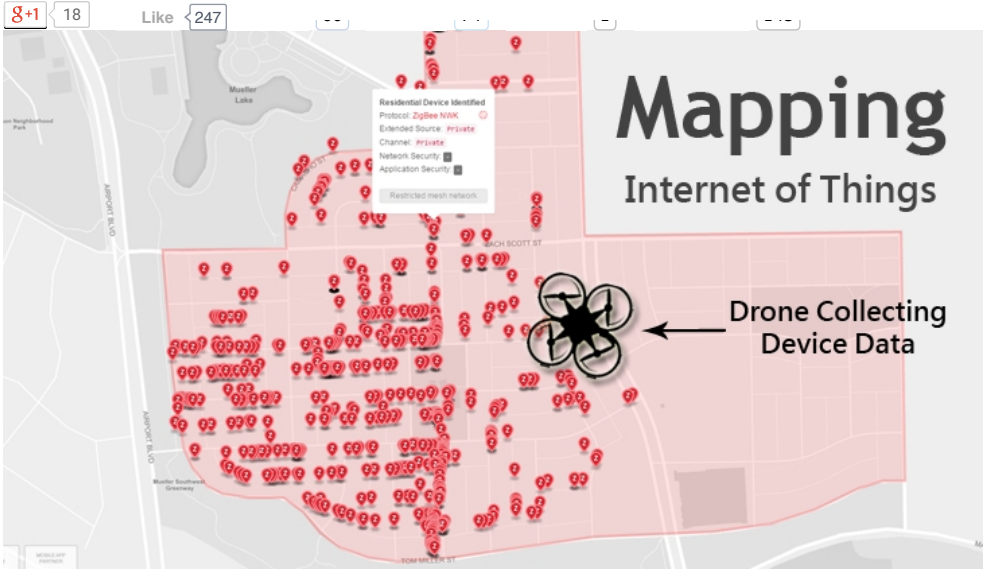
How Drones Can Find and Hack Internet-of-Things Devices From the Sky

Friday, August 07, 2015 Mohit Kumar



Security researchers have developed a *Flying Drone with a custom-made tracking tool* capable of sniffing out data from the devices connected to the Internet – better known as the Internet-of-things.

Under its **Internet of Things Map Project**, a team of security researchers at the Texas-based firm Praetorian wanted to create a searchable database that will be the Shodan search engine for SCADA devices.

Located More Than 1600+ Devices Using Drone

To make it possible, the researchers devised a drone with their custom built connected-device tracking appliance and flew it over Austin, Texas in real time.

During an 18 minute flight, the drone *found nearly 1,600 Internet-connected devices*, of which 453 IoT devices are made by Sony and 110 by Philips. You can see the full Austin map here.

How did They locate Internet of Things Devices?

The researchers located all *ZigBee-enabled smart devices* and networks and then started expanding their research.

*"When [IoT devices] communicated over a wireless protocol called **ZigBee**, this protocol is open at a network level. So when the devices start connecting, they send out beacon requests. We capture data based on this,"* says Paul West Jauregui, from Praetorian.

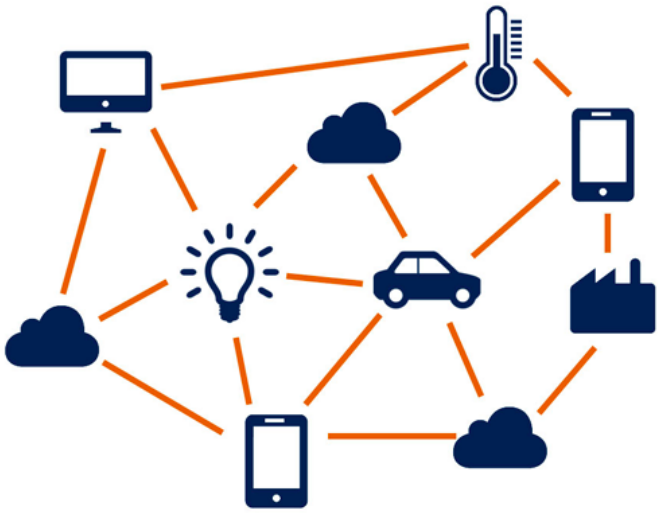
ZigBee is a *popular smart-home wireless communication standard* used by the majority of Internet of Things (IoT) devices today.

