ciscopress.com

ZigBee Wireless Security: A New Age Penetration Tester's Toolkit

Date: Jan 9, 2012 By Brad Bowers.

Penetration testers have been focusing on wireless technologies for over a decade now, and one protocol that can arguably be placed at the top of the list is the 802.15.4 protocol that ZigBee wireless rides on. New tools and techniques are being developed by penetration testers to validate the security and configuration of ZigBee-enabled devices. Brad Bowers takes a closer look at the ZigBee protocol, some of the attacks that have been leveraged against it, and the security tools that penetration testers can use.

Intro: A Change in Focus

Penetration testers have been focusing on wireless technologies for over a decade now, and those of us in the industry have seen the various families of wireless protocols evolve through a roller coaster ride of security issues, half-baked encryption schemes, and mitigation tactics.

While the 802.11 wireless protocols is by far the most popular and has stolen much of the limelight for security issues and development it's not the only show in town. Lately, other wireless protocols have become the focus of security researchers and hackers alike. One protocol that can arguably be placed at the top of the list, and is an area of growing concern, is the 802.15.4 protocol that ZigBee wireless rides on. New tools and techniques are being developed by penetration testers to validate the security and configuration of ZigBee-enabled devices.

This article takes a closer look at the ZigBee protocol, some of the attacks that have been leveraged against it, and the security tools that penetration testers can use.

ZigBee is not exactly a new technology; in fact it was originally developed in 1998, but only recently has ZigBee become more commonplace in industrial and consumer products. ZigBee was designed to fulfill a niche and previously untapped market in which regular wireless devices were unsuitable. The unique characteristics of ZigBee embedded wireless devices have opened a floodgate of new products that require its low power simplicity and functionality.

How ZigBee Differs

The ZigBee protocol differs from traditional 802.11 wireless in many ways, most notably the simplicity, low cost, and elegant function.

ZigBee was designed to provide short–distance wireless solutions in which running wires to transfer data is infeasible or cost prohibitive. ZigBee does not provide the bandwidth and advance error checking provided by its 802.11 big brothers. This stripped-down approach to networking has many advantages including ease of setup, low power consumption, and simple integration into other devices.

Easy Setup

ZigBee devices can be used in lots of different ways, but they have built-in protocol support for both mesh and star-based network topologies. Given some very basic configuration settings, a ZigBee device (node) can be joined to an existing mesh network or be assigned as the controlling device to manage the interaction of other ZigBee nodes.

As you can imagine, there are lots of security attack potential here, but we'll get into that more in a bit.

Low Power

ZigBee requires very little power to function and to maintain its association with other ZigBee devices. Many implementations can run for several years off one set of

batteries. The low power consumption of ZigBee devices comes at the cost of bandwidth and effective communication range, however.

Low Bandwidth

ZigBee is definitely not a sports car when it comes to moving large amounts of data. While there are some methods for increasing its max bandwidth, ZigBee generally tops out at 250Kbps. This makes it a poor choice for data-hungry consumer products such as cellphones or video, but superb for short communication bursts or infrequent sensor data transmissions.

Short Range

Another limitation of ZigBee is its relatively short communication range. While the ZigBee specifications state that it can effectively transmit up to 100 meters, most devices are functioning closer to the 10-meter range. The lack of complex data and error checking also plays a contributing factor into the range limitation of ZigBee devices.

ZigBee Impacts the Physical World

Now you have a little background on some of the advantages and disadvantages of ZigBee. Where is it being used, and what is all the security hubbub about? While ZigBee may not be the fastest or offer the greatest distances it still has a tremendous amount of uses.

A noted wireless security expert once said, "No wireless technology has been more integrated or impacts the physical world more than ZigBee." He was absolutely right! ZigBee radios have been integrated into all sorts of sensors and monitoring and control devices; and have found their way into hospitals, industrial facilities, and control systems that our society relies on every day.

