INF3510 Information Security
University of Oslo
Spring 2012

Lecture 1

Course Information

Background and Basic Concepts

Course information

- Scope of information security
- Syllabus and text book
- Lecture plan
- Prerequisites
- Course organization
- Home exam

- Remember to register attendance during break today!

Scope of information security

- Information security is about avoiding damage and controlling risk of damage to information assets
- Information security activities focus on:
  - Understanding threats and vulnerabilities
  - Managing threats by reducing vulnerabilities or threat exposures
  - Detection of attacks and recovery from attacks
  - Investigate and collect evidence about security incidents

Prerequisites

- Prerequisites
  - Basic computer and network technology
  - Basic mathematics

- Theoretical material used
  - Discrete mathematics, number theory, modular arithmetic
  - Information theory
  - Probability calculus
  - Computer and network architecture

How to survive INF3510

- Basic requirements
  - Attend 2 hours lectures per week
    - Lecture notes available at least one day prior to lecture
  - Work on the workshop questions
    - Will be discussed during the following week’s workshop which follows immediately after the 2-hour lecture
  - Work on the home exam
    - Topic for the assignment can be freely chosen.
- Not just about facts, you also need to
  - understand concepts
  - apply those concepts
  - think about implications
  - understand limitations

Course Resources

- Learning material will be made available on:
  - http://www.uio.no/studier/emner/matnat/ifi/INF3510/
    - CUO, staff contact details, lecture outlines, tutorial questions, etc.
- Assignment groups and topics must be specified on:
  - https://wiki.uio.no/mn/ifi/INF3510-2012
- Various online resources
  - E.g. NIST special computer security publications http://csrc.nist.gov/publications/PubsSPs.html

Course Assessment

- Course weight: 10 study points

- Assessment:
  - Home exam: 40%
  - Final examination: 60%

- Academic dishonesty (including plagiarism and cheating) is actively discouraged, see
  - http://www.uio.no/english/studies/admin/examinations/cheating/

Course Staff

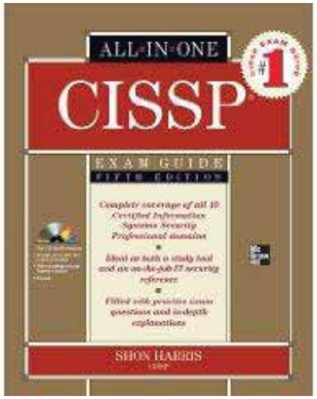
- Lecturer:
  - Prof Audun Jøsang <josang@mn.uio.no>
- Home exam organisation:
  - Kent Varmedal <kentav@ifi.uio.no>
- Informatics dep. administration
  - http://www.ifi.uio.no/adminfo/administrasjonen.html
  - Email: studieinfo@ifi.uio.no
  - Tel: 22 85 24 10

Who do I contact?

- Lecturer
  - for help with course material,
  - attendance problems, exam marking
  - for general course related matters
  - workshop and previous exam questions
- Home exam assistant
  - for registration to wiki and selecting topic for home exam
- Administration
  - for any matters external to this course,
    e.g. enrolment problems, IT access problems

Syllabus and text book

- The syllabus for this course consists of the material presented during the lectures, as described in the lecture notes.
- Adequate comprehension of the material requires that you also
  - read parts of the text book and other documents
  - work out answers to the workshop questions
  - follow the lectures.
- Text book: CISSP All-in-One Exam Guide
  5th Edition, 2010
  Author: Shon Harris



Shon Harris

- The book covers the 10 CBK domains (Common Body of Knowledge) for the CISSP Exam (Certified Information Systems Security Professional).
- 100 copies of the text book have been ordered to Akademika

CISSP CBK (Common Body of Knowledge)

1. Access Control (user authentication and identity management)
2. Telecommunications and Network Security
3. Information Security Management and Risk Management
4. Application Security (software security)
5. Cryptography
6. Security Architecture and Design (computer security)
7. Operations Security
8. Business Continuity Planning and Disaster Recovery Planning
9. Legal Regulations, Compliance and Investigation (forensics)
10. Physical and Environmental Security

How to use the text book

- 1193 pages in total
  - But exclude
    - Ch.1 (How to become a CISSP) & Ch.2 (security trends)
    - 60 pages of appendix, glossary and index
    - 150 pages of tips, Q&A
    - Parts of chapters
  - Around 800 pages of readable material
  - The book is very easy to read ☺
  - Sometimes long explanations and examples ☹
- Each chapter has **Main Sections** (big font) and **Subsections** (small font), but no numbering, a bit confusing.
- Don’t read *distracting comments in italics* under section titles

Lecture Plan

Week	Date	#	Topic
W03	17.01.2012	1	Course Information. Background and Basic Concepts
W04	24.01.2012	2	Information Security Management,
W05	31.01.2012	3	Risk Management and Business Continuity Planning
W06	*Lecture break*		
W07	14.02.2012	4	Computer Security
W08	*Winter break*		
W09	28.02.2012	5	Cryptography
W10	05.03.2012	6	Key Management and PKI
W11	13.03.2012	7	User Authentication
W12	20.03.2012	8	Identity and Access Management
W13	27.03.2012	9	Network Communication Security
W14	Easter break		
W15	10.04.2012	10	Network Perimeter Security
W16	17.04.2012	11	Computer Forensics
W17	24.04.2012	12	Privacy and Regulatory Requirements
W18	*Lecture break*		
W19	18.05.2012	13	Application and Operations Security
W20	15.05.2012	14	Review
W21			*No lecture*
W22			*No lecture*
W23	08.06.2012	Exam time: 14:30h - 18:30h	

Learning language

- All syllabus material and workshop questions to be provided in English.
- Specific Norwegian documents as background material
- List of Norwegian translations of English security related terms to be developed during the semester.
- Assignment can be written in English or Norwegian

Workshops

- The weekly workshop follows after the 2-hour lecture.
- The workshop questions relate to the lecture given the previous week.
- Written answers to workshop questions will not be provided
- The purpose of the workshops is to facilitate better learning of the lecture material

Home exam
Written report on security topic

- Select a topic related to information security
  - Can be freely chosen
  - A list of topics provided online
  - Other topics can be specified
  - All topics titles must be different, but OK to have similar topics
- To be written in groups of 2 or 3. Individually also OK
  - Deadline for selecting topic and forming group: 14.03.2012
- Self registration of topic and group on wiki
  - https://wiki.uio.no/mn/ifi/INF3510-2012
- Hand in by 14.05.2012
- Counts 40%

Other security courses @ Ifl

- UNIK4220 – Introduction to Cryptography (autumn)
  - Leif Nilsen (Thales)
- UNIK4250 – Security in Distributed Systems (spring)
  - Audun Jøsang (Ifl)
- UNIK4270 – Security in Operating Systems and Software (autumn)
  - Audun Jøsang (Ifl)
- INF5150 - Unassailable IT-systems (autumn)
  - Ketil Stølen (SINTEF)
- ITLED4230 – Security Governance (IT Management Master's)
  - Audun Jøsang (Ifl)

Information Security
Background and Basic Concepts

Norwegian terms

English		Norwegian	
• Security	→	• Sikkerhet	✓ GOOD
• Safety	→	• Trygghet	
• Certainty	→	• Visshet	

• Security • Safety • Certainty	} →	• Sikkerhet	✗ BAD

What is security in general ?

