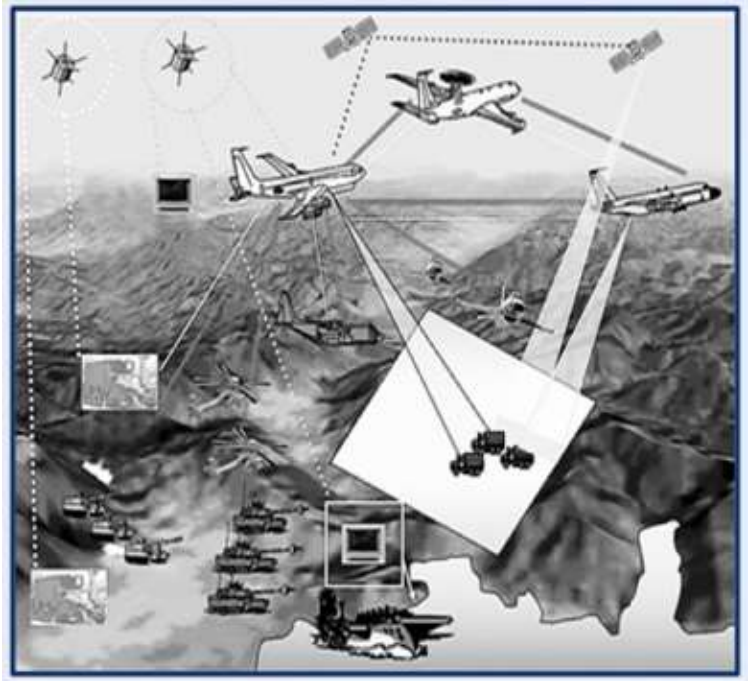
# Information Content Security

Stockholm University

- Research areas:
  - Threats to content security
  - Secure retrieval of information content
  - Analysis and identification of information contents
  - Management of contents
  - Information hiding
  - Privacy protection
  - Laws and policies to content security

# Information Countermeasure

- Obtain and “anti-obtain” information
  - Weaken, destroy adversarial devices and the use of information, and to protect own devices and the use of information
- Capture and control the information system
  - Communication countermeasure
  - Radar countermeasure
  - Photoelectricity countermeasure
  - Computer networks countermeasure



## Laws, Policies and Standardization Organizations

Stockholm University

- Laws and policies: state dependent
- International standardization organizations

IEC： International Electrotechnical Commission

ISO: International Organization for Standardization

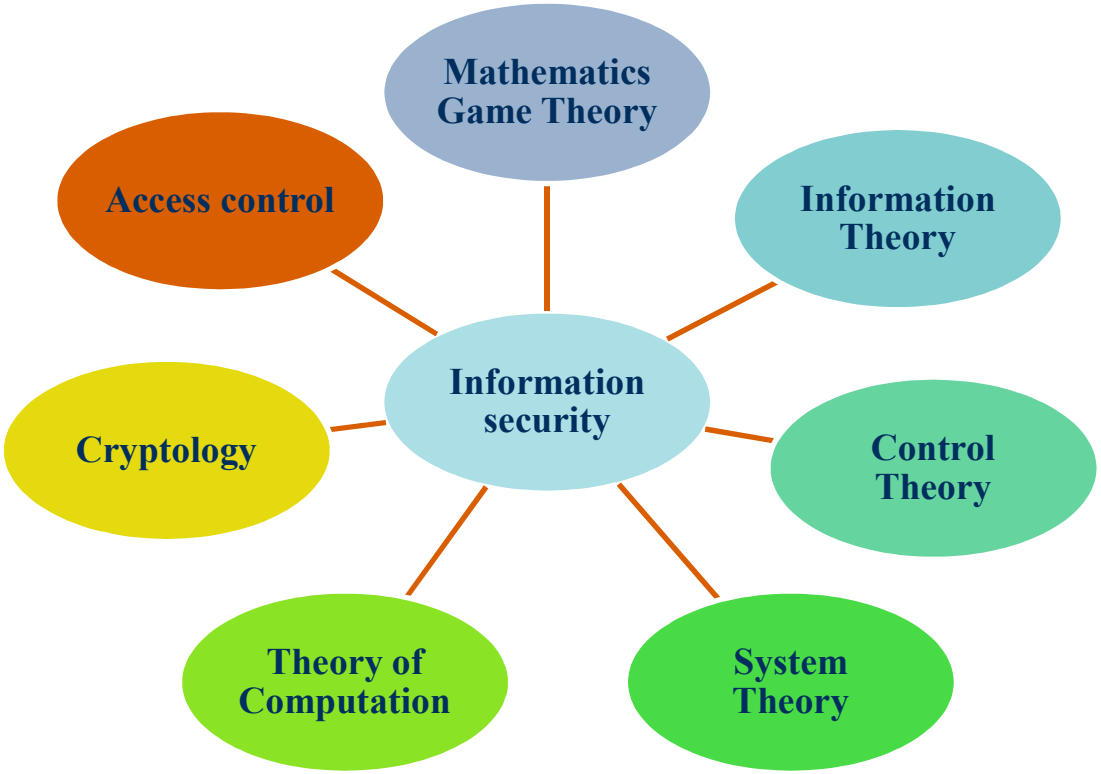
SC27: ISO/IEC JTC1 security for information technology

