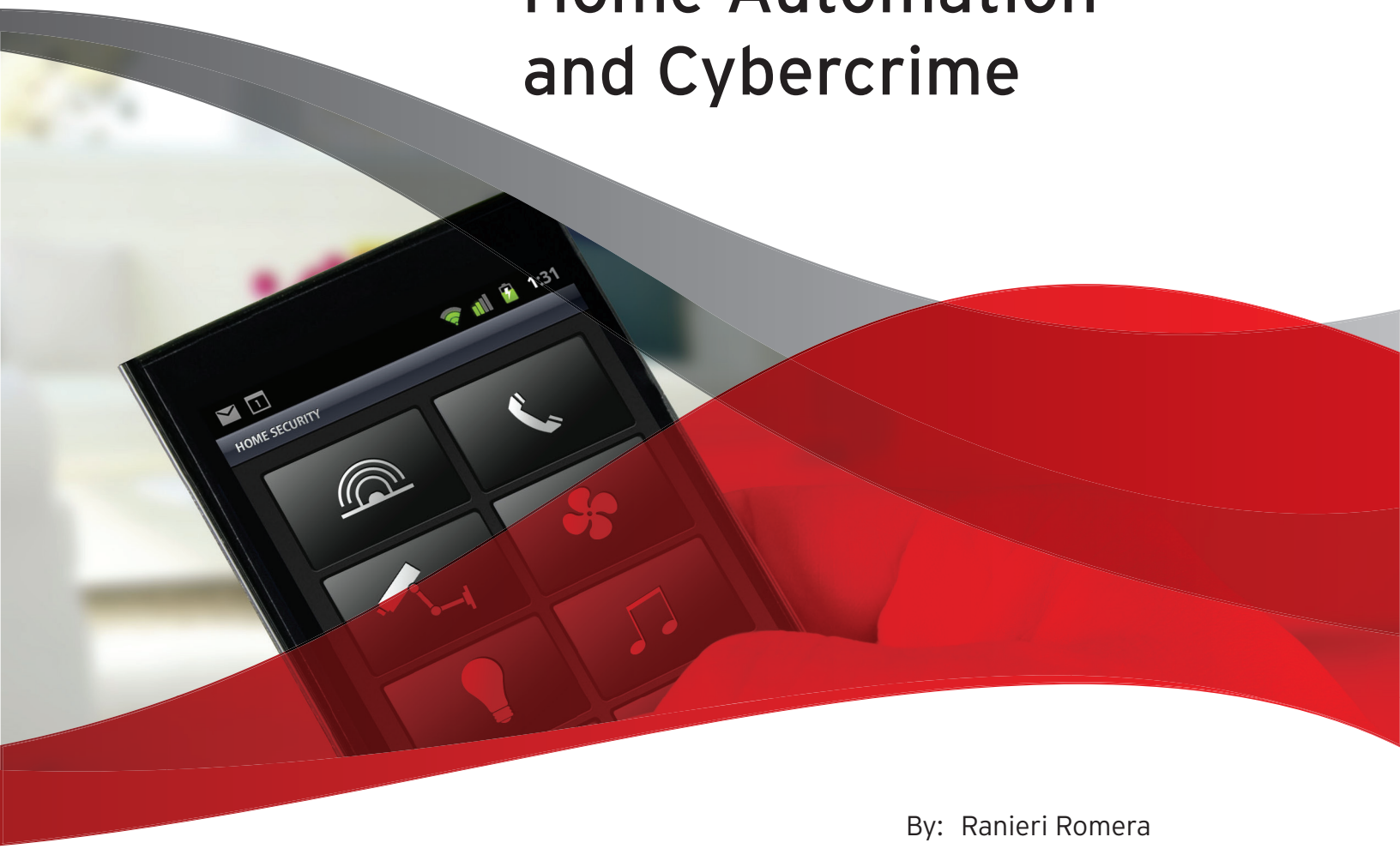
Trend Micro Incorporated
Research Paper
2013

# Home Automation and Cybercrime




By: Ranieri Romera

# Contents

# Introduction

Connectivity, whether over the Internet or a network; home automation; energy conservation; security; and various in-home applications remain driving factors of communication. All of these have varying requirements in terms of bandwidth, cost, and installation. The development of Internet-connected technologies particularly require implementing IP solutions at home to harness energy savings and improve one's quality of life while staying safe from security threats.

