People and 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 uses 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

CMM-SSE

- 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

CMM Levels

- 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

BS 7799 (-> ISO 27001) and ITIL

- 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.mspx
  - 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

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
  - 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 disparencies 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 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

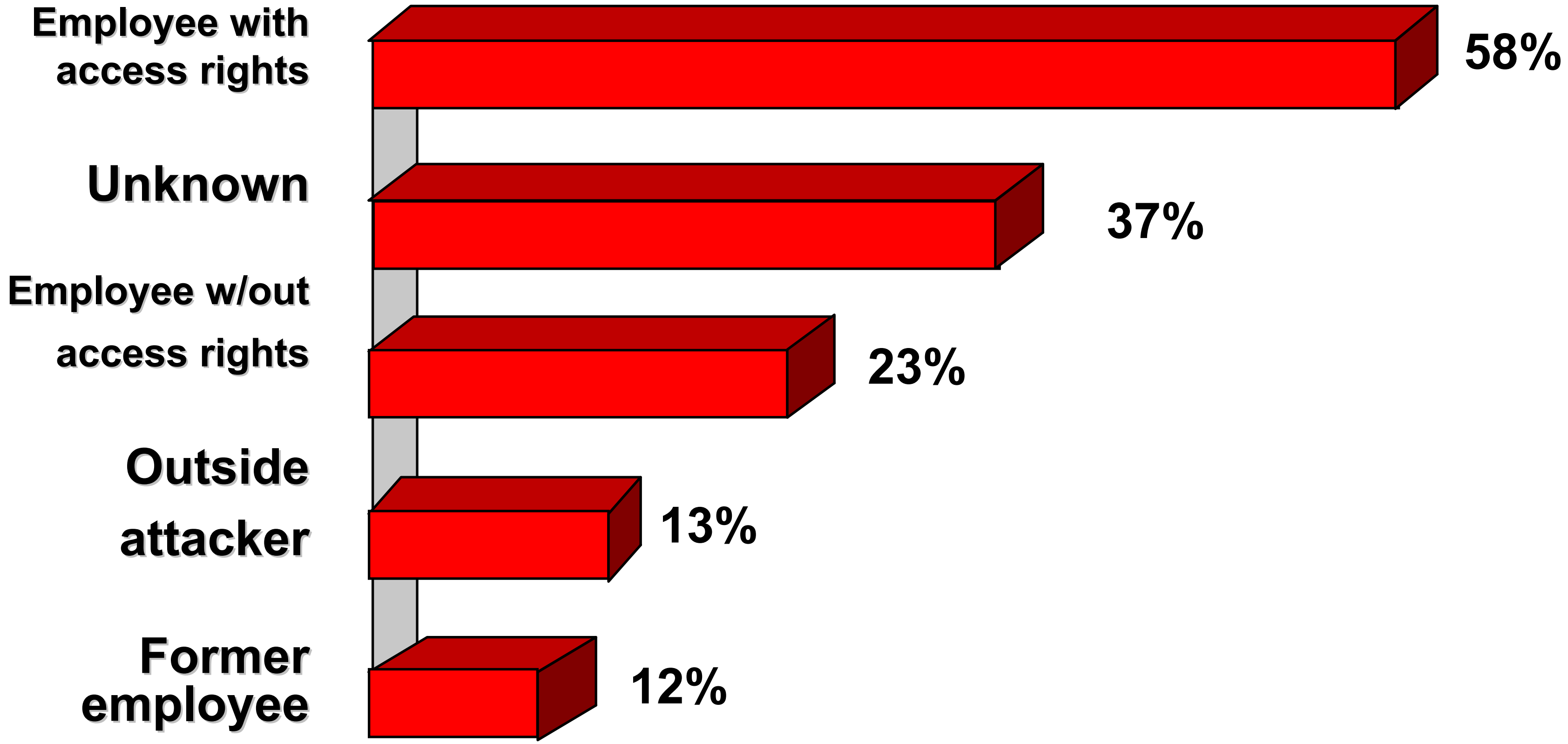
Summary

- 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

What Is the Protection Domain?

