

Vulnerability Assessment of Public Communications Infrastructure with 802.11x Technologies



Tisha Hayes
Technical Consultant, Communications
Edison Automation Inc
Nashville, Tennessee

Abstract:

This document identifies some of the vulnerabilities of 802.11x wireless technologies when they are applied to critical public safety networks. Traditionally public safety communications systems have been dedicated facilities with the availability of fully functional communications nodes generally limited to authorized organizations or users. Increased likelihood of inadvertent or deliberate interference or exploitation comes with the increasing popularity of WiFi networks and the ready availability of consumer products.

Revolution in Networking:

Wireless networking is an ongoing revolution in business and personal computing. The flexibility of wireless networks has eased the deployment of connectivity at the workplace and home. With the ever improving picture of interoperability among equipment manufacturers it is possible to connect computers without an extensive investment of physical plant. The price of wireless cards, access points and routers has fallen to where the cost of incorporating these devices in computers is minimal. Communication protocols have advanced to where open, ad-hoc networking is easy to configure and WiFi access points are becoming more commonplace.

The very features that have allowed for open access and ease of use makes 802.11x very susceptible to interception, exploitation and denial of service attacks. Security provisions have been slow to evolve and usually are in response to exploits by the hacking community. Compromises have led advances in encryption and authentication techniques. Delays between when an exploit is developed and disseminated and when the industry develops a countermeasure, distributes and deploys the patch can extend into months. In this time, networks using the compromised protocol are open for exploitation or interruption.

This formula of "hacking and patching" has been repeated with WEP, LEAP, DES and RC-4. The current authentication methods of EAP-TLS and PEAP are advertised as secure but the ingenuity of the hacking sub-culture is endless and the cracking of these standards may take longer but it is inevitable.

The Evolution of Communications:



Radio communications has been continually revolutionizing public safety communications since the 1920's. One way voice systems transitioned to dispatch radio systems for squad cars and then to portable radios that could be carried by an officer in the 1940's. In the 1960's mobile data terminals were installed in emergency vehicles for text services. Gradually radio and computer technology merged and evolved into higher bandwidth solutions but until recently the communications systems have been licensed systems regulated under FCC Part 90. Data terminals were proprietary and expensive. The general disinterest in monitoring public safety data services kept the majority of the monitoring public oblivious to the content of wireless data networks. Fortunately the value of the data content on these networks was usually not critical and was more supportive in nature to the primary function of public safety organizations.

Concurrently radio communications systems were evolving for the utility industry. Rudimentary wireless data systems appeared in the 1950's using point to point microwave systems in the petroleum pipeline and electric transmission utility industries. The wireless systems connected SCADA (Supervisory Control and Data Acquisition) systems from pumping or metering stations back to control centers. Gradually as radio and control system technologies advanced the application of SCADA systems expanded into virtually every industry and water/wastewater systems gained advanced control systems. Early on, a utility system may have required 30-40 operators staffing every station in a system, automation allowed for the consolidation into a central facility with 1-2 operators managing an entire system.

The needs for increases in data rates have driven communications systems to more complex modulation schemes and compression algorithms. The underlying protocols of the internet, TCP/IP with the addressability of nodes, routing and retries commercialized the communications standards of SCADA. More complex controllers capable of autonomous operation evolved into PLC's (Programmable Logic Controllers). Our reliance upon highly complex control systems has made it possible for us to better monitor systems, improving quality and reliability. Additional smart devices communicating with MODBUS or PROFIBUS have extended control systems to the field device. Security cameras running streaming video, VOIP (Voice over IP) and data trending have further burdened communications systems.

Public Safety (Police, Fire, Emergency Medical and Emergency Management) and utility (water, wastewater, electric, gas) systems have very different requirements but there is a common thread that permeates all systems. The data must be reliable, it must be secure and it must be resistant to attempts to interfere with or modify the content. Traditionally these requirements have been present in military communications systems where the idea that an enemy can degrade your capabilities and thereby win the war has been recognized for centuries. The attacks on 9/11 upon New York and Washington DC highlighted our vulnerability to acts of war in our homeland. The threat has been present for decades but with our highly technologically advanced society it becomes more traumatic when essential services are disrupted.