Several customized industry-standard-based networking protocols allow the fast growth and implementation of self-healing mesh networks, which are much more reliable network arrangements. These networking protocols, including X10, Z-Wave, and ZigBee, are based on the IEEE 802.15.4 protocol. They can enable cost-effective communication between devices with low latency and cheap installation costs. But because there are several available protocols, security may suffer. Each protocol represents a new area for possible security flaws.

This forward-looking paper will cite some of the ways by which the lack of standards can put users, specifically of Internet-capable home appliances for which customized protocols were created, at great personal risk. It specifically features three case studies on the previously mentioned home automation protocols based on IEEE 802.15.4.

# Case 1: X10

## Brief Overview

X10 is a standard that can be used to transmit data and/or commands over a home's electrical power line wiring. It is implemented over wireless radio as well.[1]

X10 can be used to control several automated devices at home, including electric garage doors, magnetic window and door contact sensors, and alarms.

Some people may have mixed home infrastructures. This means that some automated devices are wirelessly controlled while others are directly connected to power lines. In this case, a command or message from any connected device can communicate with all others, regardless of the way each is connected.

## Possible Attack Scenario

Each X10-based home network has a unique 4-bit ID number. This means there are only 16 possible ID numbers so it is very easy to initiate a brute force attack on the system to guess the correct ID number.

In addition, all X10 devices can be turned off using a single command. So if you have an electric socket outside your house, say your garden, a thief can plug in an X10 device and turn off all other connected X10 devices with his device's help. If one of the X10 devices he turns off is your alarm, he can then freely enter your house and steal from you.

1 http://en.wikipedia.org/wiki/X10_(industry_standard); http://www.thehomeautomationstore.com/x10.html; http://www.thehomeautomationstore.com/phc02.html; http://www.ihometouch.com/

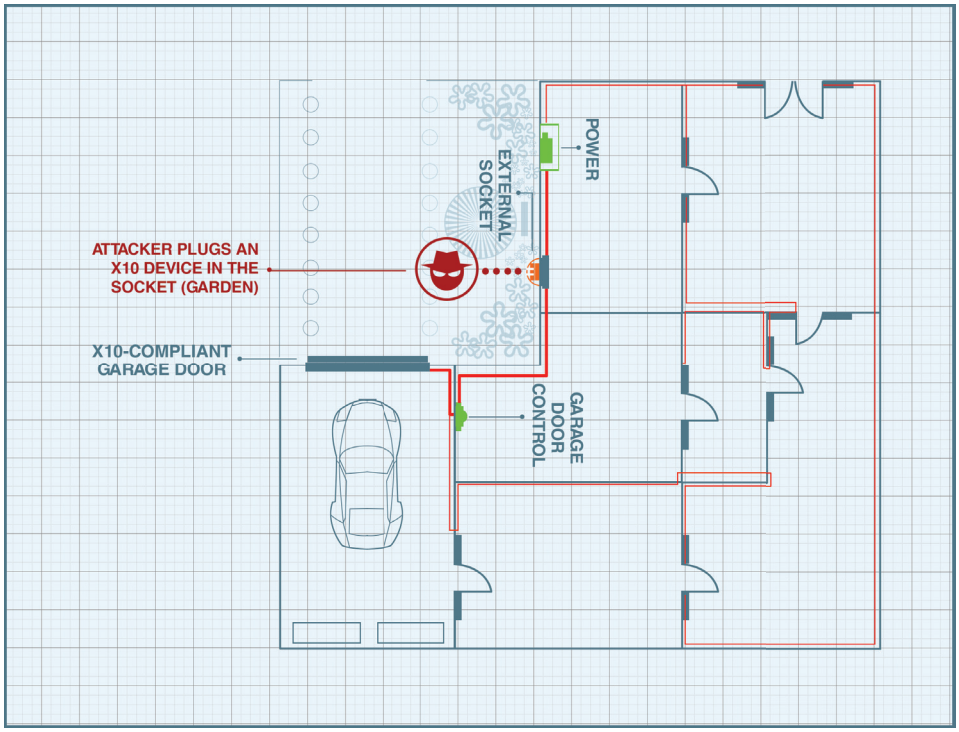



**FIGURE 1:** Possible X10 device attack scenario

## Possible Solution

For a power line network, use an isolation transformer to separate lines for X10 device use and those for non-X10 devices. Commands and messages from any X10 device can't pass through a transformer.

If you use an X10 device to wirelessly control several other X10 devices at home, keep surveillance systems out of your wireless network.