- Security is about protecting assets from damage or harm
- Focuses on all types of assets
  - Example: you, possessions, processes, environment, nation
- Types of security
  - National security (political stability)
  - Safety (body and health)
  - Environmental security (clean environment)
  - Information security
  - etc.

Rules for Right or Wrong

- ”Protecting assets from harm” assumes understanding of what is harmful, e.g. defined by:
- Laws and regulation, e.g.
  - EU Data Protection Directive 1995, mandates privacy regulation
  - Norwegian “Sikkerhetsinstruksen” 1953, mandates protection of information that is considered important for national security
- Explicit company policy
  - Defines who is authorized to do what
  - Defines appropriate use
- Implicit policy
  - e.g. your own rules for using your laptop
- Ethics and social norms
  - e.g. correct representation of goods for sale online

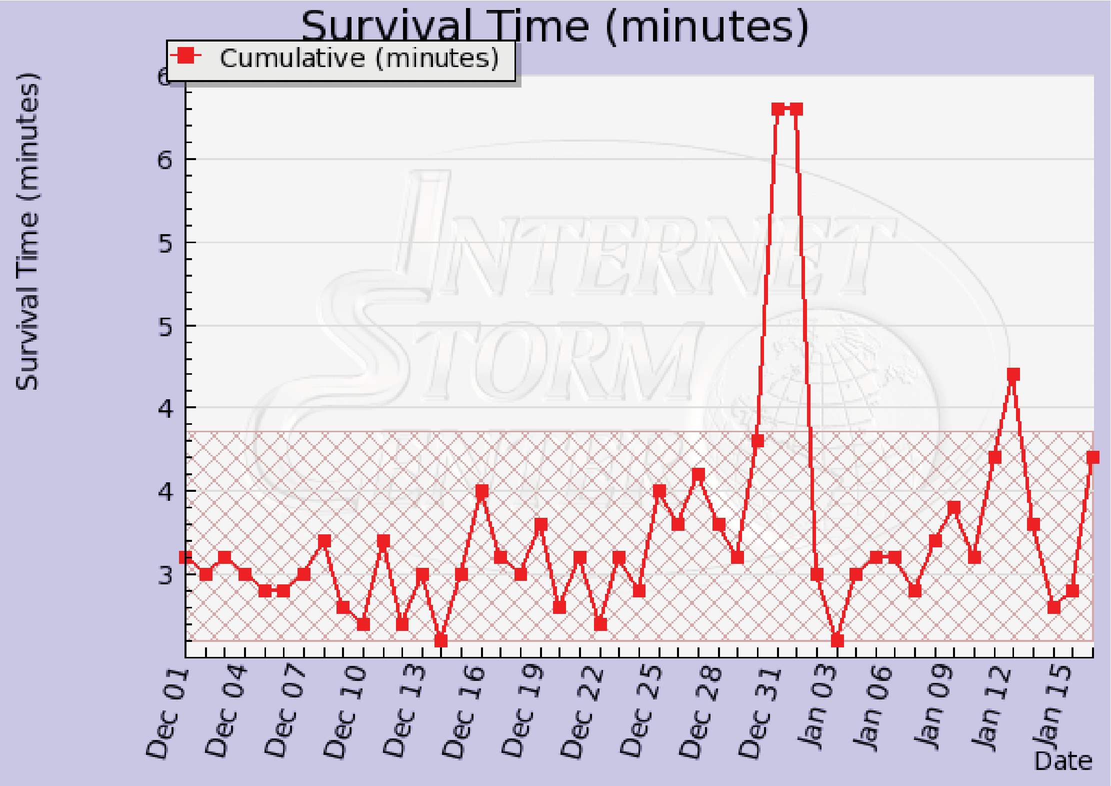
What is *information* security ?

- *Information* security is about protecting *information* assets from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT infrastructure and processes
- Threat sources can be intentional and accidental:
  - Threat agents can be people or acts of nature
  - People can cause harm by accident or by intent
- Prevention, consider:
  - Prevention of damage to information assets
  - Detection of damage to information assets – when, how, who?
  - Reaction – to recover from damage

The need for information security

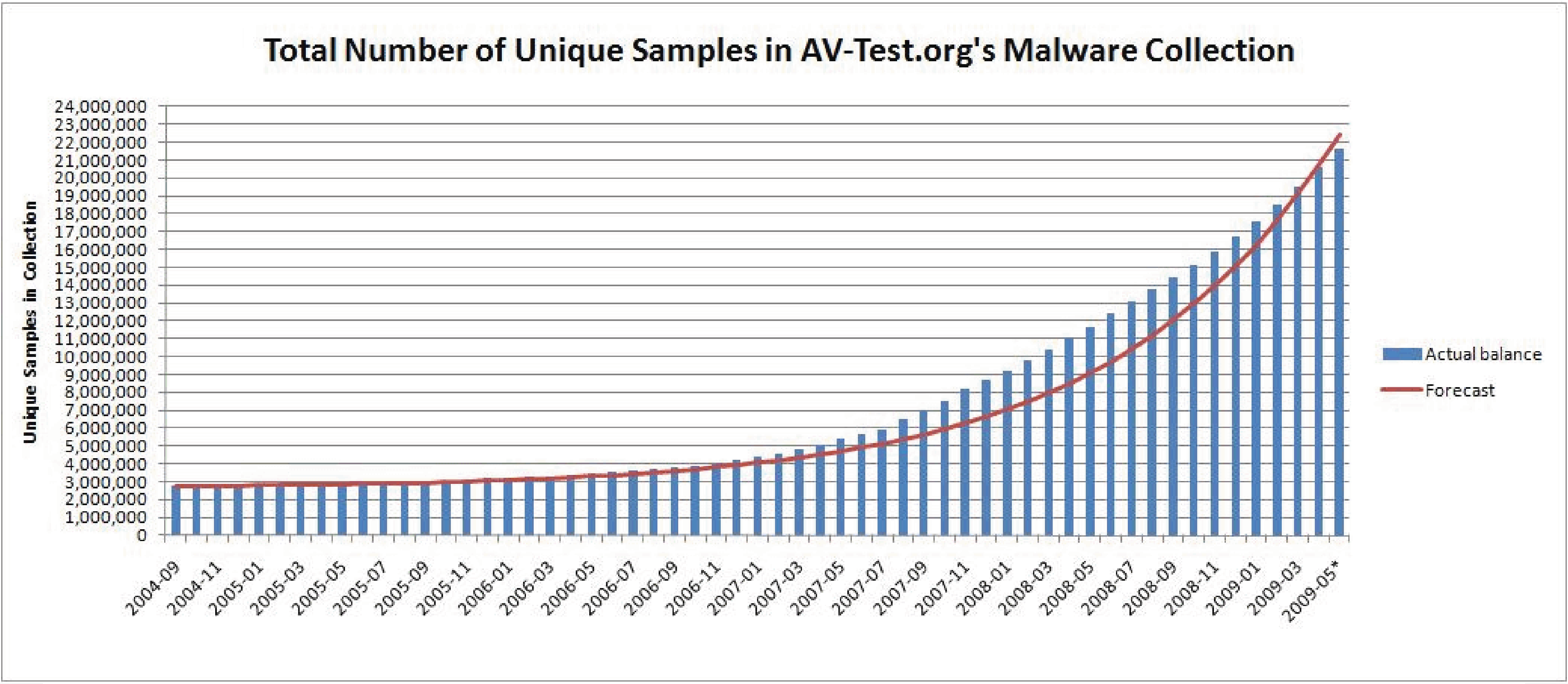
- Why not simply solve all security problems once for all?
- Reasons why that’s impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New and changing threats
  - More effective and efficient attack technique and tools are being developed
- Conclusion: Information security doesn’t have a final goal, it’s a continuing process

