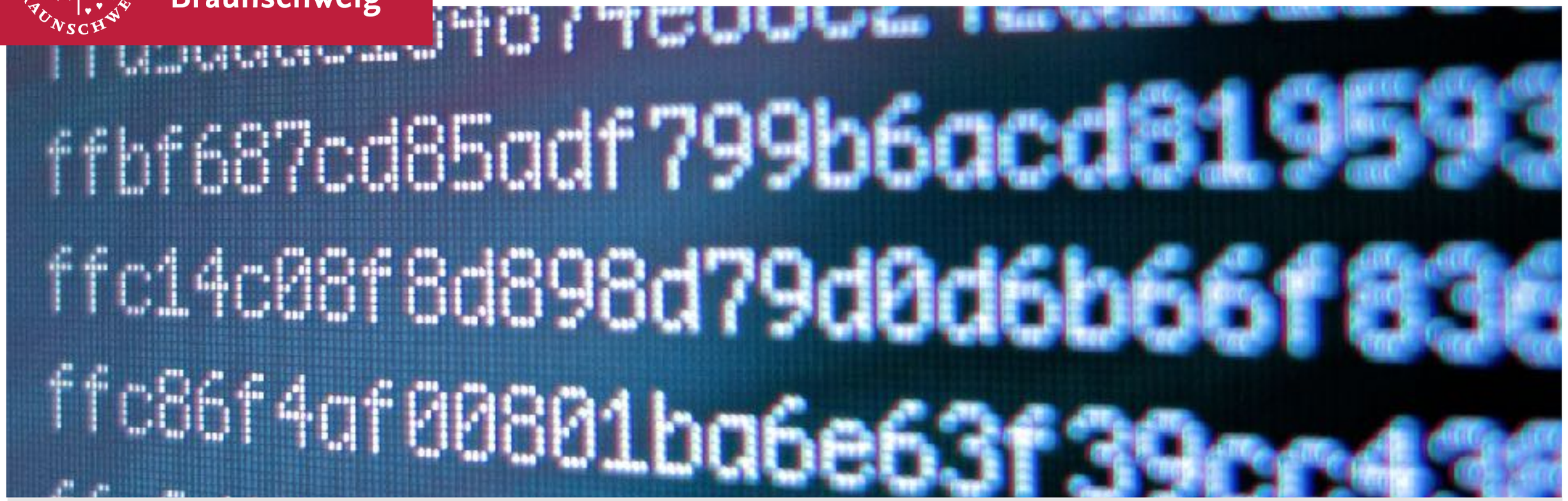
Technische Universität Braunschweig

IAS INSTITUTE FOR APPLICATION SECURITY



Introduction

Vorlesung “Einführung in die IT-Sicherheit”

Prof. Dr. Martin Johns

Institute of Application Security

- **Our institute (research group)**

  — Head —
  Prof. Dr. Martin Johns

  — Team —
  8 PhD students
  and (many) student assistants

- **Website**
  - http://www.tu-bs.de/ias

Overview

- **Topic of the unit**
  - Introduction and Organisation
- **Parts of the unit**
  - Part #1: Organisation of the course
  - Part #2: Computer security today
  - Part #3: Security goals and threats
  - Part #4: Security mechanisms

Lecture and Exercises

- Title: **"Einführung in die IT-Sicherheit"**
  - Lecture + Exercises (5 ECTS; 2+2 SWS)
  - Modules INF-ISS-007 and INF-ISS-009
  - Bachelor and Master students welcome
- Passing the class:
  - Studienleistung (weekly exercise sheets)
  - Prüfungsleistung (exam at the end of the semester)

The Lecture

- **“Crash course in IT Security**
  - Goal: Touch the majority of practical relevant security topics
- **Topics**
  - Security Mechanism (today)
  - Cryptography
  - Security Protocols
  - Authentication & Access Control
  - Network Security
  - Web Security
  - Low Level Security
  - Malware & Intrusion Detection

