



Off the Press - July 2008

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

Wireless “In”Security

By Jeremy Burris, CISA, MCP, CPTS, CEH, ECSA, S.R. Snodgrass, A.C.



This article highlights some of the ways that an attacker can circumvent your wireless security features and attempt to breach your network.

ENCRYPTION

There are two affordable and common types of encryption on the market today for wireless devices: WEP (Wireless Equivalent Privacy) and WPA (Wi-Fi Protected Access). Both wireless technologies have the ability to encrypt data up to a 128-bit cipher, but not all devices use this “strong” encryption level by default. In both cases (although taking approximately twice as long when using WPA encryption), an attacker can “sniff” and collect enough packets of

a certain type (called “Weak IVs”) from your wireless network to begin “cracking” your WEP or WPA encryption code. This is done through packet reinjection techniques, which can help an attacker generate large amounts of wireless traffic on your network, thus increasing the amount of Weak IV packets that are being sent. These need to be collected in large quantities in order to “crack” the code.

SSID (SERVICE SET IDENTIFIER) BROADCAST

Most wireless devices can now disable the clear text broadcasting of their wireless name (or its SSID – Service Set Identifier). The ability to disable this broadcast was initially designed as a security measure: by disabling the access points’ sending of the SSID, it was thought that attackers simply would not be able to “see” the wireless network when sniffing. While the disabling of SSID is still a recommended practice, it is not foolproof. When connecting to the access point, the SSID is still transmitted in clear text from the client machine during the “hand-shake” with the network. This makes it easy for an attacker to identify this SSID during authentication.

MAC (MEDIA ACCESS CONTROL) ADDRESS FILTERING

Most access points today have the ability to input a list of computer hardware addresses called Media Access Control (MAC) Addresses. The wireless access point will then only accept traffic from workstations or devices that have MAC addresses within their list of authorized devices. This is a strongly recommended practice. However, during authentication MAC addresses are sent in clear text from the client machine, again making it very easy to be “sniffed” by an attacker. Once “sniffed,” MAC addresses on an attacker’s machine can be “spoofed” or duplicated, circumventing this security.

VPN USAGE WITHIN THE WIRELESS PROTOCOL

Another common mitigation control technique is the use of a VPN (usually SSL encrypted) tunnel from the client to the server. Simply put, the client machine is using the wireless connection to gain network access but is then creating a VPN tunnel for sending traffic back and forth across the network.



Off the Press - July 2008

PENNSYLVANIA ASSOCIATION OF COMMUNITY BANKERS

THE VOICE FOR COMMUNITY BANKING IN PENNSYLVANIA SINCE 1876

This again is a best practice but only encrypts the traffic between known client machines and the other network resources. It does not provide additional security against an attacker gaining access to your network. Once network access is gained, tools can be run to sniff traffic and to search for open ports or vulnerabilities.

TAKING CONTROL

An attacker can establish a connection to your wireless network bypassing encryption entirely. In fact, they can actually “bump” your users off a wireless access point and have those users connect to THEIR wireless network. They do this by “boosting” the strength on their antennas (above the strength allowed by FCC regulations) and choosing an SSID the same as your institution’s. This type of attack comes down to who has the stronger signal, and since attackers can use non-FCC approved devices (easily purchased outside of the United States), they

will win that fight.

THE BEST PROTECTION—LIMITING WIRELESS USE

Wireless technologies, while convenient, are not as secure as their wired counterparts. Too many types of attacks can compromise your wireless network. Once on your internal wireless network, an attacker has many tools to attack the wired components of your network.

While security controls are continually improving, so are the methods of attackers. The best practice of all is not using wireless technologies or completely segregating these wireless connections from your internal network by use of a different Internet carrier, separate subnet, or additional firewall devices. Should a strong business need exist for wireless use, maintain recommended mitigating controls and keep a close eye on which users are connected to your wireless access points.

Jeremy Burris is a Senior Technology Services Consultant at S.R. Snodgrass, A.C. Jeremy's areas of expertise include Network Attack and Penetration and other IT security-related audits for financial institutions and private companies. Snodgrass is best known for our expertise in the financial services industry, where we currently serve over 175 financial institutions on a national scale. Accordingly, we have extensive industry business experience and sound working relationships with all of the regulatory agencies. Examples of that experience are displayed on our Web site's Knowledge Bank at www.srsnodgrass.com, where you can view several articles and video presentations on banking-related topics, including a live Attack and Penetration demo.