The Internet has given the world access to information, education and communications. Computer viruses, logic bombs, scripts and malware have disabled or degraded portions of the Internet and affected financial, business, personal, government and military information systems. Connectivity is the strength of the Internet and also makes it possible for less than well meaning groups or individuals to disrupt it. The use of firewalls, routers, anti-virus software and software updates have been tools to responding to vulnerabilities but are usually reactive instead of proactive. An incident usually has to happen before a patch is created to close the back-door or to relieve the impact upon systems.

It is not unreasonable to assume that future attacks upon our nation can take place through the Internet. If public safety or utility networks are integrated into networks with access to the Internet and proper precautions are not taken then it is possible to exploit, intercept, deny or forge network traffic. In a coordinated effort this can be used to bypass security systems at utility systems, contaminate public water sources, destroy facilities through mis-operation or shut down natural gas and electric systems.

Public Safety has an increasing dependence upon data services. Wireless communications makes it possible for firefighters to access MSDS (Materials Safety Data Sheets) at hazardous materials incidents, EMS to send patient telemetry to hospitals and police officers to access criminal records and vehicle records at traffic stops. The future deployment of remote sensors at disaster scenes, video streaming and collaborative networking will permit advanced ICS (Incident Command System), responder safety and will save lives.



Wireless networks under the 802.11a, b and g standards use unlicensed frequency allocations in the 2.4 and 5.8 Gigahertz radio spectrum. At these frequencies radio signals generally follow line of sight conditions and are severely attenuated by buildings, trees or terrain in the radio path. Transmitter power is limited by FCC regulation as the original intent was for 802.11 networks to be short range devices within a building or campus. Changes in FCC rules have allowed for power levels to be increased for point to point backhaul links. With good outdoor antennas a 802.11 wireless network can extend range to hundreds or thousands of feet under ideal (unobstructed) conditions.

In a practical application a good sized urban system may consist of hundreds of access points to achieve building penetration and street level coverage. As there are no guarantees that an 802.11 system will have exclusive use of any frequency (802.11a has 12 frequencies and 802.11b has 11 frequencies) the radio spectrum is shared amongst the hundreds or thousands of private 802.11x networks in a urban area. As 802.11x use increases, the theoretical range of existing systems will decrease, background noise will increase and practical data throughput will decrease. Marketing estimates forecast up to 40 million 802.11 products per year by 2006. It is not unreasonable to estimate that nearly every business and a significant percentage of households will have some form of 802.11 networking in operation, all contending for the same 23 frequencies.

The WiFi industry has been riding on the crest of the wave to sell as many units as possible. Little regard is given to the long term functionality of 802.11 wireless networks or their suitability to public utility/ public safety critical infrastructure projects. Security protocols have been broken repeatedly with a new protocol or encryption layer to follow a few months later. As it may be getting more difficult for a 802.11x network to be exploited it is actually getting easier to launch a DoS (Denial of Service) attack upon a network.

Wireless adapters are essentially software configurable devices that have R.F. characteristics to operate across their entire frequency spectrum. (802.11a in the 5.8 GHz band, 802.11b in the 2.4 GHz band) through manipulation of the firmware (basic, resident operating system of the chipset) it would be possible to modify an adapter to transmit in a promiscuous mode to shut down a wireless channel, to force access points to try to repeatedly service invalid requests or to inject sufficient errors into a link as to render it inoperable. From an RF engineering (or ham radio perspective) it is fairly simple to transmit a broadband blanking signal to shut down the entire spectrum. In the 2.4 GHz spectrum a microwave oven comes pretty close to doing this in normal operation. What is neglected is the reality that most of the 802.11 chipsets manufactured in the world come from countries who have had a decidedly unfriendly stance to the US in the past (Peoples Republic of China). Given the manufacturing capacity and our dependence upon chipsets developed, programmed and manufactured overseas we are placing a lot of eggs in the same basket. Barring the nightmare scenarios the RF spectrum in the 802.11 bands degrades every day as more and more laptops, PDA's, access points and adapters are added.

