University of Oslo
INF3510 Information Security
Spring 2014
Workshop Questions

Lecture 2: Security Management, Human Factors in Information Security

QUESTION 1

- Look at the list of standards in the ISO27000 series, e.g. on Wikipedia, http://en.wikipedia.org/wiki/ISO/IEC_27000-series
- Look at the NIST SP800 (special publications) series on: http://csrc.nist.gov/publications/PubsSPs.html

a. Try to define corresponding publications from the ISO 27000 series and from the NIST SP800 series
b. What are possible drivers for developing IT security standards in general, and for developing separate sets of similar standards.

Answer

a. Below are lists of ISO 27K and SP800 documents:

List of NISP SP800 publications

- SP800-165; Computer Security Division Annual Report (2012)
- SP800-164: Guidelines on Hardware-Rooted Security in Mobile Devices
- SP800-162: Guide to Attribute Based Access Control (ABAC) Definition and Considerations
- SP800-161: Supply Chain Risk Management Practices for Federal Info Sys. and Organizations
- SP800-155: BIOS Integrity Measurement Guidelines
- SP800-153: Guidelines for Securing Wireless Local Area Networks (WLANs)
- SP800-152: Profile for U. S. Federal Cryptographic Key Management Systems (CKMS)
- SP800-147: Basic Input/Output System (BIOS) Protection Guidelines
- SP800-146: Cloud Computing Synopsis and Recommendations
- SP800-145: The NIST Definition of Cloud Computing
- SP800-144: Guidelines on Security and Privacy in Public Cloud Computing
- SP800-142: Practical Combinatorial Testing
- SP800-137: IS Continuous Monitoring for Federal Info Sys and Organizations
- SP800-135: Recommendation for Existing Application-Specific Key Derivation Functions
- SP800-133: Recommendation for Cryptographic Key Generation
- SP800-132: Recommendation for Password-Based Key Derivation Part 1: Storage Applications
- SP800-131: Recommendation for Transitioning the Use of Crypto Algorithms and Key Lengths
- SP800-130: A Framework for Designing Cryptographic Key Management Systems
- SP800-128: Guide for Security-Focused Configuration Management of Information Systems
- SP800-127: Guide to Securing WiMAX Wireless Communications
- SP800-126: The Technical Specification for the Security Content Automation Protocol

- SP800-126: The Technical Specification for the Security Content Automation Protocol (SCAP)
- SP800-125: Guide to Security for Full Virtualization Technologies
- SP800-124: Guidelines for Managing the Security of Mobile Devices in the Enterprise
- SP800-123: Guide to General Server Security
- SP800-122: Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP800-121: Guide to Bluetooth Security
- SP800-120: Recommendation for EAP Methods in Wireless Network Access Authentication
- SP800-119: Guidelines for the Secure Deployment of IPv6
- SP800-118; Guide to Enterprise Password Management
- SP800-117: Guide to Adopting and Using the Security Content Automation Protocol (SCAP)
- SP800-116: A Recommendation for the Use of PIV Credentials in Physical AC Systems (PACS)
- SP800-115: Technical Guide to Information Security Testing and Assessment
- SP800-114: User's Guide to Securing External Devices for Telework and Remote Access
- SP800-113: Guide to SSL VPNs
- SP800-111: Guide to Storage Encryption Technologies for End User Devices
- SP800-108: Recommendation for Key Derivation Using Pseudorandom Functions
- SP800-107: Recommendation for Applications Using Approved Hash Algorithms
- SP800-106: Randomized Hashing for Digital Signatures
- SP800-104: A Scheme for PIV Visual Card Topography
- SP800-103: An Ontology of Identity Credentials
- SP800-102: Recommendation for Digital Signature Timeliness
- SP800-101: Guidelines on Mobile Device Forensics
- SP800-100: Information Security Handbook: A Guide for Managers
- SP800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems
- SP800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- SP800-96: PIV Card to Reader Interoperability Guidelines
- SP800-95: Guide to Secure Web Services
- SP800-94: Guide to Intrusion Detection and Prevention Systems (IDPS)
- SP800-92: Guide to Computer Security Log Management
- SP800-90: Series: Random Bit Generators
- SP800-89: Recommendation for Obtaining Assurances for Digital Signature Applications
- SP800-88: Guidelines for Media Sanitization
- SP800-87: Codes for Identification of Federal and Federally-Assisted Organizations
- SP800-86: Guide to Integrating Forensic Techniques into Incident Response
- SP800-85: PIV Card Application and Middleware Interface Test Guidelines
- SP800-84: Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities
- SP800-83: Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- SP800-82: Guide to Industrial Control Systems (ICS) Security
- SP800-81: Secure Domain Name System (DNS) Deployment Guide
- SP800-79: Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers
- SP800-78: Crypto Algorithms and Key Sizes for Personal Identification Verification (PIV)
- SP800-77: Guide to IPsec VPNs
- SP800-76: Biometric Data Specification for Personal Identity Verification
- SP800-73: Interfaces for Personal Identity Verification
- SP800-72: Guidelines on PDA Forensics
- SP800-70: National Checklist Program for IT Products: Guidelines for Checklists
- SP800-69: Guidance for Securing Microsoft Windows XP Home Edition
- SP800-68: Guide to Securing Microsoft Windows XP Systems for IT Professionals
- SP800-67: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher

- SP800-66: An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- SP800-65: Integrating IT Security into the Capital Planning and Investment Control Process
- SP800-64: Security Considerations in the System Development Life Cycle
- SP800-63: Electronic Authentication Guideline
- SP800-61: Computer Security Incident Handling Guide
- SP800-60: Guide for Mapping Types of Information and Info. Systems to Security Categories
- SP800-59: Guideline for Identifying an Information System as a National Security System
- SP800-58: Security Considerations for Voice Over IP Systems
- SP800-57-1: Reccmmendation for Key Management: Part 1: General (Rev
- SP800-57-2: Recommendation for Key Man: Best Practices for Key Management Organization
- SP800-57-3: Recommendation for Key Man: Application-Specific Key Management Guidance
- SP800-56-A: Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography
- SP800-56-B: Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography
- SP800-56-C: Recommendation for Key Derivation through Extraction-then-Expansion
- SP800-55: Performance Measurement Guide for Information Security
- SP800-54: Border Gateway Protocol Security
- SP800-53: Security and Privacy Controls for Federal Information Systems and Organizations
- SP800-52: Guidelines for the Selection, Configuration, and Use of TLS Implementations
- SP800-51: Guide to Using Vulnerability Naming Schemes
- SP800-50: Building an Information Technology Security Awareness and Training Program
- SP800-49: Federal S/MIME V3 Client Profile
- SP800-48: Guide to Securing Legacy IEEE 802.11 Wireless Networks
- SP800-47: Security Guide for Interconnecting Information Technology Systems
- SP800-46: Guide to Enterprise Telework and Remote Access Security
- SP800-45: Guidelines on Electronic Mail Security
- SP800-44: Guidelines on Securing Public Web Servers
- SP800-43: Systems Administration Guidance for Windows 2000 Professional System
- SP800-41: Guidelines on Firewalls and Firewall Policy
- SP800-40: Guide to Enterprise Patch Management Technologies
- SP800-39: Managing Information Security Risk: Organization, Mission, and Info. System View
- SP800-38-A: Recomm. for Block Cipher Modes of Operation - Methods and Techniques
- SP800-38-B: Recommendation for Block Cipher Modes of Operation: The CMAC mode
- SP800-38-C: Recommendation for Block Cipher Modes of Operation: The CCM mode
- SP800-38-D: Recommendation for Block Cipher Modes of Operation: GCM and GMAC
- SP800-38-E: Recommendation for Block Cipher Modes of Operation: The XTS-AES mode
- SP800-38-F: Recommendation for Block Cipher Modes of Operation: Key Wrapping
- SP800-38-G: Recommendation for Block Cipher Modes of Operation: Format-preservation
- SP800-37: Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
- SP800-36: Guide to Selecting Information Technology Security Products
- SP800-35: Guide to Information Technology Security Services
- SP800-34: Contingency Planning Guide for Federal Information Systems
- SP800-33: Underlying Technical Models for Information Technology Security
- SP800-32: Introduction to Public Key Technology and the Federal PKI Infrastructure
- SP800-30: Guide for Conducting Risk Assessments
- SP800-29: A Comparison of the Security Requirements for Cryptographic Modules
- SP800-28: Guidelines on Active Content and Mobile Code

- SP800-27: Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- SP800-25: Federal Agency Use of Public Key Technology for Dig Sig and Authentication
- SP800-24: PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does
- SP800-23: Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products
- SP800-22: A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications
- SP800-21: Guideline for Implementing Cryptography in the Federal Government
- SP800-20: Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures
- SP800-19: Mobile Agent Security
- SP800-18: Guide for Developing Security Plans for Federal Information Systems
- SP800-17: Modes of Operation Validation System (MOVS): Requirements and Procedures
- SP800-16: IT Security Training Requirements: A Role- and Performance-Based Model
- SP800-15: MISPC Minimum Interoperability Specification for PKI Components, Version 1
- SP800-14: Generally Accepted Principles and Practices for Securing IT Systems
- SP800-13: Telecommunications Security Guidelines for Telecom Management Network
- SP800-12: An Introduction to Computer Security: The NIST Handbook

List of ISO 27K standards (published and in preparation)

