

RE: palm VIIx wireless modem

Source: <http://www.derkeiler.com/Mailing-Lists/securityfocus/security-basics/2001-10/0310.html>

From: Don Weber (Don@AirLink.com)

Date: 10/09/01

From: "Don Weber" <Don@AirLink.com>
To: "Michael Kjorling" <michael@klorling.com>
Subject: RE: palm VIIx wireless modem
Date: Tue, 9 Oct 2001 12:00:07 -0700
Message-ID: <BAEBKBIMJFMJDDHPLBHKKEJKDPAA.Don@AirLink.com>

I just got this over in the Pen-Testing list, I hope the cross-post is ok.
it was posted by CKlaus, I hope you don't mind my re-post

Here is a Wireless LAN Security FAQ, specifically targetting WiFi that I'm
working on. Hope you find it useful.

Wireless 802.11b Security FAQ

By Christopher W. Klaus of Internet Security Systems (ISS)
Email: cklaus@iss.net

Version 1.1

Content

What is the overview of Wireless LAN 802.11 technology?
What are the major risks?
What are solutions to minimizing WLAN risk?

Recent Updates

Version 1.1

- Added NetStumbler, WEPCrack tools, Added WEP insecurity paper
- Added Ecutel, BlueSocket, and NetMotion as WLAN Sec. Products
- Updated Accuracy of WEP description and made it clear that SSID not being encrypted.
- Added Broadcast of SSID turned off can still be circumvented.
- Added Addtron's default SSID, a popular AP
- Added War Driving AP maps.
- Added 802.11 ArpSpoof, a technique used by ISS X-Force Consulting.
- Added hijacking SSH and SSL connections via wireless.
- Added 2 X-Force Advisories on Wireless 802.11 flaws

Version 1.0

- First draft

RE: palm VIIx wireless modem

What is

Wireless LAN technology standard 802.11b has the strongest momentum to becoming the main standard for corporate internal wireless LAN networks. The bandwidth of 802.11b is 11 mbits and operates at 2.4 GHz Frequency. The successor of this current 802.11b standard is 802.11a and it is designed to be faster speed and operate at a different frequency. While 802.11a standard and the technology behind it will be in the near distant future, 802.11b is here today and many companies and even individuals are deploying and using it now.

As more wireless technology is developed and implemented, the complexity of the types of attacks will increase, but these appear the standard main methods used to break and attack wireless systems. These attacks may be very similar against other wireless type technologies and is not unique to 802.11b. By understanding these risks and how to develop security solution for 802.11b, this will be a good stepping–stone for providing a good secure solution to any wireless solution.

The AP (access point also known as a base station) is the wireless server that connects clients to the internal network. Base stations typically act as a bridge for the clients. There is an IP address for management configuration of the base station. The base stations typically have an SNMP agent for remote management. Some clients like desktops and laptops may have a SNMP agent running, but not usually.

Base stations have become relatively inexpensive, approximately under \$300. The 802.11 client cards for PDAs, laptops, and desktops are approximately under \$100. Because of inexpensive equipment to get into wireless, attackers can get easy access to the tools necessary to apply the attack. Because of the inexpensive price, within many companies employees can purchase wireless equipment without approval and deploy this in a rogue fashion, creating additional risk.

While this FAQ focuses on the risk issues from a corporate network perspective, these same issues apply to home networks and telecommuters that are using wireless. As the corporate networks are allowing in remote users, these remote users may be using wireless at their end–point to connect in. In this case, even if wireless capabilities have not been installed on the corporate network, they may still be affected by the risk that their remote employees are using wireless at home or on the road.

Airports, hotels, and even coffee shops like Starbucks are deploying 802.11 networks so people can wirelessly browse the Internet with their laptops. As these types of networks increase, this will create additional security risk for the remote user if not properly protected.

Many of the security issues around 802.11b will continue to be an issue with 802.11a, therefore by understanding current issues will help organizations deal with future issues as well. This 802.11b security FAQ is broken into 2 parts:

SecurityFocus BASICS: RE: palm VIIx wireless modem

* Known Risks – What are the major risks that we are aware of with 802.11b?