Internet Storm Survival Time Measure



The survival time is calculated as the average time between attacks against average target IP address. http://isc.sans.org/survivaltime.html

Malware Trend



Importance of IT Security

- Issues:
  - damages “hidden” but increasing
  - organised cyber-crime is increasing
  - identity theft is major growth crime
  - 1.5 billion online users, 2 billion by 2015
- Urgent need for strengthening information security knowledge/expertise and research:
  - at application development level
  - at the operations level
  - at the management level
  - at the national and international level

National Security

- CIP (Critical Infrastructure Protection)
  - Most critical components of modern society depend on IT
- CIIP (Critical Information Infrastructure Protection)
  - Specific IT systems are by themselves critical components
- The accumulated set of non-critical systems (e.g. servers and networks in SMEs) becomes critical
- IT systems are both targets and weapons of attack in industrial, political and international conflicts
- The vulnerability of the critical information infrastructure is worrisome and needs attention

Information systems components

- OK, we need information security. What to consider?

- Information security involves
  - Hardware
  - Software
  - Data
  - People
  - Governance
  - Procedures
  - Processes
  - Physical buildings and installations

Security protection phases

- Prevention:
  - prevent attacks from succeeding in the first place
    - e.g. by removing or reducing vulnerabilities
- Detection
  - report attacks as soon as possible
    - e.g. by automated alarms or by manual reporting
- Correction
  - correct damage or irregularities as soon as possible
    - e.g. by installing back-up when file system has been corrupted
- A combination of the three types provides a layered approach to information security. One layer is never enough.

Information States

- Information is considered to exist in one of three possible states:
  - Storage
    - Information storage containers – electronic, physical, human
  - Transmission
    - Physical or electronic
  - Processing (use)
    - Physical or electronic

- Security controls for all information states are needed

Threats, Vulnerabilities and Attacks

- Threat: Type of incident that can cause harm
  - e.g. virus infection
  - made possible through the presence of vulnerabilities
- Vulnerability: Weakness in a system that could allow a threat to cause harm
  - e.g. anti-malware filter outdated or not present
  - allows threats to succeed
- Attack: Deliberate attempt to realise threats by exploiting vulnerabilities
  - e.g. sending email infected with malware

Example threats, vulnerabilities and attacks

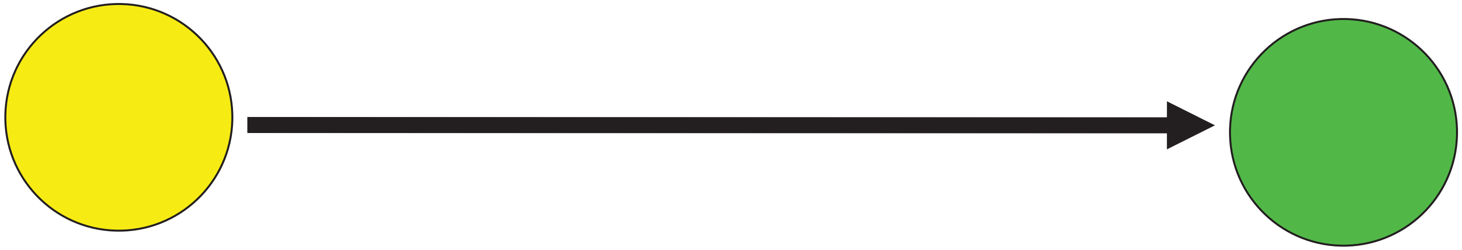
- Example 1: Your house:
  - Threat: theft of assets
  - Threat agent: burglar
  - Vulnerability: poor security of house e.g. open window
  - Attack: A burglar enters through window and steals jewellery
- Example 2: Data files on computer:
  - Threat: modification or theft of files
  - Threat agent: hacker
  - Vulnerability: poor security of computer, e.g. no malware filter
  - Attack: A hacker injects a Trojan into your computer which enables remote control of the computer to modify or steal files

Information threat classes

- Four high level classes of threats to information:
  - Interception:
    - an unauthorised party gains access to information assets
  - Interruption:
    - information assets are lost, unavailable, or unusable
  - Modification:
    - unauthorised alteration of information assets
  - Fabrication:
    - creation of counterfeit information assets

