INF3510 Information Security
University of Oslo
Spring 2010

Lecture 1

Course Information

Background and Basic Concepts

Course information

- Scope of information security
- Syllabus and text book
- Lecture plan
- Prerequisites
- Course organization
- Obligatory assignment

- Remember to register attendance during break today!

Scope of information security

- Information assets are vulnerable to threats
- Threats can be intentional or accidental
- Threats can cause considerable damage
- 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

- Formal requirements:
  - Matematikk R1 *or* Matematikk (S1+S2)
  - or equivalent from other institutions
- Theoretical material used
  - Discrete mathematics, number theory, modular arithmetic
  - Information theory
  - Probability calculis
  - 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 obligatory assignment
    - 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
- Various online resources
  - NIST special computer security publications
    http://csrc.nist.gov/publications/PubsSPs.html

Course Assessment

- Course weight: 10 study points
- Assessment:
  - Assignment: 40%
  - Final examination: 60%
- Academic dishonesty (including plagiarism and cheating) is actively discouraged, see
  - http://www.uio.no/english/academics/examinations/cheating.html

Course Staff

- Lecturer:
  - Prof Audun Jøsang
- Group teachers:
  - T.B.D
- 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
- Group teacher or lecturer
  - workshop questions and lecture material
- 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: Principles of Information Security
  by Michael E. Whitman and Herbert J. Mattord
  3rd Edition, Pub.: January 2008

- The book is relatively general, usually does not go into great detail, and mostly focuses on security management
- 75 copies of the text book have been ordered to Akademika

Lecture Plan

Week	Date	#	Topic
W04	25.01.2010	1	Course Information. Background and Basic Concepts
W05	01.02.2010	2	Cryptography
W06	08.02.2010	3	Key Management and PKI
W07	15.02.2010	4	Authentication
W08	22.02.2010	5	Security Models and Access Control
W09	01.03.2010	6	Communication Security
W10	08.03.2010	7	Identity and Access Management
W11	15.03.2010	8	Perimeter Security
W12	22.03.2010	9	Physical Security and the Human Factor
W13	*No lecture*		
W14	*No lecture*		
W15	12.04.2010	10	Computer Security and Trusted Systems
W16	19.04.2010	11	Application Security and Trust Management
W17	26.04.2010	12	Security Management and Security Development
W18	03.05.2010	13	Risk Management and Disaster Recovery
W19	10.05.2010	14	Privacy and Forensics
W20	?	15	Review
W21	*No lecture.*		
W22	04.06.2010	Exam time: 14:30h - 17:30h	

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 of 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

Obligatory Assignment

- Chose any topic in the area of information security
  - Suggestions available on the wiki website
- Work in groups of 2 or 3. Individual assignment also OK.
  - Specify group and topic by 1 March 2010.
- Write in English or Norwegian.
  - Length: between 5000 and 10000 words.
- To be written like a scientific article, including references.
  - See info about scientific writing: http://owl.english.purdue.edu/owl/
- Use LaTeX or MSWord.
- Hand in (online) by 5 May 2010.

Obligatory Assignment

- Select a topic related to information security
  - Can be freely chosen
  - A list of topics provided online
  - Other topics can be specified
  - All topics must be different, but similar is OK
- To be written in groups of 2 or 3. Individually also OK
  - Select topic and form groups by 22.03.2010
- Planned self registration of topic and group on wiki
  - https://wiki.uio.no/mn/ifi/INF3510
- Hand in online by 10.05.2010
- Counts 40%

Other security courses

Offered at the UNIK University Graduate Center

http://www.uio.no/studier/emner/matnat/unik/

- UNIK4220 – Introduction to Cryptography (autumn)
  - Leif Nilsen (Thales)
- UNIK4250 – Security in Distributed Systems (spring)
  - Audun Jøsang (UNIK) 2010
  - N.N. ? 2011 →
- UNIK4270 – Security in Operating Systems and Software (autumn)
  - Line Borgund (FFI) → 2009
  - N.N.? 2010
- UNIK4720 Trust and Reputation Systems
  - Audun Jøsang (UNIK),
  - Spring 2011

Information Security Background and Basic Concepts

Additional material for this lecture

- Whitman
  - Ch.1 p.1-19.
  - Ch.2 p.37 – 81
- X.800 *Security Architecture for Open Systems Interconnection*
  - Definitions of concepts