ITU IEEE ANSI NIST National Institute of Standards and Technology U.S. Department of Commerce

# Theoretical Foundations of Information Security

Stockholm University

- Information security as a subject has its own theoretical foundations



# Mathematics

- Mathematics is the foundation of all nature science

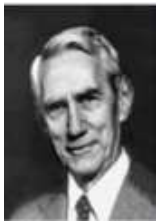
| | |
|---|---|
| Cryptology | • Number theory<br>• Algebra<br>• Combinatorial mathematics<br>• Probability statistics |
| Network security, protocols | • Logic |

- Game theory: the foundation of information security (cyber security)

# Information Theory, System Theory, Cybernetics

Stockholm University

- Foundations of information related subjects (e.g., computer science, electronics), including information security



### Information theory

- Information measurement and transmission
- Foundation for cryptology and information hiding

### System theory

- Model, structure and rules
- System as a whole
- Buckets effect

### Cybernetics

- How a system can stay stable and balanced in a dynamic changing environment
- PDR (Protection, Detection, Response) model

# Theory of Computation

Stockholm University

- Concerns three kinds of problems:
  - Computation model (formal languages and automata machine )
  - Which are computable, which not (Computability theory)
  - How long, how much storage are needed (computation complexity)
- Foundation of cryptology and information system security
  - Essentially, designing a cipher is to design a mathematical function; breaking a cipher is to solve a mathematical problem.
  - Generally, “whether an authorization system is secure” is a undecidable problem. But with some limitations, it can be a decidable problem

# Cryptology

- The foundation of information security
- As a theory based on information theory
  - One-way trapdoor function
  - PKI
  - Zero-knowledge proof
  - Secure multi-party computation
- As a technology
  - A common technique for information security

Stockholm University

# Access Control Theory

Stockholm University

- Specialized to information security (cyberspace security)
- Only the authorized entity can get some resources or take certain actions.
- Used in different branches of information security
  - E.g., cryptography -> only entities with ciphers can take certain actions (e.g., obtain information)
- As a theory
  - Access control model and the corresponding security
- As a technology
  - Common technology for information security

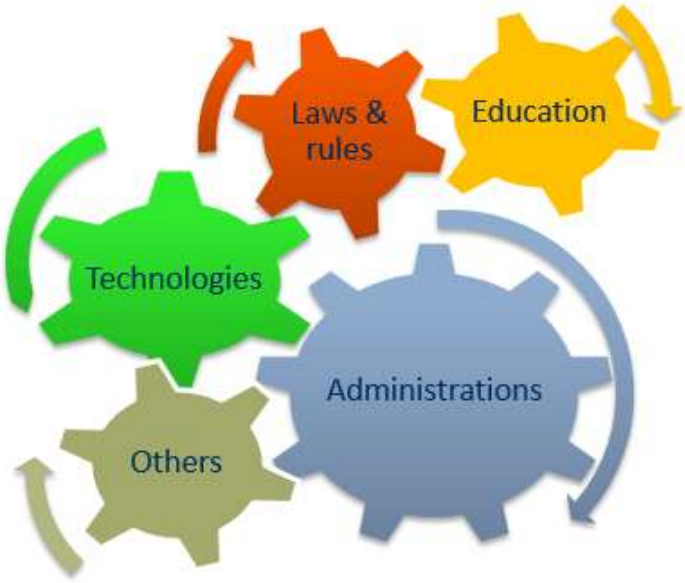
# About INTROSEC

Stockholm University

**Foundations**
- Cryptology
- Authentication
- Access control
- Privacy

**Laws and policies**
- Laws and ethics
- Policy and models

**Info. system security technologies**
- OS security
- Web security and network security
- Program security



Stockholm University

# Basics of Information Security

1.1 Significance of information security

1.2 Information security as a subject

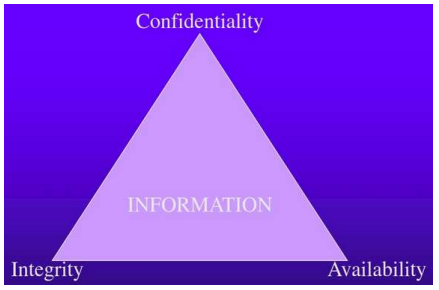
1.3 Terminologies

- CIA triad
- Threats, harms and vulnerabilities
- Controls and countermeasures

# Basic Security Properties -1

Stockholm University

- What makes the assets valuable
  - Availability: the ability of a system to ensure that an asset can be used by any authorized parties
  - Integrity: the ability of a system to ensure that an asset is not modified or modified only by authorized parties
  - Confidentiality: the ability of a system to ensure that an asset is viewed only by authorized parties
- C-I-A Triad (CIA)
  - The objectives of security threats!
  - The goals of computer security: seek to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)



