INF3510 Information Security

Lecture 01:
- Course info
- Basic concepts in information security

University of Oslo, spring 2016

Course information

- Course organization
- Prerequisites
- Syllabus and text book
- Lecture plan
- Home exam
- Assessment and exams
- Security education
- AF*Security*

Course organisation

- Course activities
  - 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 is available at:
  - http://www.uio.no/studier/emner/matnat/ifi/INF3510/v16/
  - lecture presentations, workshop questions, etc.
  - List of English security terms translated to Norwegian
- Assignment topic for home exam on:
  - https://wiki.uio.no/mn/ifi/INF3510-2016
- Various online resources
  - E.g. NIST special computer security publications http://csrc.nist.gov/publications/PubsSPs.html

Lecturer

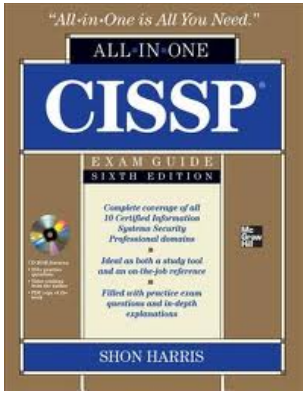
- Prof. Audun Jøsang,
- Education
  - CISSP 2005, CISM 2010,
  - PhD Information Security, NTNU, 1998
  - MSc Information Security, Royal Holloway College, London, 1993
  - BSc Telematics, NTH 1987
  - Baccalaureat, Lycée Corneille, France, 1981
- Work
  - Professor, UiO, 2008 $\rightarrow$
  - Associate Professor, QUT, Australia, 2005-2007
  - Research Leader, DSTC, Australia 2000-2004
  - Associate Professor, NTNU, 1998-1999
  - System design engineer, Alcatel, Belgium 1988-1992

Prerequisites

- Prerequisites
  - Basic computer and network technology
  - Basic mathematics
- Theoretic focus on a basic level
  - Discrete mathematics, number theory, modular arithmetic
  - Information theory
  - Probability calculus
  - Computer and network architecture

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
  6th Edition, 2013
  Author: Shon Harris
  (7th edition in May 2016)



Shon Harris

- The book covers the 10 CBK domains (Common Body of Knowledge) for the CISSP Exam (Certified Information Systems Security Professional).
- Easy to order book from amazon.com, price: US$ 50
  http://www.amazon.com/CISSP-All-One-Guide-Edition/dp/0071781749

How to use Harris' CISSP book (6th ed.)

- 1430 pages in total
  - But exclude
    - Ch.1 (Becoming a CISSP)
    - 50 pages of appendix, glossary and index
    - 300 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

Draft Lecture Plan

Week	Date	#	Topic
W04	25.01.2016	1	Course Information. Basic Concepts in IS
W05	01.02.2016	2	IS Management, Human Factors for IS
W06	08.02.2016	3	Risk Management and Business Continuity Planning
W07	15.02.2016	4	Computer Security
W08	22.02.2016	5	Cryptography
W09	29.02.2016	6	Key Management and PKI
W10	07.03.2016	7	Digital Forensics
W11	14.03.2016	8	User Authentication
W12	*Easter break*		
W13	*Easter break*		
W14	04.04.2016	9	Identity Management and Access Control
W15	11.03.2016	10	Network Security
W16	18.04.2016	11	Network Perimeter Security
W17	*No lecture*		
W18	02.05.2016	12	Development and Application Security
W19	*No lecture*		
W20	*No lecture*		
W21	23.05.2016		Review
W22	*No lecture*		
W23	08.06.2016	Digital exam, time: 09:00h - 13:00h (4 hours)	

Home Exam

- Write an essay on a security topic chosen by you
- Work individually, or in group of 2 or 3 students
- Select topic and specify group on wiki
  https://wiki.uio.no/mn/ifi/INF3510-2016/
- Length: 5000 - 10000 words (approx. 10 – 15 pages)
- Due date: 13.05.2016
- Assessment criteria:
  - Structure and presentation: weight ¼
  - Scope and depth of content: weight ¼
  - Evidence of independent research and analysis: weight ¼
  - Proper use of references: weight ¼

Assessment and Marking

- Course weight: 10 study points
- Assessment items:
  - Home exam: weight 0.4
  - Digital exam: weight 0.6
- Required to get a pass score on both assessment items
  - At least 40% on home exam and 40% on written exam
  - Relatively easy to get a high score on home exam
  - Relatively difficult to get a high score on written exam
- Academic dishonesty (including plagiarism and cheating) is actively discouraged
  - See: http://www.uio.no/english/studies/admin/examinations/cheating/
  - Should be no problem ☺

Exam statistics from previous years

Year	# students	# A (%)	# B (%)	# C (%)	# D (%)	# E (%)	# F (%)
2015	121	10 (9%)	30 (25%)	45 (37%)	9 (7%)	9 (7%)	18 (15%)
2014	103	4 (4%)	8 (7.5%)	45 (44%)	14 (13.5%)	9 (4.5%)	23 (22.5%)
2013	0	For the 2013 spring semester the course was cancelled due to faculty politics.					
2012	34	2 (6%)	6 (18%)	14 (41%)	0 (0.0%)	6 (17.5%)	6 (17.5%)
2011	70	1 (2%)	10 (14%)	33 (47%)	9 (13%)	10 (14%)	7 (10%)
2010	58	1 (2%)	15 (26%)	25 (43%)	7 (12%)	3 (5%)	7 (12%)