- Before you can do any meaningful security work, you have to define what you are protecting
  - Security planning
- Then you can decide what tools to use
- The plan must cover all aspects
  - Imagine that you are designing a submarine, not a ship
  - But the leaks are invisible
- You are most likely to find that the most important aspect is people
  - Usually your own employees

Likely Threats to Security

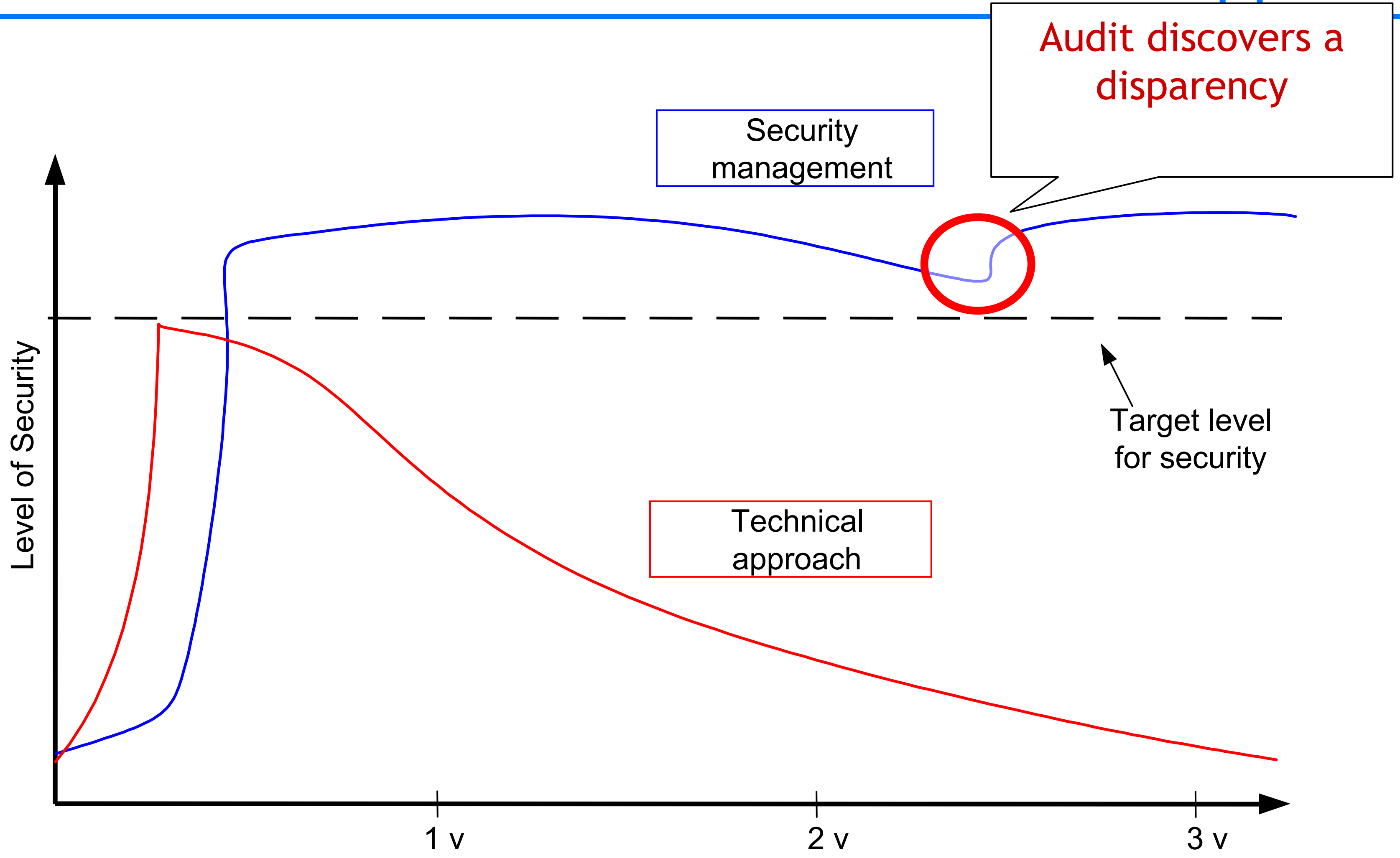


Source - Information Week/Pricewaterhouse Coopers, 1998

People Security

- The technical challenges of security are mostly conquered
  - Firewalls, encryption, virus protection
  - There is still more to do, like global PKI, SSO or federated identity and other things
- However the largest security problem and the next challenge is the people
  - Social engineering is still the most effective attack
  - Own people are the larges threat