# Confidentiality

Stockholm University

- Protected data
  - Secrete data: military secretes, business plans, diplomatic strategies
  - Sensitive data: financial transactions, tax returns, medical records
  - Data from which secrete and sensitive data can be obtained: daily activities of vehicles…
- Confidentiality: only authorized people or system can access protected data
  - “view”: usually means obtaining but not modifying
  - Difficult: who determines which or who can access which data in what ways ?
- Failure
  - An unauthorized person (process, program) access 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

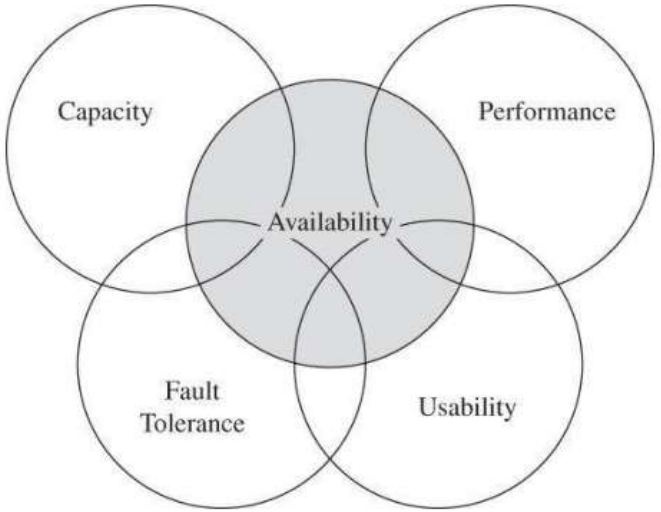
# Integrity

Stockholm University

- An asset is modified only by authorized parties
  - Precise, accurate
  - Unmodified, modified only in acceptable ways
  - Modified only by authorized people/processes
  - Consistent, internally consistent
  - Meaningful and usable
- Enforce by rigorous control of how or what can access which resources in what ways.

# Availability

- Assets (system, hardware, software, data and services..)
  - Timely response to our request
  - Can be used easily and in the way it was intended to be
  - Follows a philosophy of fault tolerance
  - Resources are allocated fairly (some requests are not favored over others)
  - Concurrency is controlled: simultaneous access, deadlock management, exclusive access are supported as required



# Basic Security Properties -2

Stockholm University

- More security properties
  - Authentication: the ability of a system to confirm the identity of a sender
  - Nonrepudiation or accountability: the ability of a system to confirm that a sender cannot convincingly deny having sent something
  - Auditability: the ability of a system to trace all actions related to a given asset

# Threats

Stockholm University

- Threats: a potential cause of harm ( a set of circumstances that could cause harm)
  - Something bad can happen to assets
  - Somebody/something can cause or allow those bad things to happen

