Network Security Series

Target Course

Networks

Learning Goals

A student shall be able to:

1. Describe foundational security concepts in securing networks and systems.
2. Describe security design principles and identify security issues associated with common threats and attacks.
3. Apply principles of secure design and defensive programming techniques when developing software.

IAS Outcomes

The CS2013 Information Assurance and Security outcomes addressed by this series are:

IAS Knowledge Topic	Outcome
Cryptography	1. Describe the purpose of cryptography and list ways it is used in data communications. [Familiarity] 2. Define the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plain text in cipher text. [Familiarity] 4. Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. [Familiarity] 5. Use cryptographic primitives and describe their basic properties. [Usage]
Foundational Concepts in Security	1. Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, and Availability). [Usage] 2. Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security). [Familiarity] 4. Explain the concept of trust and trustworthiness. [Familiarity]
Network Security	1. Describe the different categories of network threats and attacks. [Familiarity] 2. Describe the architecture for public and private key cryptography and how public key infrastructure (PKI) supports network security. [Familiarity] 3. Describe virtues and limitations of security technologies at each layer of the network stack. [Familiarity] 4. Identify the appropriate defense mechanism(s) and its limitations given a network threat. [Familiarity]
Principles of Secure Design	2. Summarize the principle of fail-safe and deny-by-default. [Familiarity] 3. Discuss the implications of relying on open design or the secrecy of design for security. [Familiarity] 4. Explain the goals of end-to-end data security. [Familiarity] 5. Discuss the benefits of having multiple layers of defenses. [Familiarity] 8. Describe the concept of mediation and the principle of complete mediation. [Familiarity] 9. Describe standard components for security operations, and explain the benefits of their use instead of reinventing fundamentals operations. [Familiarity] 11. Discuss the importance of usability in security mechanism design. [Familiarity]
Threats and Attacks	1. Describe likely attacker types against a particular system. [Familiarity] 3. Identify instances of social engineering attacks and Denial of Service attacks. [Familiarity] 4. Discuss how Denial of Service attacks can be identified and mitigated. [Familiarity]

IAS Knowledge Topic	Outcome
	6. Discuss the concepts of covert channels and other data leakage procedures. [Familiarity]

Dependencies

- A student has successfully completed a data structures course.
- A student has been introduced to the cybersecurity topics covered in Input Validation and Principles.

Summary

The ubiquitous and growing nature of the Internet and its mostly widely used application - the World Wide Web – along with the security challenges present in the Internet Protocol Stack, gives this topic great significance. It is perhaps obvious but worth saying, networking technologies are at the heart of many risks, threats, and attacks.

Modules

Modules 4 through 8 have been used in a networks course in the order listed – from the top of the Internet Protocol Stack down to the physical devices. While we believe that modules 4 through 8, as designed, could be used in a networks course starting at the bottom and working to the top of the Internet Protocol Stack, we have no evidence to support this belief. We present the layers from the top-down because a significant portion of our course is the design and implementation of an application-layer protocol for a fictitious company that distributes hardware devices. Starting at the application-layer allows this semester long project to start by week 3 of our fifteen week semester.

Name	Key Dependency
1. Overview	
2. Common Attack Types	
3. Concepts	
4. Application Layer	
5. Transport Layer	
6. Network Layer	
7. Link Layer	
8. Physical Layer	