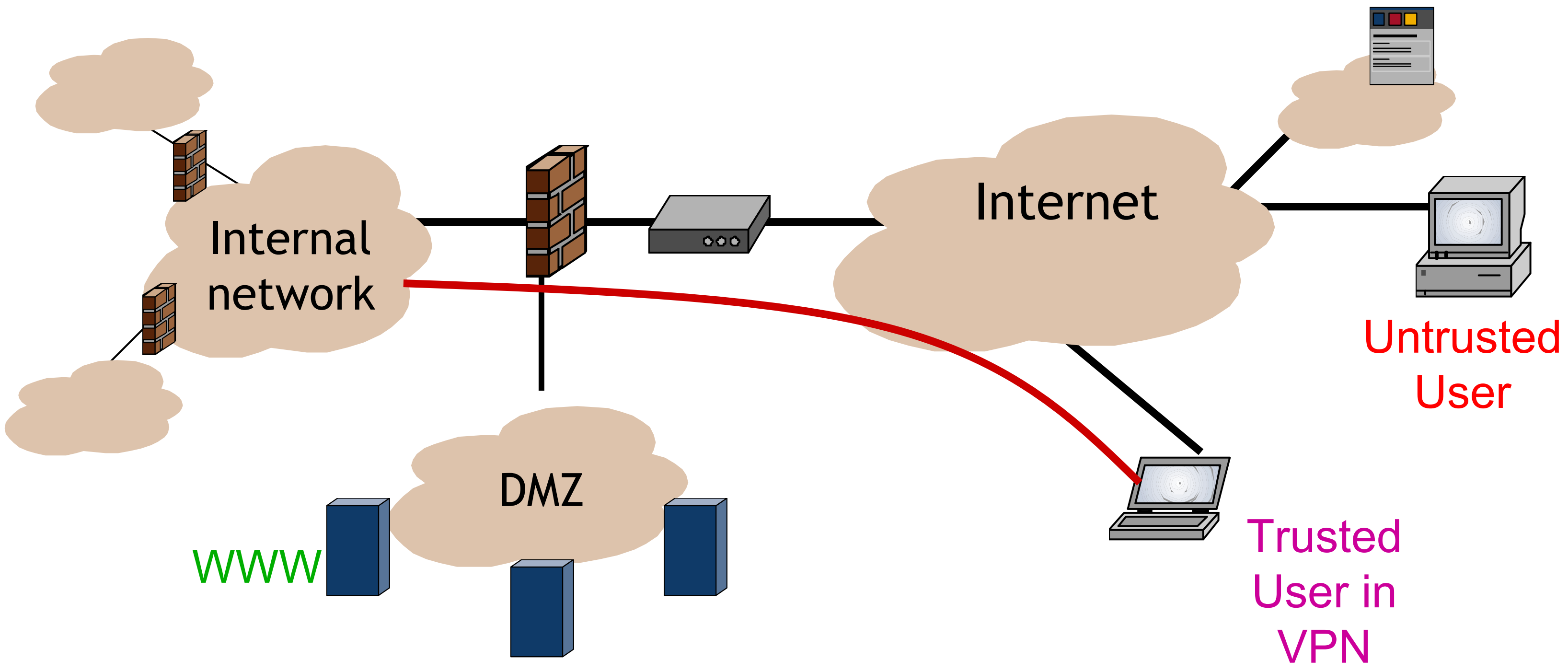
Managed Security Vs. Technical Approach



Source: Nixu Ltd.

