

The logo for Nixu, consisting of the lowercase letters 'n', 'i', 'x', and 'u' in a white, sans-serif font, positioned on a dark blue background. A thin white vertical line is located to the right of the letters.

nixu

Evaluating and Managing Security

Security Standards

- Standards exist for security components and for the organization
- Organizations and products can also be certified to meet a certain standard
- Many standards provide sensible frameworks and useful practices even without the certification
 - Often the certification would bring much work and few benefits

TCSEC, "Orange Book"

- 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

- Discretionary access control (DAC)
- Object reuse requirements
 - Memory and disk sector contents should not be transmitted to a new user
- 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

- Identification and authentication requirements
- Trusted path requirements
 - B2 and upwards
 - Trusted path between the user and the TCB
- Audit requirements
- The level and details of these requirements depends on the certification level
- The functional requirements are the requirements that the finished product has

TCSEC Assurance Requirements

- 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
- 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

More TCSEC Assurance Requirements

- 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
- Testing requirements
 - Also a search for cover channels at higher levels
- Product documentation requirement
 - Security Features User's Guide
 - Trusted Facility Manual
- The assurance requirements refer to the development process of the product

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 scope
 - US government and military requirements
 - Mandatory access control not as important for the private sector
 - Confidentiality was the main requirement
 - Integrity and availability not addressed

ITSEC and Common Criteria

- Evaluate 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 if the certification is the aim

CMM-SSE

- System Security Engineering Capability Maturity Model
- Overlaps with Common Criteria
- 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 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
 - E.g. Level 2, processes are repeated regularly
 - E.g. Level 5, processes are continuously being optimized based on automatically collected information
 - Everybody starts from level 1
 - Generally one should develop the organization one level at a time, if you are at level 2, do not focus on level 5 things
- 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

BS 7799

- British Standard 7799, Information security management
 - Also ISO 17799
- Like ISO 9000 for security, but 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

BS 7799, areas of information security

- None of these are IT specific, the standard is about information security
 - 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 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 (with service pack 3) 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://eros.cs.jhu.edu/~shap/NT-EAL4.html>

Professional certifications

- People can also be certified to have certain skills
- Professional security certifications are like degrees

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

CISA

- 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
- Quality of the certification depends on the vendor
 - Usually the certified person is competent within the vendor's products
 - The certifications do not provide tools for solving problems that can not be solved by the products
- 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 often useful
- Security is a complex issue with unknown details and human factors
 - However measures can be made, if the inherent inaccuracy is 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

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

Network and Computer System Security Auditing

- An audit is rather formal project, that produces an assessment of the state of the system by a competent auditor
 - Formal qualifications are preferred
- The audit
 - Does not guarantee the system safe, it is impossible to find all the vulnerabilities
 - Quality of the audit depends on quality of the auditor
- Idea is to collect all available information on the system and to form a comprehensive picture of the security of the system using generally accepted guidelines

Security Assessment Tools

- Audit models and frameworks
 - Useful for analyzing the organization and processes
 - Public and private models (SSE-CMM, BS7799)
- Technical tools
 - 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
 - Configuration analysis
 - Tools for analyzing firewall or router configuration exist
 - Still limited in power and manufacturer specific
 - Most configuration analysis requires an experienced analyst

Security Management Assessment

- Assessing the organization and processes
- Not as easy to get hard data as from the technical assessments
- 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

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
 - Especially the Microsoft IIS WWW server
 - 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

Nixu's Methods for Security Management Evaluation

- The evaluation is structured on the BS 7799
- The grading is structured on CMM model
- The evaluation does not measure the current level of security but the level of organization's capabilities
 - 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"

Nixu's Grading Levels

- 0 - Does not apply
- 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

Nixu's Evaluation Process

- Target levels are set with the responsible managers
 - Level 5, continuously optimized process is very expensive
- Nixu has two evaluation methods
 - Interviews of key personnel at different levels of the organization
 - Both managers and workers
 - Gives information about how well the processes are actually implemented, e.g. has the worker actually read and understood the organization's security policy
 - A workshop with selected personnel
 - Starts with a short training session
 - Participants answer selected questions from a set of 1000

Nixu's Evaluation Process cont.

- The answers are analyzed to produce a picture of the organization's state of security
 - Numerical and graphical
- One of the methods collects data from different companies and allows comparisons
- Customer's benefits:
 - 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

Nixu 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