Other security courses at IFI

- UNIK4220: Introduction to Cryptography
  - Leif Nilsen (autumn, taught at IFI)
- UNIK4250: Security in Distributed Systems
  - Nils Agne Nordbotten (spring)
- UNIK4270: Security in OS and Software
  - Audun Jøsang (Autumn, taught at IFI)
- UNIK4740: InfoSec in Industrial Sensor and Mobile Systems
  - Judith Rossebø (autumn)
- INF5150 - Unassailable IT-systems
  - Ketil Stølen (autumn)
- ITLED4230 Ledelse av informasjonssikkerhet
  - Audun Jøsang (autumn)
  - For professionals (fee NOK 25K)

Why study information security ?

- Being an IT expert requires knowledge about IT security
  - Imagine building architects without knowledge about fire safety
- Building IT systems without considering security will lead to vulnerable IT systems
- Global IT infrastructure is vulnerable to cyber attacks
- IT experts without security skills are part of the problem !
- Learn about IT security to become part of the solution
- Information security is a political issue
  - Often seen as a cost, but saves costs in the long term
  - Often given low priority in IT industry and IT education

Certifications for IS Professionals

- Many different types of certifications available
  - vendor neutral or vendor specific
  - from non-profit organisations or commercial for-profit organisations
- Certification gives assurance of knowledge and skills,
  - needed in job functions
  - gives credibility for consultants, applying for jobs, for promotion
- Sometimes required
  - US Government IT Security jobs
- Knowledge domains reflect current topics in IT Security
  - Generally kept up-to-date

ISACA Certifications
(Information Systems Audit and Control Association)

- ISACA promotes IT governance framework COBIT
  (Control Objectives for Information and Related Technologies)

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

- CISM is the most popular ISACA security certification

CISM: Certified Information Security Manager

- Focuses on 4 domains of IS management
  1. Information Security Governance
  2. Information Risk Management
  3. Information Security Program Development and Management
  4. Information Security Incident Management

- Official prep manual published by ISACA
  - 14th edition 2016
  - https://www.isaca.org/bookstore/
    Price: US $135 ($105 for ISACA members)
  - https://www.isaca.org/bookstore/Pages/CISM-Exam-Resources.aspx

CISM Exam

- Exams normally twice per year worldwide
- Next exam in Oslo (and worldwide): June 2016
  - Deadline for registering: April 2015
  - Register for exam at www.isaca.org
  - Exam fee approx. US $500
  - Multiple choice exam
  - Requires 5 years professional experience

  - Yearly CISM maintenance fee approx. US $100
  - Requires 120 hours “practice time” per 3 years

$(ISC)^2$ Certifications

International Information Systems Security Certification Consortium

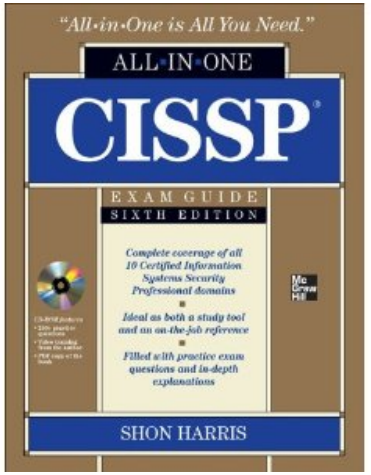
- $(ISC)^2$ provides certification for information security professionals
  - CISSP - Certified Information Systems Security Professional
  - ISSAP - Information Systems Security Architecture Professional
  - ISSMP - Information Systems Security Management Professional
  - ISSEP - Information Systems Security Engineering Professional
  - CAP - Certification and Accreditation Professional
  - SSCP - Systems Security Certified Practitioner
  - CSSLP - Certified Secure Software Lifecycle Professional
- CISSP is the most common IT security certification
  - Most IT Security Consultants are CISSP

CISSP Exam:
Certified Information System Security Professional

- Many different books to prepare for CISSP exam
- e.g. text book used for INF3510 course

  CISSP All-in-One Exam Guide
  6th Edition, 2013
  Author: Shon Harris

  (7th edition to appear in May 2016)



- € 560 fee to sit CISSP exam
- Exam through http://www.pearsonvue.com/isc2/
- Test Centre in Oslo: http://www.glasspaper.no/

  Brynsveien 12, Bryn, Oslo
- Most of the of the material presented in the INF3510 course is taken from the syllabus of the CISSP CBK (Common Body of Knowledge).