Secure Networking

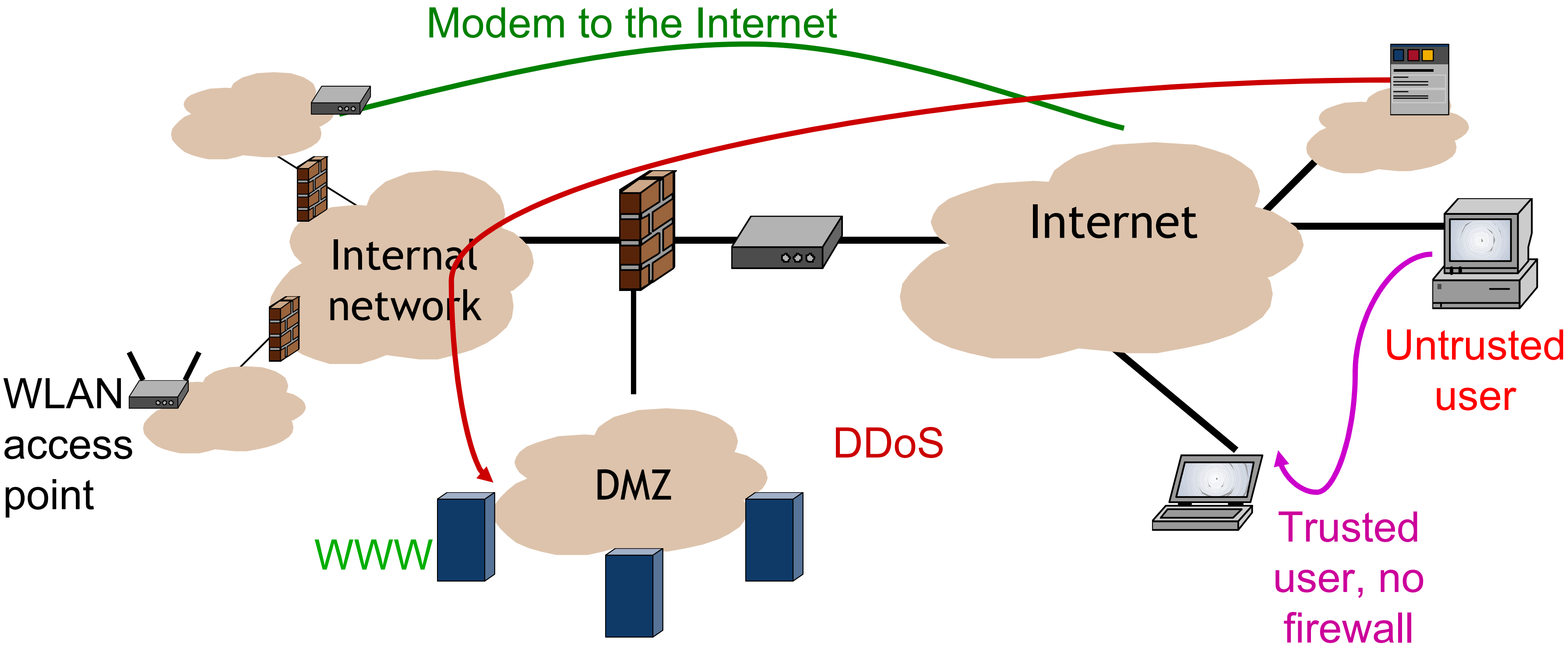
- Firewalls limit access to the network that they protect
- Encryption protects data in transit
- Cryptographic identification provides strong authentication



TEKNILLINEN KORKEAKOULU

Networking Reality

- If left unsupervised, the security is going to be broken
- Your own users can break the security intentionally or unintentionally



Experience From Other Fields

- *Safety* in manufacturing plants has a long background
  - Safety is not a separate issue, but part of the normal work processes
  - The processes are designed to allow work to be done while maintaining the required level of physical safety
- *Security* work can be modeled on physical safety work
  - Work processes
  - Supervisor training
- A major difference is that security threats are not visible, unlike physical threats

Security Is in the Processes

- Current focus on the security management area is in developing the processes of an organization in such a manner, that the organization works in a secure way
  - In the World War II allied powers could usually break most of the German Wehrmacht and Luftwaffe messages, but not Kriegsmarine messages because (besides better technology) they had good encryption discipline
    - No standard messages
    - No repeated session keys
    - No clear-text retransmissions
- This means that the security policy must be communicated to the people
  - The security policy that is delivered to the entire organization should be short, easy to understand and reasonable
  - Unreasonable security policies are usually not followed

Executing the Security Policy

- Safety regulations usually require that the correct procedures are taught personally to each employee
- For example a a four step technique:
  - Supervisor *instructs* the employee in correct procedures
  - *Training* reviews the instruction
  - Written *guidelines* are provided
  - *Monitoring* ensures that the set target is reached
- This method requires a lot of work
  - Likely to produce results, too
  - Requirements must be made concrete and practical
- Key issue:
  - How to change people's behavior?