- ISO 27000 — Information security management systems — Overview and vocabulary
- ISO 27001 — Information security management systems — Requirements
- ISO 27002 — Code of practice for information security management
- ISO 27003 — Information security management system implementation guidance
- ISO 27004 — Information security management — Measurement
- ISO 27005 — Information security risk management
- ISO 27006 — Requirements for bodies providing audit and certification of information security management systems
- ISO 27007 — Guidelines for information security management systems
- ISO 27008 — Guidance for auditors on ISMS controls
- ISO 27010 — IS management for inter-sector and inter-organizational communications
- ISO 27011 — IS Man. guidelines for telecommunications organizations based on ISO 27002
- ISO 27013 — Guideline on the integrated implementation of ISO 20000-1 and ISO 27001
- ISO 27014 — Information security governance
- ISO 27015 — Information security management guidelines for financial services
- ISO 27017 — Information security management for cloud systems
- ISO 27018 — Data protection for cloud systems
- ISO 27019 — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO 27031 — Guidelines for ICT readiness for business continuity
- ISO 27032 — Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- ISO 27033 — IT network security, a multi-part standard based on ISO/IEC 18028:2006
- ISO 27033-1 — Network security overview and concepts
- ISO 27033-2 — Guidelines for the design and implementation of network security
- ISO 27033-3 — Reference networking scenarios - Threats, design techn. and control issues
- ISO 27034 — Guideline for application security
- ISO 27035 — Security incident management
- ISO 27036 — Guidelines for security in supplier relationships

- ISO 27037 — Guideln. for identification, collection, acquisition and preserv. of dig. evidence
- ISO 27038 — Specification for redaction of digital documents
- ISO 27039 — Intrusion detection and protection systems
- ISO 27040 — Guideline on storage security
- ISO 27041 — Assurance for digital evidence investigation methods
- ISO 27042 — Analysis and interpretation of digital evidence
- ISO 27043 — Digital evidence investigation principles and processes
- ISO 27799 — Information security management in health using ISO/IEC 27002

Create a simple table with a few entries. Only a few publications match well.

b. Drivers behind standards can be:
   - a real need for a new standard,
   - interest/ambition of individuals and organisations to define their own standards
   - The US government does not want to depend on ISO, and the rest of the world does not want to depend on NIST.

QUESTION 2

a. How are the standards ISO/IEC 27001 and ISO/IEC 27002 related?
b. Which one of the standards can be used for certification, and why?
c. How should an organisation determine which security controls to implement?

Answer

a. ISO/IEC 27001 is a model for setting up and managing an ISMS, i.e. establishing and operating a security program within an organisation. ISO/IEC 27002 is a checklist of security contorols that an organisation should consider implementing.
b. Organisations can only be certified against ISO/IEC 27001 not against ISO/IEC 27002. This is possible because ISO 27001 describes a process for quality control in security management which is more or less the same for all organisations, and can be verified to be in place by an external party. ISO 27002 describes a large number of controls, of which not all are relevant for every organisastion, so it is impossible to verify that the necessary controls are in place in general. However it is of course possible to verify that specific controls are in place, which is typically done by IT auditors.
c. Risk assessment is used to determine where controls are needed. The most appropriate controls are selected to match the risk.

QUESTION 3

a. Create a mapping of the correspondence between the 14 security domains of ISO27002 and the 10 security domains of CISSP.
b. Make a judgment about how well aligned they are.

Answer

BS 7799, which was the original version of ISO 27002, contained 10 categories of security controls. Currently ISO 27002 has 14 categories of security controls. CISSP has always had 10 domains of CBK (Common Body of Knowledge). Some of the sections/domains are more or less the same, but others are specific to either ISO 27002 or to CISSP CBK, so there is no 1-to-1 mapping between the two documents.

Digital forensics and cyber security are relatively new topics. CISSP tends to integrate new topics on one of the 10 domains, whereas ISO 27001 tends to define new categories.

QUESTION 4

a. Describe ways to use social engineering for
    1. getting unauthorized acces into a company building,
    2. installing malware on the personal computer of the CEO of a company.

    Get inspiration from SANS InfoSec Reading Room on Social Engineering (http://www.sans.org/rr/whitepapers/engineering/), or other relevant sources.
b. Assume that people are the access control function against social engineering attacks. What would be a false positive and a false negative in this scenario?
c. When using a firewall as an analogy for human defense against social engineering attacks, what would be the social engineering analogy of configuring the firewall tp protect against network attacks?

Answer

a. Examples of social engineering attacks.
    1. Access to a building can e.g. happen through
        - tailgating behind others, e.g. after lunch break, or with cigarette smokers,
        - carrying heavy boxes and getting helpt to open door
        - producing and presenting a fake access card
    2. Installing malware on the computer of CEO can e.g. happen through:
        - Sending customized spear-phisning email with attached malwar to be installed and executed,
        - Sending customized spear-phishing email with attachment or link to website that contains an exploit of a zero-day vulnerability that is present on the CEO's computer.
b. A false positive is when a legitimate authorized person is challenged. A false negative is when an attacker is not identified.
c. The analogy to configuration firewalls would be to organize awareness training on the appropriate policy and practice to people about how to detect and react to social engineering attacks.