Tutorial 10

Aims

- To exemplify the security aspects of mobile computing

Questions

1. Why does mobile computing present more security challenges than fixed computers?
   Physical Security
   - Easy to steal or lose
   - Easy to temper with

   Communication Security
   - Broadcast transmission, as opposed to point-to-point connection
   - Used in public or publicly accessible places

2. A travelling salesman carries his laptop computer, and accesses his company's network when he has connectivity. He can use WiFi hotspots or mobile broadband when on the road, and a wireless network in hotels or at his home. What are the security implications of each access method? Which one is the most secure, and which one is the least?
   - Wi-Fi hotspot
     - No access control
     - Public hotspots often do not use WEP/WPA. WHY? Because they would have to advertise the "private" encryption key(s), which kills the basic idea behind encryption: wireless eavesdroppers then have the key(s) to quickly decode the Wi-Fi hotspot traffic.). So the security is up to the user or application, e.g. use HTTPS. Still, attackers can see what Web sites you're visiting.
     - The Internet is much more than just Web pages: traffic is compromised real-time.
     - The mobile device is exposed
     - Evil twin hotspots: set up to eavesdrop on mobile communication (scam)
   - Mobile broadband
     - More secure than Wi-Fi hotspot: password protected, built-in encryption, device (modem) ID may be used to verify connecting devices
   - Public wireless network (cafes, hotels etc)
     - More secure than a public hotspot, but encryption keys can still be shared between different users in the hotel
   - Private wireless network (home network – can be accessed from outside your home)
     - If using WPA / WPA2 and not sharing the encryption key with outsiders, the network would be secure. User still has to consider security from war-driving(war-walking etc)

   Most secure? – Home Wi-Fi with VPN
   Least secure? – Public hotspot

3. The travelling salesman's computer also has a Bluetooth card. When can he use it, and how secure is the connection, compared to the cases in the previous question?
   Security issues in Bluetooth
   - Only offers basic security – reason: less computing power, limited battery.

Connection is less secure than wireless / Wi-Fi technology

Advantages in using Bluetooth

- Short range communication – eavesdropper has to be really close to you (in house Bluetooth use is secure)
- Traveller should only use it to synchronize his computer with his mobile phone or access the Internet using the mobile phone's connection.
- Less secure, if he wants to use it outside his house/ secure physical location.

4. Would it affect security if he accesses his company network from his mobile, IP-enabled phone instead of using the laptop computer?

   There is no real difference in communication security, the phone's connection (Wi-Fi or mobile broadband) will determine the security.

   Network address translation (NAT), however, can hide the IP address of the computer.