* Current Security Solutions – What can we do today to protect 802.11b infrastructure?

What are the Known Risks around 802.11b security?

Here is the list of main known security risks with 802.11b.

- 1) Insertion Attacks
- 2) Interception and monitoring wireless traffic
- 3) Misconfiguration
- 4) Jamming
- 5) Client to Client Attacks

Insertion Attacks

The insertion attacks are based on placing unauthorized devices on the wireless network without going through a security process and review.

Plug-in Unauthorized Clients

An attacker tries to connect his wireless client, typically a laptop or PDA, to a basestation without authorization. Base stations can be configured to require a password before clients can access. If there is no password, an intruder can connect to the internal network by connecting a client to the base station.

Plug-in Unauthorized Renegade Base Station

Many companies may not be aware that internal employees have deployed wireless capabilities on their network. An internal employee wanting to add their own wireless capabilities to the network plugs in their own base station into the wired intranet. This is a risk if the base station has not been properly secured. This could lead to the previously described attack of unauthorized clients then gaining access to unauthorized base stations, allowing intruders into the internal network. Typically, companies may need a policy against allowing employees to add wireless base stations onto the corporate network without requesting permission and going through a security process. A sophisticated intruder may physical place a base station on the victims' network to allow them remote access via wireless.

Interception and monitoring wireless traffic

These interception and monitoring attacks are popular on broadcast wired networks like Ethernet. The same principles apply to wireless.

Wireless Sniffer

SecurityFocus BASICS: RE: palm VIIx wireless modem

An attacker can sniff and capture legitimate traffic. Many of the sniffer tools for Ethernet are based on capturing the first part of the connection session, where the data would typically include the username and password. An intruder can masquerade as that user by using this captured information. An intruder who monitors the wireless network can apply this same attack principle on the wireless.

One of the big differences between wireless sniffer attacks and wired sniffer attacks is that a wired sniffer attack is achieved by remotely placing a sniffer program on a compromised server and monitor the local network segment. This sniffer based attack can happen from anywhere in the world. Wireless sniffing requires the attacker to typically be within range of the wireless traffic. This is usually around 300 feet range, but wireless equipment keeps strengthening the signal and pushing this range further out.

If an attacker can sniff the wireless traffic, it is possible to inject false traffic into a connection. An attacker may be able to issue commands on behalf of a legitimate user by injecting traffic and hijacking their victim's session.

I Broadcast Monitoring

If a base station is connected to a hub rather than a switch, any network traffic across that hub can be potentially broadcasted out over the wireless network. Because the Ethernet hub broadcasts all data packets to all connected devices including the wireless base station, an attacker can monitor sensitive data going over wireless not even intended for any wireless clients.

ArpSpooF Monitoring and Hijacking

Normally, in regards to an AP, the network data traffic on the backbone of a subnet would be treated similarly like a network switch, thus traffic not intended for any wireless client would not be sent over the airwaves. This could reduce significantly the amount of sensitive data over the wireless network.

An attacker using the arpspoof technique can trick the network into passing sensitive data from the backbone of the subnet and route it through the attacker's wireless client. This provides the attacker both access to sensitive data that normally would not be sent over wireless and an opportunity to hijack TCP sessions. Dsniff is a popular tool that enables arpspoofing and is available at: <http://www.monkey.org/~dugsong/dsniff/>

Hijacking SSL (Secure Socket Layer) and SSH (Secure Shell) connections.

By using arpspoofing technique, an attacker can hijack simple TCP connections. There are tools that allow for hijacking SSL and SSH connections. Typically, when SSL and SSH connections get hijacked, the only alert to the end-user is a warning that the credentials of the host and

SecurityFocus BASICS: RE: palm VIIx wireless modem

certificate have changed and ask if you trust the new ones. Many users simply accept the new credentials, thus allowing an attacker to succeed. A reasonable interim measure to prevent the attack is to have users enable SSH's StrictHostKeyChecking option, and to distribute server key signatures to mobile clients.