About the Exercises

- **Weekly sheets with practical and theoretical tasks**
  - You need to solve 50% of the exercises (Studienleistung)
  - Best preparation for the written exam
- **Exercises will include programming tasks in Python**
  - Practical experimenting with security concepts
  - Implementation of attacks and defenses
  - No fear! Tutorial in the lecture

About the Exercises

- **Weekly sheets with practical and theo**
  - You need to solve 50% of the exerci
  - Best preparation for the written exa
- **Exercises will include programming t**
  - Practical experimenting with secur
  - Implementation of attacks and def
  - No fear! Tutorial in the lecture

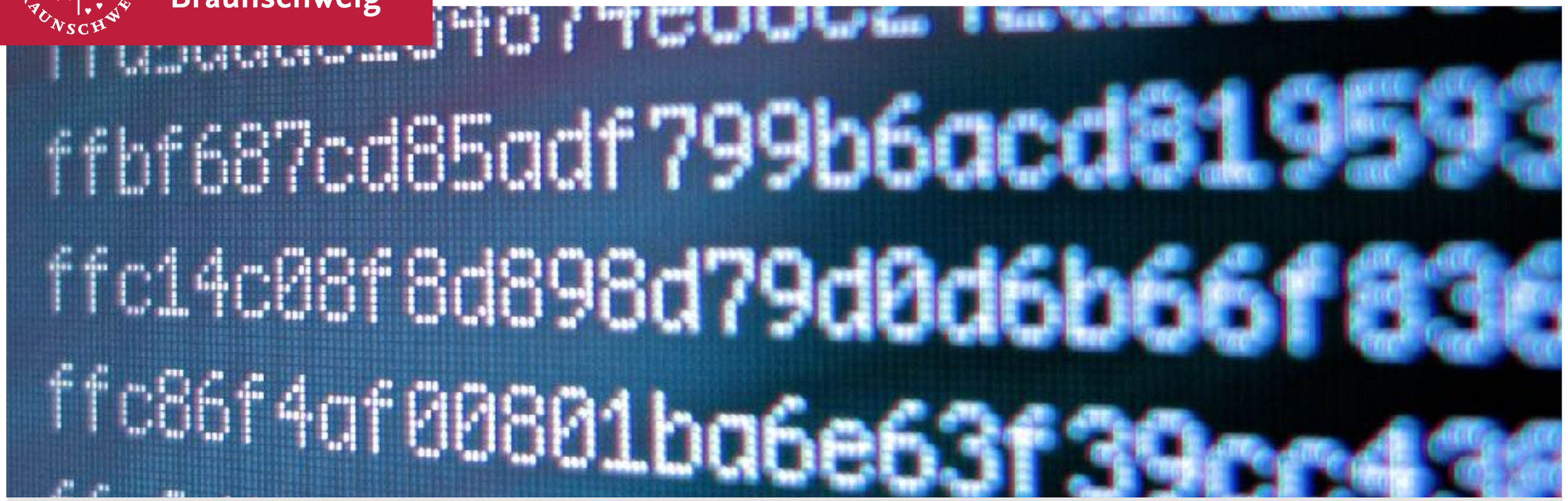
```
# Python is simple!
a = "world"
b = 10

# A function
def hello():
    print("welcome friends")

# An if statement
if b == 10:
    hello()

# A loop
for i in range(b):
    print("hello %d" % i)
```

Exam of the Course

- **Exam at the end of the semesters**
  - Day and time: To be announced
  - Format: Klausur
- **Passing the exam**
  - You need to have at least 50% of the points to pass
  - There will be no second written exam this semester

Technische Universität Braunschweig

IAS INSTITUTE FOR APPLICATION SECURITY



Computer security today

Vorlesung “Einführung in die IT-Sicherheit”

Prof. Dr. Martin Johns

Why Computer Security?

