Implementing Cisco Unified Communications Security (UCSECv1.0)

Course Objectives

- Identify vulnerabilities in Cisco Unified Communications networks and describe security strategies, cryptographic services, PKI, and VPN technologies
- Implement network infrastructure security features
- Implement Cisco Unified Communications Manager and Cisco Unified Communications endpoint security features
- Implement network infrastructure security features

Prerequisites

The knowledge and skills you must have before attending this course are as follows:

- Working knowledge of converged voice and data networks
- Working knowledge of Cisco IOS gateways, Cisco Unified SRST gateways, and Cisco Unified Border Element
- Working knowledge of Cisco Unified Communications Manager and Cisco Unified Communications Manager Express
- CCNP® Voice certification is recommended

Additional knowledge and skills that will help you benefit fully from the course are as follows:

- Knowledge of network security fundamentals
- Knowledge of Cisco IOS Firewall and Cisco ASA adaptive security appliance firewalls
- Knowledge of IPsec and SSL VPNs
- CCNA® Security certification is recommended

Cisco learning offerings:

- Implementing Cisco Voice Communications and QoS (CVOICE) v8.0 (CVOICE 8)
- Implementing Cisco Unified Communications Manager, Part 1 v8.0 (CIPT1 8)
- Implementing Cisco Unified Communications Manager, Part 2 v8.0 (CIPT2 8)
- Implementing Cisco IOS Network Security (IINS)

Course Outline

Module 1: Vulnerabilities of Cisco Unified Communications Networks and Security Fundamentals

Identify vulnerabilities in Cisco Unified Communications networks, and describe security implementation strategies, cryptographic services, PKI, and VPN technologies.

Lesson 1: Assessing Vulnerabilities of Cisco Unified Communications Networks

- Identify the threats to a Cisco Unified Communications solution
- Describe types of attackers and attacks
- Identify weaknesses of protocols that are used in Cisco Unified Communications networks
- Describe what needs to be considered regarding end users and administrators when dealing with security
- Describe identity spoofing and the identity types that an attacker can impersonate
- Explain examples of DoS attacks
- Describe an example of unauthorized privilege escalation that is achieved by exploiting a buffer overflow issue
- Describe eavesdropping attacks and the techniques that can be employed to perform them
- Describe data manipulation and discuss how data integrity can be compromised
- Describe attacks against Cisco Unified IP phones

Lesson 2: Describing Security Implementation Strategies

- Describe how risk assessment is performed
- Describe guidelines for security implementation
- Describe the function of a security policy
- Describe the need for auditing and how auditing can be performed
- Describe the need for accountability and how accountability can be implemented

Lesson 3: Describing Cryptographic Services and Functions

- Describe cryptographic services
- Describe the characteristics of symmetric encryption and what it is used for
- Describe the characteristics of asymmetric encryption and what it is used for
- Describe the characteristics of hashes and what they are used for
- Describe the characteristics of HMAC and what they are used for
- Describe the characteristics of digital signatures and what they are used for

Lesson 4: Describing Key Management and PKI

- Describe the issues of key management when using symmetric keys and when using asymmetric keys
- Describe the purpose of a PKI
- Describe how a PKI works
- Describe considerations when implementing a PKI
- Describe how commonly used applications utilize a PKI for secure communication

Lesson 5: Describing IPsec and Cisco AnyConnect SSL VPN

- Describe the purpose of IPsec and Cisco AnyConnect SSL
- Describe the characteristics of IPsec
- Describe the operation of IPsec
- Describe considerations when implementing IPsec
- Describe special implementation models of IPsec
- Describe the characteristics of Cisco AnyConnect SSL
- Describe the operation of Cisco AnyConnect SSL
- Describe considerations when implementing Cisco AnyConnect SSL

Module 2: Network Infrastructure Security

Implement network infrastructure security features such as network separation and firewalls, IEEE 802.1X in phone VLANs, and the IP Phone VPN Client.

Lesson 1: Implementing Network Separation and Packet Filtering

- Describe the function of security domains
- Describe network separation methods
- Implement voice VLANs
- Describe how network access control is implemented between security domains and describe how NAT can be used between security domains
- Describe the most important stateless packet filtering features on Cisco IOS routers, Cisco Catalyst switches, and Cisco ASA adaptive security appliances
- Describe how stateful packet filters can be used to provide network access control
- Describe the need for deep packet inspection and how it interacts with network access control
- Describe the operation of application proxies and the features that they provide
- Describe network separation considerations when implementing softphones

Lesson 2: Implementing Switch Security Features

- Describe the security features available in Cisco Catalyst switches
- Describe the characteristics of 802.1X
- Describe how 802.1X works
- Describe how to implement 802.1X

Lesson 3: Implementing Cisco AnyConnect SSL VPNs in Cisco Unified Communications Networks

- Describe the characteristics of the IP phone VPN Client feature
- Describe the trust requirements of the IP phone VPN Client feature
- Describe considerations when implementing the IP phone VPN Client feature
- Describe how to implement the IP phone VPN Client feature
- Describe how to verify proper operation of the IP phone VPN Client feature

Module 3: Cisco Unified Communications Manager and Endpoint Security Features

Harden Cisco Unified Communications endpoints and implement toll-fraud prevention features and Cisco Unified Communications Manager cryptographic security features.