# Case 2: Z-Wave

## Brief Overview

Z-Wave primarily allows reliable transmission of short messages from a control unit to one or more nodes in a network. Its architecture comprises five main layers—the physical (PHY), Medium Access Control (MAC), transfer, routing, and application layers. It uses two types of device—controllers and slaves.[2] Controllers poll or send commands to slaves, which either reply to or execute the controllers' commands.

2 http://www.z-wave.com/modules/ZwaveStart/; http://www.z-wavealliance.org/; http://en.wikipedia.org/wiki/Z-Wave

Some people's houses can be fully controlled via a home automation system (e.g., sockets, TV sets, sound systems, lights, etc.). They may have started building their wireless personal area networks (WPANs) years ago so they would have various versions of Z-Wave chips (i.e., 200, 300, and 400 series).[3] Note though that messages sent to and received from 200 and 300 series chips can't be encrypted but those to and from 400 series chips can.

## Possible Attack Scenario

Given the situation above, it's possible to sniff all of the traffic that flows in a WPAN. Anyone can even learn to use legitimate tools like Wireshark and Freakduino Chibi Wireless Arduino-compatible boards for their own malicious ends.[4]

Cybercriminals can easily view tutorials and buy tools to sniff WPAN traffic to find out what their owners do on a daily basis and what kinds of device they have at home and how these are controlled.

Knowing the day-to-day schedule of the owner of an automated home can let a thief know when the house is empty and easy to steal from, for one.

More tech-savvy thieves can also inject random commands to your WPAN, letting them turn connected devices on and off or change how these are set up. They can tinker with automated devices and/or appliances in your home, causing them to malfunction. Then they can offer you repair services, which can either make the problem go away for a hefty sum or cause you even more trouble.

Things can get even worse when this happens to a hospital or factory.

3 http://en.wikipedia.org/wiki/Personal_area_network

4 http://www.freaklabs.org/index.php/Tutorials/Software/Feeding-the-Shark-Turning-the-Freakduino-into-a-Realtime-Wireless-Protocol-Analyzer-with-Wireshark.html; http://www.freaklabsstore.com/index.php?main_page=product_info&cPath=22&products_id=187&zenid=mefh34o9g737c3pk2rgbm7eoe5; http://www.arduino.cc/en/Main/ArduinoXbeeShield

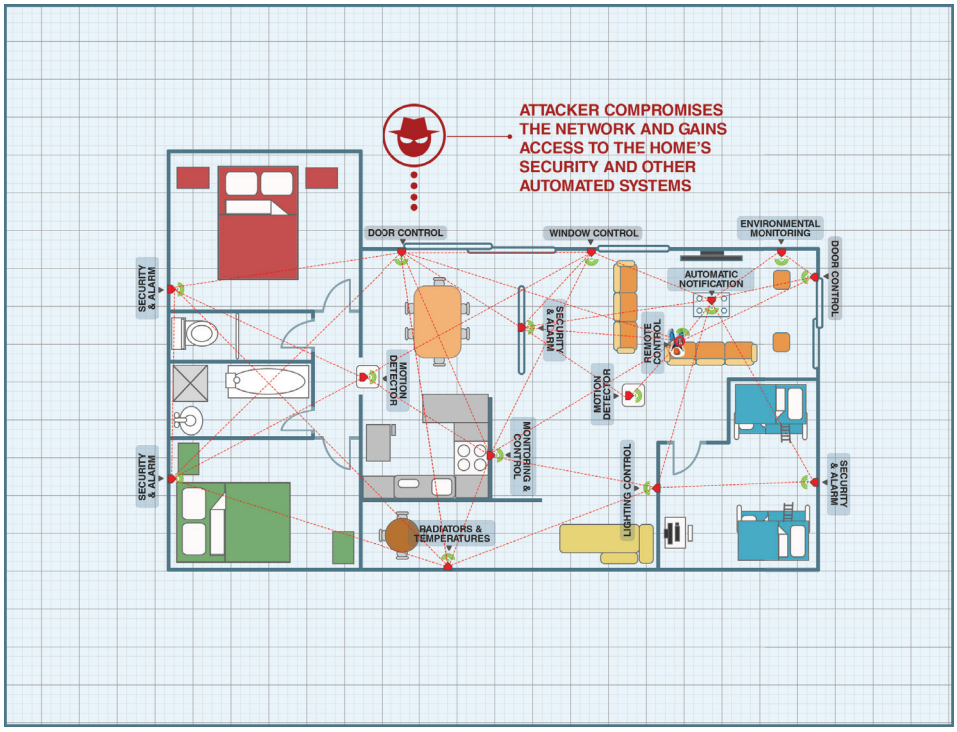



**FIGURE 2:** Possible Z-Wave device attack scenario

## Possible Solution

Replace 200 and 300 series with 400 series chips so you can encrypt your automated devices' WPAN traffic.