It is also important to note here that the most critical infrastructures, like a PKI, should be built using U.S. technology. I have concerns with foreign software of unknown trust and quality being integrated into critical U.S. systems.

- *Daniel G Wolf*
- *Director of Information Assurance*
- *National Security Agency*
- *(in testimony before congress, 7/22/03)*

With wireless data across public spectrum, using hardware available at the nearest store, specialized sniffer and decryption software downloadable across the Internet it is highly likely that someone has been trying to access your wireless network already. Wireless network wardriving is a hobby to many, a challenge to some and an opportunity to launch an attack by a select few. In a passive mode, data streams can be collected and brute force or dictionary attacked to reveal encryption keys. Newer key formats have not made the system invulnerable, it will just take a longer amount of time to yield results.

Commercial microwave systems have not had the problem of hacking or intrusion. Microwave communications systems have been deployed for more than 50 years at nearly every telephone exchange on almost every tall building or hill. Very few can look at an antenna tower and differentiate between a 3 GHz microwave dish or one for 11 GHz. Commercial microwave systems have a higher level of security by their very nature of being uncommon and unknown. Equipment to monitor a microwave system is not easily found, it's fairly expensive and it takes a certain amount of expertise to know what you are looking for. Conversely 802.11 networks are intended to be easy to use, self-configurable, inexpensive and very common. Potentially there are millions of users who have the hardware and common software tools to casually browse an 802.11 network.

All data is created equal:

Once someone has access to encryption keys, MAC authentication lists, passwords to routers or networks it becomes very difficult to determine if a message is forged. Through a wireless network the entire LAN can be exposed to external access.

Guidance and Standards:

Getting past the marketing hyperbole of 802.11 networking is difficult. Security exploits are well documented in hacker circles and usually make it to the Information Technologies/ Services journals. Patches and fixes to exploits follow a weeks or months later. The flaw in LEAP (lightweight extensible authentication protocol) could be exploited by a tool that launched a dictionary attack that checked 45 million password values per second. It would force a connected user off of the wireless network and then capture their attempts to re-authenticate on the network. Similar exploits have happened with WEP, Cisco WLSE that manages the Aironet, Cisco HSE that manages datacenters and the Cisco IOS operating system.

The US Government has issued guidance on the applicability of WiFi on government, military and utility control networks (SCADA). References and excerpts include;

**NIST (National Institute of Standards)
NIST Security Best Practices**

NIST strongly recommends that the built-in security features of Bluetooth or 802.11 (data link level encryption and authentication protocols) be used as part of an overall defense-in-depth strategy. Although these protection mechanisms have weaknesses described in this publication, they can provide a degree of protection against unauthorized disclosure, unauthorized network access, and other active probing attacks.

However, the Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules, is mandatory and binding for federal agencies that have determined that certain information be protected via cryptographic means. As currently defined, the security of neither 802.11 nor Bluetooth meets the FIPS 140-2 standard.

In the above-mentioned instances, it will be necessary to employ higher level cryptographic protocols and applications such as secure shell (SSH), Transport-Level Security (TLS) or Internet Protocol Security (IPsec) with FIPS 140-2 validated cryptographic modules and associated algorithms to protect that information, regardless of whether the nonvalidated data link security protocols are used.

-and-

A denial of network availability involves some form of DoS attack, such as jamming. Jamming occurs when a malicious user deliberately emanates a signal from a wireless device in order to overwhelm legitimate wireless signals. Jamming may also be inadvertently caused by cordless phone or microwave oven emissions. Jamming results in a breakdown in communications because legitimate wireless signals are unable to communicate on the network. Nonmalicious users can also cause a DoS. A user, for instance, may unintentionally monopolize a wireless signal by downloading large files, effectively denying other users access to the network. As a result, agency security policies should limit the types and amounts of data that users are able to download on wireless networks.



CERT Coordination Center (in cooperation with the Australian CERT team)

By William Jackson
GCN Staff

In a springtime bursting with new security worries, wireless users learned of one that's already built into IEEE 802.11 wireless networking protocols.

The alert came last month from the United States CERT Coordination Center, at www.kb.cert.org, and from the Australian Computer Emergency Response Team, at www.uscert.org.au.