CISSP CBK (Common Body of Knowledge)
8 domains (until 2015 there were 10 domains)

1. **Security and Risk Management** (Security, Risk, Compliance, Law, Regulations, and Business Continuity)
2. **Asset Security** (Protecting Security of Assets)
3. **Security Engineering** (Engineering and Management of Security)
4. **Communication and Network Security** (Designing and Protecting Network Security)
5. **Identity and Access Management** (Controlling Access and Managing Identity)
6. **Security Assessment and Testing** (Designing, Performing, and Analyzing Security Testing)
7. **Security Operations** (Foundational Concepts, Investigations, Incident Management, and Disaster Recovery)
8. **Software Development Security** (Understanding, Applying, and Enforcing Software Security)

Security Surveys

- Useful for knowing the trend and current state of information security threats and attacks
  - CSI Computer Crime & Security Survey (http://gocsi.com/survey)
  - Verizon Data Breach Report:
    http://www.verizonenterprise.com/DBIR/
  - PWC: http://www.pwc.com/gx/en/consulting-services/information-security-survey/
  - US IC3 (The Internet Crime Complaint Center):
    http://www.ic3.gov/media/annualreports.aspx
  - Mørketallsundersøkelsen; http://www.nsr-org.no/moerketall/

  + many others

Security Advisories

- Useful for learning about new threats and vulnerabilities
  - NorCERT: For government sector: https://www.nsm.stat.no/
  - NorSIS: For private sector: http://www.norsis.no/
  - US CERT: http://www.cert.org/
  - Australia AusCERT: http://www.auscert.org.au/

  + many others

Academic Forum on Security

AF*Security*

- Monthly seminar on information security
- https://wiki.uio.no/mn/ifi/AFSecurity/
- Guest speakers
- Next AFSecurity:
  - Wednesday 27 January 2016, 14:00h
  - **Topic:**
    Bluetooth Beacon Privacy
  - **Speaker:** Atle Årnes (Datatilsynet)

- All interested are welcome !

Information Security
Basic Concepts

Good and bad translation

English

- Security
- Safety
- Certainty

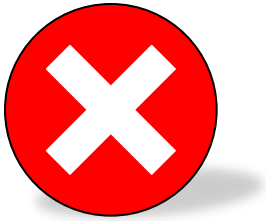
Norwegian

- Sikkerhet
- Trygghet
- Visshet

Good

- 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: your body, possessions, the environment, the nation
- Security and related concepts
  - National security (political stability)
  - Safety (health)
  - Environmental security (clean environment)
  - Information security
  - etc.

What is *Information* Security

- *Information* Security focuses on protecting *information* assets from damage or harm
- What are the assets to be protected?
  - Example: data files, software, IT equipment and infrastructure
- Covers both intentional and accidental events
  - Threat agents can be people or acts of nature
  - People can cause harm by accident or by intent
- Information Security defined:
  - The preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved. (ISO27001)

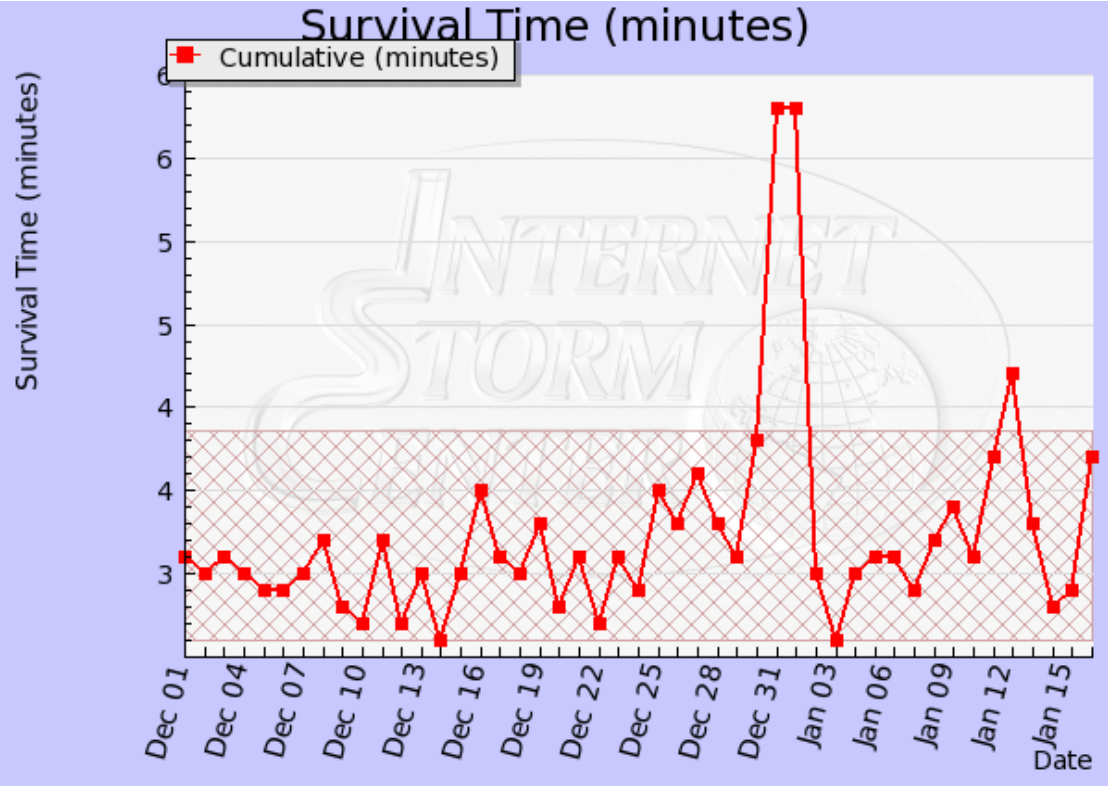
Scope of information security

- IS management has as goal to avoid damage and to control risk of damage to information assets
- IS management focuses 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 incidents (forensics)