Don't forget to regularly change their Advanced Encryption Service (AES) keys as well. Encrypting AES keys lessens the likelihood that a similar attack will occur because it is very hard to decrypt them.

# Case 3: ZigBee

## Brief Overview

ZigBee is a low-data rate, low-power consumption, and low-cost wireless mesh networking protocol for automation and remote control applications.[5] It comprises four basic layers—the PHY, MAC, network, and application layers—which provide additional security functionality.

5 http://www.sensor-networks.org/index.php?page=0823123150; http://www.ti.com/product/cc2420; http://www.zigbee.org/; http://en.wikipedia.org/wiki/ZigBee; http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf

## Possible Attack Scenario

Unlike X10 and Z-Wave, products based on ZigBee uses AES to encrypt messages. This makes it very hard to figure out possible attack scenarios.

ZigBee has cryptographic support, which is enabled by default. Problems can only surface in the gateway between a WPAN and an IP network. People normally trust ZigBee's security but forget about their IP networks. They forget that these need to be specially configured for safety.

If an attacker gains access to your gateway due to your use of a default or weak password, a misconfiguration, or lack of security, he can bypass ZigBee authentication. This will give him full access to your network, including your security cameras. He can then see your daily activities. He can also change your gateway configuration so you'll connect to a fake Domain Name System (DNS) or proxy server. He can respond to all of your DNS queries and sniff all of the HTTP and HTTPS requests you send out. This will allow him to steal your personally identifiable information (PII), including your email and bank account credentials. With uninhibited access to your router, he can change your firewall settings and get direct access to any ZigBee-compliant device of his choosing.

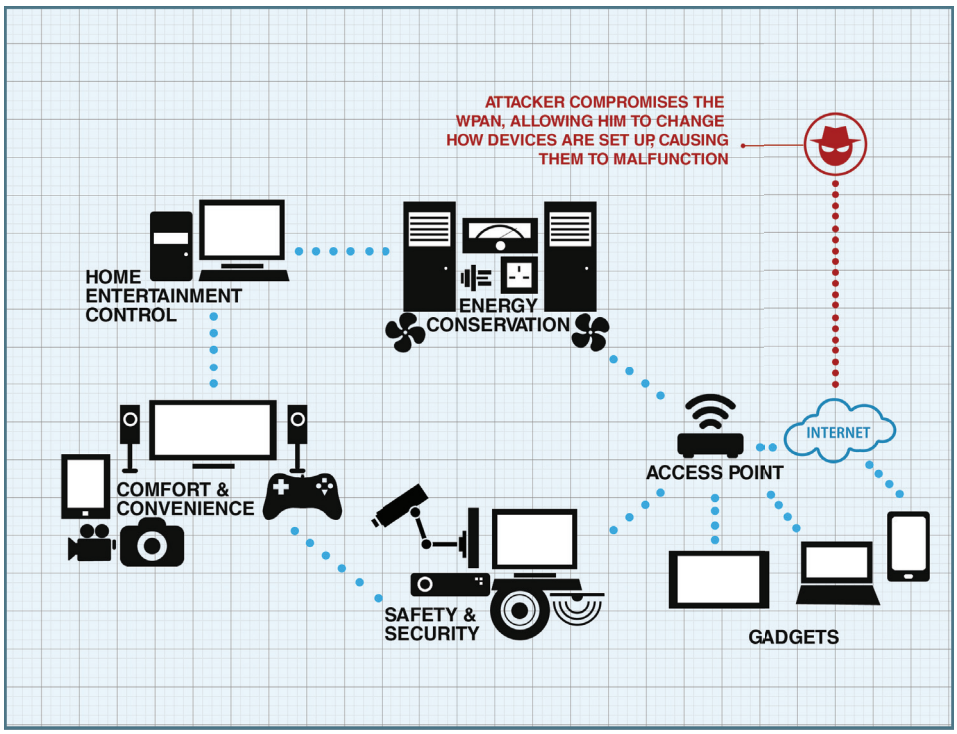



**FIGURE 3:** Possible ZigBee device attack scenario

## Possible Solution

Never make any of your automated home appliances Internet facing. But if you have to, make sure you always use strong passwords for your devices. Never use the same password for all Internet-connected devices. Make sure you periodically change your passwords and maybe even how your connected devices are configured. Try as much as possible to isolate automated home appliances from your network as well.

