# Security Standards

## Information Security

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 4

# Outline

# Two Schools of Security Standards

Security-driven (security evaluation standards) focuses on a system or product, and aims to prevent every threat (cost is not addressed). Formal and low-level approach is common.

- Orange Book – USA, work started 1967
- ITSEC – EU 1995
- Common Criteria – ISO 15048 in 1999

Business-driven (risk and security management standards) focuses on the business processes, seeing Information Systems as an integral part of the organisation. Information assets are valued relative to the business process where they are used, and secured as appropriate given their use and their value.

Examples: **ISO 27000-series, NIST 800-XX**

# Outline

# The Common Criteria

- International standard
  - verification and classification of security properties
  - accreditation for products and for systems
- Builds on and unites previous, national standards (1980s and before)
- International treaties govern the authority to verify to standard
- Standard compliance is sometimes a requirement for government contract
  - very little used in industry

*Why aren't Common Criteria used more in industry?*

# Provable security

*Provable security refers to work on formal (mathematical and logical) security models, and formal proofs to argue that given products and system have given security properties.*

- 1970s: great optimism and belief in the potential of provable security
- The Bell-LaPadula model
- The Multics operating system
  - designed to satisfy the Bell-LaPadula model
- Public-Key cryptography (late 70s onwards)
  - proving equivalence of hard problems
  - algorithmic complexity and hardness

# Wasn’t security provable after all?

- Multics grew out of hand
  - very little acceptance
  - many people left the project and created Unix instead
    - Simple and usable rather than secure
- Controversy around the security models
  - e.g. Bell-LaPadula allows a system without constraints
  - it gives a system to manage constraints
    - but no guidance on what constraints to create

# Successes of Provability

- Formal methods and proof techniques have had successes:
  - Cryptography
  - Security Protocols
- Clear formal models can be formalised
  - Employ theory of mathematics, logic, and computability
- Proofs become possible
- Especially cryptography is a well-studied area
  - well-trusted solutions

# Limitations of Cryptographic Methodology

## Side Channel Attacks as an example

- Take RSA as an example
  - encrypt: $c = m^e \mod n$
  - decrypt: $m = c^d \mod n$
- Simple mathematical problem
  - we assume that the attacker knows $c$, $e$, and $n$
  - prove that he cannot learn $m$ nor $d$ without factoring $n$ which is known to be hard
- In mathematics, the proof is clear.
- Implementation can break the assumption
  - measure power consumption, heat emission, or time taken for the CPU
    - concepts which do not exist in maths
  - leaks information about $d$

*Formal techniques work well on small, well-defined problems. They break easily in a more complex context.*

# Security Evaluation Standards

- Security Evaluation Standards (like Common Criteria) build on the 1970s philosophy of security
- Highest assurance level is
    - formally verified design and tested
- Security properties have to be verified without regard to
    - relevant threats
    - associated risks
    - cost of the evaluation
- Complexity drives the cost
- The evaluation process may work well on well-constrained and critical subsystems

# Outline

# Evolution of Information Systems

- The complexity of information systems is every increasing
- Typical number of lines of code increase ten-fold per decade
    - brain cells don’t
- Early systems were
    - specialised – affecting few people or departments
    - simple (1000 loc) and could be scrutinised exhaustively
- Modern systems are
    - enormous – millions of lines of code
    - ubiquitous – accumulating *every* piece of information
        - affecting every area of the business

*Security has to be relative to the business operation.*

# ISO 27000

## Overview of the series

ISO/IEC 27000:2009 Overview and vocabulary

ISO/IEC 27001:2005 Information security management systems (ISMS) — Requirements

ISO/IEC 27002:2005 Code of practice for information security management

ISO/IEC 27003 ISMS implementation guidance

ISO/IEC 27004 Information security management — Measurement

ISO/IEC 27005:2008 Information Security Risk Management

ISO/IEC 27006:2007 Requirements for bodies providing audit and certification of ISMS

ISO/IEC 27007 Guidelines for ISMS auditing

ISO/IEC 27011 (telecommunications; based on ISO/EIC 27002))

# ISO 27000

## Overview of the series

ISO/IEC 27000:2009 Overview and vocabulary

ISO/IEC 27001:2005 Information security management systems (ISMS) — Requirements

ISO/IEC 27002:2005 Code of practice for information security management

ISO/IEC 27003 ISMS implementation guidance

ISO/IEC 27004 Information security management — Measurement

ISO/IEC 27005:2008 Information Security Risk Management

ISO/IEC 27006:2007 Requirements for bodies providing audit and certification of ISMS