Norwegian terms

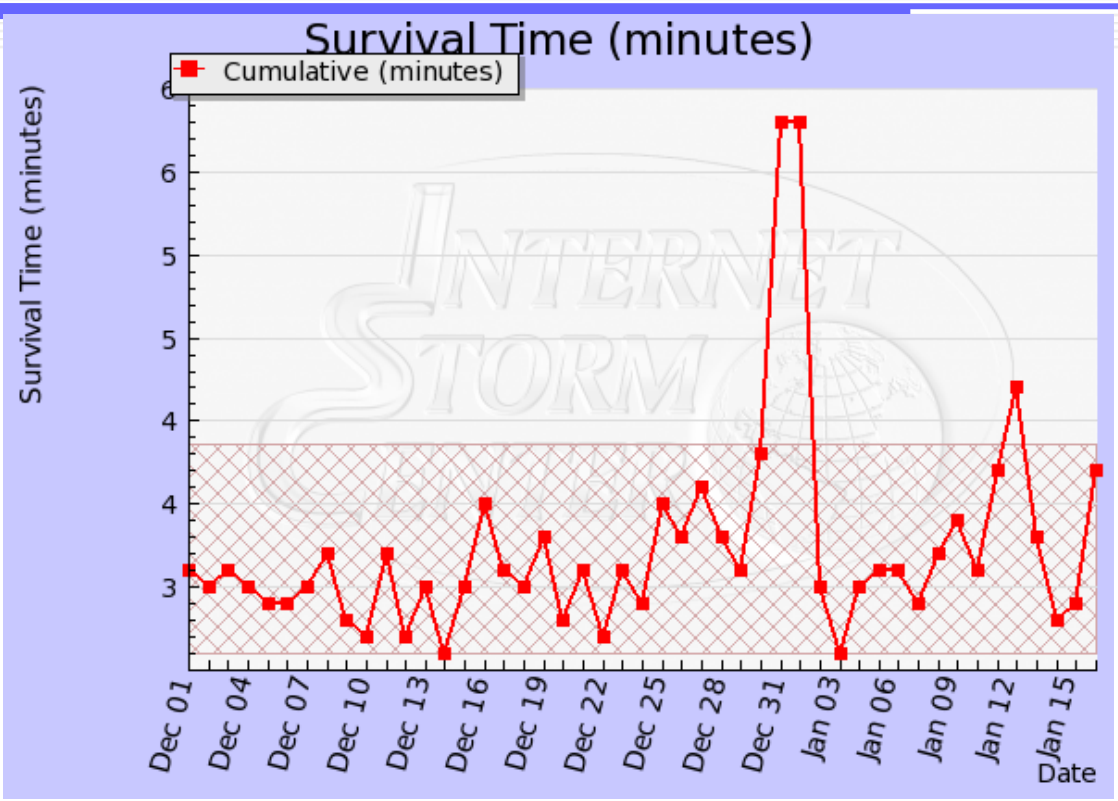
English		Norwegian
• Security • Safety • Certainty	→	• Sikkerhet

• Security	→	• Sikkerhet
• Safety	→	• Trygghet
• Certainty	→	• Visshet

The Need for Information Security

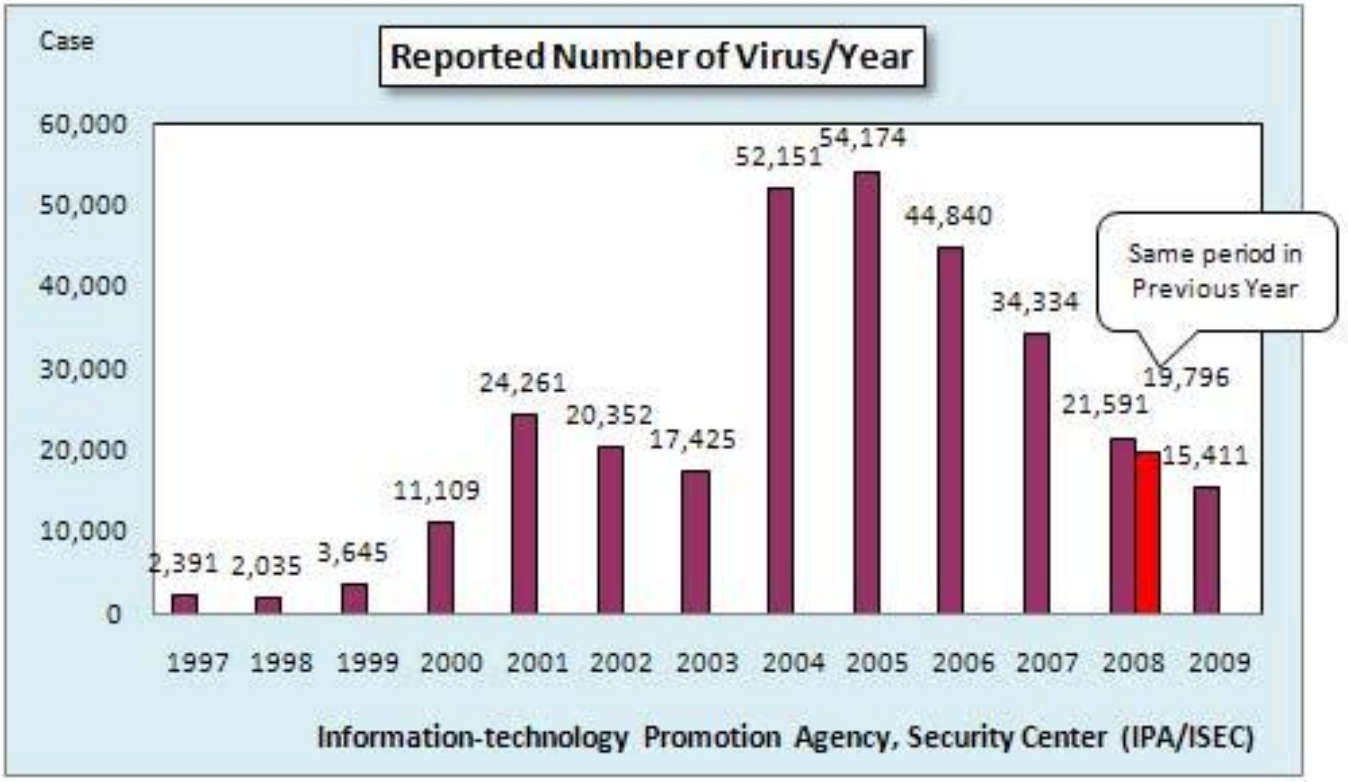
- Why not simply solve all security problems once for all?
- Reasons why that's impossible:
  - Rapid innovation constantly generates new technology with new vulnerabilities
  - More activities go online
  - Crime follows the money
  - Information security is a second thought when developing IT
  - New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