# Examples of Information Security Threats

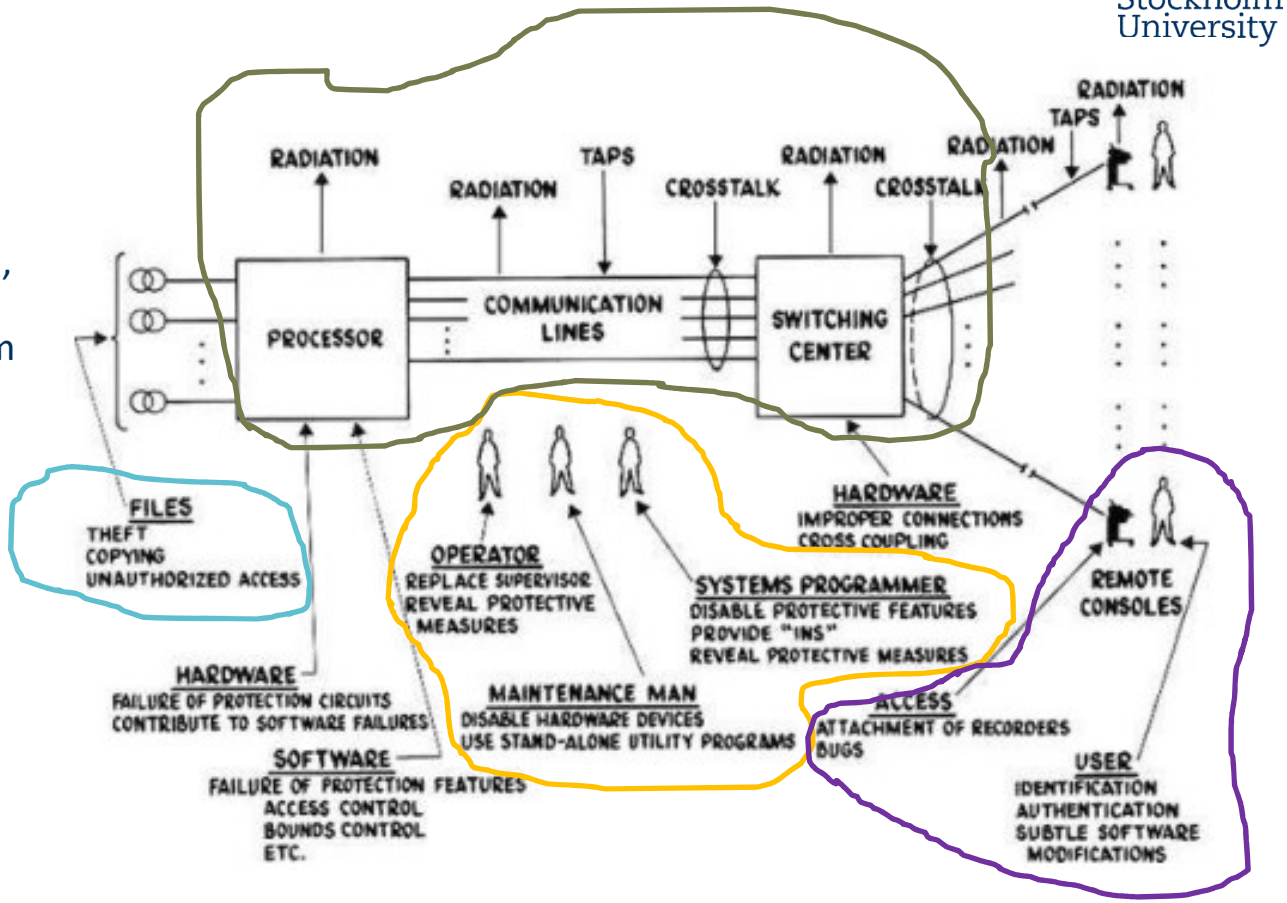
Stockholm University

- Act of human error or failure (accidents, mistakes)
- Compromises to intellectual property (piracy, copyright infringement)
- Acts of espionage or trespass (unauthorized access and/or data collection)
- Acts of information extortion (blackmail of information disclosure)
- Acts of sabotage or vandalism (destruction of systems or information)
- Software attacks (viruses, worms, macros, denial of services)

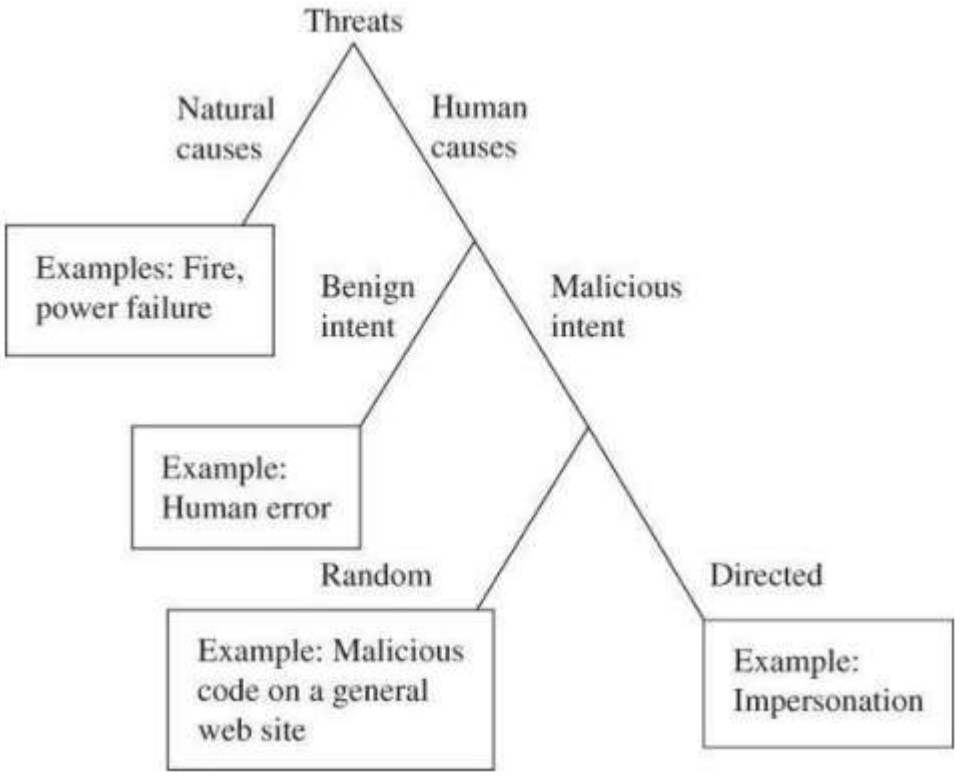
- Forces of natures (fire, flood, earthquake, lightning)
- Quality of service deviations from service providers (power and WAN service issues)
- Technical hardware failures or errors (equipment failure)
- Technical software failures or errors (bugs, code problems, unknown loopholes)
- Technological obsolescence (antiquated or outdated technologies)

# Kinds of Threats - Source

- Threats can be from
  - Attacks on the vulnerabilities
  - Natural disasters, e.g., flood, earthquake
- Vulnerabilities may be from
  - Source
  - Destination
  - Intermediate system
  - Operation and maintenance
- Vulnerabilities caused by
  - Software
  - Hardware
  - Transmission lines
  - People

