Securing IPv6 (3 days)

How to secure your network against IPv6 related threats in a multi-vendor commercial environment

Relevant Platforms:

- **Cisco IOS**
- **Juniper JunOS**
- **Linux (RHEL, CentOS, Unbuntu, Suse etc)**
- **Unix (HP-UX, AIX, Solaris)**
- **HP Routers and Switches**
- **Microsoft Windows**

You Will Learn

- The current status of IPv6
- The new features of IPv6
- How IPv6 works
- How to deploy IPv6
- The security features of IPv6
- IPv6 security risks
- The differences in IPv4 and IPv6 security
- Security threats of IPv6 transition mechanisms
- How to securely deploy IPv6
- How to secure your IPv4 network from IPv6 threats
- IPv6 threat mitigation
- How to build IPv6 firewalls
- IPv6 security best practice

Course Benefits

IPv6 is becoming widely deployed. It is standard in all modern operating systems, major network equipment and applications.

Even if not explicitly deployed in your organisation, your network devices and operating systems will support IPv6 and many of IPv6's transition mechanisms. So whilst you may not have implemented IPv6 in your network yet, you still need to secure your network against abuse using IPv6 protocols.

Modern network operating systems, including Windows, Linux, Unix, Mac OS and mobile operating systems (such as Android), support IPv6 and will use IPv6 in preference to IPv4. Further most have IPv6 turned on by default.

You need to ensure that your network is IPv6 secure and that you are ready for any future implementation of IPv6.

IPv6 brings many new security challenges and opportunities. New security techniques need to be understood and implemented. The transition to IPv6 from IPv4 presents particular security issues.

This course covers IPv6 security in detail. Each area is explained and practical guidance on mitigating each security threat is provided.

Who Should Attend

This course is intended for IT security experts, system administrators and network administrators.

A good knowledge of general networking concepts is assumed. Experience of IPv4 is necessary and experience of network security is recommended.

Course Contents

IPv6 Basics

- Comparison of IPv6 and IPv4
- What is IPv6?
- Why is IPv6 required?
- Address Space
- Is there an address shortage?
- IPv6 improvements over IPv4
- New features in IPv6
- The benefits of IPv6
- Motivations to implement IPv6
- IPv6 status summary
- Timescale predictions
- Reality Check: IPv6 verses IPv4

Overview of the IPv6 Protocols

- IPv6 datagram header
- IPv6 addresses
- IPv6 extension headers
- ICMPv6
- Multicast IPv6
- IPv6 auto configuration (SLAAC & DHCPv6)
- IPv6 neighbor discovery
- Router discovery in IPv6
- Router Renumbering
- RIPng, OSPFv3, IS-IS and ERIGP
- BGP and IPv6
- IPv6 IPsec
- Mobile IPv6
- IPv6 and QoS
- DNS and IPv6

IPv6 Transition Mechanisms Overview

- IPv6 dual stacks
- 6to4 and 6over4
- IPv6 rapid deployment (6rd)
- ISATAP and Teredo
- Dual stack Lite (DS-Lite)
- BIS and BIA
- SIIT, DNS64, NAT64 and NAT-PT
- Transport Relay Translator (TRT)
- IPv6 and MPLS: 6PE and 6VPE

General Principles of Network Security

- Network security basics
- Analysis and threat mitigation

IPv6 Security Threats

- Summary of IPv6 threats
- Comparison of IPv6 with IPv4 threats
- Threats common to IPv4 and IPv6
- IPv6 specific security threats
- IPv6 address architecture threats
- End-to-end transparency
- Scanning in IPv6
- IPv6 extension header threats
- IPv6 router header abuse
- IPv6 fragmentation threats
- ICMPv6 threats
- IPv6 neighbor discovery (ND) threats
- DHCPv6 threats
- IPv6 security testing tools
- Reality Check: IPv4 vs. IPv6 Security

Basic IPv6 Security Features

- Security features in IPv6
- Privacy addresses
- Temporary addresses
- RA-Guard
- IPv6 multicast security and MLD snooping
- Mobile IPv6 security
- DHCPv6 security and DHCPv6-Shield
- Dynamic routing security

IPv6 Security (IPsec)

- Cryptographic techniques
- IPv6 and IPsec
- IPv6 AH & ESP Headers
- Transport and tunnel modes
- Security associations
- ISAKMP & IKE

Securing Neighbor Discovery I

- Neighbor discovery threats
- Cryptographically Generated Addresses (CGA)
- SEcure Neighbor Discovery (SEND)
- Certificate Path Messages

Securing Neighbor Discovery II

- Monitoring Neighbor Discovery (ND)
- Mitigating Router Advertisement (RA) attacks
- Mitigating NDP Interference
- Securing Router Advertisements (RAs)
- Deploying and configuring RA-Guard
- Security at the datalink
- IEEE 802.1X

IPv6 Transition Security

- IPv6 transition mechanisms threats
- Transition security problems
- Dual stack threats and mitigation
- Tunnelling threats
- 6to4 threats and mitigation
- 6rd threats and mitigation
- ISATAP threats and mitigation
- Teredo threats and mitigation
- DS-Lite threats and mitigation
- Securing translation techniques (NAT64 etc)
- Securing IPv6 MPLS: 6PE and 6VPE
- IPv6 DNS threats and mitigation
- Transition security best practice

Building IPv6 Firewalls

- Configuring IPv6 firewalls
- IPv6 firewall filtering rules
- Filtering ICMPv6
- IPv6 extension headers
- Implementing IPv6 Ingress filtering
- Assigned IPv6 addresses
- Status of IPv6 firewalls and IDS
- Deploying IPv6 firewalls
- Mitigating IPv6 DDoS attacks
- Deploying IPv6 IPS

IPv6 Deployment Risks

- IPv6 pilots
- Securing dual stack hosts
- IPv6 DNS server
- Addressing schemes
- Deploying ICMPv6
- End-to-end transparency
- IPsec transport mode
- Reduced functionality
- Operational issues
- ND proxies

IPv6 Security Best Practice

- Creating an IPv6 security policy
- IPv6 security assessments
- IPv6 forensics
- Summary of IPv6 security best practice

Hands-on IPv6 Practical Labs

Each module includes detailed exercises. Hands-on IPv6 practical exercises include:

- Basic IPv6 configuration and auto configuration
- Configuring IPv6 routing
- Examining IPv6 threats
- Using the IPv6 hackers toolkit
- Using Scapy and IPv6
- Observing and mitigating IPv6 DDoS attacks
- Configuring IPv6 IPsec
- Using privacy and temporary addresses
- Protecting against router advertisement attacks
- Detecting and mitigating ND attacks
- Implementing SEND and CGA
- Securing transition mechanisms including 6to4, 6rd, ISATAP, Teredo and NAT64
- Securing IPv6 firewalls and IPv6 hosts
- IPv6 security policy and best practice

The IPv6 Trainers

Trainers are practising IPv6 consultants with extensive experience of IPv6 and network security. Further information can be found at www.erion.co.uk. Erion is the world's leading IPv6 training company.

Company Registration: 3521142

VAT Number: 698 3633 78