ITRAINONLINE MMTK

Trainers' notes: Wireless Security

Developed by: Alberto Escudero Pascual /IT +46

Introduction	This unit describes security in the context of Information Security. Five general security attributes (Confidentiality, Authentication, Integrity, Non-Repudiation and Availability) are described and later evaluated in the context of IEEE 802.11 (WLAN). The unit finishes by presenting ten security threats that needs to be consider in wireless design.
Timing/duration	This unit requires 1.5h presentation + 1.5h discussion around the proposed exercises.
Content outline and main topics covered	The unit is divided in three thematic blocks. 1. Intro to INFOSEC 2. Discussion of five security attributes 3. Ten security threats -discussion table The first block address Information Security and a brief introduction to OSI model (20 mins). The second blocks describes five security attributes in the context of WLAN (5*10 mins/attribute = 50 mins). The last block presents a table with 10 security threats related to the five security attributes (20 mins)
Target audience	• Technical staff with practical knowledge in TCP/IP.
Prerequisite skills/knowledge	Trainees should be familiar with the topics discussed in the ItrainOnline MMTK Unit “Advanced Networking”. Trainers should have theoretical and practical knowledge in wireless network architecture and design. Trainers should have some previous education in “network security”. Good understanding of the OSI model, basic cryptography and risk analysis.
Unit objectives/expected outcomes	By the end of the unit participants should • Be able to situate wireless security within the broad context of information security.

	• Understand where "security" can be built into each layer of the OSI/Internet protocol stack. • Identify the key security elements that need to be considered when performing wireless design planning.
Pre-workshop activities	If it is not covered elsewhere during the workshop, have the trainees read the Advanced Networking unit before the session.
Notes on using exercises	An exercise is included, the main goal is to discuss again the issues presented in the theoretical session. The main focus should be on discussing "security attribute by security attribute" instead talking about SSID, WEP etc. Provide constantly the INFOSEC security context.
Resources included with unit	Handout and slides.
Additional trainer resources	
Equipment needed	Optional: Access point and a wireless client (STA)
Comments	