



PRIVACY AND SECURITY FANATIC

By Ms. Smith

About |

Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues.

Researchers exploit ZigBee security flaws that compromise security of smart homes

Researchers at Black Hat and Def Con warned about security flaws in Internet of Things devices using the ZigBee protocol, leaving Philips Hue light bulbs, smart locks, motion sensors, switches, HVAC systems and other smart home devices vulnerable to compromise.



Network World | Aug 11, 2015 10:54 AM PT

If you have an Internet of Things device, then it's highly likely that you are using ZigBee whether you know it or not. There are other possibilities, including that your IoT devices use the Z-Wave protocol, which was beat up a couple ago by security researchers who used it to attack automated homes. ZigBee is a wireless standard used for connectivity to controls IoT devices. It's used in "tens of millions of smart meters" and there are 1,088 items listed as ZigBee Certified products. It depends who you listen to, I suppose, as to whether you believe ZigBee is great or if ZigBee is a great threat to the Internet of Things due to critical wireless security flaws that can be exploited to compromise smart lights, door locks, motion sensors, smart switches, temperature sensors, HVAC systems and other "smart" home devices.

Li Jun and Yang Qing of Qihoo360's Unicorn team, presented "I'm A Newbie Yet I Can Hack ZigBee – Take Unauthorized Control Over ZigBee Devices" (pdf) at Dec Con 23. Their goal was to teach users to hack ZigBee as well as to teach users techniques to prevent hackers – or anyone without authorization – from taking control of their ZigBee-enabled appliances; they showed how to find the encryption key in firmware and sniff the network key as it is sent in plaintext.

Find the encryption key by sniffing

The following screenshot shows the process of a new node joining the network, and the figure is quite self-explanatory . The network key is sent from the coordinator to the joining device in plaintext, and after receiving the network key the communication is immediately encrypted.

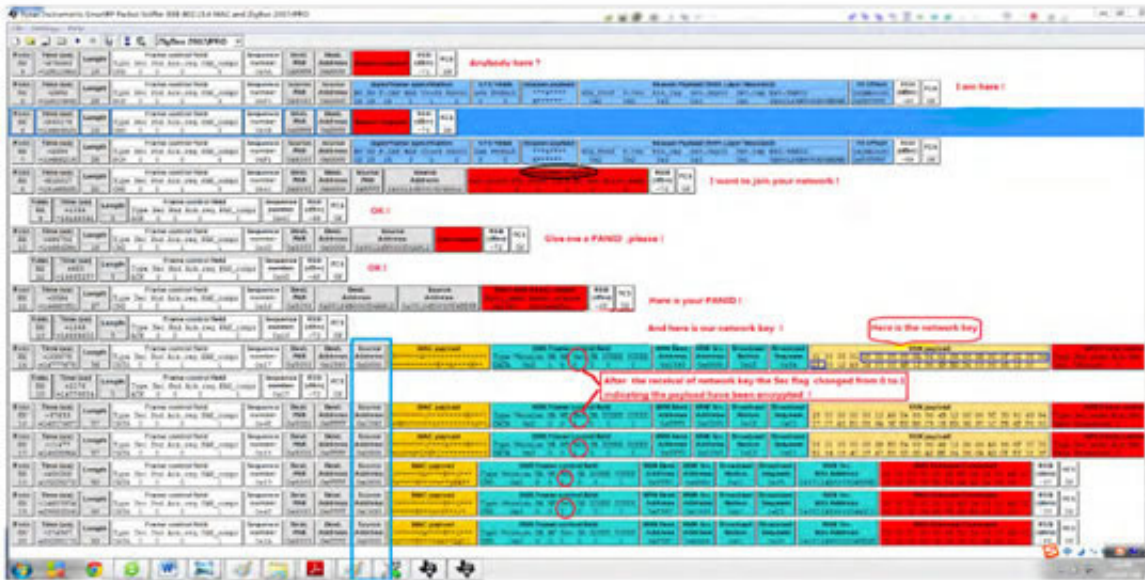


Image credit: Li Jun and Yang Qing

I'm A Newbie Yet I Can Hack ZigBee – Take Unauthorized Control Over ZigBee Devices

But that wasn't the only talk to beat up ZigBee as Tobias Zillner, senior IS auditor at IT security firm Cognosec, also warned that hackers could compromise ZigBee networks and then "take over control of all connected devices on a network." Zillner presented "ZigBee Exploited the Good, the Bad, and the Ugly" at Black Hat USA (slides [pdf](#)). Network encryption keys are briefly transmitted in the clear when a new device joins the network. Some devices use the default master key, meaning that is what is transmitted when a new device is added to the network. The key could be captured by an attacker or a thief who could, for example, pull an open sesame on a smart door lock.



No physical access is required



No knowledge of the secret key is needed



Usability overrules security

Tobias Zillner and Sebastian Strobl

Back in 2013, Philips Hue light bulbs were dubbed “highly hackable” after a researcher injected malware into the Hue bridge and blacked out the lights. The smart bulbs constantly search for new devices to pair with, Cognosec researchers said, which makes them easy to reset to factory defaults. An attacker can capture the unencrypted key transmitted by the Hue bulb when it reboots.