The Dsniff FAQ explains how to hijack in detail SSH and HTTPS connections:
<http://www.monkey.org/~dugsong/dsniff/faq.html>

BaseStation Clone (Evil Twin) intercept traffic

An attacker can trick legitimate wireless clients to connect to the attacker's honeypot network by placing an unauthorized base station with a stronger signal within close proximity of the wireless clients that mimic a legitimate base station. This may cause unaware users to attempt to log into the attacker's honeypot servers. With false login prompts, the user unknowingly can give away sensitive data like passwords.

Misconfiguration

By default, all the base stations analyzed out of the box from the factory were configured in the least secure mode possible. Adding the proper security configuration was left up as an exercise to the administrator to lock down. Unless the administrator of the base station understands the security risks, most of the base stations will remain at a high risk level. The analysis of three base station models by the leading 802.11 vendors lead to many configuration issues that should be audited and assessed by the organization. The top three base station vendors analyzed were Cisco, Lucent, and 3Com. The security risks identified may change in newer versions of the 802.11 solution as it is evolving rapidly. Each vendor had different implementation security risks, but the underlying issues are the same and can be applied to other vendors not listed here.

Server Set ID (SSID)

SSID is a configurable identification that allows clients to communicate to the appropriate base station. With proper configuration, only clients that are configured with the same SSID can communicate with base stations having the same SSID. SSID from a security point of view acts as a simple single shared password between base stations and clients.

Each of the base station models came with default SSIDs. Attackers can use these default SSIDs to attempt to penetrate base stations that are still in their default configuration. Here are some default SSIDs:

- "tsunami" – Cisco
- "101" – 3Com
- "RoamAbout Default Network Name" – Lucent/Cabletron
- "Default SSID"
- "Compaq" – Compaq
- "WLAN" – Addtron, a popular AP

"intel" – Intel
"linksys" – Linksys
"Wireless"

Lucent has Secure Access mode. This configuration option requires the SSID of both client and base station to match. By default this security option is turned off. In non-secure access mode, clients can connect to the base station using the configured SSID, a blank SSID, and the SSID configured as "any".

Bruteforce Base Station SSID

Most base stations today are configured with a server set id (SSID) that acts as a single key or password that is shared with all connecting wireless clients.

An attacker can try to guess the base station SSID by attempting to use a bruteforce dictionary attack by trying every possible password. Most companies and people configure most passwords to be simple to remember and therefore easy to guess. Once the intruder guesses the SSID, they can gain access through the base station.

The SSID could be obtained through one of the wireless clients becoming compromised or an employee resigns knowing the key, there is risk that anyone with the SSID could still connect to the base station until the SSID is changed. If there are many wireless users and clients, it can become problematic to scale this security solution if the SSID needs to be changed frequently and all clients and base stations need to be reconfigured with an updated shared single SSID each time.

WEP, the encryption standard for 802.11, only encrypts the data packets not the 802.11 management packets and the SSID is in the beacon and probe management messages. The SSID is not encrypted if WEP is turned on. The SSID goes over the air in clear text. This makes obtaining the SSID easy by sniffing 802.11 wireless traffic.

Many APs by default have broadcasting the SSID turned on. Sniffers typically will find the SSID in the broadcast beacon packets. Turning off the broadcast of SSID in the beacon message (a common practice) does not prevent getting the SSID; since the SSID is sent in the clear in the probe message when a client associates to an AP, a sniffer just has to wait for a valid user to associate to the network to see the SSID.

Wired Equivalent Privacy (WEP)

WEP can be typically configured in 3 possible modes:

- No encryption mode
- 40 bit encryption
- 128 bit encryption

SecurityFocus BASICS: RE: palm VIIx wireless modem

WEP, by default out of the box, all 3 base station models analyzed have WEP turned off. 40 bit encryption versus 128 bit encryption provides no added protection against the known flaw in WEP.