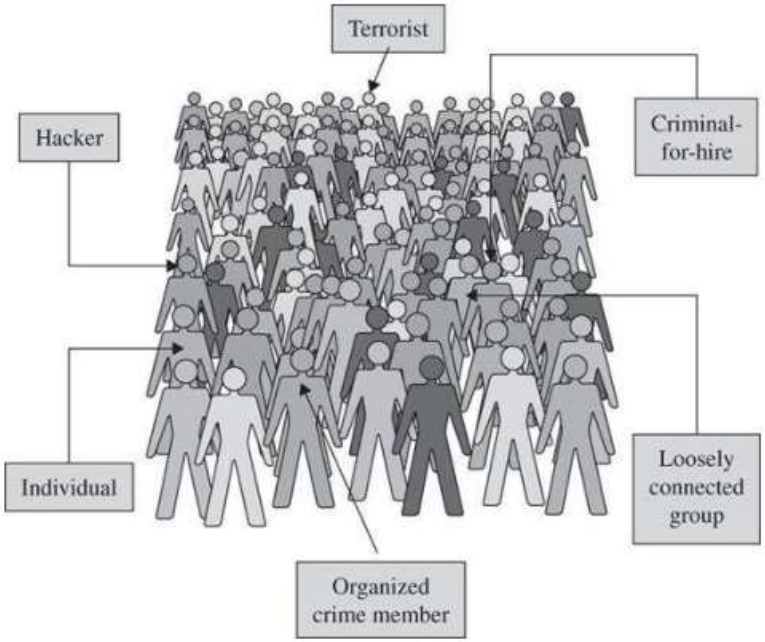


# Kinds of Threats - Classification




- Threats are caused by both human and other sources
- Threats can be malicious or not
- Threats can be targeted or random

# Types of Attackers




- Have university degrees, be pillars of their communities; High school or university students
- As a symbol, personal profit, revenge, challenge, advancement, job
- Terrorist, hacker, organized crime member,

# Security Threats

Stockholm University

- STRIDE:
  - Spoofing
  - Tampering
  - Repudiation
  - Information disclosure
  - Denial of Service (DoS)
  - Elevation of privilege