Personal Instruction

- Instructions are made practical and adapted to daily tasks
  - From abstract principles to practice
  - "If somebody asks for a copy of a contract, verify who is asking, and find out from the responsible sales person if you can give it"
  - "Never tell your password to anybody, including the system administration people"
- Daily tasks must support the security policy
  - "There is a sealed password at the office safe which allows access to the department head's files, you may use it with his or management's permission"
  - Most "exceptions" are really regular occurrences
    - Illnesses, deaths, vacations, hurry

Training

- Supports work instruction
- Additional learning and motivation
  - The reasons for guidelines and work practices are made clear
  - General security knowledge
  - Sample cases of real security incidents
  - Examples of how to deflect very persuasive reasoning
- A good time and place to show that the management is supporting the security work

Written Guidelines

- Written instructions
  - "Proposals, offerings, contracts etc. are confidential. Accounting is responsible for archiving them, sales controls the access."
- Who owns the instructions?
  - This matters, because the guidelines need periodic revising
  - For example the line organization owns the guidelines, but changes need to be approved by the security management
- Well defined processes are part of long lasting security

Monitoring

- Security guidelines and processes have any meaning only if they are actually followed
- Monitoring can be done like monitoring any other company policy or practice
  - Supervisors monitor daily work and give feedback on correct and incorrect procedures
  - There must exist a method for reporting conflicts between security guidelines and actual work requirements
  - An external organization can assist in monitoring how well the guidelines are followed in practice

Security Manager's Problems

- Many security managers see the lack of support from the top management as their largest problem
  - Getting the management support can make or break company's security
  - One way to show the support is that **everybody** follows the rules
- The security manager is usually not in the line of command
  - It takes people skills to lead from the sidelines
  - Especially as security is not a profit generator but loss avoidance function
- Shared responsibility is not good for security
  - There should be one person or committee responsible, a single point of decision making

Usable Security

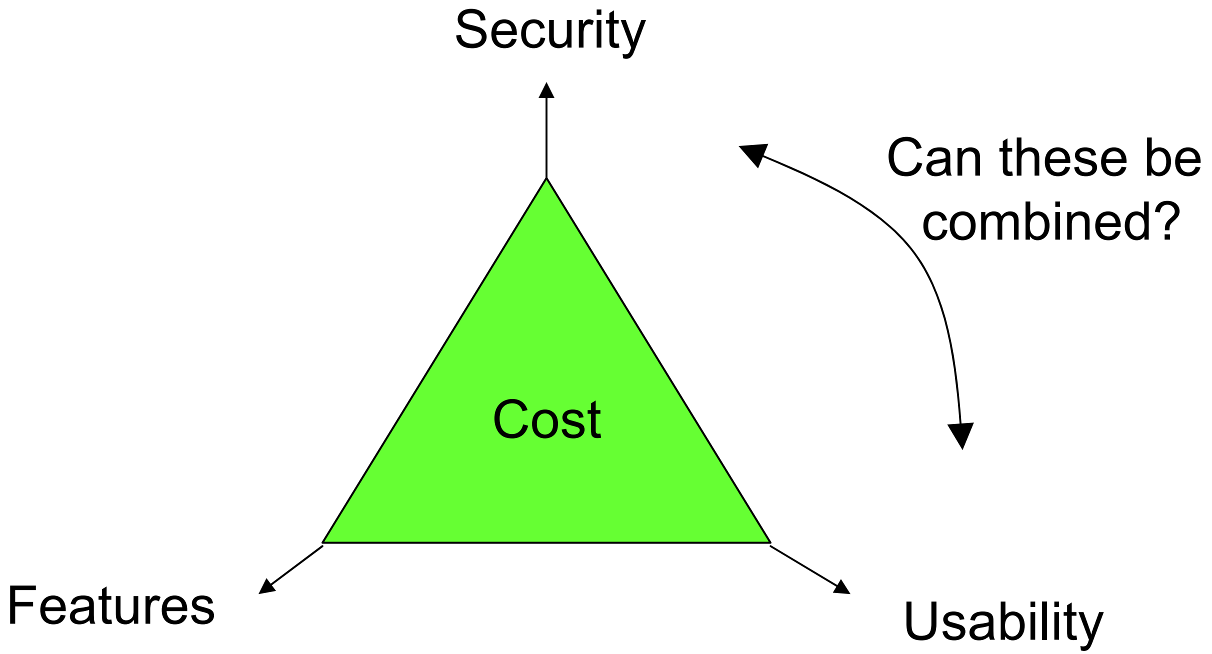
- To get the users to actually perform in a secure way it is not enough to create processes that implement security, but to also make security technology usable
- This is still a rather young branch of the security research
- The field is known as Human Computer Interaction and Security (HCISEC)