The Australian team said the vulnerability in wireless collision avoidance allows a "trivial but effective" denial-of-service attack against portions of wireless LANs using most of the 802.11 family of protocols.

The good news is that the effects of such an attack are temporary and usually limited in scope—although if an access point is targeted, it affects all clients using that point.

The bad news? No effective defense exists against such an attack, which could be carried out with low-powered equipment such as personal digital assistants.

The lesson is that wireless networks not only are subject to all the security concerns of wired networks, but they also have their own set of worries.

Queensland University of Technology's Information Security Research Center said the 802.11 protocols constantly check for clear frequencies over which devices can transmit. If the Clear Channel Assessment algorithm is used with direct-sequence, spread-spectrum (DSSS) transmissions, a specially crafted radio signal can fool a wireless device into thinking that all channels are busy, effectively blocking transmissions.

And the jamming device does not have to be authenticated by the network.

"This is not an implementation vulnerability," U.S. CERT said. "Any 802.11 DSSS device, including wireless network cards and access points, is vulnerable." Wireless security features cannot guard against it.

The solution is to avoid 802.11x devices that use DSSS at speeds below 20 Mbps.

Devices doing frequency-hopping, spread-spectrum (FHSS) or orthogonal frequency-division multiplexing (OFDM) transmission are not subject to the vulnerability. The 802.11a and 802.11g devices operating above 20 Mbps use OFDM. And 802.11 devices also can use FHSS.

Because the range of attack by a PDA would necessarily be limited, wireless networks inside a building and those that have been shielded against interference are less likely to fall victim.

Wireless networking has probably not yet become a necessity. Denial of service at a Starbucks or an airport is an inconvenience. Not being able to beam a Microsoft PowerPoint presentation into a conference room might also be an inconvenience, depending on the quality of the presentation. But denial-of-service attacks against a public safety network or a wireless LAN handling mission-critical applications could be far more serious.

Denial of Service Vulnerability in IEEE 802.11 Wireless Devices
13 May 2004

Last Revised: --

1. Description

A vulnerability exists in hardware implementations of the IEEE 802.11 wireless protocol[1] that allows for a trivial but effective attack against the availability of wireless local area network (WLAN) devices.

An attacker using a low-powered, portable device such as an electronic PDA and a commonly available wireless networking card may cause significant disruption to all WLAN traffic within range, in a manner that makes identification and localization of the attacker difficult.

The vulnerability is related to the medium access control (MAC) function of the IEEE 802.11 protocol. WLAN devices perform Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), which minimizes the likelihood of two devices transmitting simultaneously. Fundamental to the functioning of CSMA/CA is the Clear Channel Assessment (CCA) procedure, used in all standards-compliant hardware and performed by a Direct Sequence Spread Spectrum (DSSS) physical (PHY) layer.

An attack against this vulnerability exploits the CCA function at the physical layer and causes all WLAN nodes within range, both clients and access points (AP), to defer transmission of data for the duration of the attack. When under attack, the device behaves as if the channel is always busy, preventing the transmission of any data over the wireless network.

Previously, attacks against the availability of IEEE 802.11 networks have required specialized hardware and relied on the ability to saturate the wireless frequency with high-power radiation, an avenue not open to discreet attack. This vulnerability makes a successful, low cost attack against a wireless network feasible for a semi-skilled attacker.

Although the use of WLAN technology in the areas of critical infrastructure and systems is still relatively nascent, uptake of wireless applications is demonstrating exponential growth. The potential impact of any effective attack, therefore, can only increase over time.

2. Platform

Wireless hardware devices that implement IEEE 802.11 using a DSSS physical layer. Includes IEEE 802.11, 802.11b and low-speed (below 20Mbps) 802.11g wireless devices. Excludes IEEE 802.11a and high-speed (above 20Mbps) 802.11g wireless devices.

3. Impact

Devices within range of the attacking device will be affected. If an AP is within range, all devices associated with that AP are denied service; if an AP is not within range, only those devices within range of the attacking device are denied service.