- **Computer systems are ubiquitous in our daily life**
  - Computers store and process our data and information
  - Computers access and control our resources
  - Only few situations where computers are not involved

Valuable data

Private data

Dangerous data

Insecurity of Computers

- **Continuous discovery of security vulnerabilities** 🔥
  - Implementing secure software and hardware very hard
  - Often ignorance and unawareness of developers
- **Some examples of recent vulnerabilities**
  - Printer Nightmare — remote code execution on Windows
  - Dirty Cow — local privilege escalation on Linux
  - Meltdown and Spectre — hardware flaws in many processors

Security Breaches

- **Numerous security breaches at popular Internet services**
  - Millions of identifies exposed to attackers per year
  - Leaked data often includes names, addresses, passwords …

Wall Street Journal, 2021

T-Mobile hacker who stole data on 50 Million Customers: 'Their Security Is Awful'

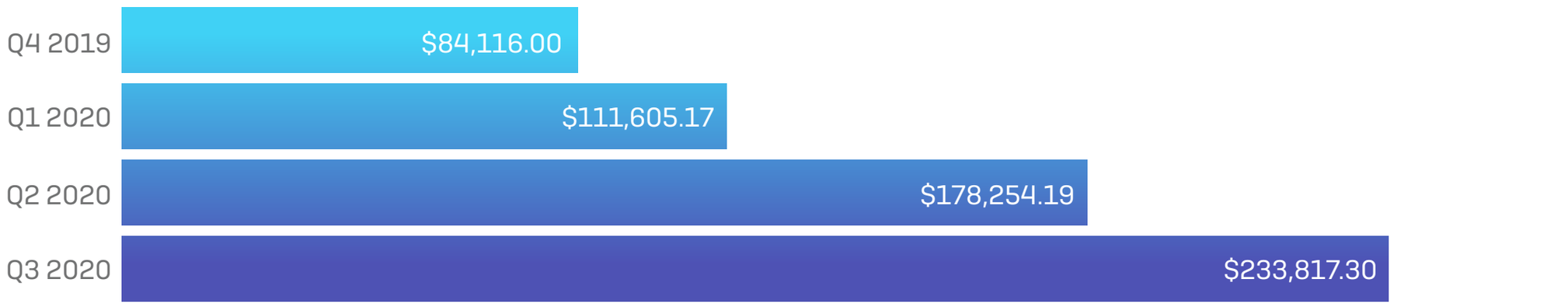
Forbes, 2020

235 million Instagram, TikTok and YouTube user profiles exposed in massive data leak

Cybercrime

- **Criminal economy**
  - Wide range of attacks targeting users and companies
  - Often combination with malicious software (malware)
  - Example: Recent ransomware campaigns