ZigBee protocol, which lets IoT devices talk to each other, is implemented by major vendors including Toshiba, Philips, Huawei, Sony, Siemens, Samsung, Motorola, and many more.

Exploiting 'ZigBee' to Hack Internet of Things Devices Remotely

Such drone experiments could be even worse if hackers were able to hijack smart-home and Internet-enabled appliances remotely...

⋯that's Evil! But it has been demonstrated by a Vienna-based team of security researchers at Black Hat security conference.



Tobias Zillner and Sebastian Strobl from 'Cognosec' have discovered some critical security flaws in ZigBee that could allow hackers to compromise ZigBee networks and take over control of all connected devices on a network, including door locks, alarm system and even controlling your light bulbs.

The vulnerability actually relies in the way ZigBee protocol handles the keys it uses to authenticate the IoT devices it adds to its mesh network, allowing hackers to sniff out exchange authenticate keys.

> *"Tests with light bulbs, temperature sensors, motion sensors and even door locks have shown that the vendors of the tested devices implemented [minimum features] required to be certified,"* says Zillner.

Even Worse:

The worse part pointed out by the researcher is that there is nothing users could do to make their

smart devices more secure, and since the flaw affects a broad range of devices, it's quite unclear how quickly vendors will come up with a fix.

Drone Hacking, Hacking Internet, Hacking News, Internet Of Things, Vulnerability, ZigBee Wireless Technology

ABOUT THE AUTHOR

Mohit Kumar

Founder and Editor-in-Chief of 'The Hacker News'. Cyber Security Analyst, Information Security Researcher, Developer and Part-Time Hacker.

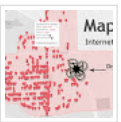
SUBSCRIBE FOR UPDATES

Want more Interesting News like this? Sign up here to receive the best of 'The Hacker News' delivered daily straight to your inbox.

Email address

Subscribe

LATEST STORIES


How Drones Can Find and Hack Internet-of-Things Devices From the Sky


"Certifi-Gate" Android Vulnerability Lets Hackers Take Complete Control of Your Device

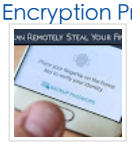

Windows Updates Can be Intercepted to Inject Malware into Corporate Networks


Warning! Update Mozilla Firefox to Patch Critical File Stealing Vulnerability


Self-Service Bank Passbook Printing Machines Leak Customers Financial Details


Microsoft Open-Sources Tool for Porting iOS Apps to Windows


Web Encryption Protocol That Even Quantum Computers Can't Crack


Hackers Can Remotely Steal Fingerprints From Android Phones

COMMENTS

Sadly, Windows 10 Is Stealing Your Bandwidth 'By Default' — Disable It Immediately

AntiVirus Firm BitDefender Hacked; Turns Out Stored Passwords Are UnEncrypted

Tip — Installing Windows 10? Fix 35+ Privacy Issues With Just One Click

Despite Issues, 6 Reasons Why Windows 10 is Best Windows Ever

Windows 10 Wi-Fi Sense Explained: Actual Security Threat You Need to Know

How to Hack Millions of Android Phones Using Stagefright Bug, Without Sending MMS

Thunderstrike 2: World's First Firmware Worm That Infects Mac Computers Without Detection

Hacker Finds How Easy Is to Steal Money Using Square Credit-Card Reader

Unpatched Mac OS X Zero-day Bug Allows Root Access Without Password

Web Encryption Protocol That Even Quantum Computers Can't Crack

About | THN Magazine | The Hackers Conference | Sitemap | Advertise on THN | Submit News | Privacy Policy | Contact