Chapter 3:

SECURITY ASSESSMENT, ANALYSIS AND ASSURANCE

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Intro

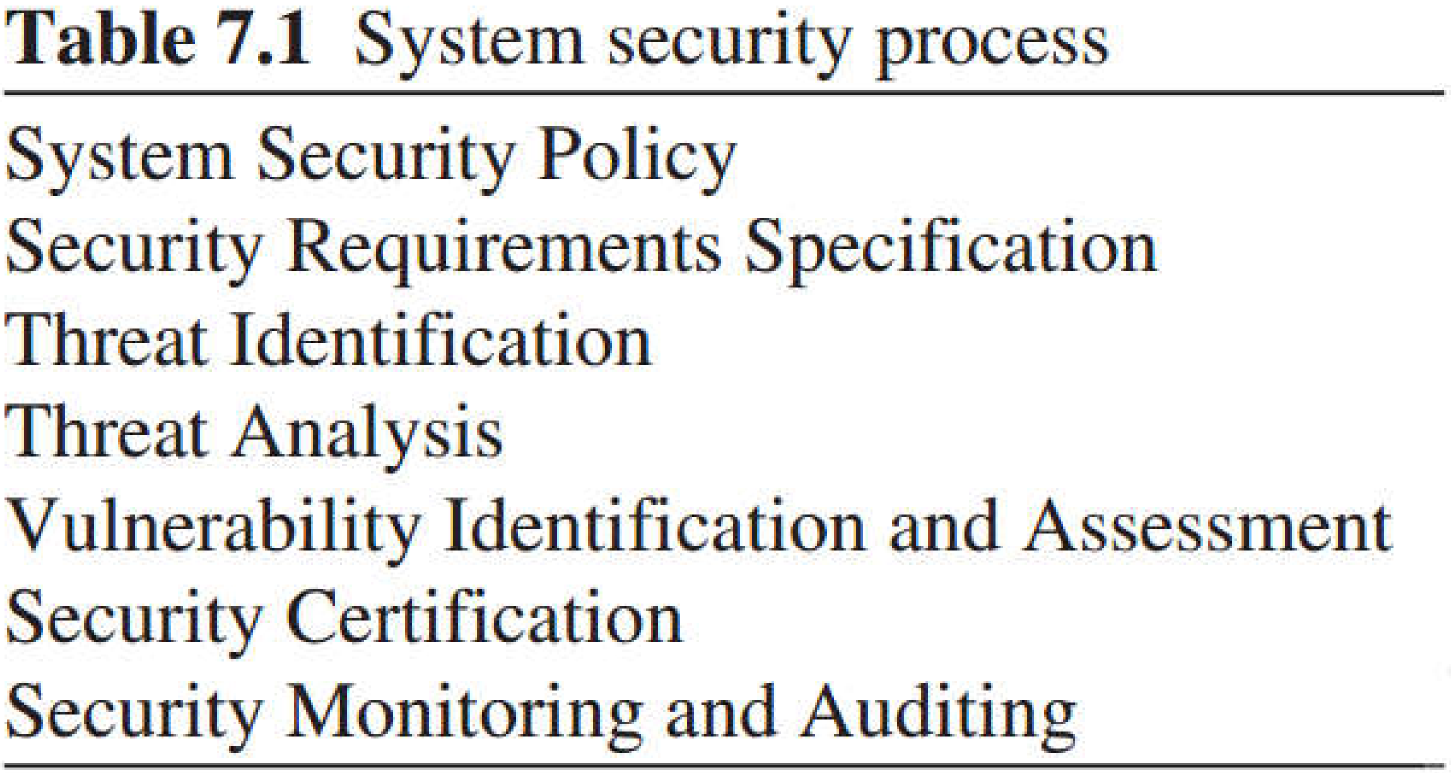

Table 7.1 System security process

System Security Policy

Security Requirements Specification

Threat Identification

Threat Analysis

Vulnerability Identification and Assessment

Security Certification

Security Monitoring and Auditing

System Security Policy

- The security policy also spells out what resources need to be protected and how organization can protect such resources.
- Security policies are still important in the security plan of a system, for several reasons including:
    - Firewall installations: If a functioning firewall is to be configured, its rule base must be based on a sound security policy.
    - User discipline: All users in the organization who connect to a network such as the Internet, through a firewall, say, must conform to the security policy.

