



TEKNILLINEN KORKEAKOULU

---

# Security Standards Evaluating Security



# Security Standards

---

- Standards exist for
  - Security components
  - Organization's capabilities and processes
  - People's skills
- Most standards include a certification process
- Besides the certification, many standards provide sensible frameworks and useful practices
  - Sometimes the certification brings much work and few benefits
- Several standards for different areas of security are presented here



# TCSEC, "Orange Book"

---

- The "first" security standard, presented here due to its historical significance
- Trusted Computer System Evaluation Criteria
  - By the US government, 1983 - 1999
    - No longer in use
- Sets six different evaluation classes
  - From C1 (lowest) through C2, B1, B2, B3 to A1 (highest)
- Important concepts
  - TCB, Trusted Computing Base
  - Reference validation mechanism
    - Verifies access for multilevel and multilateral security
- Focus is on operating systems



# TCSEC Classes

---

- D, has not passed the evaluation
- C1, discretionary protection
- C2, controlled access protection
- B1, labeled security protection
- B2, structured protection
- B3, security domains
- A1, verified protection



# TCSEC Functional Requirements

---

- Functional requirements are the requirements that the finished *product* has
  - Concern the result of the process
- Discretionary access control (DAC)
- Mandatory access control (MAC)
  - B1 and upwards
  - Bell-LaPadula -like multilevel security, with the \*-property
- Label requirements
  - B1 and upwards
  - For MAC
  - Both subjects and objects labeled



# More TCSEC Functional Requirements

---

- Object reuse requirements
  - Memory and disk sector contents should not be transmitted to a new user
- Identification and authentication requirements
- Trusted path requirements
  - B2 and upwards
  - Trusted path between the user and the TCB
- Audit requirements
- As seen, the details of these requirements depends on the certification level



# TCSEC Assurance Requirements

---

- The assurance requirements refer mostly to the development process of the product
- System architecture requirement
  - Modularity, minimization of complexity
  - Aim is to keep the TCB small and simple
  - Begins at C1
  - B3 must have full reference validation mechanism
- Design specification and verification requirement
  - Informal security policy model at B1
  - Top level specification and a formal security policy model at B2
  - System specification must be shown to meet the model at B3
  - Formal top level specification and mapping to the source code at A1



# More TCSEC Assurance Requirements

---

- Testing requirements
  - Also a search for cover channels at higher levels
- Configuration management requirements
  - B2 and upwards
  - Identification, correspondence mapping and documentation of configuration items and code
- Trusted distribution requirement
  - Level A1 only
  - A controlled process from source code to customer delivery that protects the integrity of the product
- Product documentation requirement
  - Security Features User's Guide
  - Trusted Facility Manual



# The Importance of TCSEC

---

- Created the approach which has been followed by later standards
  - Design analysis
  - Implementation analysis
  - Documentation analysis
  - Development and deployment process analysis
  - External review
- Limited in scope
  - US government and military requirements
    - Mandatory Access Control
    - Confidentiality as the main requirement
  - Developed before networks become common



# ITSEC and Common Criteria

---

- Standards for evaluating the security of a software or hardware product
  - Often cover only part of a product
    - Might cover a smart card but not the software that uses it
  - Intention is to produce more secure computing components
- Certify that security has been attended to when a product has been developed
- Several things must be assessed
  - Threat models
  - Security mechanisms
  - Testing
  - Documentation
  - Instructions on secure use
  - Possibly penetration testing
  - Version management plan, design documentation



# ITSEC and Common Criteria

---

- Both standards are very nonflexible
  - The aim is to get a meaningful assessment of the security
  - Difficult to use on complex products (much work)
- The usage environment is always specified
  - These presumptions are very crucial to the security of the final system
  - Often certain user groups like system administrators are assumed to be trustworthy and careful
  - When the certification is used for advertising purposes unrealistic presumptions can be included, like no network connection or only a secure network
- Usually these standards are useful only aiming for the certification