Lesson 1: Hardening Cisco Unified Communications Endpoints

- Describe general guidelines for device hardening, including Cisco IOS devices
- List IP phone and Cisco Unified Communications Manager hardening options
- Describe how to control access to the Settings button on the IP phone in Cisco Unified Communications Manager
- Describe how to control PC port access at the IP phone in Cisco Unified Communications Manager
- Describe how to process GARP packets at the IP phone in Cisco Unified Communications Manager
- Describe how to control IP phone web server access in Cisco Unified Communications Manager

Describe how to harden Cisco IOS gateways

Lesson 2: Implementing Toll-Fraud Prevention

- List toll-fraud prevention features
- Describe the purpose and the configuration of class classification in Cisco Unified Communications Manager
- Describe how Cisco Unified Communications Manager can be configured to block external-to-external transfers
- Describe how Cisco Unified Communications Manager can be configured to drop ad hoc conferences when no on-net party remains in the conference
- Describe how CoS can be implemented in Cisco Unified Communications Manager in order to avoid toll fraud
- Describe how Cisco Unified Communications Manager can be configured to force an end user to enter a valid FAC before processing calls
- Describe how call monitoring and accounting can be configured in Cisco Unified Communications Manager in order to detect and prevent toll fraud
- Describe how Cisco Unified Communications Manager Express and Cisco IOS gateways can be configured for toll-fraud prevention

Lesson 3: Implementing Native Cisco Unified Communications Manager Security Features

- Describe how Cisco Unified Communications Manager protects IP phones by using firmware that is digitally signed
- Describe SIP digest authentication, what attacks it can mitigate, and how it is implemented for IP phones and SIP trunks
- Describe how SIP trunks can be configured to use TLS for signaling and SRTP for media
- Describe how IPsec is supported in Cisco Unified Communications Manager
- Describe the purpose of the Security by Default feature
- Describe the components of the Security by Default feature
- Describe how an IP phone can validate received certificates using CVS and describe how configuration file protection is provided by Security by Default
- Describe how Security by Default interacts with other security features

Lesson 4: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens

- Describe the issuers of certificates that are used in a secure Cisco Unified Communications Manager environment
- Describe the purpose of the CTL file
- Describe how a CTL file is created or updated
- Describe how the CTL file interacts with the ITL file
- List the security features that rely on the CTL file
- Describe how Cisco Unified Communications Manager provides secure signaling to IP phones
- Describe how Cisco Unified Communications Manager enables IP phones to use secure media exchange to other IP phones
- Describe how Cisco Unified Communications Manager provides IP phone configuration file encryption
- Describe how Cisco Unified Communications Manager can provide secure conference bridges to IP phones

- Describe the impact of encrypted signaling on intermediate network devices providing NAT or firewall services

Module 4: Secure Cisco Unified Communications Integration and Features

Implement secure Cisco Unified Communications Manager integration with external devices such as gateways, firewalls, and application proxies.

Lesson 1: Implementing SRTP to Gateways and Signaling Protection by IPsec

- Provide an overview of secure Cisco IOS gateway communication
- Describe the signaling and media protection options between the Cisco Unified Communications Manager and a SIP gateway
- Describe the media protection to MGCP gateways
- Describe the media protection to H.323 gateways
- Describe how to configure IPsec for signaling encryption

Lesson 2: Implementing Secure Signaling and SRTP in SRST and Cisco Unified Communications Manager Express

- Describe the trust requirements for secure SRST
- Describe how IP phones can trust their SRST gateway
- Describe how SRST gateways can trust IP phones
- Describe secure SRST operation
- Describe how to implement secure SRST
- List security features provided by Cisco Unified Communications Manager Express
- Describe the PKI topology and trust requirements when implementing secure Cisco Unified Communications Manager Express
- Describe additional Cisco Unified Communications Manager Express security features
- Describe how to implement security features in Cisco Unified Communications Manager Express

Lesson 3: Implementing Trusted Relay Points

- Describe the purpose of trusted relay points
- Describe the characteristics of trusted relay points
- Describe the components of trusted relay points
- Describe how trusted relay points work
- Describe how to implement trusted relay points

Lesson 4: Implementing Proxies for Secure Signaling and SRTP

- Describe the purpose and function of an application layer gateway, also known as a proxy
- Describe the purpose and functions of Cisco Unified Border Element
- Describe Cisco Unified Border Element security features including signaling and media proxy
- Describe how to configure Cisco Unified Border Element as signaling and media proxy
- Describe the purpose and functions of the Cisco ASA adaptive security appliance TLS proxy feature
- Describe how to configure a TLS proxy in the Cisco ASA adaptive security appliance
- Describe the purpose and functions of the Cisco ASA adaptive security appliance phone proxy feature
- Describe how to configure a phone proxy in the Cisco ASA adaptive security appliance

- Describe the differences between Cisco Unified Border Element, TLS proxy, and phone proxy

UCSEC v1.0 Labs

- Lab 1-1: Identifying Security Weaknesses in a Cisco Unified Communications Network
- Lab 2-1: Implementing Firewalls
- Lab 2-2: Implementing 802.1X
- Lab 2-3: Implementing Cisco AnyConnect SSL VPNs
- Lab 3-1: Implementing Cisco Unified Communications Manager Security Features Based on Security Tokens
- Lab 4-1: Implementing SRTP to Gateways and Signaling Protection by IPsec
- Lab 4-2: Implementing Secure SRST and Secure Cisco Unified Communications Manager Express
- Lab 4-3: Implementing Trusted Relay Points
- Lab 4-4: Implementing Proxies for Signaling and RTP