Average ransom payouts, quarterly

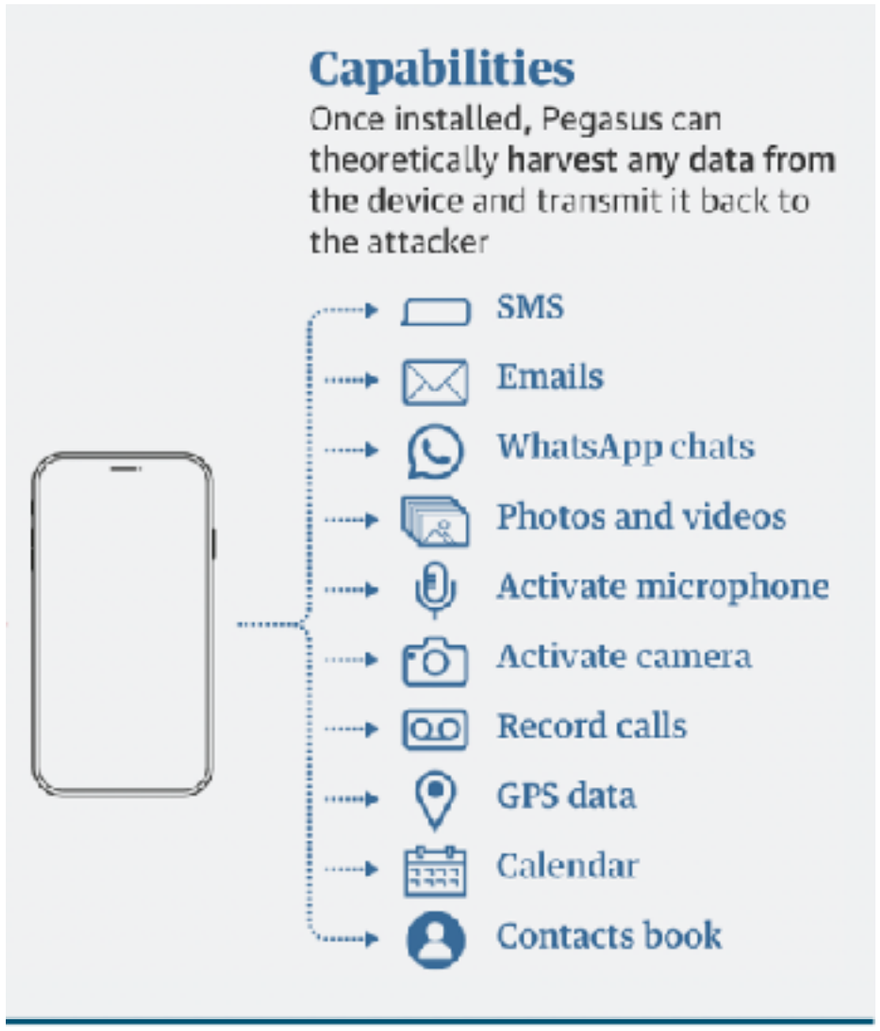


SOPHOSlabs

Skilled Attackers

- **Targeted attacks**
  - … against industry
  - … against governments
  - … against NPOs
- Example: **Stuxnet Worm**
  - Malware detected in 2010
  - Disruption of ICS systems
  - Sabotage against Iran

Pegasus malware



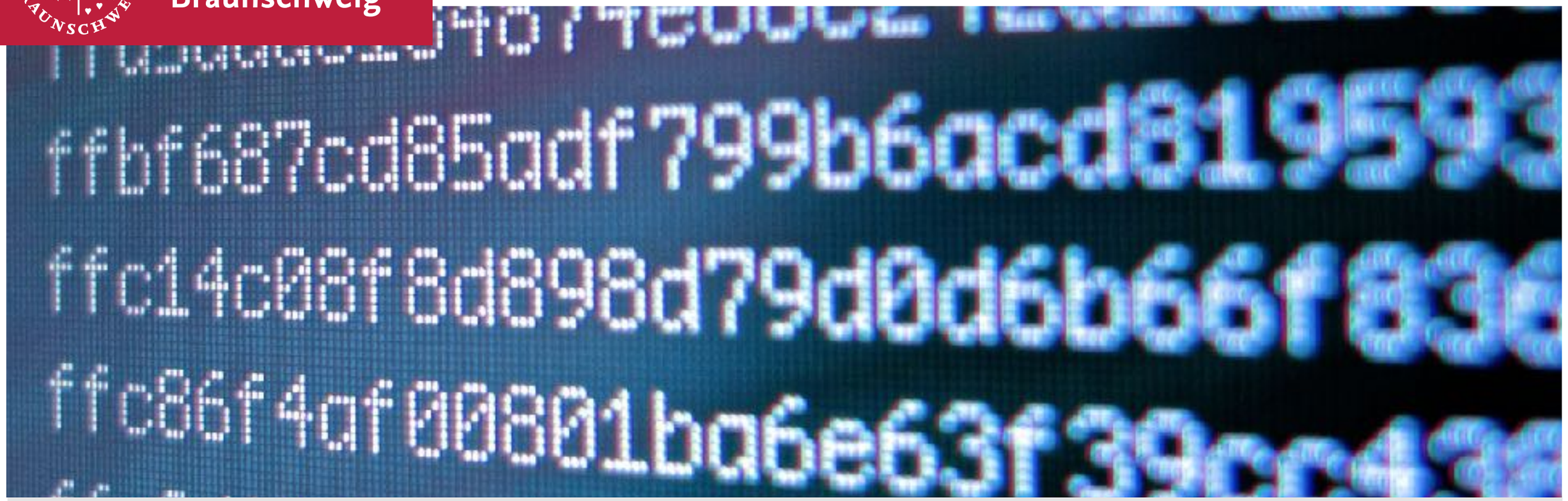
(The Guardian, 2020)