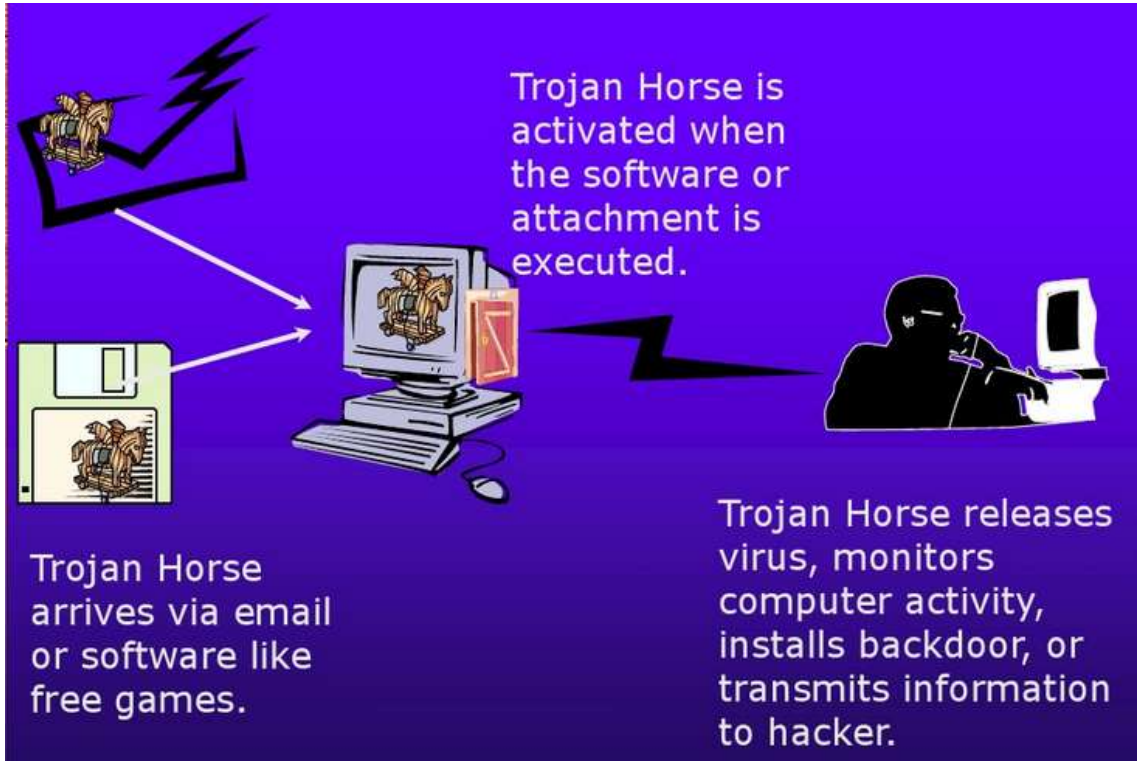


# Spamming Attacks

Stockholm University

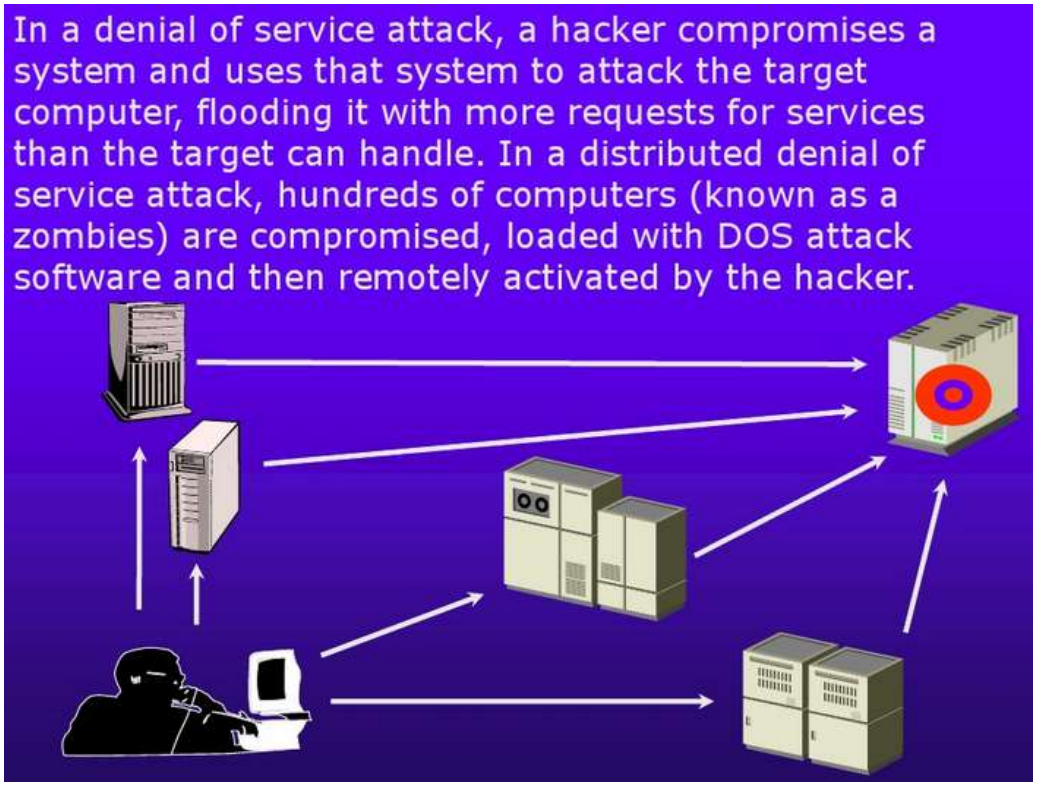
- Sending out e-mail messages in bulk. -> “electronic junk mail”
- Spamming can leave the information system vulnerable to overload
- Less destructive, used extensively for e-marketing purposes

# Trojan Horse Attack



# Denial of Service (DoS) Attack

Stockholm University

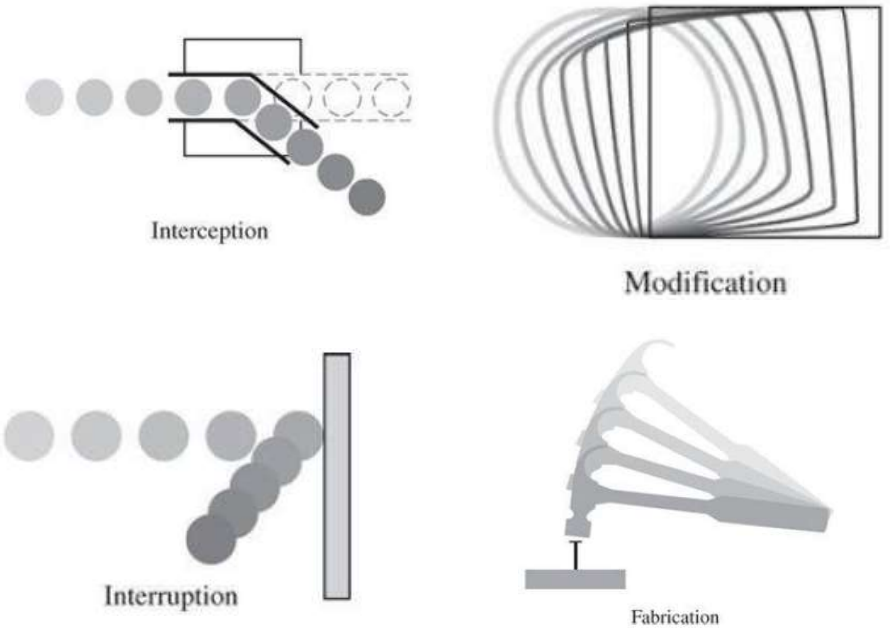


## Harm

- Loss of value of assets
- Consequence of actualized threat
- Depends on assets' owner or outsider perception and need
  - Can change with time, e.g., a computer can become older, or a business plan can become no value

# Acts Causing Harm

- Interception: on the way
- Interruption: interfere or terminate
- Modification: change
- Fabrication: make up something artificial or untrue



# Risk Management

Stockholm University

- Choosing which threats to control and what resources to devote to protection
  - Prioritize: only so much time, energy, money available
  - Address some risks and let others slide; consider alternative courses or actions
  - Residual risk: those remained uncovered by controls
- Basic model:
  - calculating value of all assets ->
  - determining the amount of harm from all possible threats ->
  - computing the costs of protection ->
  - selecting countermeasures ->
  - applying the countermeasures

⟹Difficult to measure!