Diagram

Normal information flow

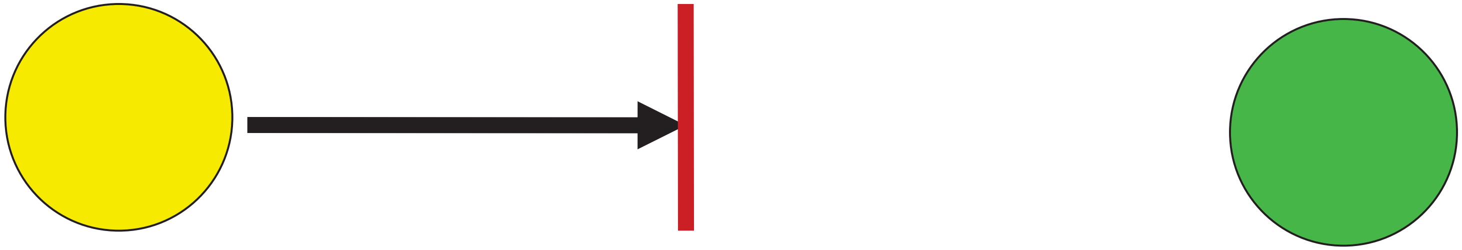


Information Source

Information Destination

Threats to information: Interruption

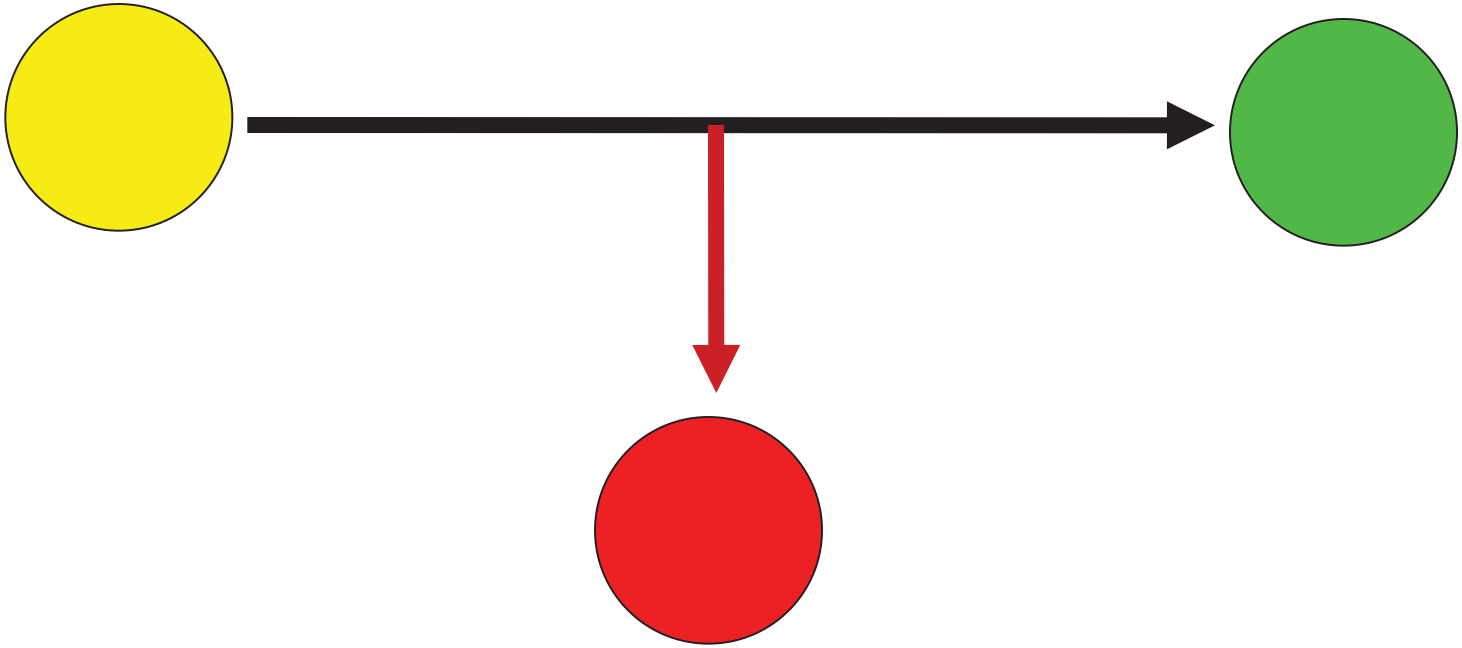
your assets become unavailable



Attack on availability

Threats to information: Interception

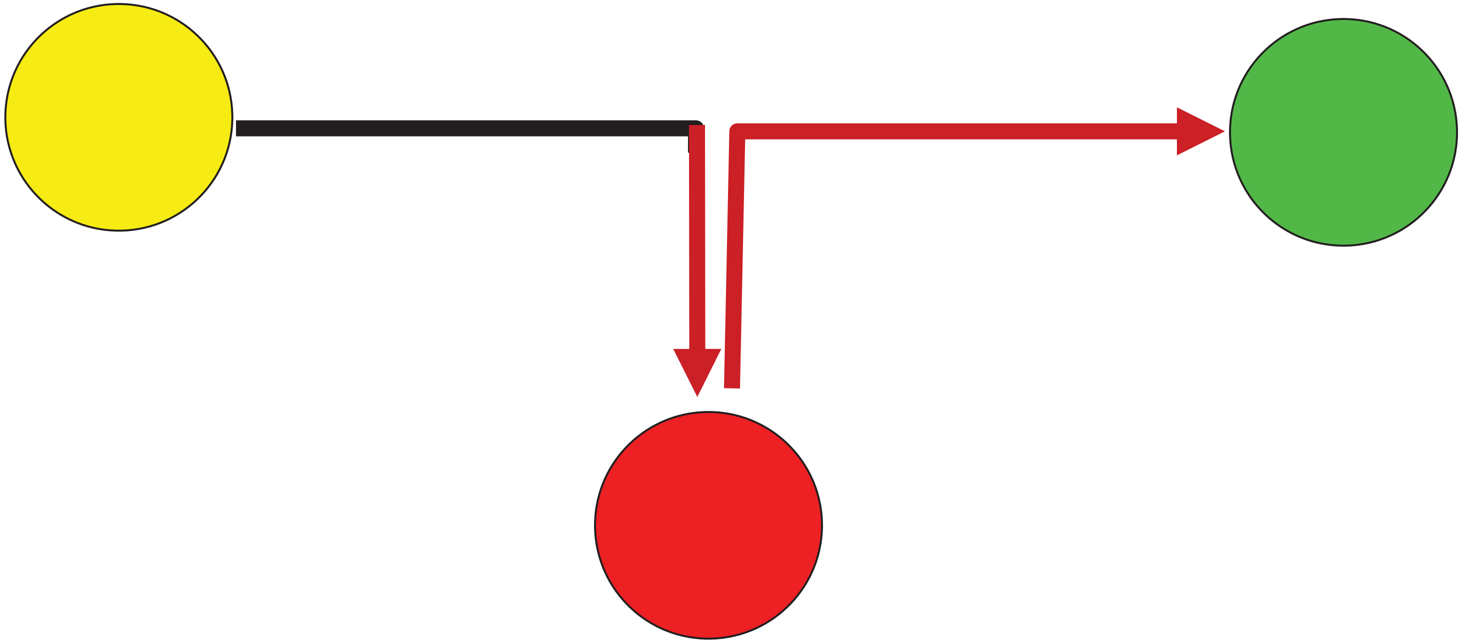
some unauthorised party has gained access to your assets