In hospitals, ZigBee radios are more frequently found in patient-monitoring systems to provide data collection while allowing uninhibited mobility of the person wearing the device. They are even finding a home "inside" patients as a means for doctors and medical professionals to communicate with patients that have been fitted with an implanted defibrillator or other heart-monitoring device.

The short range and low output power limits the problem of radio interference with other radio devices or medical equipment. Doctors can simply use another ZigBee radio to interact with the patient's device, collect data, or even change the configuration settings of the implanted device.

ZigBee radios are also heavily used in industrial applications. They are integrated into refineries, chemical plants, and water-treatment facilities as sensors or to control processing equipment.

The explanation and business drivers behind why companies are utilizing ZigBee radios are very simple to understand. Running physical wires has a significant labor and material cost, while using a self-contained, battery-operated ZigBee radio limits these costs and provides administrative advantages when troubleshooting issues.

Other organizations are switching to ZigBee radio devices for monitoring and regulating the temperature in buildings, or communicating with controllers to shut down lights when people are not in the room.

Another area where ZigBee devices have become very popular is in our homes. New residential housing is often implemented with ZigBee–enabled water and gas meters. Utility providers use specially configured ZigBee radios as data collectors to collect the water and gas meter's transmissions from their utility vehicles. This process greatly increases the efficiency of utility companies collecting meter and billing data.

Security Issues

If you are an information security professional, your spidey senses are probably tingling[md]and frankly they should! It doesn't take a lot of imagination to think about how these real-life implementations of ZigBee radios could be used by malicious actors to cause life-threatening events or significant harm to individuals or our infrastructure.

At first glance, this may seems like your traditional Fear, Uncertainty, or Doubt (FUD)

about the risks associated with ZigBee radios. When you consider some of the actual attacks that have been leveraged against real organizations, however, you start to get an eye-raising dose of reality.

Attacks against ZigBee

ZigBee wireless attacks and security has attracted a lot of interest by government- and industry-security professionals as well as the hacker community. Each is looking at the security capabilities of the 802.15.4 protocol as well as how manufacturers are implementing the ZigBee radios into products and equipment. Often it is the "implementations" part of the equation that is causing most of the security risks. This is clearly evident in the types of attacks used against the devices.

ZigBee and the 802.15.4 framework it rides on were designed with security in mind, but as we have all learned, security is only effective if it's implemented properly. While there are numerous types of attacks that have been successfully leveraged against ZigBee devices, they generally fall into three categories: physical attacks, key attacks, and replay and injection attacks.

Physical Attacks

If a knowledgeable attacker can gain physical access to a device containing a ZigBee radio, chances are good that they can compromise it. What makes physical attacks so effective is being able to interact *physically* with the device to obtain an encryption key used by the target ZigBee network. Many ZigBee radios use a hard-coded encryption key that is loaded in RAM memory when the device is powered.

Since these keys are typically written (flashed) on all the devices in a ZigBee network, it's highly unlikely that the keys will ever be changed. Knowing this, attackers can utilize special serial interfaces on the ZigBee device to attempt to capture the encryption keys as those keys are moved from flash to RAM during power up.

There are numerous low-cost and open-source tools that make this form of attack within the grasps of any attacker. Two of the most popular are Bus Pirate and GoodFet.

The Bus Pirate and GoodFet interface boards provide support of numerous industry standard serial protocols, including 1-wire, JTAG, SPI, and asynchronous serial. Once physically connected to a ZigBee device through a simple serial interface such as a Bus Pirate, an attacker can unravel the security of an entire ZigBee network and potentially intercept and alter data.

Key Attacks

Other forms of key attacks are possible by utilizing remote means to obtain encryption keys. ZigBee radios often use one of two encryption key methodologies to ensure that devices have the appropriate keys to talk to each other. These methodologies are known as pre-shared keying and Over the Air (OTA) key delivery. Larger, more sophisticated ZigBee networks will typically utilize OTA for security and ease of updating.

Did I say "for security"? Unfortunately, this methodology can be attacked by having a device that mimics a node on the ZigBee network and collects the network's wireless transmissions. The collected packets can be further analyzed or potentially decrypted using free and open-source equipment.