Usability Studies in Security Systems Design

- The target is to design systems that make it easy for the users to comply with various security requirements
- This requires analysis of the
  - Work processes and flow
  - User habits
  - Exception handling
  - Informal processes
- This method can be used to develop the security features of existing systems or to create new ones
- Usability testing tools can be used when developing existing or prototype systems

Balancing the Requirements

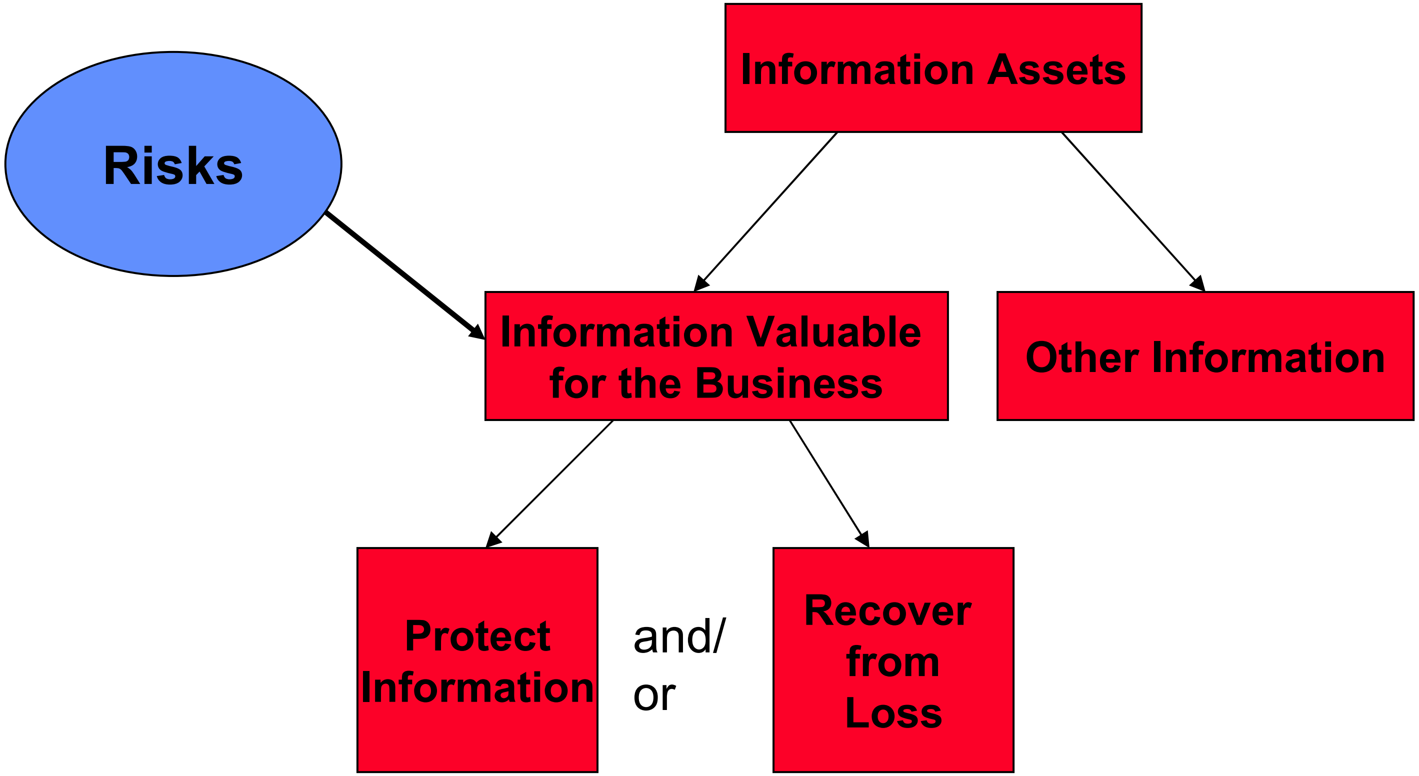
- Different system requirements are usually competing against each other to increase costs
- "Clever engineering" can overcome this