The Need for Information Security

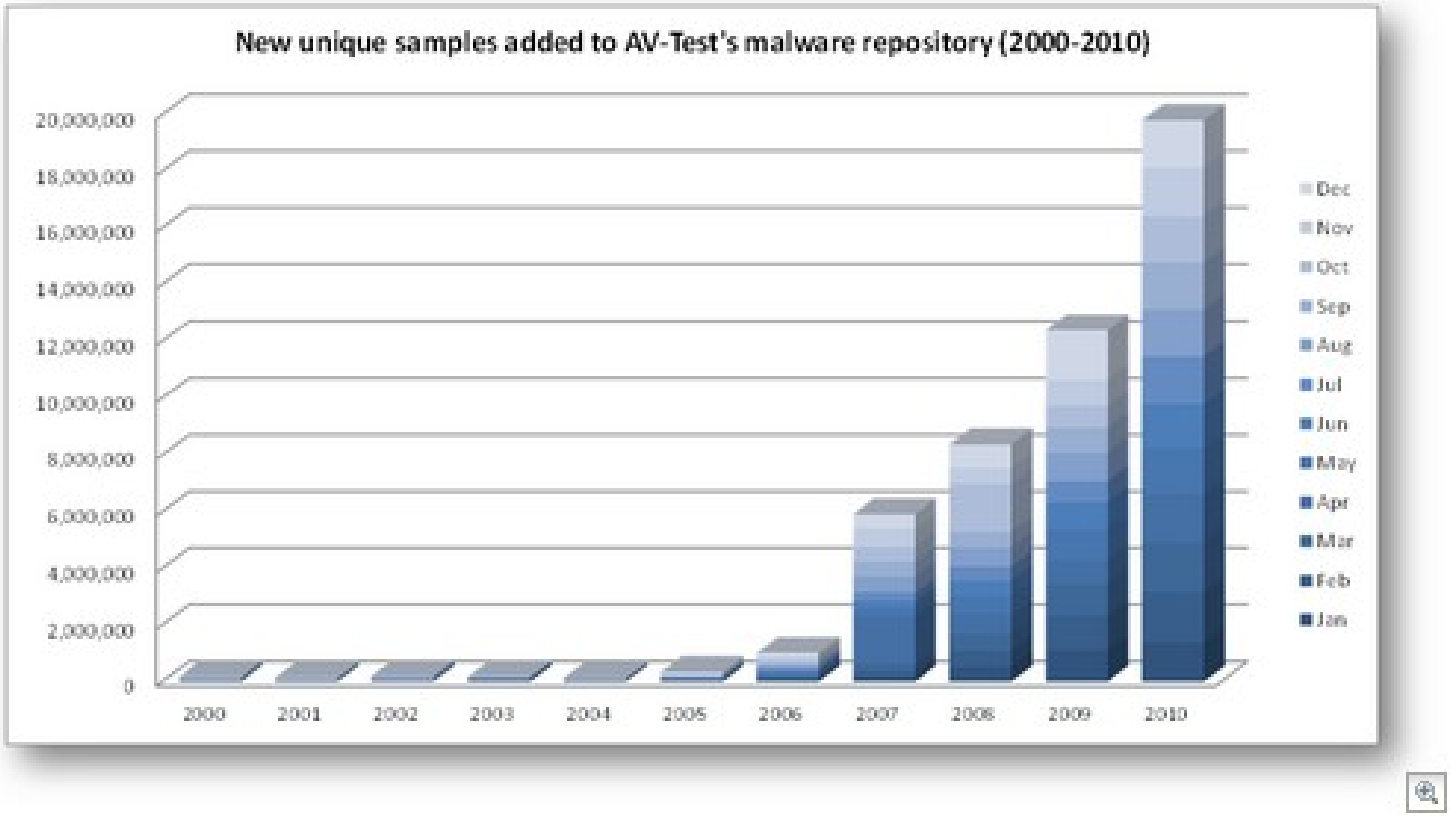
- Why not simply solve all security problems once for all?
- Reasons why that's impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New 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