Since there is minimal session checking built into the 802.15.4 protocol and currently no intrusion-detection capabilities, this type of attack is nearly impossible to detect.

One toolset that is very effective for this type of key analysis is called the KillerBee framework, which was created by Joshua Wright, a noted wireless security expert, and has been made freely available to everyone. KillerBee is really a suite of hardware and software tools that allow sophisticated interception, analysis, and even transmission of 802.15.4 packets. The software included in KillerBee is a collection of Python scripts that are easily modified and can be built upon to create even more capabilities and interaction with ZigBee radios. The hardware portion of the framework requires a specially programmed ZigBee radio, but don't let that fool you into thinking they are hard to obtain.

While several low-cost ZigBee radios are supported, the recommended device of choice

is the RZ Raven AVR, which can be obtained online for approximately $40. This puts the hardware and programs well within the reach of security researchers and malicious hackers alike.

An attacker using a combination of hardware- and software-based tools to perform their illicit actions has the obvious advantage of not needing to physically connect to the device to perform an attack. This makes it extremely unlikely that the attack will be discovered and even less likely that the attacker will be caught. To make matters worse, an attacker could use specially crafted high-powered transmitters or special Yagi antennas so the attacker could potentially be a great distance away from the devices they attempting to compromise.

Replay and Injection Attacks

One final type of attack we'll discuss can utilize key-based attacks blended with packet replay and/or injection attacks to trick the ZigBee device into performing unauthorized actions. ZigBee radios are susceptible to these types of attacks because of the lightweight design of the protocol, which has very minimal replay protection. A simple scenario will help drive the point home.

Bob, our malicious user, uses a ZigBee radio that is collecting packets transmitted from a target ZigBee network. While Bob may not be able to decode the packets *per se*, he knows enough about the system to know that the target node controls the water flow for a cooling system.

All Bob has to do in this case is to replay the captured packets back to other nodes on the ZigBee network mimicking the originating node. Since there is minimal session checking performed by the ZigBee radios, the network will think the traffic is legitimate and respond as if the commands came from a valid node. A spinoff of this type of attack was used at the 7th annual Mid-Atlantic Collegiate Cyber Defense Challenge. A more comprehensive write up of the event can be found here in the articles of InformIT.

Penetration Testers Toolkit

Now that we have discussed where ZigBee radios are being used and some of the attacks and tools that can be used against the devices, what can an Information Security professional do to help the organization deal with the onslaught of potential attacks against the business? The answer, like some many things in Information Security, is complicated.

The simple truth is that most Information Security Professionals are not typically trained to mitigate against hardware-based attacks. With that said, Information Security Professionals with experience in wireless security mitigation tactics often have the building blocks to quickly get up to speed on the various attacks and defenses used with ZigBee radios.

The first thing that an Information Security Processional needs is a collection of hardware and software tools that will help assess the environment and give them the ability to develop the traditional defense in depth.

Many of the tools that have been mentioned previously in this article have assessment and defensive capabilities that will help identify problems within a ZigBee network, but there are additional ones that deserve to be mentioned. Enter the Chibi!

Chibi Can Help

The FreakLabs's *Chibi* is an Arduino-compatible microcontroller with an integrated ZigBee radio build into it. The Chibi has become very popular with penetration testers and security researchers alike.

On the surface, this network device may seem ill fitted for assisting with assessing security on its ZigBee networks. Especially when you consider the fact that it was not designed to be a security tool. Those doubts fade away, however, when you take a closer look at the Chibi's capabilities and ease with which code can be developed for it.

FreakLabs is a small organization that builds open-source hardware and software with a loose focus on security. What makes these Chibi ZigBee radios special is the fact that the device is built on what the FreakLabs's team calls FreakZ, an open-source, ZigBee–compliant protocol stack. This may seem like a trivial detail, but it's actually one of the key reasons why penetration testers and security researchers are flocking to the device.

One of the biggest challenges for researchers looking into ZigBee security is the high cost and complexity of obtaining software and API code from major semiconductor providers.