Attack on confidentiality

Threats to information: Modification

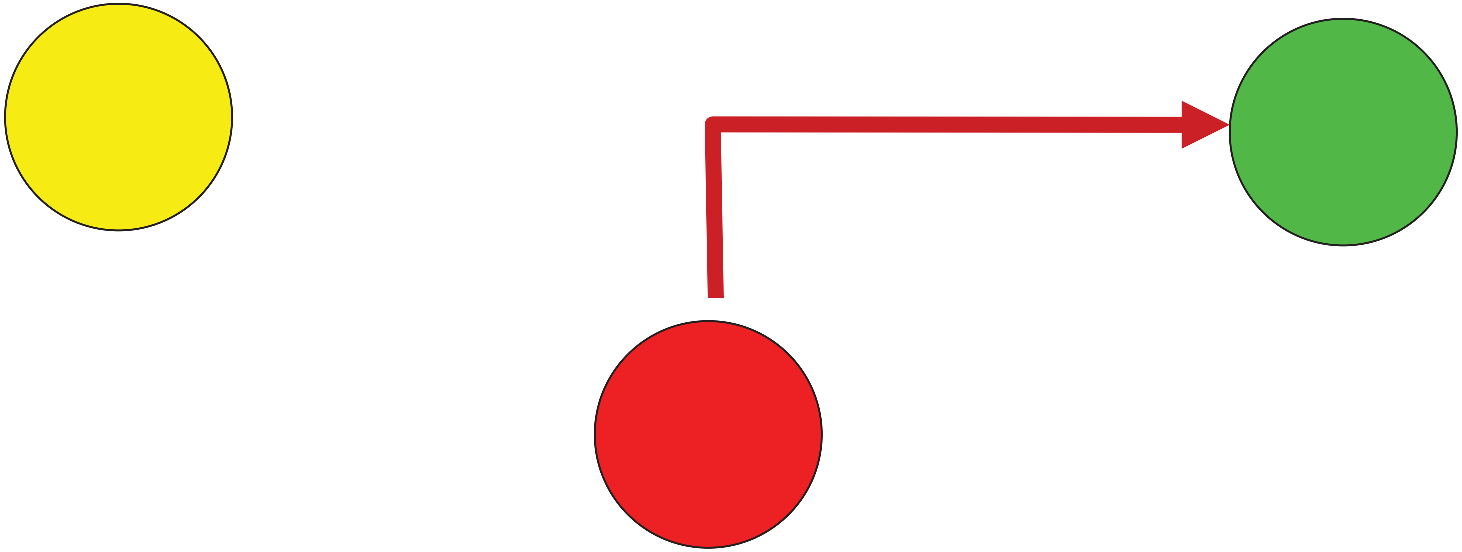
some unauthorised party tampers with your assets



Attack on integrity

Threats to information: Fabrication

unauthorized copies of your assets are made



Attack on authenticity

Passive or active attacks

- Attacks can be divided into two classes:
  - Passive:
    - E.g. eavesdropping, shoulder surfing
    - Attacker's goal is to obtain information
    - Difficult to detect; usually try to prevent the attack.
  - Active:
    - E.g. Phishing, Denial of service, Man-in-the-middle
    - Attacker's goal may be to modify, replicate or fabricate information
    - Difficult to prevent (physical protection required)
    - Usual approach is to detect and recover

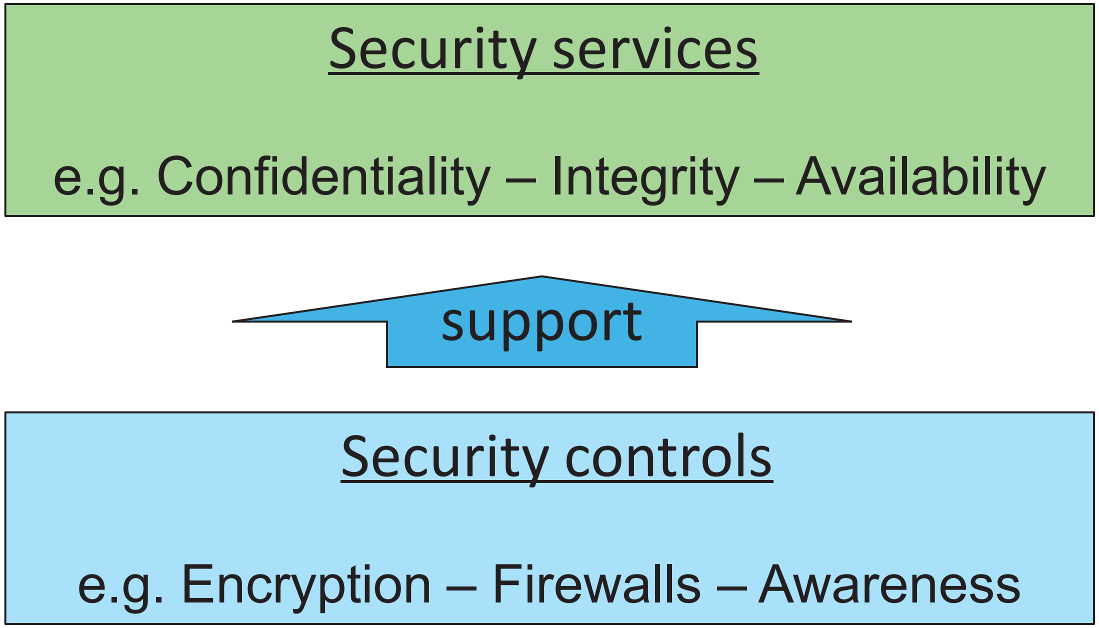
High Level Security Services / Goals

- The traditional definition of information security is to ensure the three CIA security services/goals:
  - **Confidentiality**: preventing unauthorised disclosure of information
  - **Integrity**: preventing unauthorised (accidental or deliberate) modification or destruction of information
  - **Availability**: ensuring resources are accessible when required by an authorised user

CONFIDENTIALITY
INFORMATION
AVAILABILITY
INTEGRITY

Security services and controls

- Security services are:
  - implementation independent
  - supported by specific controls / mechanisms



Security services

e.g. Confidentiality – Integrity – Availability

support

Security controls

e.g. Encryption – Firewalls – Awareness

Confidentiality

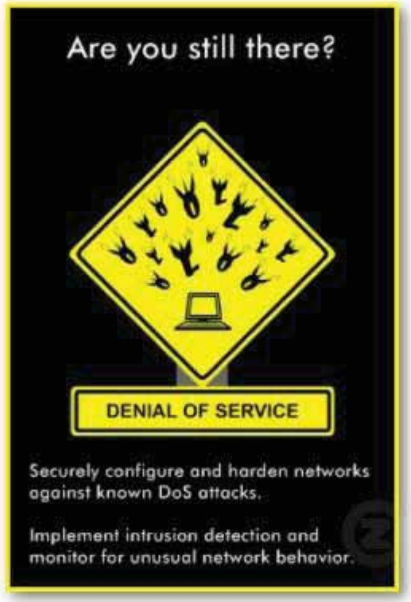
- The property that information is only accessible to authorized entities
- Can be divided into:
  - Secrecy
    - Protecting business data
  - Privacy
    - Protecting personal data
  - Anonymity
    - Hide who is engaging in what actions
- Main threat: Information theft
- Controls: Encryption, Access Control, Perimeter defence

Integrity

- **Data Integrity:** Only authorized persons can create, modify or delete data.
- **System Integrity:** State of system is according to policy.
- Main threat: Information and system corruption
- Controls:
  - Cryptographic integrity check,
  - Encryption,
  - Access Control
  - Perimeter defence
  - Verify correctness of systems and applications

Availability

- The property that information resources are accessible and usable upon demand by an authorized entity
- Main threat: Denial of Service (DoS)
  - The prevention of authorized access to resources or the delaying of time critical operations
- Controls: Redundancy of resources, traffic filtering, incident recovery, international collaboration and policing


Are you still there?
DENIAL OF SERVICE
Securely configure and harden networks against known DoS attacks.
Implement intrusion detection and monitor for unusual network behavior.