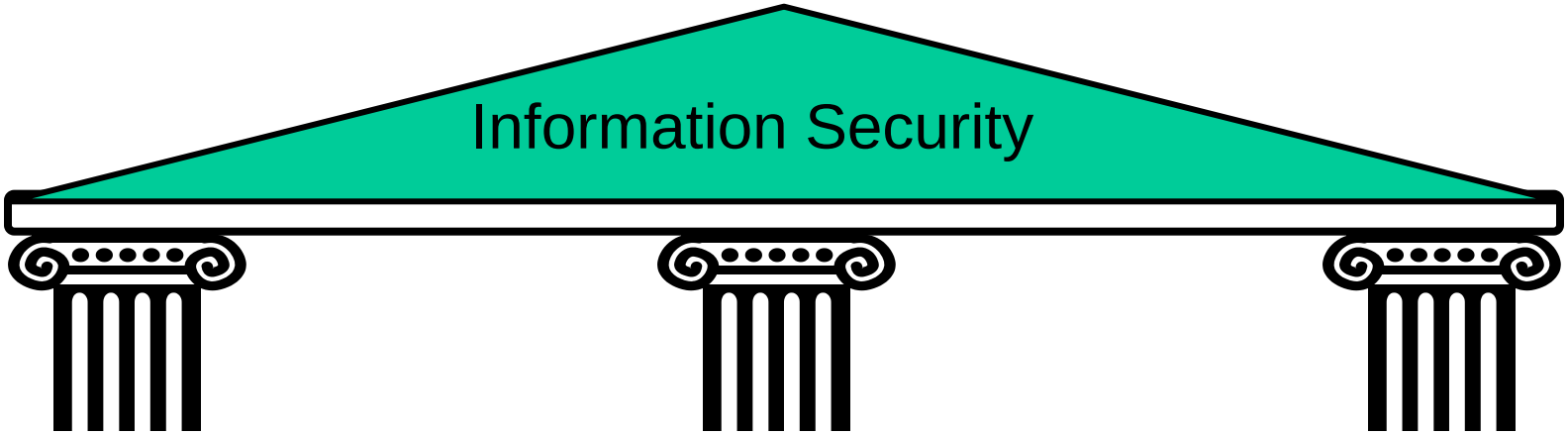


The survival time is calculated as the average time between attacks against average target IP address.
http://isc.sans.org/survivaltime.html

Malware Trend



Security control categories



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

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

Administrative controls
- Policies
- Standards
- Procedures & practice
- Personnel screening
- Awareness training

Security control functional types

- 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

- Use a combination of controls to help ensure that the organisational processes, people, and technology operate within prescribed bounds.

Controls by Information States

- Information security involves protecting information assets from harm or damage.
- Information is considered in one of three possible states:
  - During storage
    - Information storage containers
    - Electronic, physical, human

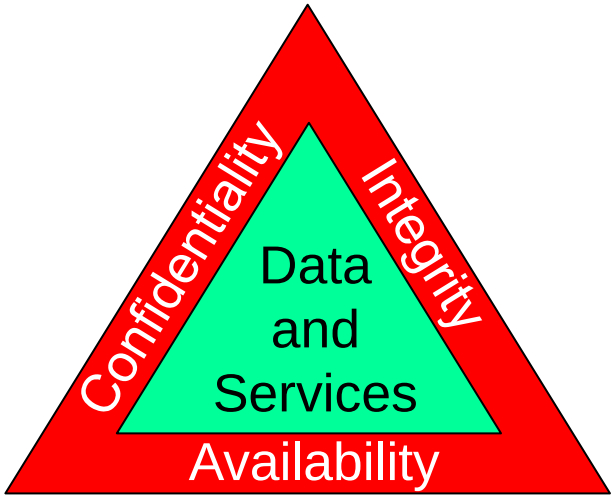
  - During transmission
    - Physical or electronic

  - During processing (use)
    - Physical or electronic

- Security controls for all information states are needed

Security Services and Properties

- A security service is a high level security property
- The traditional definition of information security is to preserve the three CIA properties for data and services:
  - **Confidentiality**:
  - **Integrity**
  - **Availability**:



- The CIA properties are the three main security services

Security services and controls

- Security services (aka. goals or properties)
  - implementation independent
  - supported by specific controls
- Security controls (aka. mechanisms)
  - Practical mechanisms, actions, tools or procedures that are used to provide security services

Security services:

e.g. Confidentiality – Integrity – Availability

support

Security controls:

e.g. Encryption – Firewalls – Awareness

Confidentiality

- The property that information is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 27001)
- Can be divided into:
  - Secrecy: Protecting business data
  - Privacy: Protecting personal data
  - Anonymity: Hide who is engaging in what actions
- Main threat: Information theft, unintentional disclosure
- Controls: Encryption, Access Control, Perimeter defence

Integrity

- **Data Integrity:** The property that data has not been altered or destroyed in an unauthorized manner. (X.800)
- **System Integrity:** The property of safeguarding the accuracy and completeness of assets (ISO 27001)
- Main threat: Data and system corruption
- Controls:
  - Cryptographic integrity check,
  - Encryption,
  - Access Control
  - Perimeter defence
  - Audit
  - Verification of systems and applications

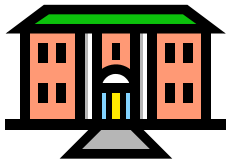
Availability

- The property of being accessible and usable upon demand by an authorized entity. (ISO 27001)
- 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

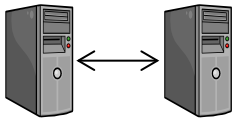
Authenticity (Security Service)

The CIA properties are quite general security services.
Other security services are often mentioned.
Authentication is very important, with various types:

- User authentication:
  - The process of verifying a claimed identity of a (legal) user when accessing a system or an application.