# Method, Opportunity, Motive

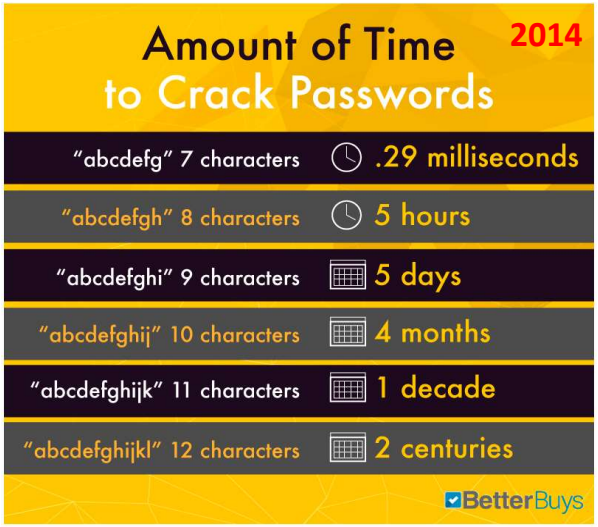
Stockholm University

- Assessing risks
  - Impact of the harm (the amount of damage)
  - Likelihood of the thread
- Malicious attacker to be successful: how, when and why
- Method-Opportunity-Motive
  - Method: skills, knowledge, tools,…
  - Opportunity: the time and access to execute an attack
  - Motive: money, fame, self-esteem, politics, terror

# Vulnerabilities

Stockholm University

- Weakness in the system that can allow harm to occur.
  - Procedures, design, implementation
    - Design and implementation flaws in system, protocols, applications, configurations; poor system operation and maintenance …
    - Users' lack of awareness
    - Openness (e.g., interconnected system): exposes weakness of devices to criminals
- Weak authentication, lack of/weak access control, errors in programs, finite or insufficient resources, inadequate physical protection…



## Attack Surface

Stockholm University

- The system's full set of vulnerabilities, actual and potential
  - Physical hazards
  - Malicious attacks by outsiders
  - Stealth data theft by insiders
  - Mistakes
  - Impersonations

## Controls (Countermeasures)

Stockholm University

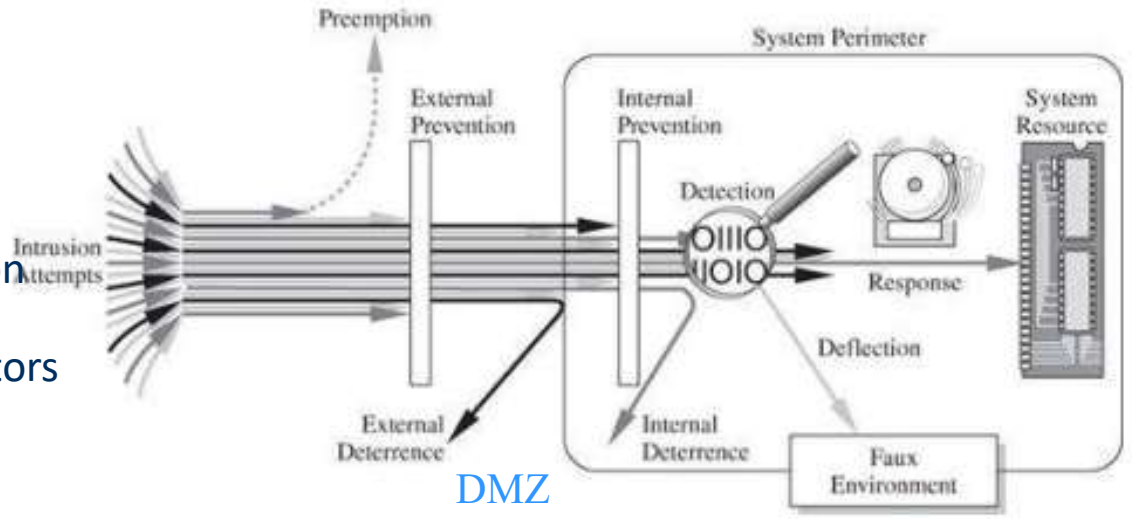
- Means to counter threats
  - Prevent: blocking the attack or closing the vulnerability
  - Deter: making the attack harder, but not impossible
  - Deflect: making another target more attractive
  - Mitigate: making its impact less severe
  - Detect: when it happens or some time after it happens
  - Recover: from the effect
- Can be used simultaneously

## Combination of Controls -1

- Physical controls
  - Locks, guards, sprinklers and other fire extinguishers
- Procedural or administrative controls
  - Laws, regulations, policies, guidelines
  - Copyrights, patents
  - Contract, agreements

# Combination of Controls -2

- Technical controls
  - Passwords, program or OS access controls,
  - Network controls (Access control, Authentication)
  - Encryption
  - Firewalls, intrusion detection systems
  - Network traffic flow regulators