Cognosec researchers wrote, “If an attacker is able to sniff a device and join using the default link key, the active network key is compromised and the confidentiality of the whole network communication can be considered as compromised.” They added, “Key secrecy should not be the foundation of ZigBee product’s security architecture.”

- Security measures provided are good
- Requirements due to interoperability weaken the security level drastically
- Vendors only implement the absolute minimum to be compliant
- Usability overrules security



Tobias Zillner and Sebastian Strobl

That doesn't mean you should avoid ZigBee-enabled devices like the plague. The "security features provided by ZigBee standard can be considered as very strong and robust," Cognosec wrote in its white paper ([pdf](#)). "ZigBee encryption is based on the well-known AES algorithm for data encryption and data authentication. The security is dependent on the secrecy of the encryption keys as well as their secure initialization and distribution of the encryption keys."

The problem is the weak way ZigBee is implemented by vendors in a race to sell Internet-connected gadgets. Some vendors don't give a thought to security and "implement the minimum of the features required to be certified." That may help keep costs down, but Zillner said it is "essential for security" to fulfill the following "preconditions on the implementation side:"

- Device tampering: "A tamper-resistant node could erase the sensitive information including the security keys if tampering is detected."
- Key transport: "The default TC link key should not be used since this key is considered as public knowledge and therefore provides the same level of security as unencrypted key transport."
- Key establishment: "The master keys used during key establishment shall be distributed via out-of-band channels." That could be accomplished by something as simple as a sticker with the master key being attached to the device for the user to enter during setup.
- Key rotation: "The security of the communication is dependent on the secrecy of the network key and of the link keys. The network key shall be changed periodically. Key management in the form of changing the network key in a meaningful time period or after a certain number of messages should be introduced. Otherwise known plaintext or other attacks on the security of AES may be possible."

After the attack on ZigBee at the hacker conferences, the ZigBee Alliance issued a long statement published in full on Engadget.

Remember back when David Petraeus was the CIA Director and he said the CIA couldn't wait to spy on Americans via their smart appliances? Cognosec researchers quoted Petraeus as saying, "Items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio frequency identification, sensor networks, tiny embedded servers, and energy harvesters - all connected to the next-generation internet."

There are serious privacy requirements when it comes to home automation as it generates massive amounts of personalized data. You pay high dollar for smart devices, yet you then have to hand over massive permissions to the same vendors in order to the use a smartphone app to control the device you already paid for! That alone is crazy cause it's not like they gave you the device for free, but they still slurp and store all your data as if it is the cost for a free product. Gartner predicted there will be over 500 smart devices per household by 2022, so vendors need to take privacy and security seriously, instead issuing statements after they are hacked about how much they care about security and users' privacy.

SmartThings v2

Nevertheless, if you were bit by the IoT bug and want to know which platform is a good bet...the IoT company SmartThings, which was acquired by Samsung last year, has now joined the ZigBee Alliance which intends to put all forms of ZigBee under one ZigBee 3.0 standard. SmartThings is hacker-friendly and seemed to be a real contender in the smart home platform arena. At CES 2015, SmartThings announced that a new SmartThings hub and sensors would be available in the second quarter of this year. In March, SmartThings said those devices weren't ready and changed the projected release to the third quarter which started in July and ends on September 30. There was some speculation that Samsung, or the battery backup function, was behind the delay.

SmartThings has teased potential hub 2.0 buyers with a few images, but that is about it. A week ago, SmartThings said there are still no official specs for 2.0 yet. You are no doubt impatient if you've been waiting for it since the announcement at CES, but the new release is still supposedly coming this quarter.



Ms. Smith


Ms. Smith (not her real name) is a freelance writer and programmer with a special and somewhat personal interest in IT privacy and security issues. She focuses on the unique challenges of maintaining privacy and security, both for individuals and enterprises. She has worked as a journalist and has also penned many technical papers and guides covering various technologies. Smith is herself a self-described privacy and security freak.



➤ **Must read: 11 hidden tips and tweaks for Windows 10**

 **View Comments**

YOU MIGHT LIKE

Promoted Links by Taboola 

Hillary wants to stop gun violence in America. Join her.

Hillary Clinton

Shark Tank Just Revealed a Trillion-Dollar Idea

The Motley Fool

3 Ultra-High Paying Miles Rewards Cards Have Hit The Market

LendingTree

Read Ebooks? Here's The Worst Kept Secret Among Book Lovers

BookBub

“Normal” Belts Are Going the Way of the Dinosaur. Here’s Why.

SlideBelts

Winos Rejoice! There's a Netflix for Wine

Popdust by Tasting Room

Touchjet Wave turns your TV into a giant Android tablet for only \$200

7 wireless charging solutions

Microsoft's Surface Pro 4, the tablet that can finally replace your laptop

7 Credit Cards You Should Not Ignore If You Have Excellent Credit

NextAdvisor

Copyright © 1994 - 2015 Network World, Inc. All rights reserved.