

7<sup>th</sup> - 8<sup>th</sup> December 2011 Jw Marriot Dubai UAE

## Overview:

The training will focus on the fundamental security deployment issues for IPv6-enabled networks. The training will attempt to enumerate all of the considerations to be accounted for when creating an appropriate security policy and architecting the IPv6 network to incorporate appropriate security measures. The technical merits and tradeoffs are discussed to add a practical component based on recent deployment experiences. It is assumed that the participant is familiar with basic IP operations and has a fundamental understanding of network security issues.

As IPv6 networks migrate from lab environments into dependable production systems, operations are presented with both the challenge of adapting to a new protocol and the opportunity to leverage new features to enhance network security. Native IPv6 networks will coexist with environments where IPv6 capabilities are introduced into production networks with existing IPv4-based infrastructures. While security of current production networks must be evolved for IPv6, there are features in IPv6 and new trends in networking that should lead to changing security paradigms. End-to-end security between hosts has had limited practicality in IPv4-based networks but is a key feature of IPv6. A return to the end-to-end network model should be architected into any dual stacked transition architecture with careful consideration for not compromising IPv4 security. A combination of application, host and network-based security is required to securely conduct business on the network of networks which make up the Internet.

The 2 days training will enumerate the security advantages which are relevant in today's IPv6 networks and will detail the deployment considerations to effectively design and architect secure IPv6 networks.

## Objectives of the course:

After attending this training, you will be able to:

- Understand the basics of IPv6 Security
- Secure IPv6 networks against threats and attacks
- Implement security standards and processes to protect your IPv6 network
- Create a secure IPv6 infrastructure
- Plan ahead to avoid IPv6 security problems before widespread deployment
- Identify known areas of weakness in IPv6 security and the current state of attack tools and hacker skills
- Analyze and react to denial-of-service (DoS) attacks
- Understand each high-level approach to securing IPv6 and learn when to use each
- Protect service provider networks, perimeters, LANs, and host/server connections
- Harden IPv6 network devices against attack
- Utilize IPsec in IPv6 environments
- Secure mobile IPv6 networks
- Secure transition mechanisms in use during the migration from IPv4 to IPv6
- Monitor IPv6 security
- Understand the security implications of the IPv6 protocol, including issues related to ICMPv6 and the IPv6 header structure
- Protect your network against large-scale threats by using perimeter filtering techniques and service provider-focused security practices
- Understand the vulnerabilities that exist on IPv6 access networks and learn solutions for mitigating each

## Who Should Attend:

- **IP networks Engineers, Staff,Managers**
- **I.T Security Staff, Managers**
- **Technical Staff,Managers**

# 2 Days Course Outline

## 1 – Part 1

### IPv6 characteristics

#### 1.1 - Reintroduction to IPv6

- IPv6 in a nutshell
- Comparing IPv4 and IPv6
- IPv6 Header Format
- IPv4 Compatibility
- IPv6 Operation
- IPv6 Addressing Architecture
- ICMPv6 and Neighbor Discovery Protocol
- Using DNS and DHCP with IPv6
- Supporting Security and Mobility with IPv6
- Routing in IPv6 Networks
- Using IPv6 services
- IPv6 operation and Architecture
- Basic transition mechanisms
- Tunneling protocols create new risks
- IPv6 autoconfiguration

#### 1.2 - IPv6 and IPv4 Threat Comparison

- Encryption
- Digital Signatures
- Public Key Infrastructure (PKI)
- Dealing with Technology Evolution
- Network Security Awareness
- Best-Practice Evaluation
- Threat Analysis Attacks with New Considerations in IPv6
- Reconnaissance
- Unauthorized Access
- Header Manipulation and Fragmentation
- Layer 3-Layer 4 Spoofing ARP and DHCP Attacks Broadcast Amplification Attacks (smurf)
- Routing Attacks
- Viruses and Worms
- IPv6 and IPv4 Threat Comparison
- Translation, Transition, and Tunneling Mechanisms
- Attacks with Strong IPv4 and IPv6
- Similarities
- Sniffing
- Application Layer Attacks
- Rogue Devices
- Man-in-the-Middle Attacks
- Flooding
- IPv6 and IPv4 Threat Comparison
- IPv6 Security Considerations
- Authorization for Automatically Assigned Addresses and Configurations
- Protection of IP Packets
- Host Protection from Scanning and Attacks
- Control of What Traffic is Exchanged with the Internet
- Reconnaissance Tools

#### 1.3 - IPsec and IPv6

- IPsec architecture
- The Security Policy Database (SPD)
- Security Association Database (SAD)
- Peer Authorization Database (PAD)
- SA and Key Management
- IP Traffic Processing
- AH and ESP Headers AH and ESP security protocols
- Tunnel mode and transport mode
- Security policy (SP)
- Selector