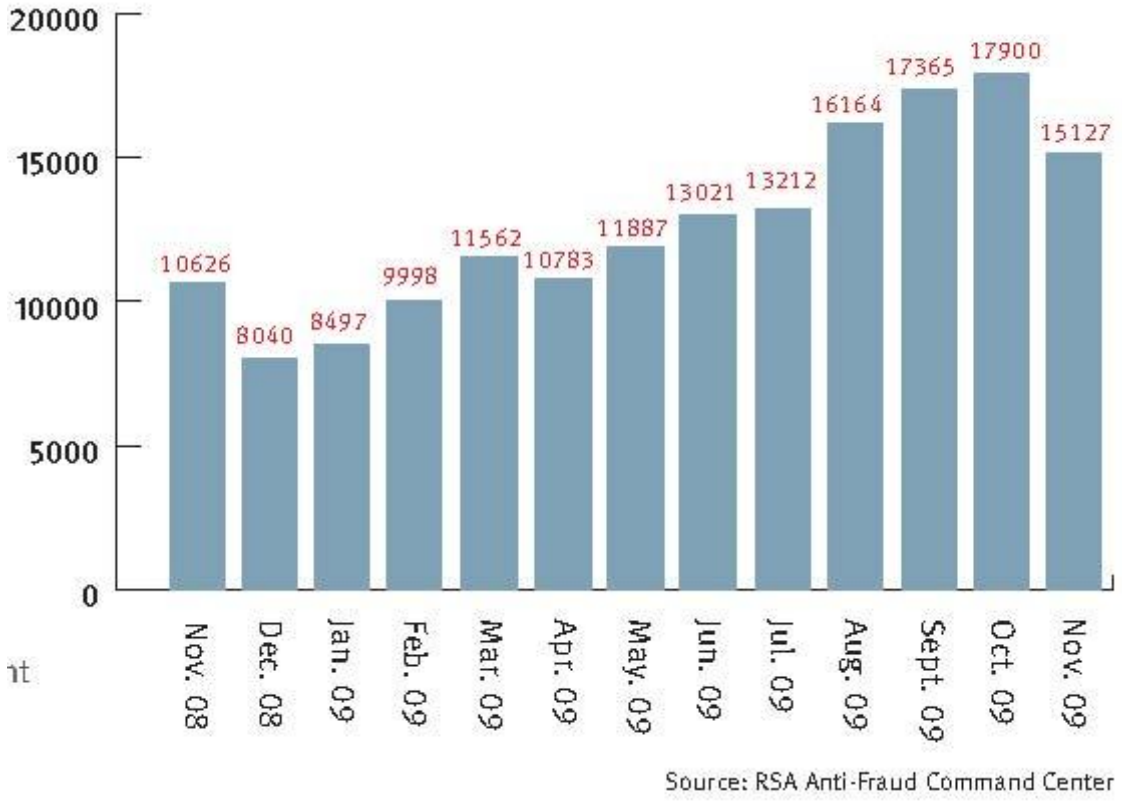


The survival time is calculated as the average time between reports for an average target IP address.
http://isc.sans.org/survivaltime.html

Virus Trend


Case
Reported Number of Virus/Year
60,000
50,000
40,000
30,000
20,000
10,000
0
2,391
2,035
3,645
11,109
24,261
20,352
17,425
52,151
54,174
44,840
34,334
21,591
19,796
15,411
Same period in Previous Year
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
Information-technology Promotion Agency, Security Center (IPA/ISEC)