# Conclusion

The IEEE 802.15.4 standard was mainly created for the use of the residential and industrial markets.[6] We expect the industrial market to automate more and more devices for home use. They will ensure that these products are easy for anyone to install. We then expect the residential market to follow, taking advantage of lower costs enabled by the first step taken by the industrial segment.

IEEE 802.15.4 has already caught other communities' attention, giving way to other standards like IEEE 1451, which deals with sensor networking.[7] We also expect other users of proprietary wireless technologies to shift to IEEE 802.15.4 use due to lower costs and performance improvement.

Home automation allows people to control all kinds of automated system and device in their homes from virtually anywhere as long as these are Internet connected. With it, you can control all of your WPAN-connected devices from anywhere, normally via a remote control, a tablet, or a smartphone. You can even create macros to turn multiple devices on and off at once. You can, for instance, program all of the lights in your home to turn off when it's time for you to sleep. Or turn the lights on in your kitchen from your bedroom when you wake up in the middle of night. You can even dim the lights in your dining room during an intimate dinner. Or better yet, you can schedule when lights and other electronic devices should go on and off to simulate human presence in your home when you're actually on a trip. Home automation, if done properly and securely, can enable people to enjoy the highest quality of life.

6 http://en.wikipedia.org/wiki/IEEE_802.15.4; http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf; http://www.ieee802.org/15/pub/TG4.html

7 http://www.nist.gov/el/isd/ieee/ieee1451.cfm

# References


- http://cocoontech.com/portal/lists/android-home-automation-apps/details/6/346-MB---Remote-Control
- http://cocoontech.com/portal/lists/android-home-automation-apps/details/6/334-iMControl
- http://en.wikipedia.org/wiki/IEEE_802.15.4
- http://en.wikipedia.org/wiki/X10_(industry_standard)
- http://www.nist.gov/el/isd/ieee/ieee1451.cfm
- http://pages.cs.wisc.edu/~suman/courses/838/papers/zigbee.pdf
- http://standards.ieee.org/about/get/802/802.15.html
- http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf
- http://tulsagrad.ou.edu/samuel_cheng/tuesday_seminar/802.15.4%20Presentation.ppt
- http://www.arduino.cc/en/Main/ArduinoXbeeShield
- http://www.elechouse.com/elechouse/index.php?main_page=product_info&cPath=90_92&products_id=2169
- http://www.ieee802.org/15/pub/TG4.html
- http://www.ihometouch.com/
- http://www.sensor-networks.org/index.php?page=0823123150
- http://www.ti.com/product/cc2420

# What Is IEEE 802.15.4?

The IEEE 802.15.4 standard aims to provide support for the two lower Open Systems Interconnection (OSI) layers when implementing WPANs to enable cheap and low-speed communication between varying devices.[8] It primarily aims to develop a network all devices can communicate in at low cost while consuming less power.

IEEE 802.15.4 was developed with lower data rate, simpler connectivity, and more efficient battery power consumption in mind. It allows communication to occur in the 868–868.8MHz, 902–928MHz, or 2.400–2.4835GHz Industrial Scientific and Medical (ISM) bands. While any of the said bands can technically be used by IEEE 802.15.4-compliant devices, the 2.4GHz band is more popular as it is open to most of countries worldwide. 868MHz band use is specifically limited to European use while 902–928MHz band use is limited to the United States, Canada, and a few other countries and territories governed by Federal Communications Commission (FCC) regulations.

IEEE 802.15.4 specifically controls only the PHY and MAC layers. It allows compatible implementations to utilize different networking techniques and technologies. Many technologies that use this standard like X10, Z-Wave, and ZigBee have been developed to implement mesh and sensor networks in automated home appliances. Note, however, that apart from home automation, IEEE 802.15.4 is also used for a variety of applications, including industrial control and monitoring; public safety, including sensing and location determination in disaster sites; automotive sensing like tire pressure monitoring; and smart badges and tags.

8 http://en.wikipedia.org/wiki/Personal_area_network; http://standards.ieee.org/about/get/802/802.15.html


## TREND MICRO INCORPORATED

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.


## TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003

www.trendmicro.com


TREND MICRO™

Securing Your Journey to the Cloud