Security is different!

- **Security is different from other disciplines**
  - Established concepts are put into questions
  - Intersection with many areas of computer science
  - Often, it's a game of good and evil players
- **Practice and theory of security are often fun**
  - Monitoring, detection and analysis of real attacks
  - Reasoning about limits of attacks and defenses

Technische Universität Braunschweig

IAS INSTITUTE FOR APPLICATION SECURITY



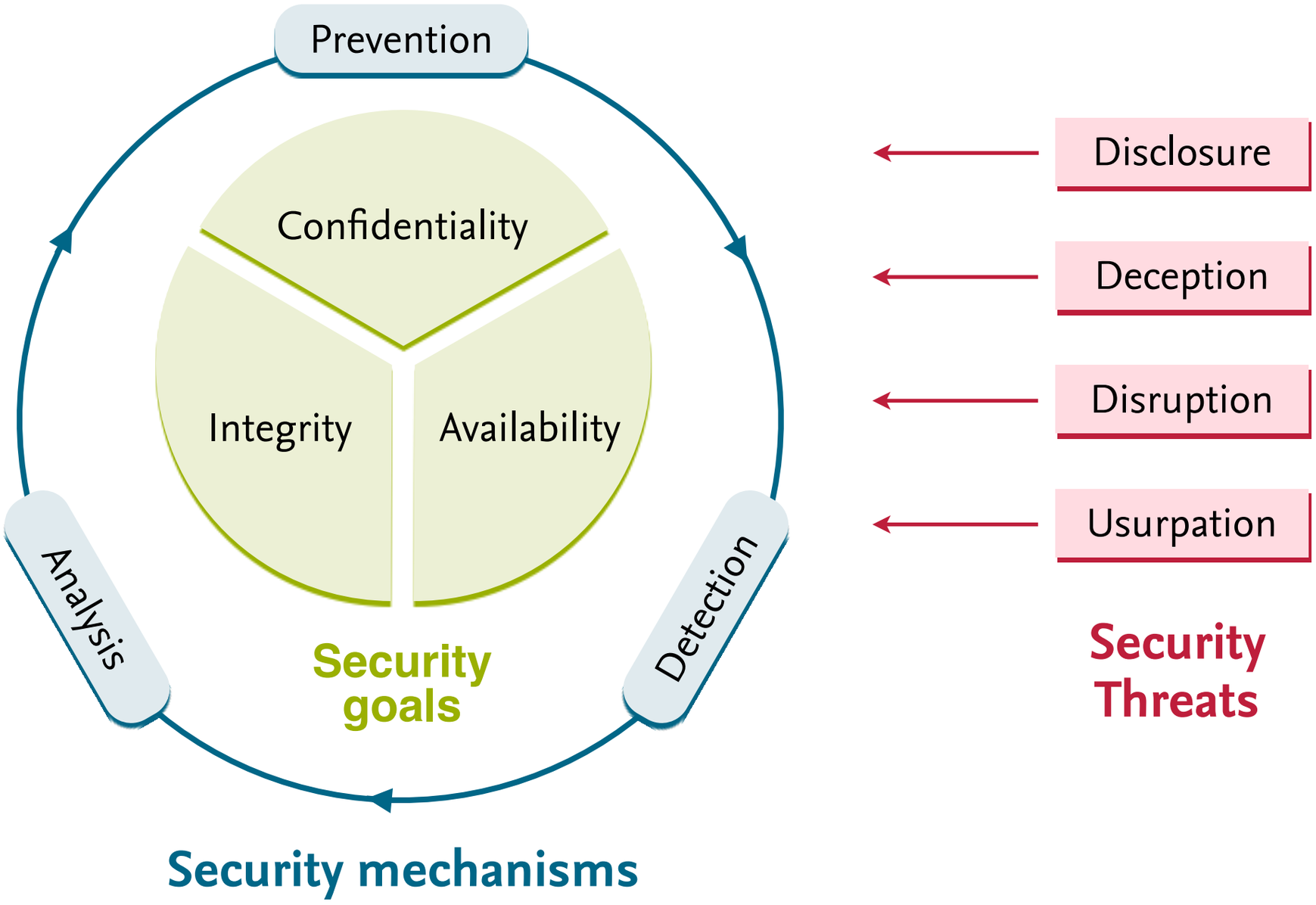
Security goals and threats

Vorlesung “Einführung in die IT-Sicherheit”

Prof. Dr. Martin Johns

Part #3

The “Big Picture”



Security Goals

- **Security goals** (memory hook: “CIA”)
  - Confidentiality of information and resources
  - Integrity of information and resources
  - Availability of information and resources

- **Basic definitions**
  - Threat = potential violation of a protective goal
  - Security = protection from intentional threats