Phishing Attack Trend



Information Security

- Issues:
  - damages `hidden' but mounting
  - organised cyber-crime is increasing
  - identity theft is major growth crime
  - 1 billion online users, 2 billion by 2015
- Urgent need for information security knowledge/expertise and research:
  - at the long-term infrastructure level,
  - at application development level
  - at the operations level
  - at the management level
  - at the national and international level

National Security

- Many critical components of nations depend on IT
  - Critical Infrastructure Protection
- Many IT systems are by themselves critical components
  - Critical Information Infrastructure Protection
- The accumulated set of non-critical systems (e.g. servers and networks in SMEs) becomes critical
- IT systems become increasingly complex
  - Difficult to detect vulnerabilities
- IT systems are targets (and weapons) of attack in industrial, political and international conflicts
- The vulnerability of the critical information structure is worrisome and needs attention

Information systems components

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

- Information systems involve
  - Hardware
  - Software
  - Data
  - People
  - Procedures
  - Physical buildings

Security

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

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 equipment and infrastructure
- Consider intentional and accidental events
  - Threat agents can be people or acts of nature
  - People can cause harm by accident or by intent
- Consider:
  - Prevention of damage to information assets
  - Detection of damage to information assets – when, how, who?
  - Reaction – to recover from damage

Rules for Right or Wrong

- The term ”harm” assumes that there is a difference between doing right or wrong, defined by rules such as:
- Law and regulation, e.g.
  - US HIPAA 1996, regulates protection of personal health information
  - 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

Authorization

- To authorize is to specify access and usage permissions for roles, individuals, entities or processes
  - Authorization policy normally defined by humans
  - Assumes the existence of an authority
  - (correct usage of term e.g. p.342 in Whitman)
- 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
- *Authorization management* is as about efficient implementation of authorization policies
  - Essential for managing information security within organizations

Confusion about Authorization

- The term “authorization” is often wrongly used in the sense of “access control”
  - e.g. *“to get authorized the user must type the right password”*
  - Common in text books literature (p.5, 46, 276, 279 in Whitman)
  - Specifications (RFC 2196 …)
  - Cisco AAA Server (Authentication, Authorization and Accounting)
- Wrong usage of “authorization” leads to absurd situations:
  1. You steal somebody’s password, and access his account
  2. Login screen gives warning: *“Only authorized users may access this system”*
  3. You get caught for illegal access and prosecuted in court
  4. You say: *“The text book at university said I was authorized if I typed the right password, which I did, so I was authorized”*

Authorization and Access Control

- Authorization defines policy
  - Specifies access and usage rights
  - Example: Political agreements between nations authorizes to travel between them.

- Access control enforces policy
  - Verifies claim and access requests
  - Example: Border police verifies that travellers are entitled to entry before they pass the border.
  - Access control is not to authorize, it uses the authorization policy to make access decisions

High Level Security Properties and Goals

- The traditional definition of information security is to have preservation of the three CIA properties:
  - **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

Additional Security Goals and Services

The CIA properties 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
- Non-repudiation:
  - create evidence that an action has occurred, so that the user cannot falsely deny the action later
- Access and Usage Control:
  - enforce that all access and usage happen according to policy

Information States

- Information security involves protecting information assets from harm or damage.
- Information is considered in one of three possible states:
  - Storage
    - Information storage containers – electronic, physical, human
  - Transmission
    - Physical or electronic
  - Processing (Use)
    - Physical or electronic

Vulnerabilities, Threats and Attacks

- Vulnerability: Weakness in a system that could allow a threat to cause harm
- Threat: Set of circumstances with the potential to cause harm
  - can compromise security goals
  - made possible through the presence of vulnerabilities
- Attack: Deliberate attempt to realise one or several threats
  - by exploiting vulnerabilities

Vulnerabilities, Threats and Attacks

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

Information Security - Threats

- Four high level classes of threats:
  - 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