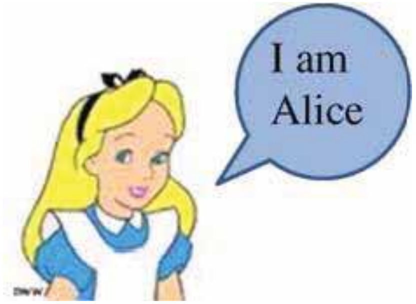
Additional Security Services

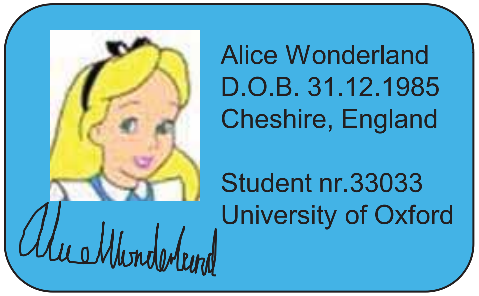
The CIA services apply to information, but are often inappropriate. e.g. for controlling usage of resources, for which additional security services are needed.

- Authentication:
  - **Entity authentication**: the process of verifying a claimed identity
  - **Data Origin Authentication**: the process of verifying the source (and integrity) of a message
- Accountability and Non-repudiation:
  - Create evidence that an action has occurred, so that the user cannot falsely deny the action later
- Access Control:
  - Enforce that all access and usage happen according to policy

Additional security service
User Identification and Authentication

- Identification
  - Who you claim to be
  - Method: (user)name, biometrics
- Entity authentication
  - Prove you are the one you claim to be
- Main threat: Unauthorized access
- Controls:
  - Passwords,
  - Personal cryptographic tokens,
    - OTP generators, etc.
  - Biometrics
    - Id cards




Alice Wonderland
D.O.B. 31.12.1985
Cheshire, England

Student nr.33033
University of Oxford

Alice Wonderland

Authentication token

Additional security service
Message authentication

- Goal: Recipient of a message (i.e. data) can verify the correctness of claimed sender identity
  - But 3rd party may not be able to verify sender Id.
- Main threats:
  - False transactions
  - False messages
- Controls:
  - Encryption with shared secret key
  - MAC (Message Authentication Code)
  - Security protocols
  - Digital signature with private key
  - Electronic signature,
    - i.e. any digital evidence

Additional security service Accountability

- Goal: Trace action to a specific user and hold them responsible
  - *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*

    (TCSEC/Orange Book)
- Main threats:
  - Inability to identify source of incident
  - Inability to make attacker responsible
- Controls:
  - Identify and authenticate users
  - Log all system events (audit)
  - Electronic signature
  - Non-repudiation based on digital signature
  - Forensics

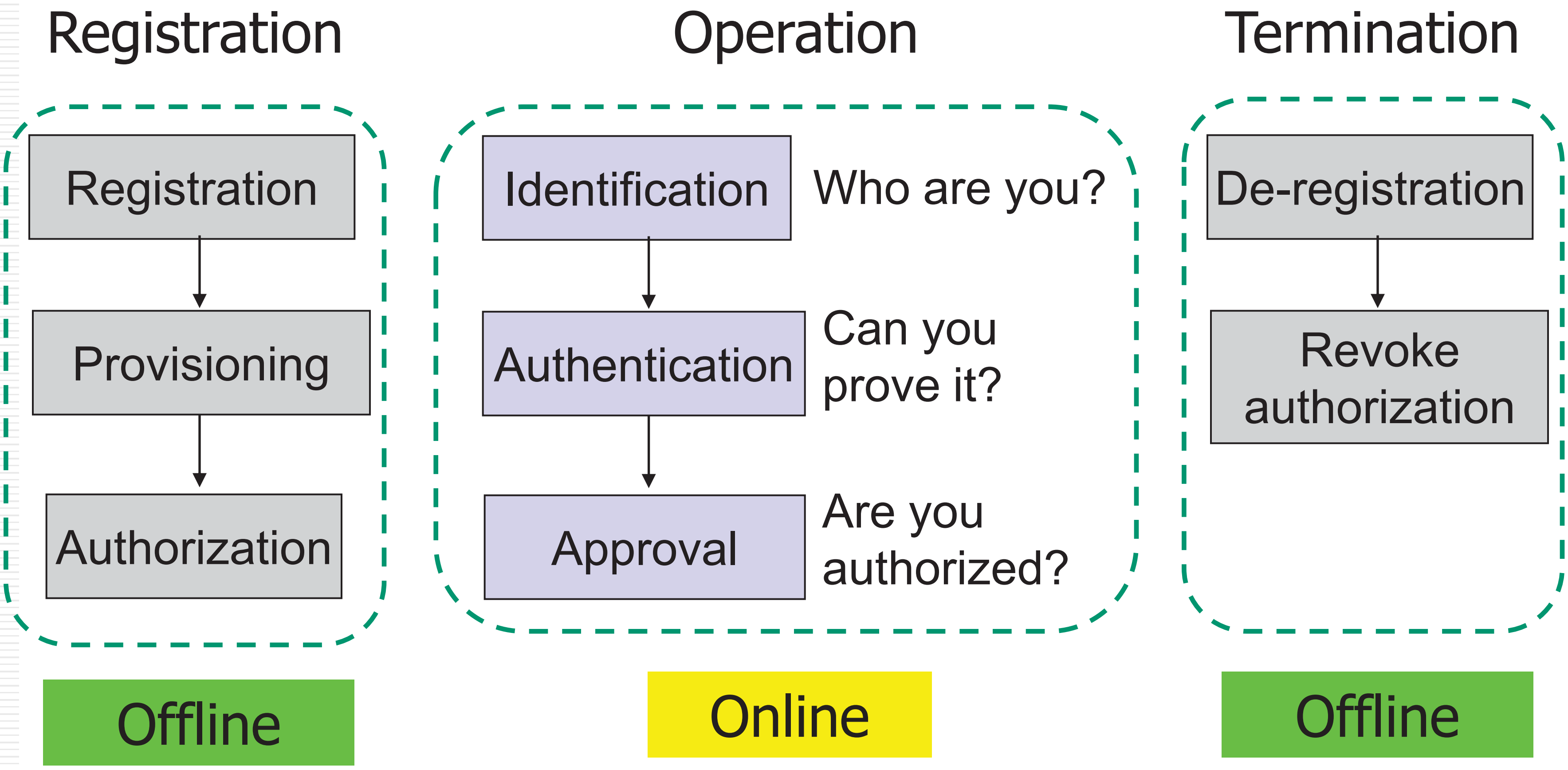
Additional security service
Non-repudiation