System Security Policy

- Without a strong security policy, the organization may suffer from data loss, employee time loss, and productivity loss all.
- A security policy must:
  - Have the backing of the organization top management.
  - Involve every one in the organization
  - Precisely describe a clear vision of a secure environment stating what needs to be protected and the reasons for it.
  - Set priorities and costs of what needs to be protected.
  - Be flexible enough to adapt to new changes.
  - Be consistently implemented throughout the organization.
  - ….

System Security Policy

- To achieve these sub goals, the core steps are:
  - Determine the resources (physical, logical, network) that must be protected, and for each resource, draw a profile of its characteristics.
    - For each identifiable resource, determine the type of threat and the likelihood of such a threat. For each threat, identify the security risk and construct an ordered table for these based on importance. Such risks may include: Denial of service, Disclosure or modification of information, Unauthorized access.
    - For each identifiable resource, determine what measures will protect it the best and from whom.

System Security Policy

- To achieve these sub goals, the core steps are:
  - Develop a policy team consisting of at least one member from senior administration, legal staff, employees, member of IT department, and an editor or writer to help with drafting the policy.
  - Determine what needs to be audited, for example, the following logs can be audited: Logfiles for all selected network hosts, object accesses.
  - Define acceptable use of system resources such as: email, news, web.

System Security Policy

- To achieve these sub goals, the core steps are:
  - Consider how to deal with each of the following: encryption, password , key creation and distributions, wireless devices that connect on the organization’s network.
  - Provide for remote access to accommodate workers on the road and those working from home and also business partners who may need to connect through a Virtual Private Network (VPN).

System Security Policy

- From all this information, develop two structures, one describing the access rights of users to the resources identified and the other structure describing user responsibilities in ensuring security for a given resource.

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Security Requirements Specification

– Security requirements specification derives directly from the security policy document. The specifications are details of the security characteristics of every individual and system resource involved.