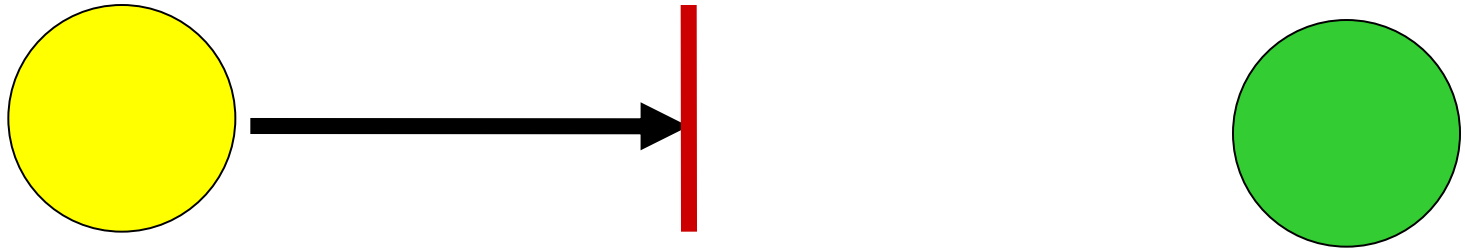
Threats:
Normal information flow

Information Source

Information Destination

Threats: Interruption

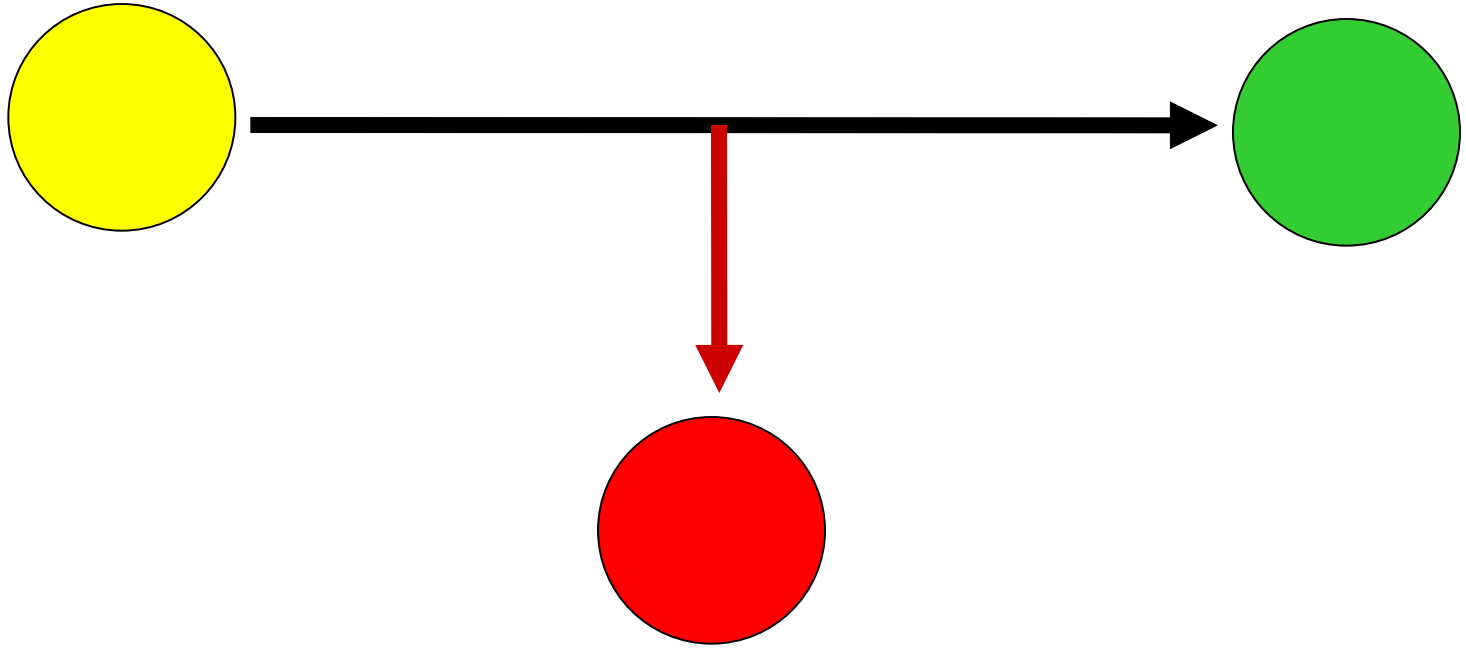
your assets become unavailable



Attack on availability

Threats: Interception