- Goal: Making an action undeniable through unforgible evidence.
  - Non-repudiation of origin: proof that data was sent.
  - Non-repudiation of delivery: proof that data was received.
  - NB: imprecise interpretation: Has a message been received and read just because it has been delivered to your mailbox?
- Main threats:
  - Sender falsely denying having sent message
  - Recipient falsely denying having received message
- Control: digital signature
  - Cryptographic evidence that can be confirmed by a third party

Authorization and Access Control

- To authorize is to specify access permissions for roles, individuals, entities or processes
  - Authorization policy normally defined by humans
  - Assumes the existence of an authority
- Authority can be delegated
  - Company Board → Department Manager → Sys.Admin. → User
  - Delegation can be automated by IT processes
- Implemented in IT systems as rules for access and usage
- Systems approve access based on existing authorization

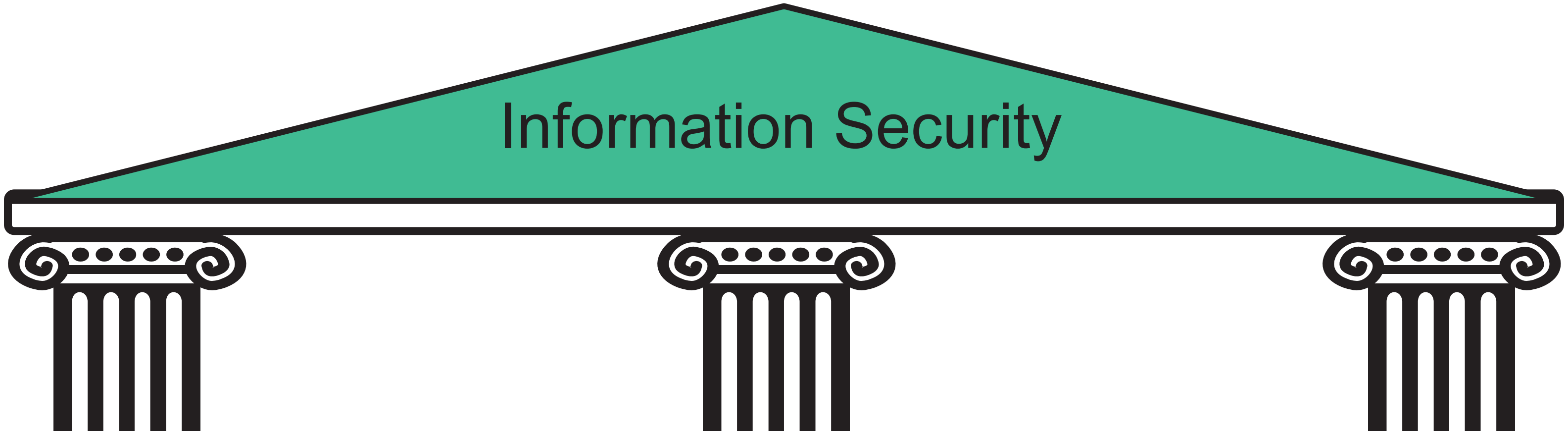
Access Control Phases



Security controls to support security services

- Information security services are provided by security controls and mechanisms.
- Examples of security control and services:
  - Ciphers (control) → provide confidentiality (service)
  - Dig.sig. (control) → provides non-repud. (service)
  - Access Control (control) → provides integrity (service)
- X.800 OSI Basic Reference Model - Security Architecture (p.15)
  - Describes correspondence between security services and some technical controls

Security control categories



Physical controls
- Facility protection
- Security guards
- Locks
- Monitoring
- Environmental controls
- Intrusion detection

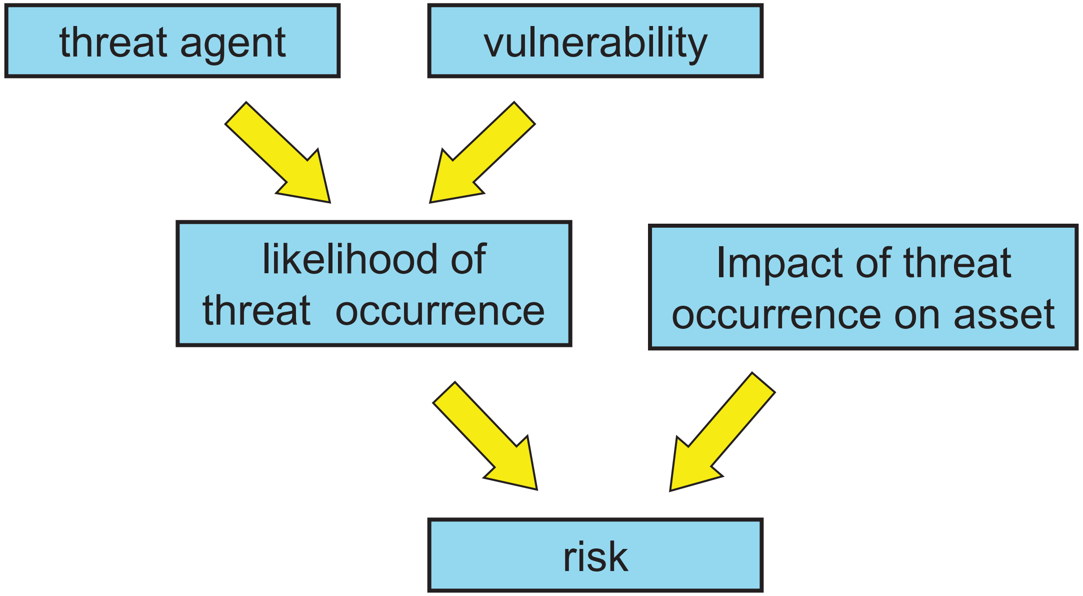
Technical controls
- Network security
- Logical access control
- Cryptographic controls
- Security devices
- User authentication
- Intrusion detection
- Forensics

Administrative controls
- Policies
- Standards
- Procedures
- Guidelines
- Personnel screening
- Awareness training

Security controls by protection phases

- Preventive controls:
  - prevent attempts to exploit vulnerabilities
    - Example: encryption of files
- Detective controls:
  - warn of attempts to exploit vulnerabilities
    - Example: Intrusion detection systems (IDS)
- Corrective controls:
  - correct errors or irregularities that have been detected.
    - Example: Restoring all applications from the last known good image to bring a corrupted system back online
- Controls from all three categories (physical, technical and administrative) as well as from all three phases are needed to have complete layered protection.