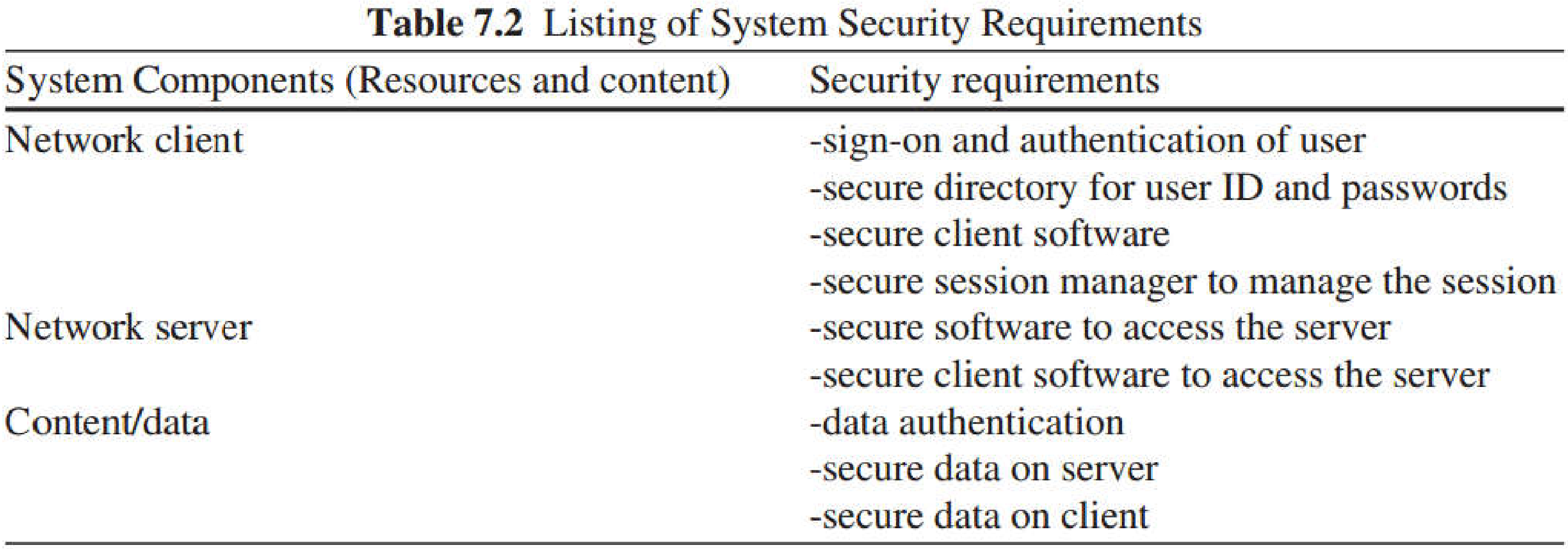

Table 7.2 Listing of System Security Requirements

System Components (Resources and content)	Security requirements
Network client	-sign-on and authentication of user -secure directory for user ID and passwords -secure client software -secure session manager to manage the session
Network server	-secure software to access the server -secure client software to access the server
Content/data	-data authentication -secure data on server -secure data on client

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Threat Identification

- Threat identification is a process that defines and points out the source of the threat and categorizes it as either a person or an event
- The security threats to any system component can be deliberate or nondeliberate.
- The sources of threats are many and varied including:
  - human factors
  - natural disasters
  - infrastructure failures: hardware, software, humanware

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Threat Analysis

- System security threat analysis a process that involves ongoing testing and evaluation of the security of a system’s resources
- to continuously and critically evaluate their security from the perspective of a malicious intruder
- then use the information from these evaluations to increase the overall system’s security.

Threat Analysis

- The process of security threat analysis involves the following:
  - Determining those resources with higher intrinsic value, prioritizing them
  - Documenting why the chosen resources need to be protected in the hierarchy they are put in
  - Determining who causes what threat to whose resources
  - Identifying known and plausible vulnerabilities for each identified resource in the system
  - Identifying necessary security services/mechanisms to counter the vulnerability
  - Increasing the overall system security by focusing on identified resources

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Vulnerability Identification and Assessment

- A security vulnerability is a weakness in the system that may result in creating a security condition that may lead to a threat.
- it is extremely difficult to identify all system vulnerabilities before a security incident occurs
- In fact, many system vulnerabilities are known only after a security incident has occurred
- Searching for system vulnerabilities should focus on system hardware, software, and also humanware.

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Security Certification

- Phases of a Certification Process:
  - Developing a security plan to provide an overview of the system security requirements
  - Testing and evaluation must be done
  - Risk assessment to determine threats and vulnerabilities in the system, propose and evaluate the effectiveness of various security controls
  - Certification to evaluate and verify that the system has been implemented as described in the security policy and that the specified security controls are in place and operating properly

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Security Monitoring and Auditing

- Security monitoring is an essential step in security assurance for a system.
- Tools used to monitor, type of data gathered, and information analyzed from the data.

Security Monitoring and Auditing

- Monitoring Tools
  - System performance: This category includes most operating system performance loggers.
  - Network security: This includes all IDS, firewalls and other types of event loggers.
  - Network performance and diagnosis: These are for monitoring all network performance activities.
  - Networking links: To monitor the wiring in a network.
  - Dynamic IP and DNS event logger.
  - Remote control and file sharing applications event logger.
  - File transfer tools.

Security Monitoring and Auditing

- Type of Data Gathered:
  - Most event loggers are preset to monitor events based on the set conditions.
  - For example, for workstations and servers, the monitor observes system performance, including CPU performance, memory usage, disk usage, applications,DNS Server,… syslog messages from other computers, routers, and firewalls on a network.

Security Monitoring and Auditing

- Analyzed Information:
  - The purpose of a system monitoring tool is to capture vital system data, analyze it, and present it to the user in a timely manner and in a form in which it makes sense.
  - The logged data is then formatted and put into a form that the user can utilize: alert, chart, log, report

Security Monitoring and Auditing

- Auditing: is another tool in the security assessment and assurance of a computer system and network.
- Unlike monitoring, auditing is more durable and not ongoing, and therefore, it is expensive and time consuming.

- System Security Policy
- Security Requirements Specification
- Threat Identification
- Threat Analysis
- Vulnerability Identification and Assessment
- Security Certification
- Security Monitoring and Auditing
- Product and Services

Product and Services

- A number of products and services are on the market for security assessment and audit. These products fall under the following categories:
  - Auditing tools
  - Vulnerability assessment
  - Penetration testing tools
  - Log analysis tools
  - Other assessment toolkits