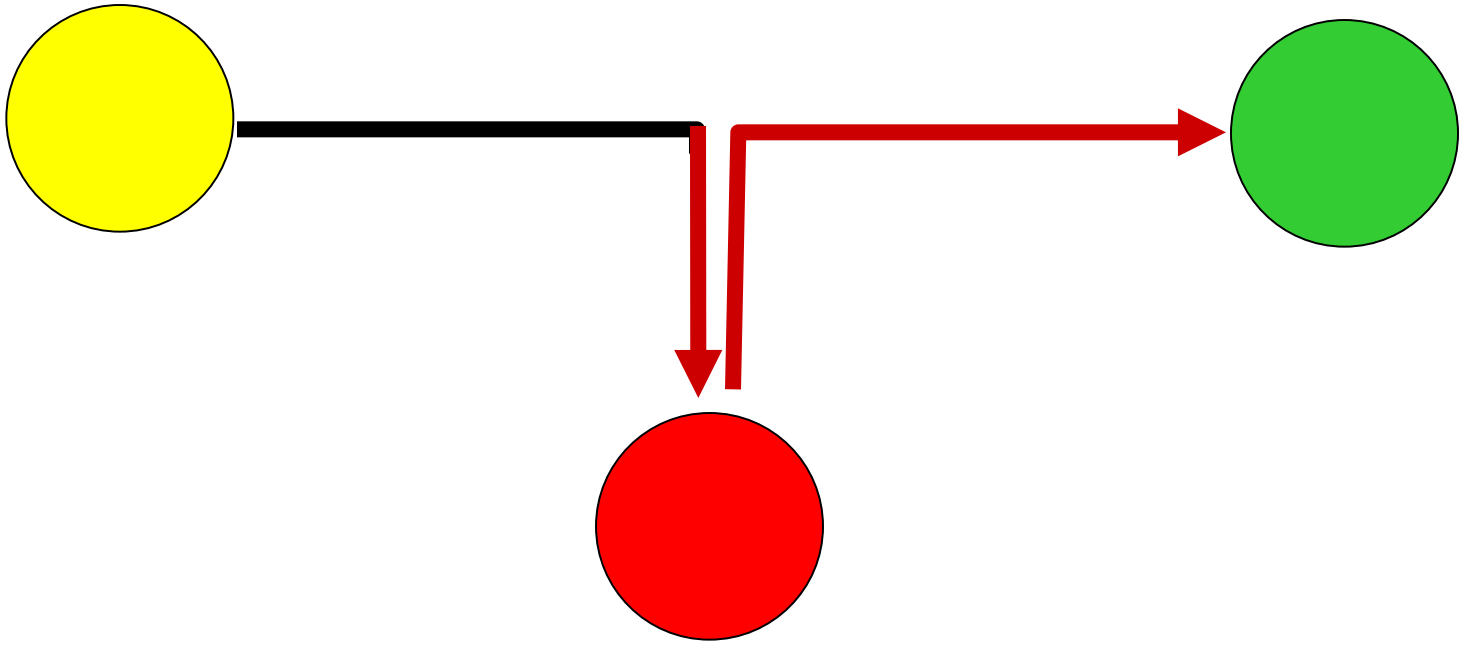
some unauthorised party has gained access to your assets



Attack on confidentiality

Threats: Modification

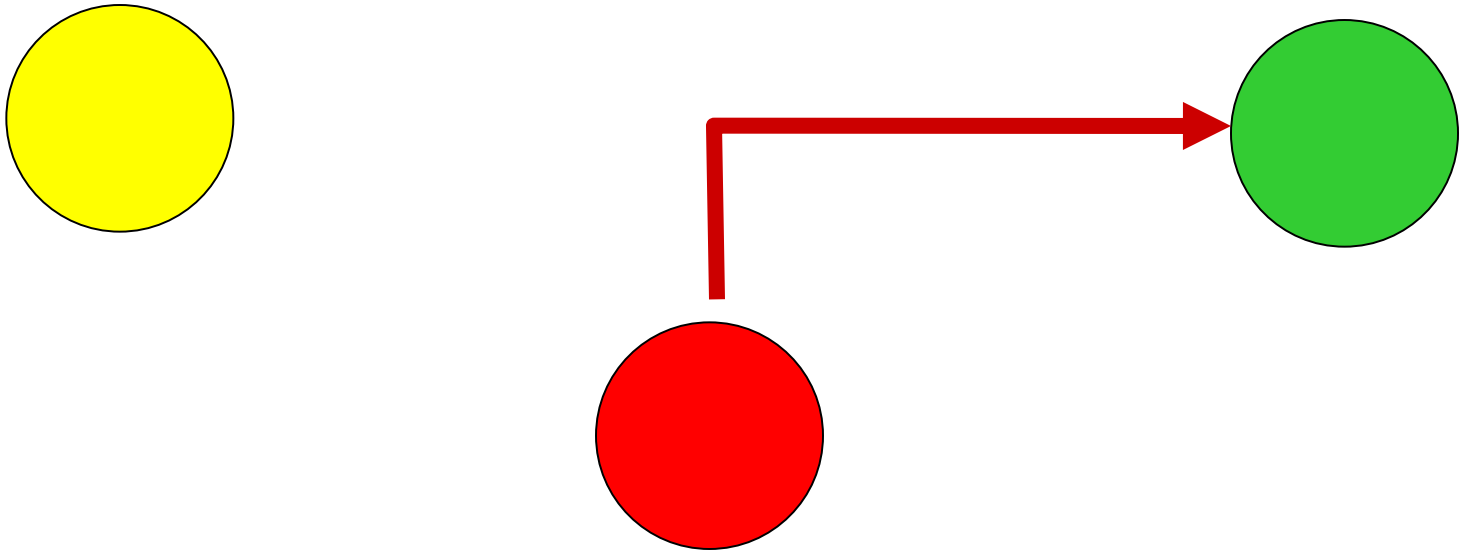
some unauthorised party tampers with your assets