DMZ

Honeypots & Honeynets

## Vulnerability-Threat-Control Paradigm-1

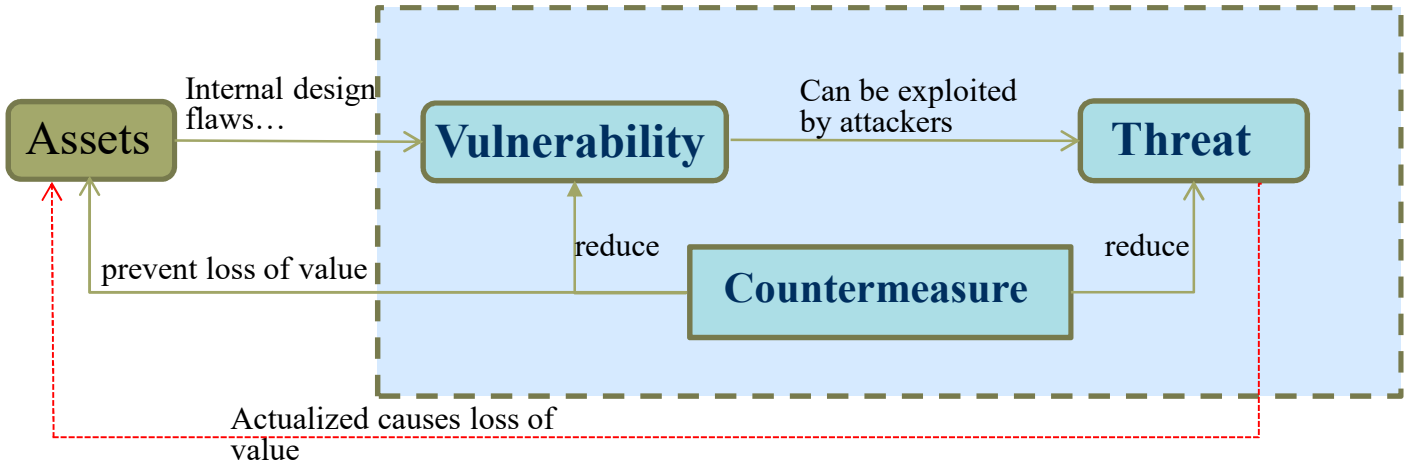
Stockholm University

- A framework to describe how assets may be harmed and how to counter or mitigate the harm
  - **Vulnerability:** a weakness in the system.
    - Design, implementation, using
    - Vulnerable to be exploited by attackers, e.g., the password is too week (short or simple)
  - **Threat:** a potential cause of harm – a set of circumstances that could cause harm
    - A man with a gun; the simple or short password
  - **Control**: measures (countermeasures) that prevent threats from exercising vulnerabilities.

# Vulnerability-Threat-Control Paradigm-2

Stockholm University

- Harm: assets lose value, e.g., stolen computer, modified/lost files, revealed private letter, denied to access/cannot use data…
- Attack: exploits a vulnerability
  - A human (e.g., steal password and log into a system)
  - A system (e.g., denial of services (DoS) )

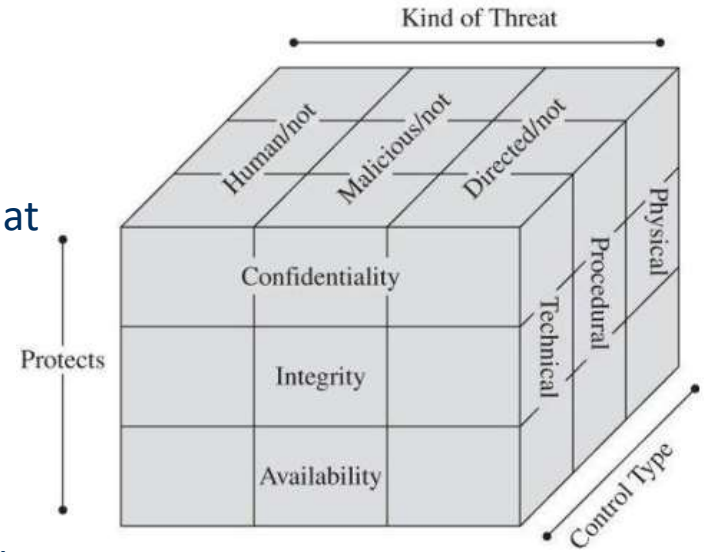



**Attackers leverage threats that exploit vulnerabilities against valuable assets to cause harm!**

# Summary

- Computing systems subject to attack: hardware, software, data, communications among them
- Computer security: attempts to ensure- confidentiality, integrity, availability (CIA)
- Vulnerability: a weakness through which harm could occur.
- Threat: an incident that could cause harm (condition that exercises vulnerability)
- Countermeasures/controls can be applied to computer systems.

- Hard to achieve perfect security: no viable threats, no exercisable vulnerabilities
- Attacks are inevitable: method-opportunity-motive, not in short supply



# Expected Learning Outcomes of Lecture 1

Stockholm University

You should be able to

- Have a general idea about information security
- Describe and apply the basic concepts and terms of information security, such as
  - CIA, AAA, STRIDE, …
  - Threats, harms, vulnerabilities, vulnerability-threat-countermeasure paradigm,…

Stockholm University

# END