  - Safety = protection from accidental threats

Confidentiality

Confidentiality

Protection of resources from unauthorized disclosure

- **Security measures**
  - Encryption of data, resource hiding
- **Examples of attacks**
  - An attacker eavesdrop a telephone conversation
  - An attacker reads the emails on your computer

Integrity

Integrity

Protection of resources from unauthorized manipulation

- **Security measures**
  - Authorization, checksums, digital fingerprints
- **Examples of attacks**
  - An attacker changes the receipt of a bank transaction
  - An attacker tampers with files on your computer

Availability

Availability

Protection of resources from unauthorized disruption

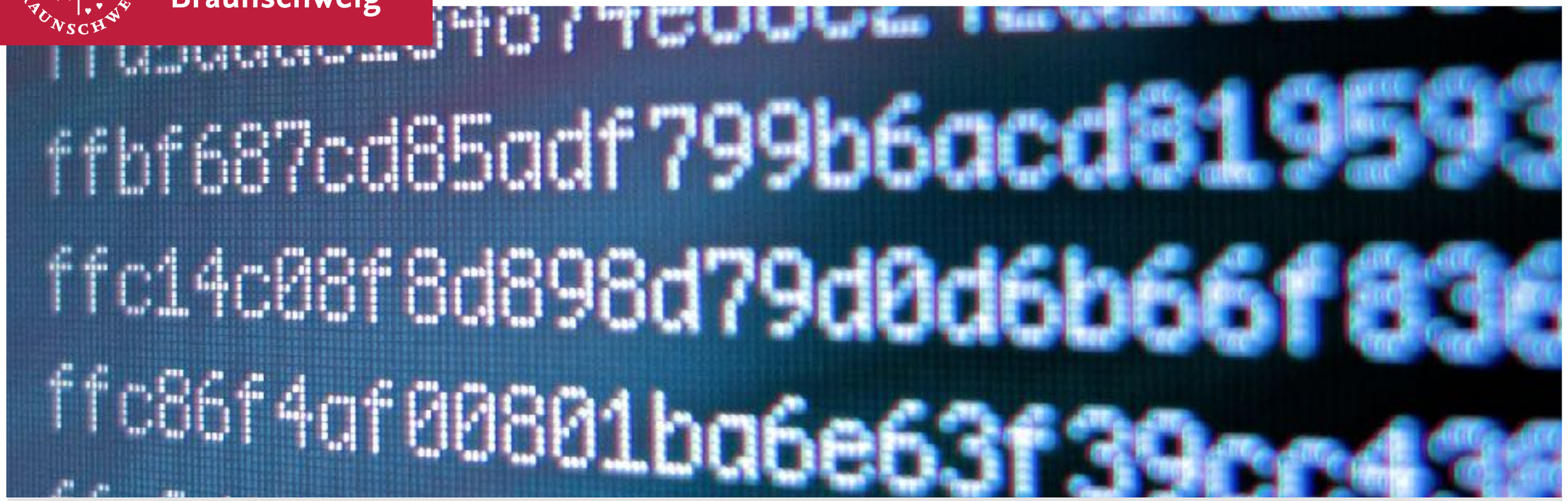
- **Security measures**
  - Restriction, redundancy, diversity
- **Examples of attacks**
  - An attacker crashes the web server of a company
  - An attacker formats the hard disk of your computer

