System and Network Security Introduction

Building a Secure Organization

Real threats that impact cybersecurity

- Hackers inside and out
- Eavesdropping
- Spoofing
- Sniffing
- Trojan horses
- Viruses
- Wiretaps

A cyber security policy: the foundation of your protection

- Defining your information assurance objectives
- Assessing your exposure

A Cryptography Primer

Securing data with symmetric encryption

- Choosing your algorithm: DES, AES, Rc4 and others
- Assessing key length and key distribution

Solving key distribution issues with asymmetric encryption

- Generating keys
- Encrypting with RSA
- PGP and GnuPG
- Evaluating Web of Trust and PKI

Ensuring integrity with hashes

- Hashing with Md5 and SHA
- Protecting data in transit
- Building the digital signature

Verifying User and Host Identity

Assessing traditional static password schemes

- Creating a good quality password policy to prevent password guessing and cracking
- Protecting against social engineering attacks
- Encrypting passwords to mitigate the impact of password sniffing

Evaluating strong authentication methods

- Preventing password replay using one-time and tokenized passwords
- Employing biometrics as part of multi-factor authentication

Authenticating hosts

- Distrusting IP addresses
- Address-spoofing issues and countermeasures
- Solutions for wireless networks

Preventing System Intrusions

Discovering system vulnerabilities

- Searching for operating system vulnerabilities
- Discovering file permission issues
- Limiting access via physical security

Encrypting files for confidentiality

- Encryption with application-specific tools
- Recovering encrypted data

Hardening the operating system

- Locking down user accounts
- Securing administrator's permissions
- Protecting against viruses

Guarding Against Network Intrusions

Scanning for vulnerabilities

- Searching for rogue servers
- Profiling systems and services

Reducing Denial of Service (DoS) attacks

- Securing DNS

- Limiting the impact of common attacks

Deploying firewalls to control network traffic

- Preventing intrusions with filters
- Implementing cyber security policy
- Deploying personal firewalls

Protecting web services and applications

- Validating user input
- Controlling information leakage

Ensuring Network Confidentiality

Threats from the LAN

- Sniffing the network
- Mitigating threats from connected hosts
- Partitioning the network to prevent data leakage
- Identifying wireless LAN vulnerabilities

Confidentiality on external connections

- Ensuring confidentiality with encryption
- Securing communication with IPSec