Minimum threat characteristics:

- o An attack can be mounted using commodity hardware and drivers - no dedicated or high-power wireless hardware is required*

o An attack consumes limited resources on attacking device, so is inexpensive to mount

o Vulnerability will not be mitigated by emerging MAC layer security enhancements ie IEEE 802.11 TGi

o Independent vendors have confirmed that there is currently no defence against this type of attack for DSSS based WLANs. The range of a successful attack can be greatly improved by an increase in the transmission power of the attacking device, and the use of high-gain antennae.

3. Workarounds/Mitigation

At this time a comprehensive solution, in the form of software or firmware upgrade, is not available for retrofit to existing devices. Fundamentally, the issue is inherent in the protocol implementation of IEEE 802.11 DSSS.

IEEE 802.11 device transmissions are of low energy and short range, so the range of this attack is limited by the signal strength of the attacking device, which is typically low. Well shielded WLANs such as those for internal infrastructures should be relatively immune, however individual devices within range of the attacker may still be affected. Public access points will remain particularly vulnerable. The model of a shared communications channel is a fundamental factor in the effectiveness of an attack on this vulnerability. For this reason, it is likely that devices based on the newer IEEE 802.11a standard will not be affected by this attack where the physical layer uses Orthogonal Frequency Division Multiplexing (OFDM).

It is recognised that the 2.4G Hz band suffers from radio interference problems, and it is expected that operators of the technology will already have in place measures to shield their networks as well as a reduced reliance on this technology for critical applications.

The effect of the DoS on WLANs is not persistent - once the jamming transmission terminates, network recovery is essentially immediate.

The results of a successful DoS attack will not be directly discernable to an attacker, so an attack of this type may be generally less attractive to mount.

At this time, AusCERT continues to recommend that the application of wireless technology should be precluded from use in safety, critical infrastructure and/or other environments where availability is a primary requirement. Operators of wireless LANs should be aware of the increased potential for undesirable activity directed at their networks.

Defense—at last—issues wireless policy

*By Dawn S. Onley
GCN Staff*

The Defense Department has released its long-awaited wireless policy, making it mandatory for all DOD personnel, contractors and even visitors entering Defense facilities to encrypt unclassified information transmitted wirelessly.

The policy, DOD 8100.2, comes nearly two years after DOD issued a Pentagon wireless policy. The new policy, which supersedes the earlier Pentagon policy, takes effect immediately. DOD officials had suggested the policy was imminent for nearly three months.

“For data, strong authentication, nonrepudiation and personal identification are required for access to DOD information systems in accordance with published DOD policy and procedures,” said Paul Wolfowitz, deputy secretary of Defense. “Identification and authentication measures shall be implemented at both the device and network level.”

The directive views wireless devices, services and technologies that are integrated or connected to Defense networks as part of those networks. Data encryption, at a minimum, must be implemented end-to-end over an assured channel and must be validated against Federal Information Processing Standards requirements under the Cryptographic Module Validation Program.

The policy, released late Friday, will allow exceptions on a case-by-case basis.

The new law prohibits the use of wireless devices for storing, processing, or transmitting classified information without “explicit written approval of the cognizant designated approving authority. If approved by the DAA, only assured channels employing National Security Agency-approved encryption shall be used to transmit classified information,” Wolfowitz noted in the directive.

Furthermore, cellular, PC, radio frequency and infrared wireless devices are not allowed—without written approval—in areas where classified information is discussed, electronically stored, processed or transmitted.

Wolfowitz directed Defense agencies to screen for wireless devices within their organizations by using active electromagnetic sensing to detect and prevent unauthorized access of Defense systems.

**Department of Energy
21 Step Booklet to Improve Cyber Security of SCADA Networks**

This is directly applicable to the SCADA question.

<http://www.ea.doe.gov/pdfs/21stepsbooklet.pdf>

A copy of the DOE 21 Step Booklet is included.

For assistance in identifying vulnerabilities and in the design of resistant networks please contact us.

Ms. Tisha A Hayes
Sr. Communications Engineer

Edison Automation Inc.
1800 Elm Hill Pike
Nashville, TN
37210
Office: (615) 256-2522
www.edisonautomation.com



Technical Products, Technical People, Real Solutions

