ISA 562
Internet Security Theory & Practice

11. Security Architecture & Evaluation
Domain 5

Objectives

- Security Architecture Description and benefits
- Definition of Trusted Computing Base (TCB)
- System level and Enterprise Security Architectures
- Trusted Systems

Introduction

Security architecture describes how system security is integrated to satisfy security requirements.

Balance requirements ➔ capability, flexibility, , security, performance...

- Security architecture is one aspect of system architecture

Security requirements are not just added steps to the development process but they are specifications or guidelines influencing the life cycle

Major Concepts

- Security related terminology
  - ISMS (Information Security Management System)
  - ISA (Information Security Architecture)
  - Trusted Computing Base (TCB)
  - Security model
- Enterprise Security Architecture
  - Objectives in any enterprise security architecture
    - Guidance
    - Aligning business and security objectives
    - Using security best practices

Major Concepts

- Benefits
  - Manage IT risk at a reduced cost
  - Interoperability, integration, and ease-of-access.
- Components
  - Architecture model
  - Language to be used
  - Use of some architectural framework
- Perspectives
  - People, process, and Technology

Process framework for a Security Architecture

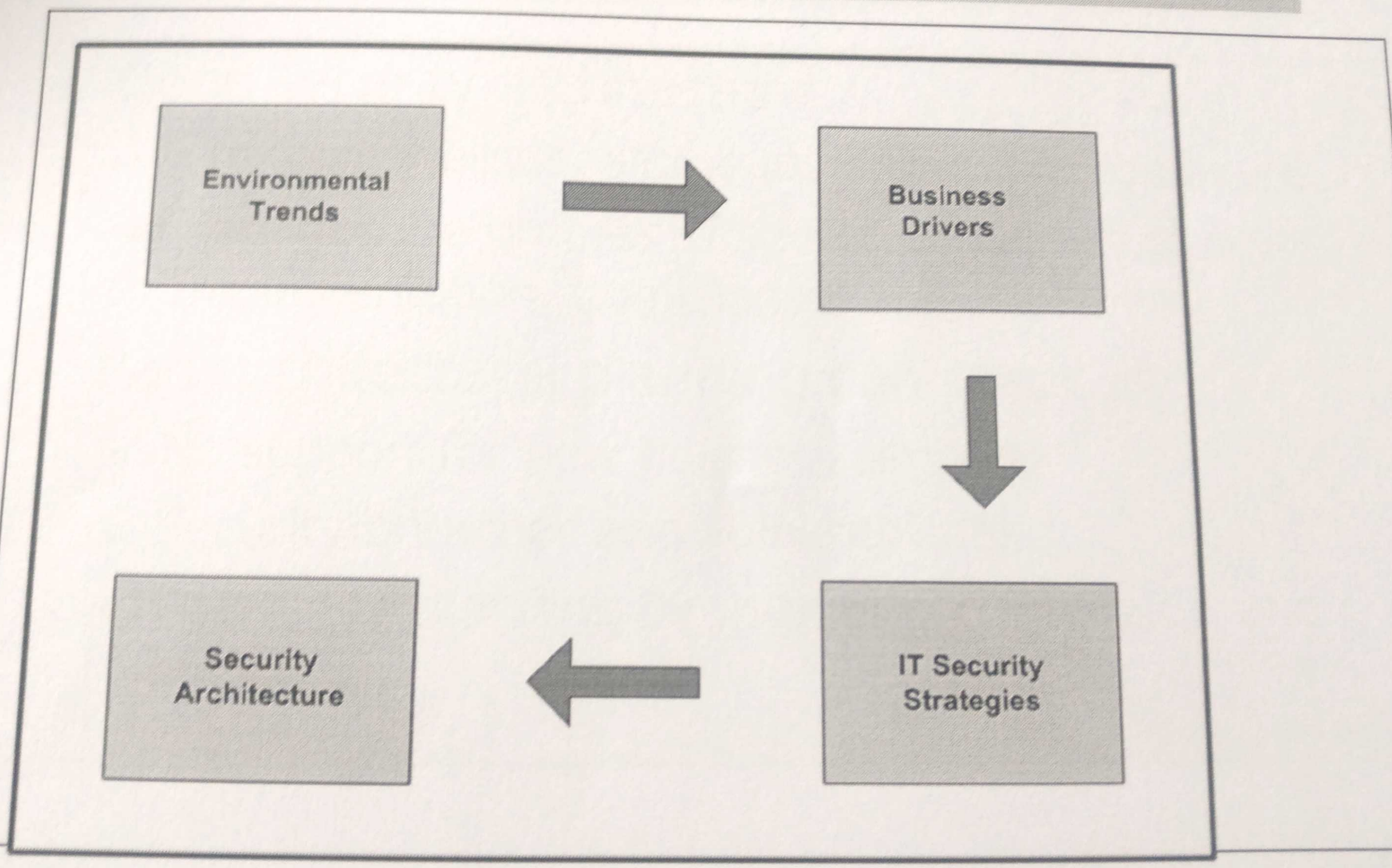
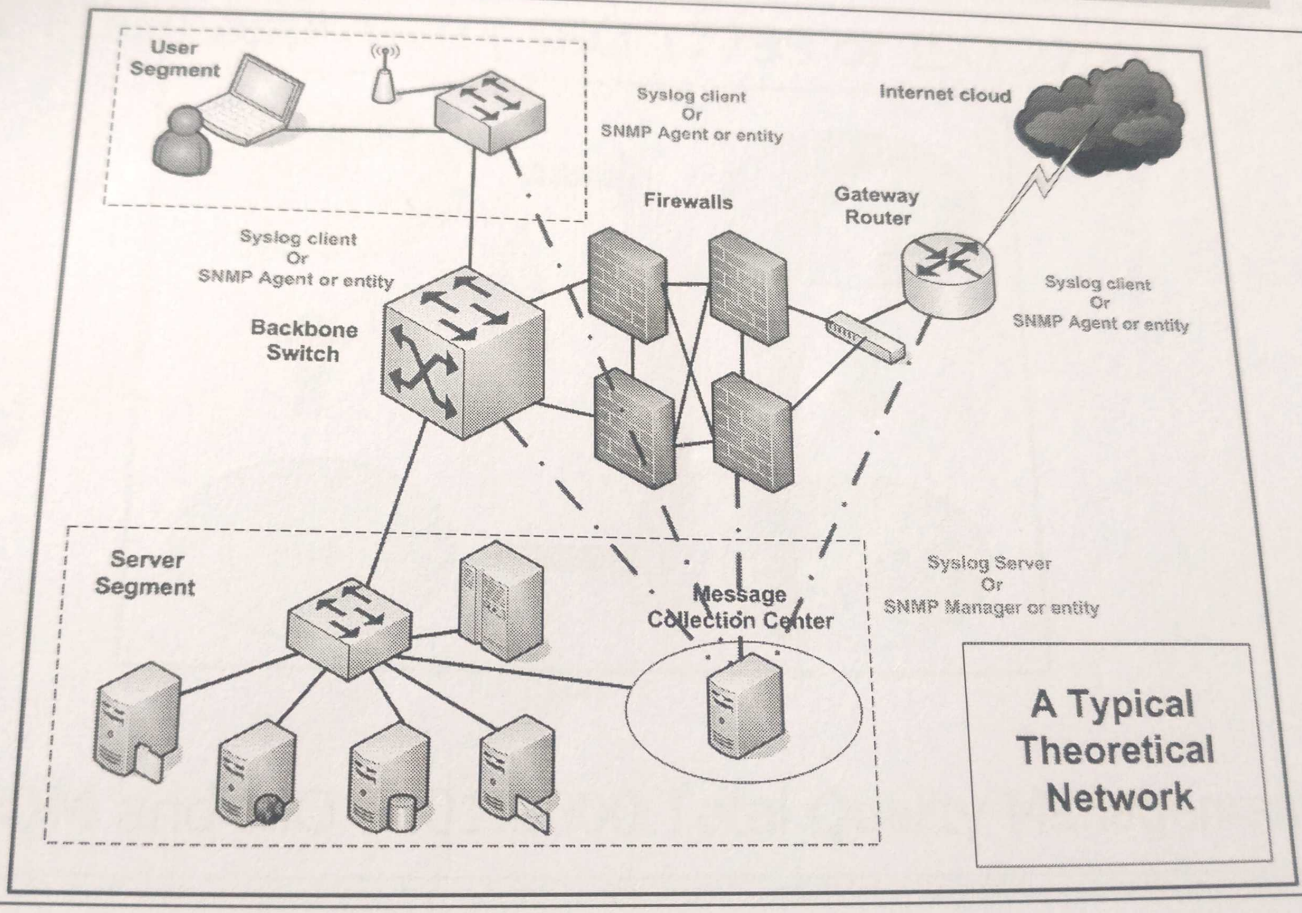