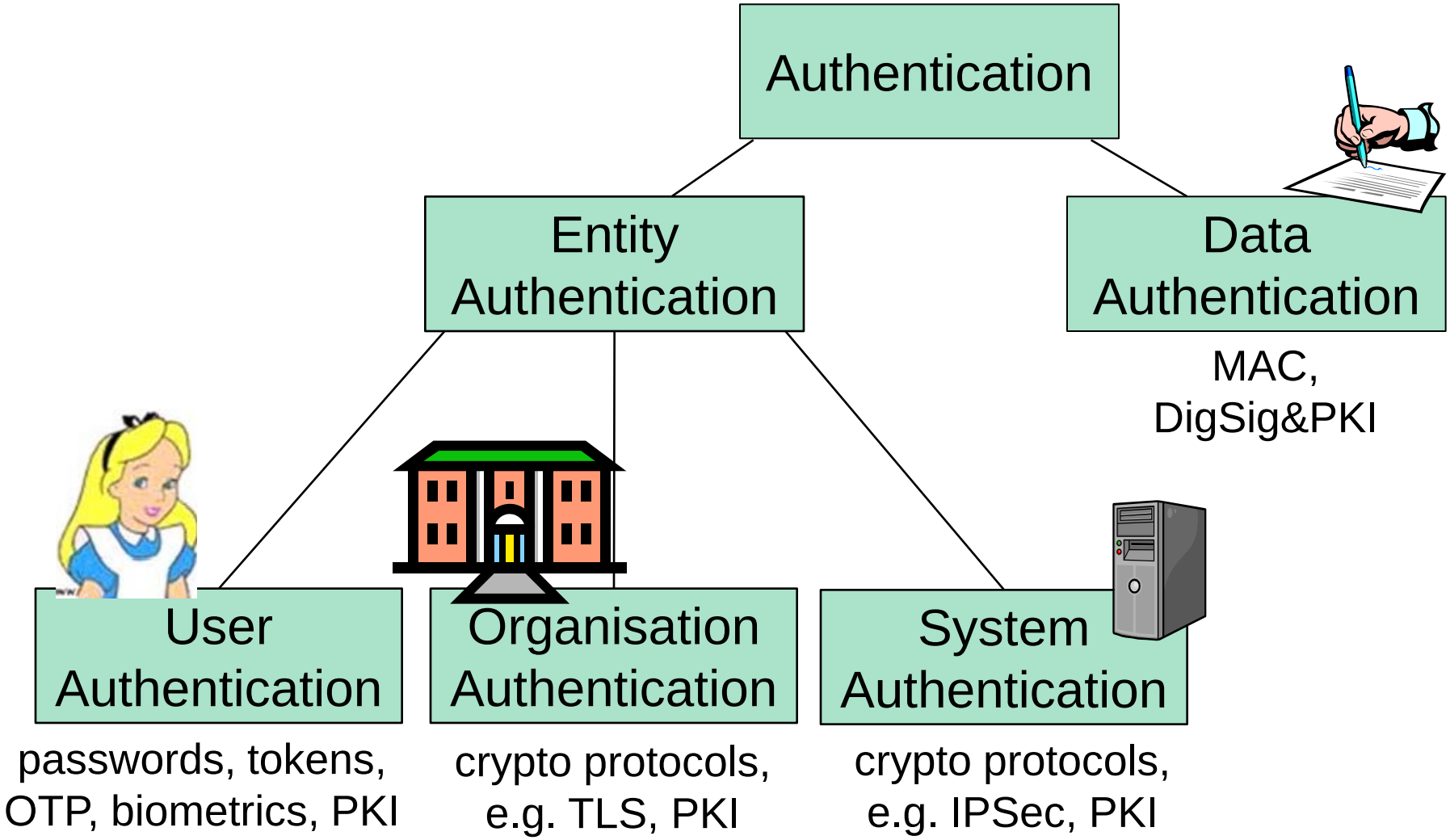
- Organisation authentication:
  - The process of verifying a claimed identity of a (legal) organisation in an online interaction/session



- System authentication (peer entity authentication):
  - The corroboration (verification) that a peer entity (system) in an association (connection, session) is the one claimed (X.800).

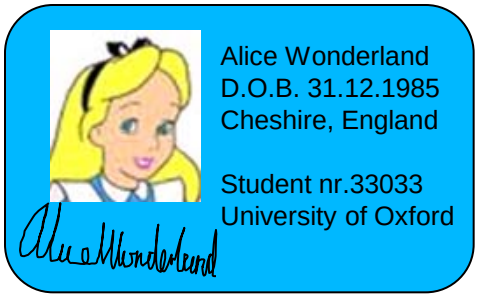
- Data origin authentication (message authentication):
  - The corroboration (verification) that the source of data received is as claimed (X.800).