#### 1.3 Continue...

- Security Association (SA), Key exchange protocols
- Security Protocols
- AH and ESP
- Security Parameter Index (SPI)
- Sequence Number
- Virtual Private Networks (VPNs)
- Host-to-Host IPsec
- Site-to-Site IPsec Configuration
- Remote Access with IPsec
- SSL VPNs
- IP VPN Services
- Attacking IPsec VPNs
- Check Point VPN Security Issues
- Microsoft PPTP
- VPN Services Countermeasures

## 2 – Part 2

### IPv6 Security Issues

#### 2.1 - Introduction to IPv6 Security

- IPv6 Security Essentials
- Popular and Famous Attacks
- Hacker Threats for IPv6
- Neighbor Discovery
- DHCPv6
- Denial of Service
- Neighbor Spoofing Attack
- Neighbor Poisoning
- ICMPv6 Attacks
- Anycast Threat
- Hacker Experience
- IPv6 Security Mitigation Techniques
- Large-Scale Internet Threats
- Ingress/Egress Filtering
- Securing BGP Sessions
- IPv6 over MPLS Security
- Prefix Delegation Threats
- Multihoming Issues
- IPv6 Perimeter Security
- IPv6 Firewalls
- Physical Security
- Developing Security Policies, Assessments and Procedures
- IPv6 Security Considerations and Recommendations
- IPv6 Neighbor Discovery trust models and threats
- Implementing Security for IPv6, Cisco Documentation
- Security Implication of Mixed IPv4/IPv6 Network
- IPv6 end-to-end security
- Managing privacy extensions
- IPsec, VPNs, IKE, PKI
- IPv6 autoconfiguration
- Mobile IPv6 Operation
- MIPv6 Messages
- Threats Linked to MIPv6
- Using IPsec with MIPv6
- Filtering for MIPv6
- Other IPv6 Mobility Protocols

### Daily Course Schedule

0830 – 0845	Registration
0900 –	Training Starts
1030 – 1045	Coffee Break
1045 –	Training Starts
1245 – 1345	Lunch Break
1400 –	Training Starts
1500 – 1515	Coffee Break
1515 –	Training Starts
1600 –	End of The Training

## 2.2 - IPv6 Network Vulnerabilities and Attacks

- Detailed analysis of IPv6 headers
- Elimination of NAT
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)
- Ethernet LAN Security
- Frame Relay Network Security: Vulnerabilities and Mitigations
- ICMP Attacks
- IPv6 Spoofing
- ICMP, ICMP Attack, Ping Attack, Smurf Attack, PING Flood, Ping of Death
- Land Attack
- Network Security at the Data Link Layer (Layer 2) of LAN
- Network Security at the Network Layer (Layer 3: IP)
- Network Security at the Transport Layer (Layer 4: TCP and UDP)
- Pharming and Anti-pharming Mitigations and Technologies
- Phishing and Anti-phishing Mitigations and Technologies
- Port Scan Attack
- Public-Key or Asymmetric Cryptography
- RIP Routing Attacks
- Smurf Attack and Fraggle Attack
- SPAM and Anti-Spam Technologies
- Spyware and Anti-Spyware Mitigations and Technologies
- TCP Connecting Hijacking: MAN-In-The-Middle Attack
- TCP "SYN" Attack
- TCP/IP Network Vulnerability and Security
- UDP Flood Attack
- Widely Used Attack Tools
- Virus and Antivirus Technologies
- Top Information and Networking Threats

## 2.3 - IPv6 Security Considerations

- ICMPv6 Protocol Protection
- Hardening IPv6 Network Devices
- Threats Against Network Devices
- Disabling Unnecessary Network Services
- IPv6 Device Management
- Threats Against Interior Routing Protocol
- First-Hop Redundancy Protocol Security
- Controlling Resources
- QoS Threats
- Server and Host Security
- IPv6 Host Security
- IPsec and SSL VPNs
- Implementing Dual-Stack Security
- Hacking the Tunnels
- Attacking NAT-PT
- IPv6 Latent Threats Against IPv4 Networks
- Security Monitoring
- Managing and Monitoring IPv6 Networks
- Managing IPv6 Tunnels
- Forensics Techniques
- Using Intrusion Detection and Prevention Systems
- Managing the Security Configuration
- Changing Security Perimeter
- Creating an IPv6 Security Policy
- Securing the Transition Mechanisms
- Understanding IPv4-to-IPv6 Transition Techniques

## 2.4 - Firewalls, Perimeter Protection, and VPNs

- IPv6 Stimulus/Response and Fragmentation
- Complex IP Transports and Services
- TCPdump, WINDump, Ethereal and Other Sniffers
- Static Packet Filtering
- Stateful Packet Filtering and Inspection
- Proxies