Without the software that allows interaction with commercial ZigBee radios, a researcher has limited ability to develop tools or other equipment that will run on multiple manufacturers' equipment. The FreakZ protocol stack is completely open source, and all the code is readily available. This provides a fertile ground for security researchers to develop code and to help automate their ZigBee assessments.

Chibi in Action

The Chibi radio is versatile from a security assessor's perspective. Virtually every nuance of the 802.15.4 protocol stack can be manipulated and monitored to provide a comprehensive view into the network to which it's connected.

While the Chibi provides an excellent platform for interacting with ZigBee networks and performs most of the timing requirements of the radio, the majority of the magic comes from the array of tools and scripts that the security community has developed to interact with the device.

- **Scripting**: Penetration testers can easily incorporate their own functionality and code into a Chibi device using the Python scripting language. Python provides a very straightforward approach for interacting with all aspects of the Chibi hardware as well as acting as a glue to provide interoperability between disparate hardware software components.

  Python scripting support also helps provide some cross-platform compatibility between hardware devices. As an example, the KillerBee's firmware and python scripts can be modified to work on the Chibi's hardware.

- **Packet Capturing**: Nothing quite gets a Security Professional's heart pumping faster than a packet capture of an attack that has been waged against their systems. This is one area where the Chibi radio with a bit of open source code shows its value against even the most expensive of commercial tools. The Chibi radio, with a piece of open source software called WSBridge, can perform a complete packet capture of all 802.15.4 frames that it's configured to listen to.

  These packet captures can be directly imported into one's favorite packet analysis tool such as WireShark or TCPDump, which can provide a tremendous value from a security perspective! Not only does it provide an excellent method for troubleshooting technical issues, but it also offers Security Professionals a window into what's happening on their ZigBee networks.

  With a little bit of scripting, it is even possible to create a rudimentary Intrusion Detection System for a ZigBee network by send captured packets to into an Intrusion Detection System such as Snort.

- **Penetration Testing**: From a Security Assessor's point of view, the Chibi radio has much of the same capabilities as the KillerBee framework discussed earlier—with several unique advantages.

  Since the Chibi is essentially an Arudino microcontroller with a ZigBee-compliant radio embedded on it, there are lots of hardware additions that can easily be integrated to make the device an independent piece of equipment that doesn't require the direct connectivity of a computer to function.

  As an example, a Security Assessor can easily incorporate a microSD memory card and a set of batteries to the Chibi board. With the addition of a little bit of code, the Security Assessor could have a self-contained ZigBee packet inject or capturing device that can run for several days without the need to be connected to a computer. An example of this very setup was presented at the 2011 Defcon Security Conference.

Another advantage for Security Assessors is the ability to craft and transmit malformed or exotic packets to devices on a ZigBee network. Since ZigBee has minimal session and error check, the packets could cause nodes to respond inappropriately, perform an unintended function or even cause the node to crash requiring physical intervention to fix the issue. Security Assessors can use tools like the Chibi to identify these potential security concerns and help organizations proactively mitigate the risk or impact of

attacks against their ZigBee networks.

The Wrapup

The focus of attackers is changing, and Information Security professionals need to change with it. It is no longer acceptable to be an Information Security Professional with no working knowledge of hardware-based attacks. It's no longer acceptable to understand traditional 802.11 wireless security without knowing the other wireless protocols that are being rapidly adopted by businesses.

New kinds of attacks are starting to emerge that are challenging our preconceived notions of what wireless security is all about. Unlike traditional wireless security, new ZigBee wireless technology risks can impact both corporate data and even the physical world.

There is little doubt that ZigBee radios will continue to be widely deployed in both consumer and industrial applications. This rapid escalation and adoption of ZigBee-enabled devices requires trained and vigilant Information Security Professionals who can detect, assess, and defend against a myriad of new and emerging wireless attacks.

While there are many tools that are at their disposal, it will take an increased awareness of ZigBee attacks and a deep understanding of these tools to better defend businesses.