- System Security Engineering - Capability Maturity Model
- Based on the CMM model
  - Measures the maturity and capability of an organization's software development process
  - Assumes that good methods will produce a good product
- CMM-SSE focuses on development of secure software
- CMM-SSE suits organizations that develop software and want to ensure quality of the security of the software
  - Not as inflexible as Common Criteria



# How the CMM-SSE Works?

---

- About twenty practices are defined
  - Based on *processes*, not security areas or technologies
  - E.g. evaluating threats, defining production processes, developing production processes
- An organization can be graded (1-5) on how far they are on a process area
- A company can be evaluated internally or externally
- CMM measures the organization, not the capabilities of individual developers or individual products
  - A high CMM level means that performance can be repeated



- 1 - The action is taken occasionally, unpredictable, depends on individual's initiative
  - 2 - An informal process exists and the action can be repeated
  - 3 - A well defined and communicated process exists for this item
  - 4 - The process is measured and controlled
  - 5 - The process is being continuously optimized
- Generally one should develop the organization one level at a time
    - If you are at level 2, do not focus on level 5 things yet
  - Level 5, continuously optimized process, is very expensive



- British Standard 7799, Information security management
  - Also ISO 17799
  - Being replaced with ISO 27001
- Like ISO 9000, but for security and not as heavy
- Useful also without certification
  - Generally going through the BS 7799 is useful for every security manager
- Aids in developing a security policy
- Mostly a long checklist of things that must be attended to
- Also the basis for the ITIL Security Management Process
  - Information Technology Infrastructure Library (ITIL), a best practice set of guidelines for managing information technology



# BS 7799, Areas of Information Security

---

- None of these are IT specific, as the standard is for *information* security, not computing
  - Information security policy
  - Security organization
  - Asset classification and control
  - Personnel security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Systems development and maintenance
  - Business continuity management
  - Compliance



# Other Standards and Certifications

---

- **FIPS 140-1 and 140-2 certification**
  - Federal Information Processing Standard (USA) for crypto modules
  - Certifies e.g. that a library implements an algorithm correctly
  - Need for sales to certain customers
- **Cobit**
  - Control Objectives for Information and related Technology
  - Auditing of IT functions of a company, how to run an IT department correctly
  - Developed from the point of view of a financial audit
  - Security is not the focus



# Meaning of Certifications

---

- Microsoft has received
  - Common Criteria certification for Windows 2000 (SP3) at
    - Evaluation Assurance Level (EAL) 4
  - Provides a level of protection which is appropriate for an
    - Assumed non-hostile and
    - Well-managed user community requiring
  - Protection against threats of
    - Inadvertent or casual attempts to breach the system security
- More info at:
  - <http://www.microsoft.com/presspass/press/2005/dec05/12-14CommonCriteriaPR.msp>
  - <http://eros.cs.jhu.edu/~shap/NT-EAL4.html>



# Professional Certifications

---

- People can also be certified to have certain skills
- Professional security certifications are like educational degrees
  - But more specific
  - Some certifications are less valued than educational degrees, some are more valued



# CISSP Certification

---

- Certified Information Systems Security Professional
  - <http://www.cissps.com/>
- An information security management certification
  - Not very technical
- Administered by the International Information Systems Security Certification Consortium
- Includes
  - Training
  - Exams
  - Membership of a professional society
- Needs to be renewed yearly



# SANS GIAC Certification

---

- System Administration, Networking and Security Institute's Global Information Assurance Certification
  - <http://www.giac.org/>
- Practical network security oriented, technical certification
- Available on several areas
  - Essential security (basics)
  - Firewall security
  - Intrusion detection
  - Unix, Windows
  - Others



- 
- Certified Information Systems Auditor
  - By Information Systems Audit and Control Association
  - A certification for auditors auditing IT services, not focused on security



# Vendors' Certifications

---

- Vendors of security software and hardware have their own certification programs
  - Microsoft, Sun, Cisco etc.
- Quality of the certification depends on the vendor
  - Usually the certified person is competent within the vendor's products on some level
  - The certifications do not provide tools for solving problems that can not be solved by the products
    - "Thinking inside the box"
- The vendor certification is useful to indicate that a *product reseller has reasonable competence* on the product