In some base stations, it is optional whether the encryption is enforced. The WEP encrypted may be turned on, but if it is not enforced, a client without encryption with the proper SSID can still access that base station.

Attacks against WEP

802.11b standard uses encryption called WEP (Wired Equivalent Privacy). It has some known weaknesses in how the encryption is implemented.

Papers on WEP Insecurities

Researchers at Berkeley have documented these findings at:
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

Using the Fluhrer, Mantin, and Shamir Attack to Break WEP
http://www.cs.rice.edu/~astubble/wep/wep_attack.html

Using WEP is better than not using it. It at least stops casual sniffers. Today, there are readily available tools for most attackers to crack the WEP keys. Aircrack and others tools take a lot of packets (several million) to get the WEP key, on most networks this takes longer than most people are willing to wait. If the network is very busy, the WEP key can be cracked and obtained within 15 minutes.

The fix for encryption weakness for the standard is not slated to be addressed before 2002.

Because of the WEP weakness, wireless sniffing and hijacking techniques can work despite the WEP encrypted turned on.

There is the IEEE 802.1X standard which allows network access to be authenticated and keys to be distributed. This allows access to APs to be authenticated and WEP keys to be distributed and updated. More APs are starting to support this standard.

SNMP community words

Many of the wireless base stations have SNMP (Simple Network Management Protocol) agents running. If the community word is not properly configured, an intruder can read and potentially write sensitive information and data on the base station. If SNMP agents are enabled on the wireless clients, the same risk applies to them as well.

By default, all three base stations are read accessible by using the community word, "public".

By default, the 3com base station has write access by using the community word, "comcomcom". Cisco and Lucent/Cabletron require the write community

word to be configured by the user before it is enabled.

SNMP information

With the default of most base stations using the community word "public", potentially sensitive information can be obtained from the base station.

Configuration Interfaces

Each base station model has its own interfaces for viewing and modifying the configuration. Here are the current interface options for each base station:

- Cisco - SNMP, serial, Web, telnet
- Lucent / Cabletron - SNMP, serial (no web/telnet)
- 3Com - SNMP, serial, Web, telnet.

3com base station lacks any access control from the web interfaces for reading the configuration options. By connecting to the 3com base station web interface, it provides SSID on the "system properties menu" display. An attacker who finds a 3com base station web interface can easily get the SSID.

3com base station does require a password on the web interface for write privileges. The password is the same as the community word for write privileges, therefore 3com base stations are at risk if deployed using the default, "comcomcom" as the password. This gives an attacker easy write access.

Client side security risk

For the clients connecting to the base station, they store sensitive information for authenticating and communicating to the base station. If the client is not properly configured, access to this information is available.

- Cisco client software stores the SSID in the Windows registry. Cisco stores the WEP key in the firmware, which is difficult to gain access to.

- Lucent/Cabletron client software stores the SSID in the Windows registry. The WEP is stored in the Windows registry but it is encrypted. The encryption algorithm is not documented.

- 3Com client software stores the SSID in the Windows registry. The WEP key is stored in registry with no encryption.

Windows XP has 802.11 configuration and has a display of the available SSID's built-in to the OS.

Installation

By default, all installations are optimized for the quickest configuration to get users successful out of the box. Inversely, by default, the

installations are configured the least secure mode as possible.

>*From out of the box experience, Cisco was simple and easiest to install.*
3Com installation was straight forward out of the box. And Lucent/Cabletron had many firmware upgrades which led to confusion on which upgrades to install.

Jamming

Denial of service attacks for wired networks are popular. This same principle can be applied to wireless traffic, where legitimate traffic gets jammed because illegitimate traffic overwhelms the frequencies, and legitimate traffic can not get through.

2.4 GHz Interfering Technology

An attacker with the proper equipment and tools can easily flood the 2.4 GHz frequency, so that the signal to noise drops so low, that the wireless network ceases to function. This can be a risk with even non-malicious intent as more technologies use the same frequencies and cause blocking. Cordless phones, baby monitors, and other devices like Bluetooth that operate on the 2.4 GHz frequency can disrupt a wireless network.