Figure 2

Good and bad architectures

- Good security architecture
  - Strategic, holistic, allows multiple implementations.
  - Manages the process of setting the architecture, Implementation, Compliance, and Monitoring
- Bad architectural planning can result in
  - No support for new business services
  - Security breaches and vulnerabilities
  - Poor understanding by usersof security goals and objectives

A High-Level Design



Enterprise Architecture Frameworks

- PDCA Approach (ISO 17799 or ISO 27001)

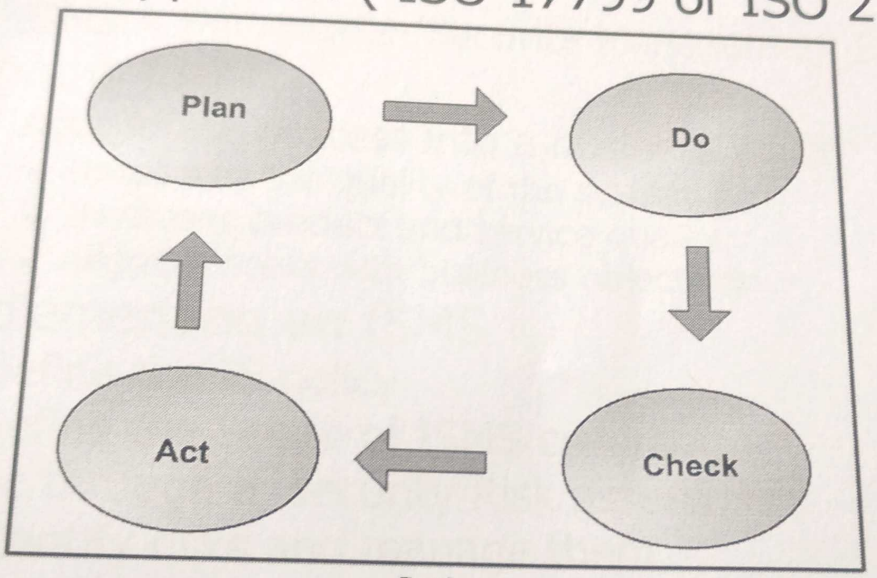


Figure 3

- **TQM** and ISO 9001:2000 Total Quality Management

Enterprise Architecture Frameworks

- What is an ISMS?
  - ISMS = Information Security Management System.
- What is for?
  - Incorporate process into a business which
    - Influences the quality of the system
    - Increases product and service quality
    - Aligns process with business objectives
- Implementing an ISMS
  - Define the IS policy
  - Define the Scope of ISMS coverage
  - Go through a security Risk assessment
  - Identify risks and manage them
  - Select security controls
  - Prepare a statement of applicability

Enterprise Architecture Frameworks - 1

- Zachman Framework
  - Aligns business and IT objectives
- ITIL (Information technology infrastructure Library)
  - Published in the UK: British Standard 15000
  - IT Services delivery
- COBIT (Control Objectives for information Technology)
  - Emphasizes regularity compliance
- Basel II (Financial Risk Management Framework)
  - Establishes basic requirements for risk management
  - Guarantees financial stability standards

Enterprise Architecture Frameworks - 2

- ***Six Sigma*** (process variance control framework)
  - Data driven and measurement based
    - DMAIC
    - DMADV
- COSO (Committee of Sponsoring Organizations)
  - The importance of Identifying and managing risk
- ***CMMI*** (Capability Maturity Model Integration)
  - Based on TQM
  - Improving process
  - Different Maturity levels

System Level Architectural Concepts

- Components which provide basic security services
  - Integrity of computing processes
  - Controlled access to system resources
  - Predictable computing services
- Two components:
  - Hardware
  - Software
- Computer layers include
  - End user
  - Application, which sits on top of
  - Utilities, that sit on top of
  - Operating systems, which sit on top of
  - Hardware

System Level Architecture Concepts

- Some of the operating system services are
  - Process execution
  - Input and output processing
  - Error detection and handling
  - Communication
- Security kernel provides critical security services
- CPU - two different privilege states
  - Supervisor state where system programs execute
  - Application state where application programs and non-privileged programs execute
  - Process states
    - Stopped, running, waiting, etc

System Level Architecture Concepts

- Applications
  - Current applications are portable and execute in a multi-threaded OS.
- System approaches
  - Open or Closed systems
  - Single level or multi-level systems
- System architectures
  - Centralized vs. Distributed

System Level Architecture Concepts

- Memory management requirements
  - Protection: users cannot generate address, users can share access, etc
  - Relocation and Sharing
  - Logical and Physical organization
- Memory Addressing
  - Logical: requires translation to a physical address
  - Relative: location relative to known point (ex: array)
  - Physical: absolute address or actual location

System Level Architecture Concepts

- Virtual memory
  - A process uses more memory than what is available in the physical memory
  - Limited by swap space on disk
  - Uses the concept of pages and segments
- I/O
  - Inter-process communication which involves locating and relocation data and instructions between a number of storage facilities (I/O controller, managing memory, etc)

Basic System Security Concepts

- Trusted Computing base (TCB)
  - Includes all the components and their operating processes and procedures that ensure the security policy of the organization is enforced
  - It should also be simple and testable
  - Enforces security policy
  - Monitors
    - Process activation
    - Execution Domain Switching
    - Memory protection
    - Input/output Operations

Basic System Security Concepts

- Objects that require protection
  - Anything on the system such as: Memory, Operating system tables, Directory files, Data structures, etc
- Reference Monitor Concept
  - Abstract machine
    - Tamperproof
    - Verifiable
    - Always invoked (cannot bypass)
  - Includes
    - Subjects and objects
- What is a Security Kernel?
  - Hardware, firmware, and software elements of a trusted computing base that implements the reference monitor

Establishing Confidence in Trusted Systems

- Evaluation criteria are standardized methods for establishing confidence that products satisfy the **functional** and **assurance** requirements of the organization
  - Trusted Computer System Evaluation Criteria (TCSEC) – The ***Orange book*** (1983-1999)
  - Information Technology Security Evaluation Criteria (ITSEC) (1991-2001)
  - Federal criteria 1992
  - FIPS 140-1 of 1994 and FIPS-2 of 2001
  - ***Common Criteria*** (ISO 15408) (1998-present)