Attack on integrity

Threats: Fabrication

unauthorized copies of your assets are made



Attack on authenticity

Information Security: Attacks

- Two types of attacks:
  - 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

Mechanism support of services

- Information security services and goals are achieved through security mechanisms and controls.
- Examples of security mechanisms and services:
  - Ciphers (mech.) → confidentiality (serv.)
  - Dig.sig. (mech.) → non-repud. (serv.)
  - AC rules (mech.) → integrity (serv.)
- ISO 7498.2 OSI Basic Reference Model - Security Architecture
  - Aka. CCITT Recommendation X.800 (1991)
  - Describes service – mechanism correspondence

Security Controls

- 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 the three types of controls to help ensure that the organisational processes, people, and technology operate within prescribed bounds.

Security Controls

- Technology based controls:
  - Use of ciphers, digital signatures
  - Firewalls, IDS
  - Trusted systems, tamper-resistant systems
- Management based controls:
  - Information security policy
  - Procedures for handling information security
  - Employee training e.g. against social engineering

Risk Management

- Need to justify the controls to be used by weighing up benefits gained against their cost.
- Risk management covers
  - Identification
  - Analysis
  - Evaluation
  - Treatment
  - Monitoring and
  - Communication

  of risk

Risk Management

- Everyday risks:
  - Crossing the road
  - Driving to work
  - Buying food from a vending machine
- Question: What is risk?
- Answer:
  - The likelihood of a threat exploiting a vulnerability, resulting in a negative impact
  - The expected cost of the negative impact caused by a threat exploiting a vulnerability

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?

Risk Management

How much should I spend on securing  ?




?

Why ?

How much should I spend on securing my reputation ?

Risk Management

- The Proportionality Principle:
  - Identify and apply a set of controls (protective mechanisms and procedures) which match the perceived risk to, and value of, an organisation's information assets

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* is a recent concept that better reflects that we necessarily have an imperfect insight into the security of information systems
  - E.g. "Assurance Level" is used to denote the level of perceived security of systems certified according to the Common Criteria
- "Information security is a well-informed assurance that information risks and controls are in balance" (p.3 book)

Methods for obtaining information assurance

- Apply principles for secure design and development
- Evaluate the security of a system before buying
- Keep systems updated
- Manage security by having a *security organisation* within an organisation
- Implement secure practices and security awareness
- Test for vulnerabilities
- Security audits
- Constant vigilance

- Not easy

IS Management Standards: Why?

For organisations anywhere in the world, information security management is based on relevant ISM standards. These standards provide:

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

ISO 27K Series

- ISO27001
  - *Information Security Management System (ISMS) requirements*
- ISO27002
  - *Code of practice for information security management*
- ISO27003 (not yet published)
  - *Implementation guidance for ISO/IEC 27001*
- ISO27004
  - *Information security management measurement*
- ISO27005
  - *Information security risk management*

Well structured, but you have to buy them.

Popular e.g. in Europe, Japan, Australia.

27002 Topics 1-6

1. Risk assessment
2. Security policy
   - management direction
3. Organization of information security
   - governance of information security
4. Asset management
   - inventory and classification of information assets
5. Human resources security
   - security aspects for employees joining, moving and leaving an organization
6. Physical and environmental security
   - protection of the computer facilities

27002 Topics 7-12

7. Communications and operations management
   - management of technical security controls in systems and networks
8. Access control
   - restriction of access rights to networks, systems, applications, functions and data
9. Information systems acquisition, development and maintenance
   - building security into applications
10. Information security incident management
   - anticipating and responding appropriately to information security breaches
11. Business continuity management
   - protecting, maintaining and recovering business-critical processes and systems
12. Compliance
   - ensuring conformance with information security policies, standards, laws and regulations

NIST Standards/Publications

- Many different publications, e.g.
  - SP800-12 *An Introduction to Computer Security: The NIST Handbook*
  - SP800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*
  - SP800-18 *Guide for Developing Security Plans for Federal Information Systems*
  - SP800-27, *Engineering Principles for Information Technology Security*
  - SP800-30, Risk Management Guide for Information Technology Systems
- http://csrc.nist.gov/publications/PubsSPs.html
- Available for free
- Popular in USA
- Provide a well of information

IETF RFC2196 - Site Security Handbook

- The handbook is a guide to developing computer security policies and procedures for sites that have systems on the Internet. The purpose of this handbook is to provide practical guidance to administrators trying to secure their information and services. The subjects covered include policy content and formation, a broad range of technical system and network security topics, and security incident response.

