Hidden Rogue APS

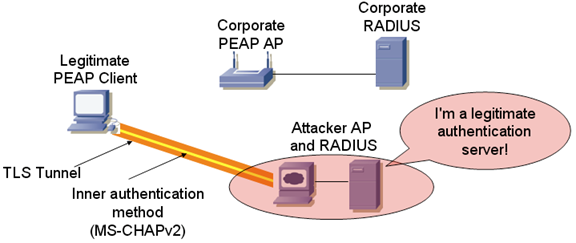
**Hidden Rogue APs**  
The threat of a rogue AP is significant for any network, effectively offering an attacker the equivalent of a RJ45 jack in the parking lot (or across the street, or in the high-rise building next door). Standards bodies such as the Payment Card Industry Data Security Standard (PCI DSS) require that organizations regularly assess their networks for these rogue AP threats, and many vendors have implemented products designed to address this threat. Despite the attention to this threat, many organizations remain vulnerable, and many analysis mechanisms provide an inadequate defense against rogue AP devices:

* **WKnock** WKnock is a software package for common access points such as the Linksys WRT. Using WKnock, an attacker or an insider can plug-in a rogue access point which will lay dormant, silent to analysis systems. This often defeats quarterly or monthly monitoring systems, since the device is silent until it is used by an attacker, after which it returns to its dormant state.[3]
* **IEEE 802.11n GreenField Mode** Many organizations are planning to deploy IEEE 802.11n technology, but even without the adoption of this new platform, organizations are exposed to 802.11n rogue APs operating in GreenField mode. GreenField mode is an operating mechanism to maximize the speed of 802.11n technology by using a new technology that effectively renders these networks invisible to existing 802.11a/b/g wireless cards. As a result, rogue AP analysis systems are unable to identify these GreenField APs, including all commercially sold wireless IDS products today.[4,5]
* **Bluetooth Rogue AP** Bluetooth technology is making its way into all kinds of devices, and is especially attractive due to its low cost and minimal resource requirements. Devices such as Bluetooth APs are available that provide similar connectivity and range as their 802.11 counterparts, but escape analysis mechanisms since Bluetooth operates using Frequency Hopping Spread Spectrum instead of traditional 802.11 transmission mechanisms.[6]

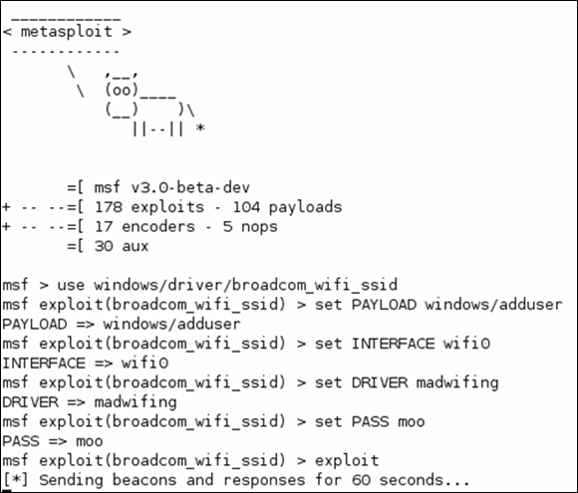
**Bluetooth Attacks**  
Bluetooth technology is growing and being adopted at an amazing rate, surpassing one billion Bluetooth devices shipped in 2006! With increased prevalence in adoption and use comes increased scrutiny from attackers, who have uncovered significant security vulnerabilities in Bluetooth technology. Attacks including unauthorized access, information disclosure, remote eavesdropping, device manipulation and full host compromise are all possible against Bluetooth technology in use today. Due to the ad-hoc and decentralized nature of Bluetooth technology, administrators are often unaware of the amount of Bluetooth technology in use, and their exposure to Bluetooth attacks. While many organizations disregard Bluetooth threats, thinking the technology is limited to short-range communication, the reality is that tests have shown it is possible for an attacker to communicate to a short-range Bluetooth device from over a mile away!   
  
Recently, a colleague was working on a wireless assessment that included a Bluetooth analysis. Below is an extract from a discussion we had following his tests:

Joshua Wright: What did you turn up in the BT audit?   
*Colleague: Besides walking into the CEO's N95?*  
Joshua Wright: Sweet! How did you get into it?   
*Colleague: Btscanner -> got the BT MAC plus the device ID; connected to it using the standard OBEX transfer; it was wide open; sent a few .sisx files; you can imagine the rest*  
Joshua Wright: :)   
*Colleague: I just used iSync; after OBEXing over the Apple "high-speed iSync app"*

In this example, a recent Nokia Communicator phone was vulnerable to unauthorized access, allowing the attacker to upload arbitrary malware to the phone, and to retrieve potentially sensitive information including contacts, calendar information and notes files.  
 **PEAP and TTLS Configuration Weaknesses**  
Many organizations have turned to stronger authentication protocols such as PEAP and TTLS to authenticate wireless users and protect access to the wireless network. When deploying PEAP and TTLS networks, the configuration of client systems is a critical component of the overall security of the wireless network. Often, PEAP and TTLS networks are poorly configured on client systems, exposing them to network impersonation attacks.  
  
In a network impersonation attack, the adversary adopts the enterprise SSID, and provides enough of a realistic network environment to simulate the legitimate network while attempting to steal network credentials, or to attack client systems directly.

  
  
*Figure 1:* Attacker impersonates a legitimate AP and RADIUS Server

**Mobile Device Weaknesses**  
Mobile devices such as PDAs, smart-phones, communicators such as the Nokia 800 and even point-of-sale devices, all require wireless connectivity to be effective. Often, these embedded device platforms are well behind what is generally considered to be modern security options for wireless networks, with operating systems that do not receive regular patch updates for application flaws. In many cases, organizations cannot upgrade the operating system or applications on mobile devices until the patches are certified by application vendors, leaving the device vulnerable to attacks for an extended period of time.  
  
**Wireless Driver Attacks**  
The next generation of attacks against wireless networks aren't targeting the wireless network itself; rather, these attacks are targeting client vulnerabilities directly. Exploitable vulnerabilities in wireless drivers have been discovered in all major wireless card manufacturers, with working exploits readily available through tools such as the Metasploit Framework.

  
  
*Figure 2:* Sample Metasploit attack targeting a flaw in Broadcom wireless drivers