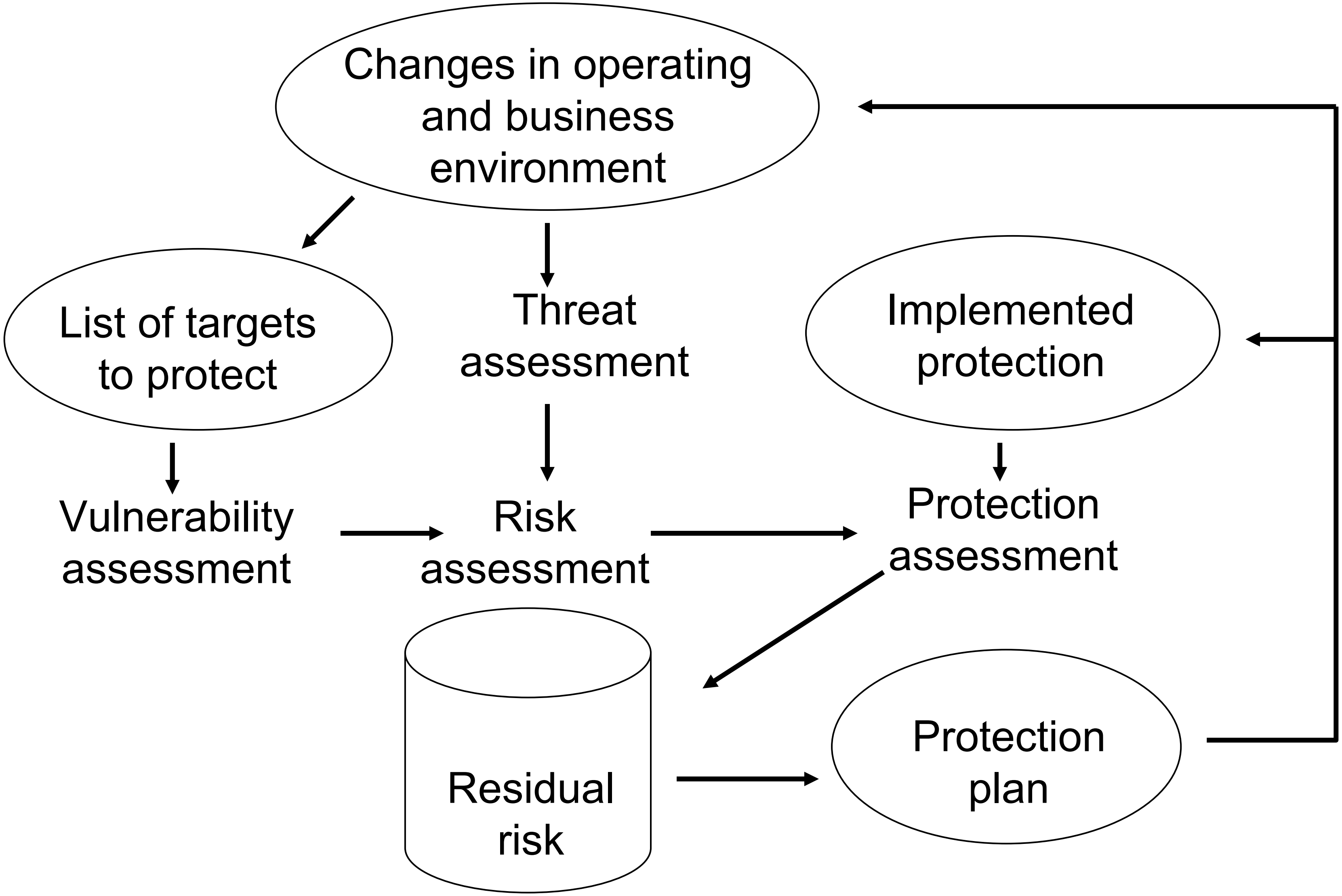
Security Is a Process

- Security is never finished
- The world changes
  - Technology changes
  - People forget working methods
- Security is a continuous loop of
  - Plan
  - Implement
  - Evaluate

What to Secure?



Risk Management Is a Continuous Process



Exam

- This lecture contains excessive details that are not going to be asked
- Your should know the main standard names and their uses, like BS7799 or SSE-CMM
  - Subdivisions or classes are not needed
- Questions might be like:
  - Of the standards and practices presented on the course, TCSEC, Common criteria, ... which would you use for ... and why? (2p)
  - T/F: it is possible to evaluate an organization's security level
  - T/F: The more security the better
    - a: Nyet, security costs, cost may be larger than benefit