What is risk?


threat agent
vulnerability
likelihood of threat occurrence
Impact of threat occurrence on asset
risk

Risk is:

– The expected cost of the negative impact caused by a threat exploiting a vulnerability

– Risk is thus a function of the likelihood of threat and the magnitude of negative impact

Risk Management

- Controls have a cost
- Need to justify implementing controls by balancing benefits against cost of controls.
  - Complex task which needs proper management
- Risk management covers
  - Inventory of assets
  - Identification of threats and vulnerabilities
  - Analysis and evaluation of risks levels
  - Selection and implementation of controls
  - Monitoring and communication of risk

Risk Management

How much should I spend on securing ?

? Why ?

How much should I spend on securing my reputation ?

- The Proportionality Principle:
  - Identify and apply a set of controls (physical, technical and administrative controls) that match the perceived risk to, and value of, an organisation's information assets

Risk Management

- Things to think about:
  - What is the likelihood of the event occurring
    - probabilities are values between 0 and 1
  - What is the impact (loss) if the event occurs?
  - What could be done (control measures) to
    - Avoid the impact
    - Reduce the impact
  - and what does this action cost?

How do you know if a system is secure?

- You don’t
  - Kant’s philosophy: Das Ding an sich und das Ding für mich
- Systems are becoming increasingly complex
  - Impossible to know all their properties
- We can only have a subjective perception of robustness
- *Information Assurance* denotes perceived security level of information systems
  - E.g. “Assurance Level” is used to denote the level of perceived security of systems certified according to the Common Criteria
- Security assessment in practice:
  - “Information security is a well-informed assurance that information risks and controls are in balance”

Methods for obtaining information assurance

- Apply principles for secure design and development
- Let 3rd parties evaluate the security of systems
- Implement secure practices and security awareness
- Maintain compliance with regulation
- Conduct risk assessments
- Keep systems updated
- Test for vulnerabilities
- Security audits
- Constant vigilance

- Not easy

Why IS Management Standards?

Don’t invent the wheel again!

Use various standards and frameworks which provide:

- evidence of management commitment to and responsibility for IS
- assurance to other departments and organizations
- assurance to staff
- a checklist of measures

IS management standards & frameworks

- ISO 27K Security Management standards:
  - ISO 27001, 27002, 27003 etc.
- NIST (US National Institute for Standards and Technology) Special Publications SP800-X series
  - SP800-12, SP800-14, SP800-18, SP800-26 and SP800-30 etc.
- CobiT
  - Control Objectives for Information and Related Technology (CobiT)
- Information Security Forum (ISF)
  - Standard of Good Practice for Information Security
- ITIL
  - Information Technology Infrastructure Library
  - Management guidelines for IT, including IT security

Certification for IS Professionals

- Many different types of certifications available
  - Vendor neutral or vendor specific
  - Non-profit organisations or commercial for-profit organisations
- Programs and content mostly kept up-to-date
- Certification gives some credibility and advantage to
  - consultants bidding for contracts
  - individuals applying for jobs and promotion
- Sometimes required for job functions
  - US Government IT Security jobs
- Programs and contents reflect current topics in IT Security

(ISC)^2

International Information Systems Security Certification Consortium

- (ISC)^2 provides certification for information security professionals

CISSP	- Certified Information Systems Security Professional
ISSAP	- Information Systems Security Architecture Professional
ISSMP	- Information Systems Security Management Professional
ISSEP	- Information Systems Security Engineering Professional
CAP	- Certification and Accreditation Professional
SSCP	- Systems Security Certified Practitioner
CSSLP	- Certified Secure Software Lifecycle Professional

- CISSP CBK - Common Body of Knowledge
  - A set of 10 themes that a CISSP is supposed to know something about
- Costs about US$ 500 to pass exam
- CISSP is the most common IT security certification
  - Next exam in Oslo 24 March 2012, then probably in June 2012

ISACA
(Information Systems Audit and Control Association)

- ISACA provides certification for IT professionals
  - CISM - Certified Information Security Manager
  - CISA - Certified Information System Auditor
  - CGIT - Certified in the Governance of Enterprise IT

- CISM defines 5 knowledge domains:
  1. Information Security Governance
  2. Information Risk Management
  3. Information Security Program Development
  4. Information Security Program Management
  5. Incident Management

Vendor Specific Certifications

- CISCO
  - INFOSEC - Information Systems Security Professional
  - CCSP - Cisco Certified Security Professional
  - IPS Specialist - Intrusion Prevention Systems Specialist
  - Firewall Specialist
- Microsoft
  - MCSA - Microsoft Certified Systems Administrator
  - MCSE - Microsoft Certified Systems Engineer
- Linux
  - Certificates from Red Hat, IBM, HP, GIAC etc.

SANS certificates

- Certification Program of the SANS Institute
  - (**S**ysAdmin, **A**udit, **N**etworking, and **S**ecurity)
  - For-profit privately owned and operated
  - Connected to the Internet Storm Center

SANS certifications cover four IT security job disciplines:

- Security Administration
- Security Management
- IT Audit
- Software Security

Academic Forum on *Security*

- AF*Security* is IfI's monthly IT security seminar series
- Focus on current issues and research questions related to information security
- Speakers from industry, government and academia
- https://wiki.uio.no/mn/ifi/AFSecurity/
- Next AFSecurity: Wednesday 25 January 2012 at 14:00h in meeting room Awk on 3rd floor.
- All interested are welcome

Reports and Advisories

- Reports: Useful for knowing the current state of security
  - PWC: http://www.pwc.com/gx/en/information-security-survey/
  - US IC3: http://www.ic3.gov/media/annualreports.aspx
  - CSI Computer Crime & Security Survey (www.gocsi.com)
  - + many others
- Advisories: Useful for knowing threats and vulnerabilities
  - US CERT: http://www.cert.org/
  - Japan IPA: http://www.ipa.go.jp/security/english/
  - Australia AusCERT: http://www.auscert.org.au/
  - NorCERT: For government sector: https://www.nsm.stat.no/
  - NorSIS: For private sector: http://www.norsis.no/
  - + many others

Example Report webcast

websense

2012 Security Predictions

Websense Labs
Host: Tom Clare
December 2011

TRITON

- Web security
- Email security
- Data security

http://www.websense.com/content/webcast-what-security-threats-can-we-expect-in-2012-december-2011.aspx

End of Lecture