Taxonomy of Authentication



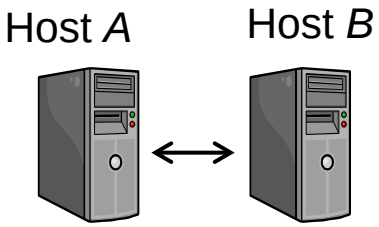
User Identification and Authentication

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



Authentication token

System Authentication



- Goal
  - Establish the correct identity of remote hosts
- Main threat:
  - Network intrusion
  - Masquerading attacks,
  - Replay attacks
  - (D)DOS attacks
- Controls:
  - Cryptographic authentication protocols based on hashing and encryption algorithms
  - Examples: TLS, VPN, IPSEC

Data Origin Authentication (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 it
- Main threats:
  - False transactions
  - False messages and data
- Controls:
  - Encryption with shared secret key
  - MAC (Message Authentication Code)
  - Security protocols
  - Digital signature with private key
  - Electronic signature,
    - i.e. any digital evidence

Non-Repudiation
(Security Service)

- Goal: Making sending and receiving messages 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
- Data origin authentication and non-repudiation are similar
  - Data origin authentication only provides proof to recipient party
  - Non-repudiation also provides proof to third parties

Accountability
(Security Service)

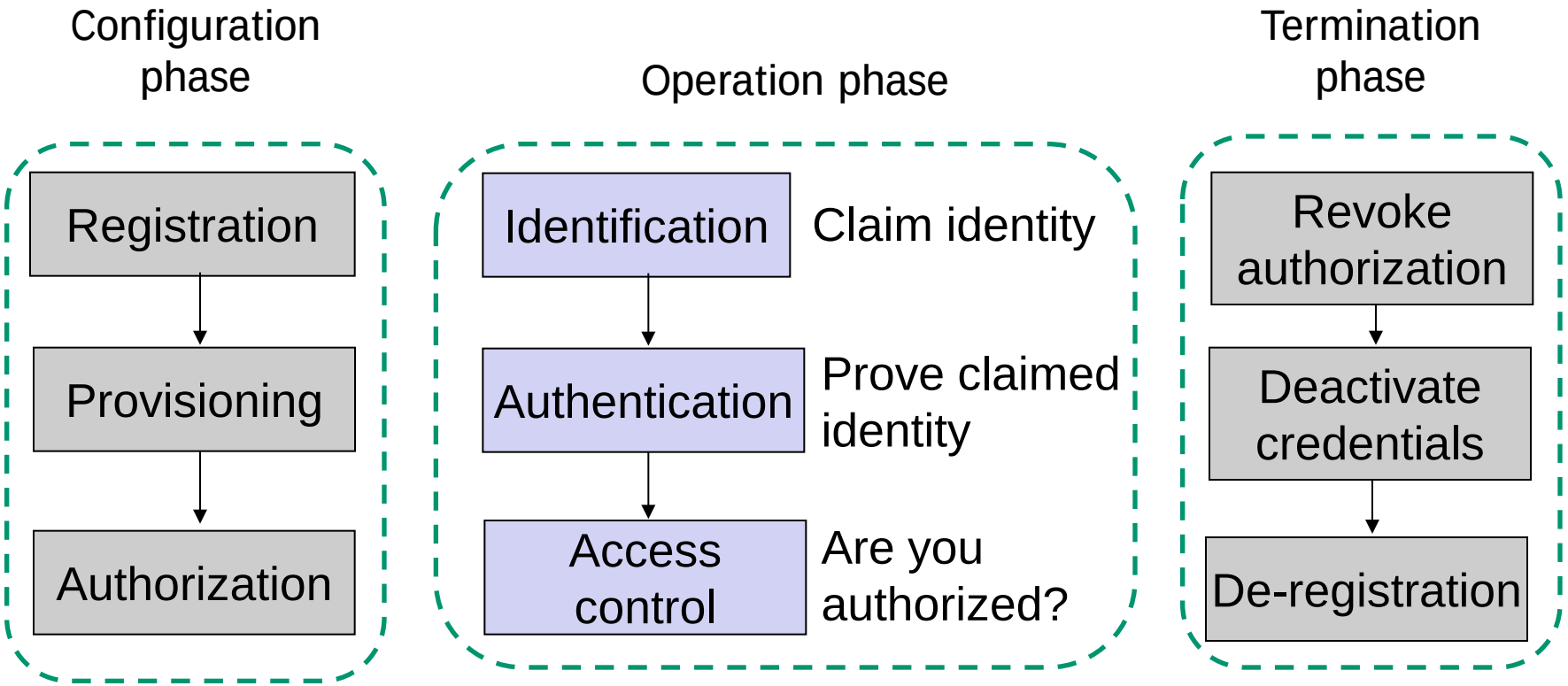
- Goal: Trace action to a specific user and hold them responsible
  - *Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party*

    (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

Authorization

- Authorization is to specify access and usage permissions for entities, roles or processes
  - Authorization policy normally defined by humans
  - Issued by an authority within the domain/organisation
- Authority can be delegated
  - Management → Sys.Admin
  - Implemented in IT systems as configuration/policy
- Beware of confusion (also in Harris text book):
  - Correct: Harris 6th ed. p.161: *"A user may be authorized to access the files on the file server, but until she is properly identified and authenticated, those resources are out of reach."*
  - Wrong: Harris 6th ed. p.161: *"If the system determines that the subject may access the resource, it authorizes the subject".*