ISO/IEC 27007 Guidelines for ISMS auditing

ISO/IEC 27011 (telecommunications; based on ISO/EIC 27002))

# ISO 27000

## Overview of the series

ISO/IEC 27000:2009 Overview and vocabulary

ISO/IEC 27001:2005 Information security management systems (ISMS) — Requirements

ISO/IEC 27002:2005 Code of practice for information security management

ISO/IEC 27003 ISMS implementation guidance

ISO/IEC 27004 Information security management — Measurement

ISO/IEC 27005:2008 Information Security Risk Management

ISO/IEC 27006:2007 Requirements for bodies providing audit and certification of ISMS

ISO/IEC 27007 Guidelines for ISMS auditing

ISO/IEC 27011 (telecommunications; based on ISO/EIC 27002))

# ISO 27000

## Overview of the series

- ISO/IEC 27000:2009 Overview and vocabulary
- ISO/IEC 27001:2005 Information security management systems (ISMS) — Requirements
- ISO/IEC 27002:2005 Code of practice for information security management
- ISO/IEC 27003 ISMS implementation guidance
- ISO/IEC 27004 Information security management — Measurement
- ISO/IEC 27005:2008 Information Security Risk Management
- ISO/IEC 27006:2007 Requirements for bodies providing audit and certification of ISMS
- ISO/IEC 27007 Guidelines for ISMS auditing
- ISO/IEC 27011 (telecommunications; based on ISO/EIC 27002))

# Information Security Management System

*ISO 27001 explains how to set up an information security management system*

- System = Organsiation or Organisational Framework
- Learn security management from the standard
    - even if you do not have the resources to comply fully

# Establish the ISMS

## ISO 27001 Section 4.2.1

- Define scope and boundaries
- ISMS policy
- Risk assessment approach
- Identify the risks
- Analyse and evaluate risks
- Options for risk treatment
- Control objectives and controls for risk treatment
- Management approval for residual risks
- Authorisation for implementation and operation of ISMS
- Statement of Applicability

*Very formalised procedure – allow certification*

# Identifying risks

4.2.1 d)

1. Identify assets (within the scope of the ISMS)
2. Identify threats to those assets
3. Identify vulnerabilities that might be exploited by the threats
4. Identify impacts (on those assets of losses of CIA )

# How can you used the ISO 27000 standards

- Two ways

1. As a textbook on security management and risk management
    - How do you assess security needs
    - How do you formulate requirements
    - How do you validate and authorise approaches
2. As a standard for certification
    - Certification gives assurance to your customers
    - Compliance is guaranteed for the world to see

- State of the Art(?)
- Best industry practice

# Outline

# NIST 800 series

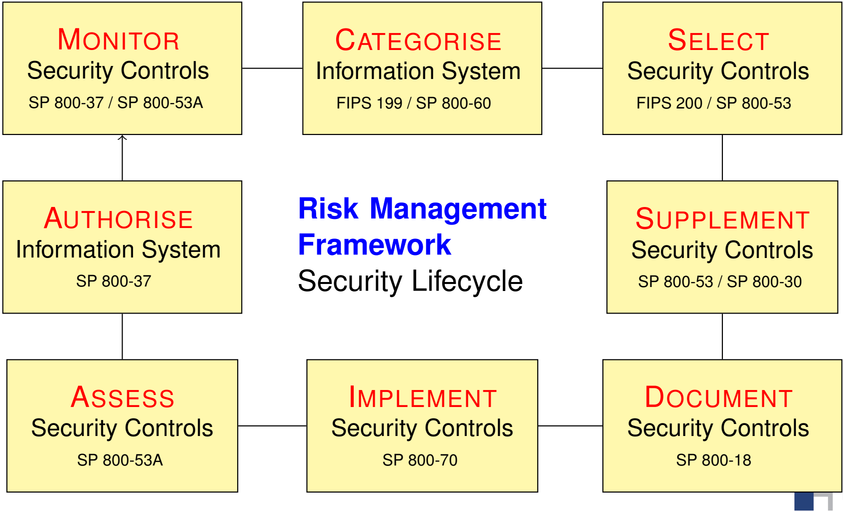
- National Institute of Standards and Technology
    - U.S. Department of Commerce
- No international standard
- Open documents — available world wide
    - good source of advice
    - by organisations that have invested money in good practice