## 2.4 Continue...

- Popular IPv6 Firewall Products
- Implementing Security with Cisco Routers
- Intrusion Detection
- Centralized Logging
- Firewall Log File Analysis
- Log File Alerting
- IPsec, SSL, and SSH
- Designing a Secure Perimeter
- Network and Host Based Auditing
- Network-Based Attacks
- Memory Attacks, Buffer Overflows
- File System Attacks, Race Conditions
- Trojan Horse Programs and Rootkits
- Monitoring and Alerting Tools
- Network Security Tools
- Policies and Operations
- DMZ: DeMilitarized Zone in Networks
- Layered Defenses of Network and Information Security

## 3 – Part 3

### 3 - IPV6 Security Audit & Control

- Host- and Network-based Intrusion Detection
- Firewalls and Honeypots
- Vulnerability Scanners
- Computer Security Policies
- Password Management
- Incident Handling
- Information Warfare
- Encryption
- VPN's, PKI, and PGP
- Common Vulnerabilities in Wireless IPsec/VPN Deployments
- Firewall Test, Port Scan, Spy Ware and Security Audit
- Find Security Holes
- Developing IPV6 security standards



### Your Trainer

**Luis Sousa Cardoso**

**Senior Consultant of Network Security,  
Quality & Fraud, FIINA President**

Luis is a Senior Consultant who is engaged in Network Security, Quality of Service, and Fraud within Telecom industry. His previous assignments have included technical and management positions in the areas of planning, quality control and traffic engineering. He was Company representative to CCITT Study Group 1 during 1984-1988 study period and has been company representative to CCITT Study Group 2 and Quality of Service Development Group since 1985. Since March 92 he is acting as Chairman of Quality of Service Development Group (ITU).

In addition he has been the Company representative in FIINA (Forum International Irregular Network Access) in which he became member of the Executive Committee during 1995 and was appointed as President in October 2001 being re-elected with mandate till 2012.

since September 2001 he is acting as Chairman of the Working Group on "Network Security, Cybercrime and Fraud Control".

He has worked as a Consultant on the Telecommunications Security area for several companies in USA, Europe, Africa and Asia, and acting as Vice President of the Portuguese National Quality Committee for Information Technology. He is member of the Institute of Electrical and Electronics Engineers, Inc. and of Computer Society. Since June of 1996 he is an active member of the New York Academy of Sciences.

**Registration Form**

1st Delegate  
 Name Mr/Mrs/Ms   
 Position   
 Telephone  Mobile   
 Email   
 2nd Delegate  
 Name Mr/Mrs/Ms   
 Position   
 Telephone  Mobile   
 Email   
 3rd Delegate  
 Name Mr/Mrs/Ms   
 Position   
 Telephone  Mobile   
 Email

**AUTHORIZATION**

(This form is invalid without a signature or company stamp)

Organization   
 Address   
 Country   
 Telephone  Fax   
 Authorizing Person   
 Position   
 Signature-----Date



www.invention-i.com  
 Phone:+603-2162 5485  
 Fax:+603-2162 7485  
 Email: telecom.training@invention-i.com

**IPv6 Security**

7<sup>th</sup> - 8<sup>th</sup> December 2011 JW Marriot Hotel Dubai UAE

- Single Booking**      USD 1,995 / Per Delegate
- Group of 3 and above**      USD 1,795 / Per Delegate

**FOR INVOICE PURPOSE**

Contact Person

Name   
 Position   
 Tel  Fax   
 Email

**Terms and Conditions:**

- 1. Training Fee**  
 Fee is inclusive of course materials and refreshments and does not include accommodation or transportation
- 2. Payment Terms**  
 Once a completed registration form is received, full payment is required within 5 business days from receipt of invoice. PLEASE NOTE: payment must be received prior to the event date. A receipt will be issued once payment is received.
- 3. Confirmation Details**  
 Joining instructions such as Confirmation Letter, Location Map, etc will be sent to the concerned delegate (s) or contact person once a completed registration form is received.
- 4. Cancellation/Substitution/Addition of Delegate (s)**  
 Substitutes for registered delegates is welcome at any time, provided the organizer is notified either by official fax or email. Additional delegates are welcome subject to seat availability. All cancellations after a registration is communicated to the organizer either by fax or email will carry a 10% penalty of the regular fee. Cancellation with less than 2 weeks prior to the event date carry a 100% liability.
- 5. Invention reserves the right to cancel/omit or re-schedule the event.**
- 6. Certificate**  
 All participants who complete the course will receive a Certificate of Attendance, signed by the trainer. Please ensure when registering that your name is written the way you want it to appear on your Certificate.
- 7. Copyright**  
 All intellectual property rights in all materials produced or distributed in relation with this event is expressly reserved with INVENTION INTERNATIONAL and any unauthorized duplication, publication and distribution is prohibited.