

Securing Your Wireless Networks

Nature and Objectives: The rapid development of wireless technologies and industry standards enables organizations to strengthen their communication and enhance the applications of IT at reduced costs. Wireless technologies provide unique benefits of quick, flexible and inexpensive deployment and modification. However, it also creates concerns in deployment, management and security. Even if you are experienced with traditional / wired networks, you need to take a step back and survey the technology, the facility where the network will be installed, and the equipment that is available before you jump in and start building wireless networks. The course provides participants with comprehensive information to design, implement and manage wireless networks.

Who Should Attend: Professionals responsible for making decision to invest, design, implement and administer of wireless networks.

Fee(HK\$): 4,000 / 3,600(*Enrolment on or before Oct.6, 2008*)

Course Outline

OVERVIEW OF WIRELESS COMMUNICATION

- ◆ WiFi/2G/3G/Bluetooth Security
- ◆ Wi-Fi standards and Surveying other wireless technologies
- ◆ 802.11(Wi-Fi) Standards and Bluetooth WPANs (802.15)
- ◆ Advantages of the Wi-Fi Networks

WIRELESS NETWORK FUNDAMENTALS

- ◆ Wireless Communication Basics
- ◆ Radio Frequency and Spectrum, DSSS, FHSS, OFDM: Radio bands, Channels, Range
- ◆ Basic Wi-Fi network components: Access Points, client stations; Ad-hoc and Infrastructure mode

WIRELESS NETWORKS IMPLEMENTATION

- ◆ Wireless Network Architecture and Design
- ◆ Wireless Network Deployment
- ◆ Optimizing coverage topography
- ◆ Eliminating interference: Wi-Fi channels, Frequency reuse
- ◆ Extending range with antennas: Measuring signal strength, Attenuation, Antenna characteristics
- ◆ MIMO (Multiple-In, Multiple-Out) Smart Antenna
- ◆ Site survey
 - Enforcing Access Controls, MAC filtering etc.
 - Identifying interference sources
 - Defining the trusted boundary
 - Integrated corporate WLAN
 - Visitor and guest networks
 - Public hot spots

WIRELESS SECURITY

- ◆ Security Management, Wireless Security Policy into the Corporate IT Security Policy.

WIRELESS SECURITY

- ◆ Understanding 802.11 Security Threats: Risks of Packet Analysis and MAC address Spoofing
- ◆ Assessing network vulnerabilities
 - Types of Attacks
 - Peer attacks and Information Theft.
 - Susceptibility of wireless-enabled laptops
 - WAR driving
- ◆ Detecting Wireless Attacks
 - Discovering WLANs
 - Probing for Wireless Access Points
- ◆ Security weaknesses of and attacks to wireless LANs
 - Exploiting the Collision Avoidance (CA) mechanism
 - RF Jamming and Data Flooding (DoS)
 - Rogue Hardware and Default Settings for WLAN equipment
 - Malicious and inadvertent interference
 - Intercepting Wi-Fi traffic
 - Forcing client de-authentication
- PROTECTING DATA AND ACCESS CONTROLS**
- ◆ Wired Equivalent Privacy (WEP)
 - Cryptography in Wireless Network
 - RC4, AES, RSA
 - Breaking Wireless Equivalent Privacy (WEP)
- ◆ Security protocols for Wireless LANs
 - Wi-Fi Protected Access 802.11i (WPA/WPA2)
 - Temporal Key Integrity Protocol (TKIP)
 - 802.1x, Extensible Authentication Protocol (EAP)
- ◆ Enterprise Wireless network.
 - Deployment of Wireless Access Points
 - VPN technologies in Legacy Wireless Networks

Code: 40088103

Date: Oct. 27-28, 2008

Time: 9:30am - 5:00pm

Venue: Hong Kong Productivity Council

Medium of Instruction:
Cantonese (with handout in English)

Award of Certificate:
Certificate of Attendance

Tel: 852 2788 6266 or 852 2788 6271 / Fax: 852 2788 6260 / ait@hkpc.org

Name: _____	Job Title: _____
Organization: _____	Fee: _____
Address: _____	
Tel: _____	Fax: _____
Email: _____	Signature: _____

- To enroll, please complete the enrolment form and send it together with the appropriate fee to ICT & Logistics Unit, **Productivity Training Institute, HKPC Building, 78 Tat Chee Avenue, Kowloon, Hong Kong**. All cheques should be crossed and made payable to "**Hong Kong Productivity Council**".
- Course fee must be accompanied with this form (or its photocopy), otherwise enrolment may be rejected.
- HKPC has adopted a Personal Data (Privacy) Policy. Information about the policy is available at HKPC enrolment counters for collection. You may also contact our Personal Data Controlling Officer for further details.
- Applicants are encouraged to pay by credit cards, EPS or cheques, if possible. Amount received will be imprinted. Cheques are subject to bank clearance.
- Enrolment fee is not refundable unless HKPC is notified in writing of your withdrawal at least 5 working days before the course commences. A handling charge of HK\$200 will also be levied.
- An applicant may, subject to approval from HKPC, nominate a person to attend the course on his/her behalf.
- HKPC reserves the right to change the contents, venue and / or time as necessary.
- Classes in the morning, afternoon or evening will be cancelled if typhoon signal No. 8 or above OR black rainstorm warning is still hoisted after (or is announced by the Hong Kong Observatory to be hoisted at/after) 6:00 a.m., 11:00 a.m. and 4:00 p.m. respectively. Participants will be notified when the class will be made up as soon as possible.

Organized by