- http://tools.ietf.org/html/rfc2196

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
  - Consultants
  - 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

$(ISC)^2$ CISSP CBK 1 - 5

1. Access Control
   - Categories and Controls
   - Control Threats and countermeasures
2. Application Security
   - Software Based Controls
   - Software Development Lifecycle and Principles
3. Business Continuity and Disaster Recovery
   - Planning Response and Recovery Plans
   - Restoration Activities
4. Cryptography
   - Signatures and Certification
   - Cryptanalysis
5. Information Security and Risk Management
   - Policies, Standards, Guidelines and Procedures
   - Risk Management Tools and Practices

$(ISC)^2$ CISSP CBK 6 - 10

6. Legal, Regulations, Compliance and Investigation
   - Major Legal Systems
   - Regulations, Laws and Information Security
7. Operations Security
   - Media, Backups and Change Control Management
   - Controls Categories
8. Physical (Environmental) Security
   - Layered Physical Defense and Entry Points
   - Site Location Principles
9. Security Architecture and Design
   - Trusted Systems and Computing Base
   - System and Enterprise Architecture
10. Telecommunications and Network Security Network Security
    - Concepts and Risks
    - Business Goals and Network Security

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.

GIAC
Global Information Assurance Certification

- 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

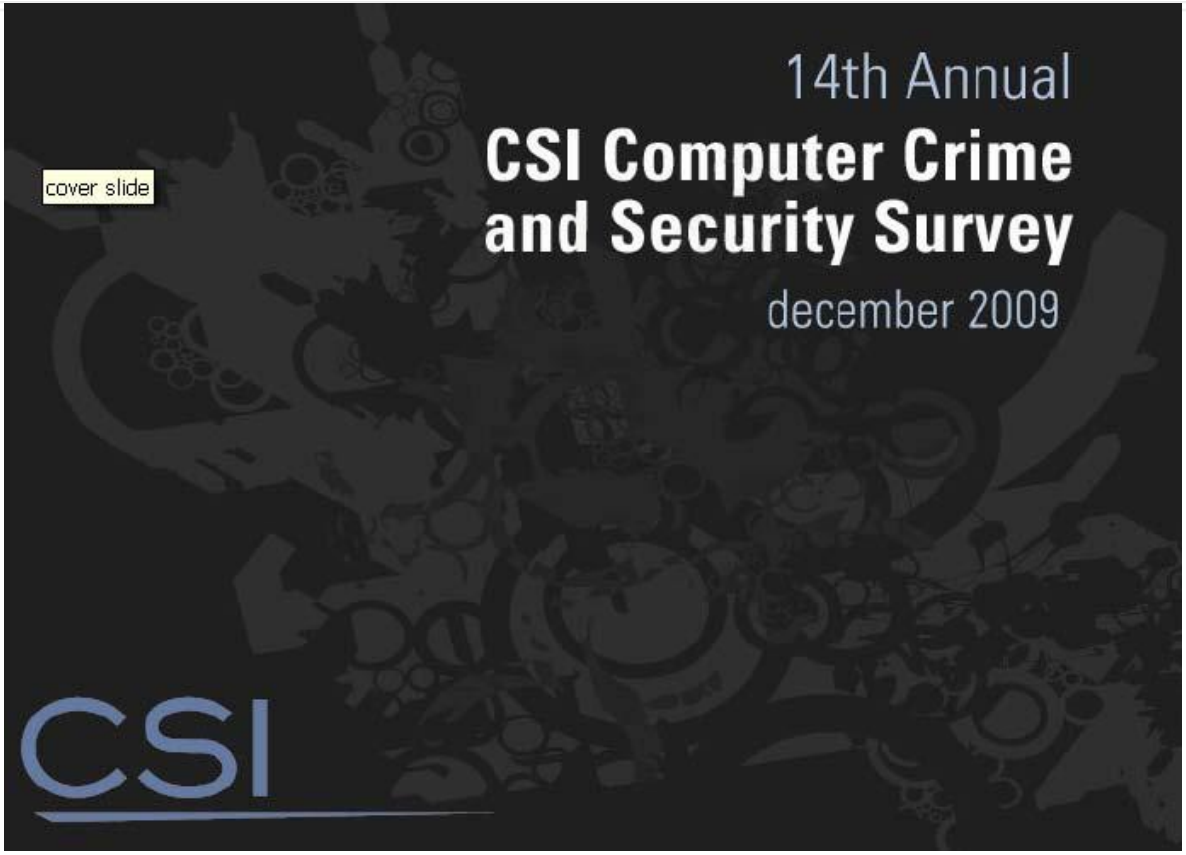
GIAC certifications cover four IT security job disciplines:

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

Surveys and Advisories

- Surveys: Useful for knowing the current state of security
  - CSI Computer Crime & Security Survey (www.gocsi.com)
  - IPA/ISEC (Information Technology Promotion Agency Japan)
  - PWC: http://www.pwc.com/gx/en/information-security-survey/
  - US IC3: http://www.ic3.gov/media/annualreports.aspx
  - + 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 Survey



- www.gocsi.com