# Assessing Security

---

- Being able to *measure* things is usually a nice thing
- Security is a complex issue with unknown details and human factors, measures can be made, but the inherent *inaccuracy* must be accepted and understood
- The result of security assessment is a reasonable confidence in the level of security that the evaluation has found
  - If plenty of vulnerabilities were found, there are likely to be other problems not found
  - If security was found to be "perfect" it does not prove that there are no problems



# Auditing and Evaluating

---

- An *audit* is usually used to refer an external formal and through assessment by a competent auditor
  - The goal is usually to get an external certification of the state of the organization
- An *assessment* or *evaluation* is less formal task
  - The goal is usually to get information for internal use



# Before the Assessment

---

- What is being assessed?
  - Security policy
  - Security policy implementation
  - Network and computer security
  - Security processes
  - Security in organization's processes
  - Hardware and software design or installation
- Security assessments can contain procedures that would be illegal without authorization
  - Before any evaluation, internal or external, get a permission from the person who is authorized to allow this
    - Usually the IT manager is not authorized



# Who Is Assessing the Security

---

- Internal staff assessment
  - Better knowledge of the system
  - Less risk of an information leak
  - Lack of skills
  - Own interests in the evaluation
  - Lack of new perspective
- External organization evaluation or audit
  - Less knowledge of the system
  - More objective
  - More general knowledge and knowledge of best practices
  - Auditing can be done by outside experts only



# Security Management Assessment

---

- Assessing the organization and processes
- Not always easy to get hard data
- Interviewing the key people is one method
  - A comprehensive plan is needed
    - For example questions based on the BS 7799
  - The results should be analyzed
    - It is easy to collect much numerical data, but difficult to produce meaningful information from that
  - The experience of the evaluator is important
- Often half the benefit of the evaluation is to get key people to think about security



# Methods for Security Management Evaluation

---

- Audit models and frameworks
  - Useful for analyzing the organization and processes
  - Public and private models (SSE-CMM, BS7799)
- Combining BS7799 and CMM would produce an evaluation that does not measure the current level of security but the level of organization's capabilities
  - As done at Nixu Ltd.
  - A very important difference
  - Not: "Do you have a firewall?"
  - But: "Do you have a process for periodically verifying that the firewall configuration meets your needs?"
    - "Is the process documented?"
    - "Is there a measurement for the process?"



# Assessment benefits

---

- Based on Nixu's experience
  - Major discrepancies in expectations and execution stand out
  - An independent evaluation of organization's state
  - Increased security awareness
  - A report with recommendations on how to improve the current state



TEKNILLINEN KORKEAKOULU

# Nixu Ltd's Experiences From Security Management Assessments

---

- Usually the security managers are too optimistic about the real situation
  - Making people behave in a secure way is a big issue
- Top level management does not often see security as an important issue
- Sometimes there are gaps in the security coverage



# Technical Security Assessment

---

- Goal to evaluate the network and services
- Configuration analysis
  - Firewall, router, service configuration analysis
  - Most configuration analysis requires an experienced analyst
- Automated analysis using portscanners and other vulnerability analysis tools
  - Produce a lot of information
  - Human reading of the results is needed to make sense
  - Several different tools should be used
- "Tiger Team" break-ins do not usually produce meaningful results
  - Steady and methodical analysis is more effective for developing the quality of protection



# Nixu's Technical Network Assessment Experiences

---

- Usually the reality does not match the design
  - Extra computers found in the network
  - Extra services found on those and other computers
  - Old vulnerabilities are found on computers that have not been updated
- Often the reason is that the responsibilities are not clearly defined
  - If another department brings a computer to the IT department's computer room, who is responsible
  - Equipment set up for testing and development is not disconnected



- There are plenty of security-related standards, certifications and methods
- These are becoming better and new ones are still appearing
- A security customer should understand that some of these standards and certifications are very specific or limited in scope
- A security professional should have knowledge of the major standards and to be able to select which one to apply for a particular need