Client to Client Attacks

Two wireless clients can talk directly to each other by-passing the base station. Because of this, each client must protect itself from other clients.

Filesharing and other TCP/IP service attacks

If a wireless client, like a laptop or desktop, is running TCP/IP services like a web server or file sharing, an attacker can exploit any misconfigurations or vulnerabilities with another client.

DOS (Denial of Service)

A wireless client can flood another wireless client with bogus packets, creating a denial of service attack. An attacker and sometimes employees unintentionally can configure their client to duplicate the IP or MAC address of another legitimate client causing disruption on the network.

War Driving Access Point Maps

As people are "War Driving", and locating the APs and recording the GPS coordinates of the AP location, these AP maps are being shared to any attacker on the Internet. If a company has their AP location and information shared on the Internet, their AP becomes a potential target and increases their risk. One of the popular places to upload War Driving AP maps, is to <http://www.netstumbler.com>. It includes a visual map and a database query tool for locating various AP's.

Current Solutions

There are many options that organizations can do today to put proper security protection around their wireless strategy and technology.

Wireless Security Policy and Architecture Design

Many organization need to develop a wireless security policy to define what is and what is not allowed with wireless technology. From a holistic view, the wireless network should be designed with the proper architecture to minimize risk.

Treat BaseStations as Untrusted

>From an network security architecture, the base stations should be evaluated

and determined if it should be treated as an untrusted device and need to be quaranteed before the wireless clients can gain access to the internal network. The architecture design may include appropriately placing firewalls, VPNs, IDSes, vulnerability assessments, authentication requirements between base station and the Intranet.

Base Station Configuration Policy

The wireless policy may want to define the standard security settings for any 802.11 base station being deployed. It should cover security issues like the Server Set ID, WEP keys and encryption, and SNMP community words.

Base Station Discovery

>From a wired network search, an organization could identify unknown and rogue base stations by searching for SNMP agents. The rogue base stations are identified as 802.11 devices through SNMP queries for host id.

Some base stations have a web and telnet interface. By looking at the banner strings of these interfaces, this provides another method of identifying some 802.11 devices.

An additional means is by using unique TCP/IP attributes like a fingerprint, it can help identify devices as base stations. Most TCP/IP implementations have a unique set of characteristics and many OS fingerprinting technologies use this method for identifying the OS type. This concept can be applied to the base stations.

>From a wireless network search, an organization can identify these rogue base stations by simply setting up a 2.4 GHz sniffer that identifies 802.11 packets in the air. By looking at the packets, you may find the IP addresses to help identify which network they are on. In a densely populated area with many businesses close together, running a sniffer may pick up more the intended organization's traffic, but a close neighboring company.

Base Station Security Assessments

An organization can examine and analyze the base station configuration. A security audit and assessment could determine whether the passwords and community words are still default or easily guessed and if better security modes have been enabled like encryption.

With router ACLs and firewall rules, an organization can minimize access to the SNMP agents and other interfaces on the base station. A security assessment can determine how widely accessible is the configuration interfaces to the base stations are allowed to within the organization.

Wireless Client Protection

The wireless clients should be assessed for having the following security technologies:

- firecell (distributed personal firewalls) – lock down who can gain access to the client
- VPN – adds another layer of encryption and authentication beyond what 802.11 can provide.
- intrusion detection – identify and minimize attacks from intruders, worms, viruses, Trojans and backdoors.
- desktop scanning – identify security misconfigurations on the client.

802.11 Security Products

BlueSocket

<http://www.bluesocket.com/>

The WG-1000 Wireless Gateway(tm) offers a single scalable solution to the security, quality of service (QoS) and management issues facing enterprises and service providers that deploy wireless LANs based on the IEEE 802.11b and Bluetooth(tm) standards.

EcuTel

<http://www.ecutel.com/>

Viatores Secure WLAN edition is different from legacy virtual private networks (VPNs) in that it maintains VPN and application sessions uninterrupted with no configuration or re-boot required.