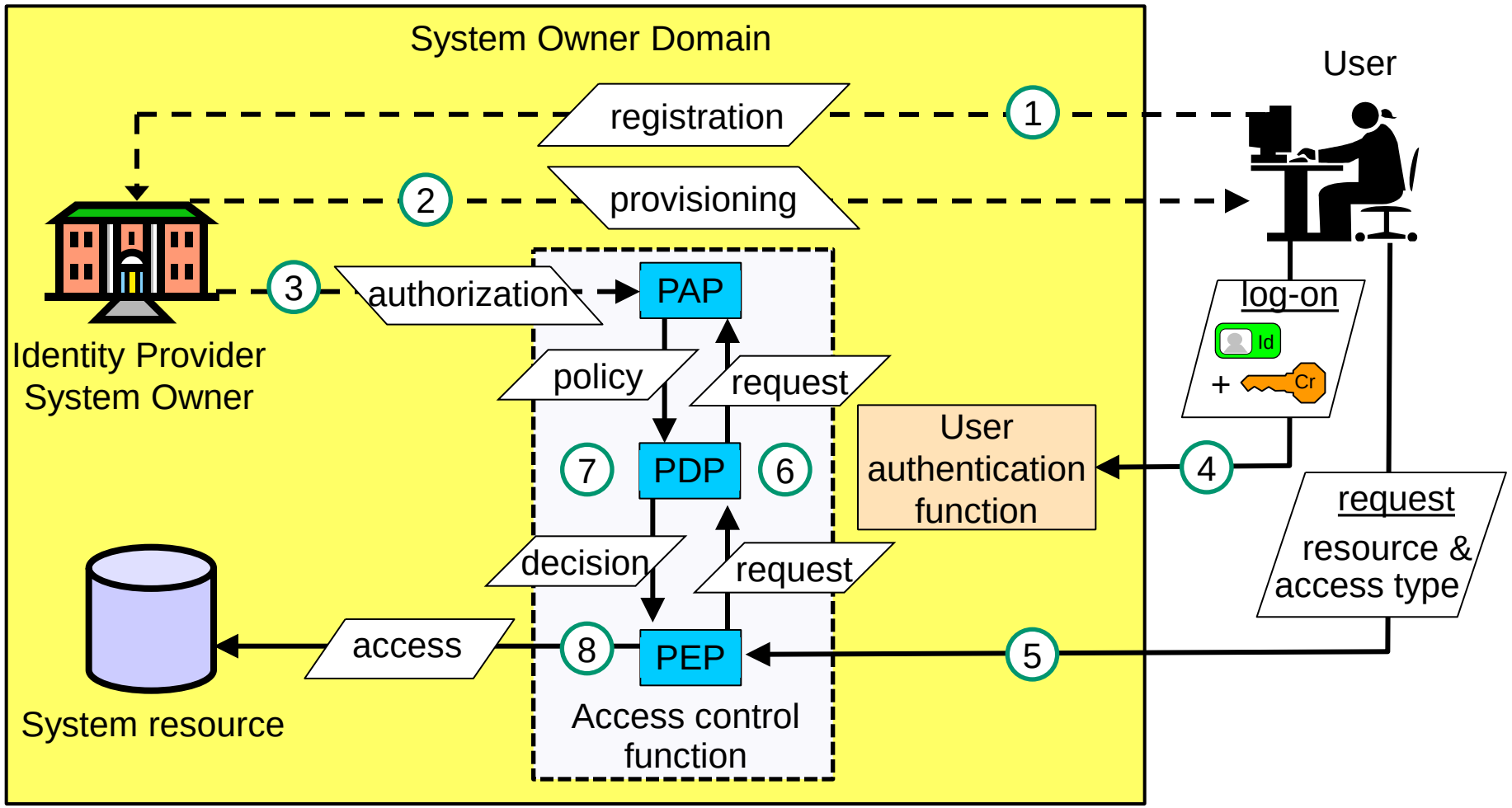
Identity and Access Management (IAM) Phases



Confusion about Authorization

- The term “authorization” is often wrongly used in the sense of “access control”
  - e.g. *“If the system determines that the subject may access the resource, it **authorizes** the subject”* (e.g. Harris 6th ed. p.161)
  - Common in text books and technical specifications (RFC 2196 …)
  - Cisco AAA Server (Authentication, Authorization and Accounting)
- Wrong usage of “authorization” leads to absurd situations:
  1. You get somebody’s password, and uses it to access account
  2. Login screen gives warning: *“Only authorized users may access this system”*
  3. You are caught and taken to court
  4. You say: *“The text book at university said I was authorized if the system granted access, which it did, so I was authorized”*

Identity and Access Management Concepts



PAP: Policy Administration Point

PDP: Policy Decision Point

PEP: Policy Enforcement Point

IdP: Identity Provider

Registration

Operations

End of lecture