Threats & Attacks

- **Basic classes of threats**
  - **Disclosure** = unauthorized access to information
  - **Deception** = acceptance of false data (e.g. masquerading)
  - **Disruption** = interruption or prevention of correct operation
  - **Usurpation** = unauthorized control of resources
- **Attack** = attempt to violate a security goal (intentional threat)
  - Often combinations of different threat classes

Technische Universität Braunschweig

IAS INSTITUTE FOR APPLICATION SECURITY



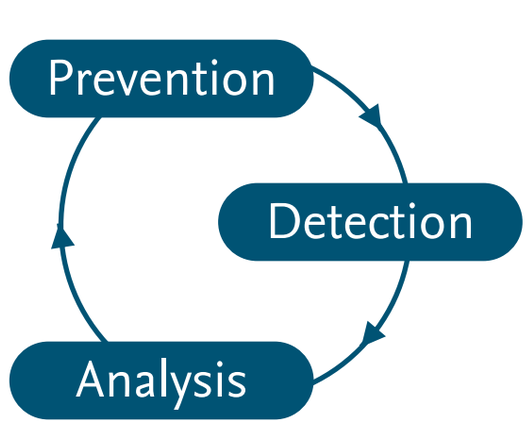
Security mechanisms

Vorlesung “Einführung in die IT-Sicherheit”

Prof. Dr. Martin Johns

Security Mechanisms

- **Security policies and mechanisms**
  - Policy = statement of what is and what is not allowed
  - Mechanism = method or tool enforcing a security policy
- **Strategies for security mechanisms**
  - Prevention of attacks, e.g. encryption
  - Detection of attacks, e.g. virus scanner
  - Analysis of attacks, e.g. forensic



- Security is a cyclic and never-ending process

Strategy: Prevention

Prevention of attacks

Prevention of attacks prior to violation of security goals

- **Example**
  - Authentication and encryption
    Restriction of access to information/resources
- **Limitations**
  - Inapplicable in many settings, e.g. open services

Strategy: Detection

Detection of attacks

Detection of attacks during violation of security goals

- **Example**
  - Anti-virus scanners
    Detection of malicious code on computers
- **Limitations**
  - Ineffective against unknown and “invisible” attacks