Viatores combines two advanced protocols for mobility and security to enable roaming from LANs to WLANs and between WLAN subnets seamlessly and securely. Application sessions and security tunnels are maintained while the user moves from one subnet to another. Roaming users can communicate easily with colleagues, regardless of where they are or how they are connected, because Viatores maintains a single network address.

Viatores Secure WLAN edition includes:

- Industry-strength secure communication well beyond the WEP standard;
- Seamless roaming from wired to wireless networks and between different wireless networks;
- Support for two-way, peer-to-peer communication;

SecurityFocus BASICS: RE: palm VIIx wireless modem

- Data confidentiality and integrity, including key exchanges, digital signatures, and industry–strength encryption;
- Option to upgrade to secure and seamless roaming from public networks.

NetMotion Wireless

<http://www.netmotionwireless.com/>

NetMotion Mobility provides a VPN designed to work with WLAN security.

http://www.netmotionwireless.com/resource/whitepapers/netmotion_security.asp

has an overview of wireless security and how NetMotion Mobility(tm) prevents unauthorized users from accessing your system and stops eavesdropping, replay, and other network–level attacks.

802.11 Security Analysis Tools

AirSnort is a wireless LAN (WLAN) tool that recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

AirSnort will work for both 40 or 128 bit encryption.

<http://freshmeat.net/projects/airsnort/>

WEPCrack is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of RC4 key scheduling.

<http://sourceforge.net/projects/wepcrack>

Network Stumbler scans for networks roughly every second and logs all the networks it runs into—including the real SSIDs, the AP's MAC address, the best signal–to–noise ratio encountered, and the time you crossed into the network's space. If you add a GPS receiver to the notebook, it logs the exact latitude and longitude of the AP.

<http://www.netstumbler.com/>

Internet Scanner 6.2, the market leading network vulnerability assessment tool, was the first to assess many 802.11b security checks. 802.11 checks are in several X–Press Updates (XPU 4.9 and 4.10).

RealSecure 6.0, the market leading IDS, was the first to monitor many 802.11b attacks. Recommend to make sure you are up to the latest X–Press Updates. 802.11 checks for IDS were in XPU 3.1.

About Internet Security System's Wireless 802.11b Solution

ISS offers the comprehensive wireless security solution:

Wireless Security Assessments and Penetration Testing

Wireless Policy Design and Workshops

Vulnerability Scanning with specific 802.11 configuration checks

Intrusion Detection for Wireless LAN networks

Wireless 802.11 Security Classes

ISS X–Force Advisories:

<http://xforce.iss.net/alerts/advise83.php> WEP Key exposed

<http://xforce.iss.net/alerts/advise84.php> 802.11 SNMP Auth. Flaw

RE: palm VIIx wireless modem

SecurityFocus BASICS: RE: palm VIIx wireless modem

Copyright © 2001, Internet Security Systems. All rights reserved.
This document may be redistributed only in its entirety with version date, authorship notice, and acknowledgements intact. No part of it may be sold for profit or incorporated in a commercial document without the permission of the copyright holder. Permission will be granted for complete electronic copies to be made available as an archive or mirror service on the condition that the author be notified and that the copy be kept up to date. This document is provided as is without any express or implied warranty.

Christopher W. Klaus
Founder and CTO
Internet Security Systems (ISS)
6303 Barfield Road
Atlanta, GA 30328
Phone: 404-236-4051 Fax: 404-236-2637
web <http://www.iss.net>
NASDAQ: ISSX

Internet Security Systems ~ The Power To Protect

This list is provided by the SecurityFocus Security Intelligence Alert (SIA) Service. For more information on SecurityFocus' SIA service which automatically alerts you to the latest security vulnerabilities please see: <https://alerts.securityfocus.com/>

- **Previous message:** [Keith CTR Hill: "Re:RE: Personal firewalls for laptops"](#)
- **Maybe in reply to:** [Milk: "palm VIIx wireless modem"](#)
- **Messages sorted by:** [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)