# NIST 800-53

- Focus on controls
  - as opposed to focus on risks as in ISO 27000
- Includes a catalog of controls
- Classification of controls

*We will return to this when we discuss controls.*

# NIST 800-53 Information Security Life Cycle



Monitor
Security Controls
SP 800-37 / SP 800-53A

Categorise
Information System
FIPS 199 / SP 800-60

Select
Security Controls
FIPS 200 / SP 800-53

Authorise
Information System
SP 800-37

**Risk Management Framework**
Security Lifecycle

Supplement
Security Controls
SP 800-53 / SP 800-30

Assess
Security Controls
SP 800-53A

Implement
Security Controls
SP 800-70

Document
Security Controls
SP 800-18

# Risk Management Guide

## NIST 800-30

- Risk Management Guide
    - read this for next week ...
- Generally similar ideas to ISO 27000

# Outline

# The range of security

- Many agencies – government and otherwise
    - same situation in most countries
- Different mandates
    - overlapping mandates
- Illustrates how ill-defined security is

*What is the difference between security and safety?*

# Security versus Safety

- Security Services — Health and Safety
  - Sikkerheitstenesta — Helse, Miljø og Sikkerheit
- Different agencies focus on
  - Information security
  - Security of physical infrastructure
  - Safety (life and health)
  - Crime preventation and response
  - Accident and catastrophe response

*I'll try to sort and structure the list of agencies from the book.*

# Datatilsynet

- Independent ombudsman role
- Watchdog for data privacy legislation
  - *Personopplysingslova*

# Nasjonal Sikkerhetsmyndighet

## National Security Authority

- National, Civilian Security Agency
- Security in Government Administration (Statsforvaltninga)
    - under Minister of Defence since 1965
- NSM established 1 Jan 2003
    - Transferred duities and some personell from FO/S
        - Forsvarets Overkommando/Sikkerhetsstaben
        - Defence Central Command/Security Staff
- Remaining services within the Defence became
    - Forsvarets Sikkerhetsavdeling (FSA)

# Responsibilities of NSM

- Development of security measures (fagmyndighet)
- Check compliance to regulations (tilsynsmyndighet)
- This includes
  - Gather and assess information relevant to preventive security operations
  - Develop technical and administrative controls
  - Produce crypto solutions
  - Provide information, advice, and guidance
- NorCERT – Computer Emergency Response Team
- SERTIT – Certifaction authority

*Focus on computer and information security*

# Direktoratet for Samfunnssikkerhet og Beredskap

*Focus goes beyond computers and information ...*

- Life, health and environment
- Accidents, catastrophes and other undesired events
  - During peace, crisis and war
- Assessment of vulnerability/fragility (sårbarheit)

# Sårbarhetsutvalget

- Project group(s)
  - last one completed 4 July 2000
- Assessment of the state of the nation
  - security and vulnerability
- Recommendations across all sectors
  - reorganisations
  - new functions
  - et cetera

# Police Departments

- Kripos (Criminal Investigation Centre) — Datakrimavdelinga
  - Datainnbrot (computer break-in)
  - Databedrageri (computer fraud)
  - Informasjonsheleri (information fencing)
  - Skadeverk (sabotage)
  - Ulovleg bruk av datakraft (unauthorised use of computer resources)
  - Dokumentfalsk (forgery)
  - Piratkopiering (piracy)
  - Beskyttelsesbrot – radio/TV
- Økokrim (Economic Criminal Investigation Unit)
  - originally created the computer crime squad
- PST — Police Intelligence

# Kredittilsynet/Finanstilsynet

## Financial Services Authority

*Financial Services are particular targets for fraud and forgery.*

- Information Security becomes a focus for
  - Specialist national authorities
  - Branch organisations
- Finanstilsynet – Financial Services Authority
- Industry fora like
  - Forsikringsselskapenes Godkjennelsesnemnd (FG)
  - Næringslivets Sikkerhetsråd

# Academic centres and competency clusters

- Gjøvik kunnskapspark/«Bluelight»/Security Value
  - Høgskulen på Gjøvik covers many areas of information security
  - Norsk senter for informasjonssikring (NorSIS)
- SINTEF and UNINETT ... orignal host for NorSIS
  - SINTEF has branches dedicated to various areas of security and safety
- Selmersenteret (University of Bergen)
  - Mathematical cryptography; some systems security
  - Some interesting critisisms against current state of the art