Strategy: Analysis

Analysis of attacks

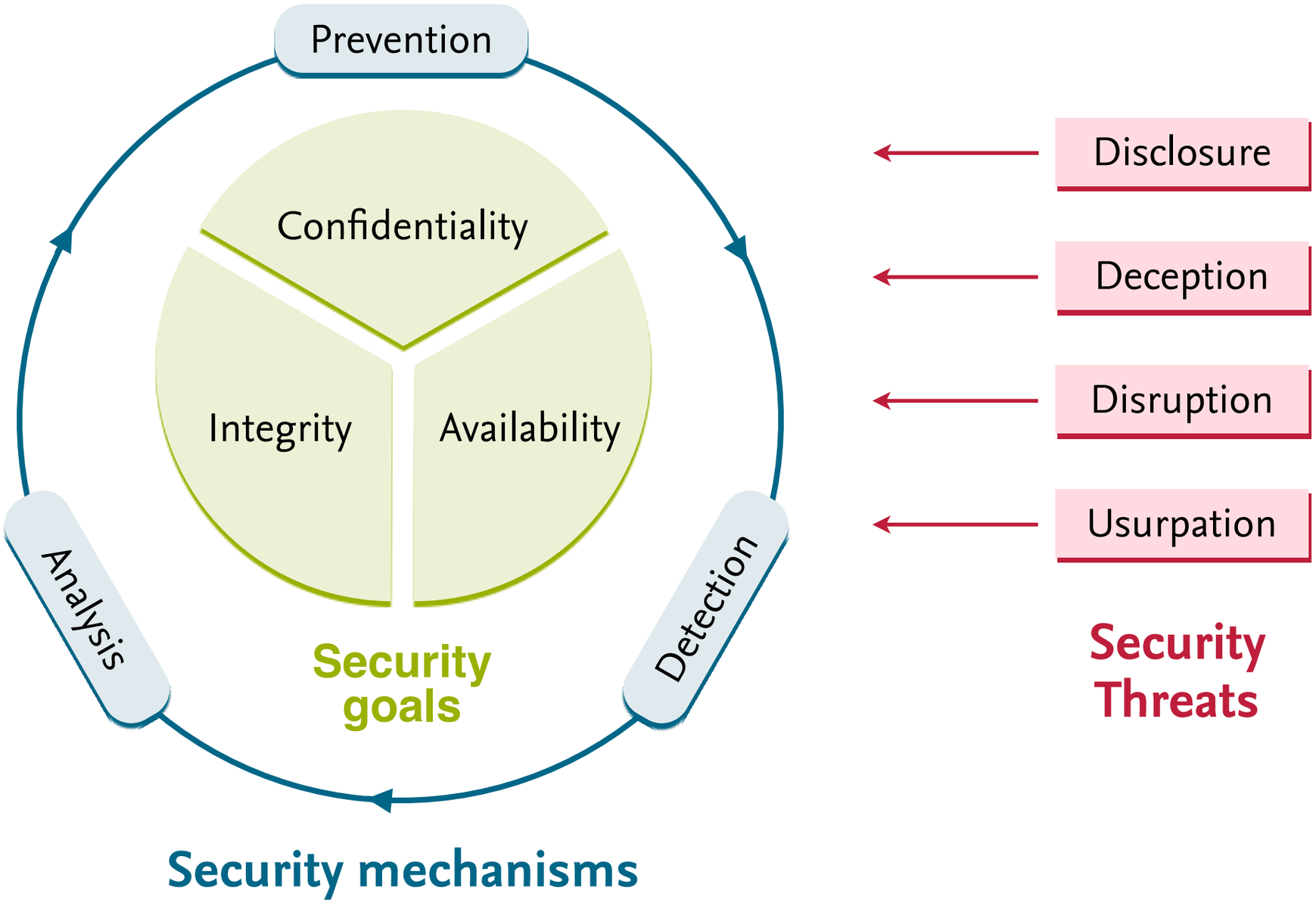
Analysis of attacks after violation of security goals

- **Example**
  - Computer forensics
    Investigation and analysis of security incidents
- **Limitations**
  - Severe damage might have already occurred

Further Concepts

- **Authenticity** = truthfulness of information and resources
  - May be viewed as an aspect of integrity
- **Accountability** = linking of actions and users
  - Realization of non-repudiation in computer systems
- **Privacy** = Security and control of personal information
  - Property of individuals and not of data
- … and many more

The “Big Picture” (again…)



Summary

Summary

- **Security central issue of computer science**
  - Omnipresence of threats and attacks
  - Increasing importance due to cybercrime
- **Key concepts of security**
  - Basic security goals: confidentiality, integrity, availability
  - Various types of threats and attacks
  - Security mechanisms for prevention, detection, analysis