Hacking Everything
The Dark Side of the Internet of Things

Jeff Crume, CISSP-ISSAP
Distinguished Engineer
Master Inventor
IBM
crume@us.ibm.com
IoT: The Next Evolution In Computing

Growth

10B mobile phones by 2016; more than people on the planet (Source: Strategy Analytics*)

Employees

34% employees in 2012 are mobile (Source: IDC*)

Security

8X increase in security risk driven by proliferation of mobile data and devices

Mobile/Wireless/Cloud

85 billion mobile applications will be downloaded in 2012 (Source: IDC)

Mobile Applications

“Consumerisation of IT”

62% individual-liable (BYOD*) devices used for business, compared to 38% corporate-liable in 2012 (Source: IDC*)

Unified Communications (UC)

78% of multinational corporations plan to adopt mobile UC by 2015, including mobile video streaming and conferencing

Employees

34% employees in 2012 are mobile (Source: IDC*)

Growth

10B mobile phones by 2016; more than people on the planet (Source: Strategy Analytics*)

Web/Desktop

Employees

34% employees in 2012 are mobile (Source: IDC*)

Growth

10B mobile phones by 2016; more than people on the planet (Source: Strategy Analytics*)

Client/Server

Employees

34% employees in 2012 are mobile (Source: IDC*)

Growth

10B mobile phones by 2016; more than people on the planet (Source: Strategy Analytics*)

Host/Mainframe

Employees

34% employees in 2012 are mobile (Source: IDC*)

Growth

10B mobile phones by 2016; more than people on the planet (Source: Strategy Analytics*)
Problem Statement

IoT $\rightarrow$ everything is a computer

Computers can be hacked

$\therefore$ everything can be hacked
Vehicle Hacking
UConnect Strikes Again

“Fiat Chrysler said Friday it is voluntarily recalling 7,810 SUVs due to a software glitch that could make the vehicles vulnerable to remote control.”

http://www.pcworld.com/article/2980936/ fiat-chrysler-voluntarily-recalls-7810-suvs-over-software-issues.html#tk.nl_today
Researchers hack a Corvette's brakes via insurance black box

Researchers exploit a Web-connected insurance monitor to hijack a car using text messages.

by Artuan Goodwin
@antipoo
August 11, 2015

The list of ways to electronically hijack cars is growing thanks to devices used to monitor drivers’ roadway behavior.

Recently, we’ve seen a wave of devices vying for placement in your car’s onboard diagnostics port (known as OBD-II). These little plastic boxes promise to connect your car to the Web, help you boost your fuel economy and even lower insurance rates by reporting your driving habits wirelessly to your insurance company. But some of these little boxes could also be an Achilles’ heel that leaves their host cars vulnerable to hacking, warns a group of digital security researchers at the University of California at San Diego.

Connected OBD-II dongles like these could be the Achilles’ heel that leaves a car vulnerable to hacking.
Artuan Goodwin/CNET


#ITDEVCONNECTIONS | ITDEVCONNECTIONS.COM
“What freaked Volkswagen out was that the researchers accessed the transponder’s 96-bit secret key and then they were able to start a keyless car in half an hour.”
www.informationisbeautiful.net/visualizations/million-lines-of-code

#ITDEVCONNECTIONS | ITDEVCONNECTIONS.COM
“Security concerns have been raised after a fitness tracking firm showed the exercise routes of military personnel in bases around the world.

Online fitness tracker Strava has published a ‘heatmap’ showing the paths its users log as they run or cycle.

It appears to show the structure of foreign military bases in countries including Syria and Afghanistan as soldiers move around them.”

Cracked in two minutes

“... hung an ‘Anrai’-branded DVR on the net, with default configuration and password ‘xc3511’ unchanged, power cycled it every five minutes and watched for 45 hours and 42 minutes.

The results of that effort were scary: 1,254 logins with the default password. Or one every two minutes.”

https://www.theregister.co.uk/2017/08/29/sans_mirai_dvr_research/
Rise of the Machines

The source code that powers the “Internet of Things” (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released, virtually guaranteeing that the Internet will soon be flooded with attacks from many new botnets powered by insecure routers, IP cameras, digital video recorders and other easily hackable devices.
"Like any other IoT device, these robot vacuum cleaners could be marshaled into a botnet for DDoS attacks," said Leigh-Anne Galloway, Cyber Security Resilience lead at Positive Technologies.

"But that's not even the worst-case scenario, at least for owners," she adds. "Since the vacuum has Wi-Fi, a webcam with night vision, and smartphone-controlled navigation, an attacker could secretly spy on the owner."

“The main security problem is that users aren't changing the device's default passwords,” Xiongmai said in a Chinese-language statement posted online.

“The problem is the patching ecosystem requires a certain price point of device to make it viable. We are dropping below that price.” – Bruce Schneier

source: PCWorld.com
Hacking the friendly skies

A team of government, industry and academic officials successfully demonstrated that a commercial aircraft could be remotely hacked in a non-laboratory setting …

“We got the airplane on Sept. 19, 2016. Two days later, I was successful in accomplishing a remote, non-cooperative, penetration,” said Robert Hickey, aviation program manager within the Cyber Security Division of the DHS Science and Technology (S&T) Directorate.

The cost to change one line of code on a piece of avionics equipment is $1 million, and it takes a year to implement. For Southwest Airlines, whose fleet is based on Boeing’s 737, it would “bankrupt” them if a cyber vulnerability was specific to systems on board 737s, he said, adding that other airlines that fly 737s would also see their earnings hurt. Hickey said newer models of 737s and other aircraft, like Boeing’s 787 and the Airbus Group A350, have been designed with security in mind, but that legacy aircraft, which make up more than 90% of the commercial planes in the sky, don’t have these protections.

“… found the more serious vulnerabilities in several models of pumps made by the same manufacturer, which would allow a hacker to surreptitiously and remotely change the amount of drugs administered to a patient.”

http://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/
Heart Hacking

St. Jude Medical is facing fresh allegations its heart implant devices are vulnerable to cyberattacks. The claims were introduced by the defense as part of St. Jude's defamation lawsuit against short seller Muddy Waters and security firm MedSec.

In a legal filing submitted Monday, experts hired by Muddy Waters and MedSec back their claims that St. Jude's cardiac implants are vulnerable to cyberattacks. The report is from independent security firm Bishop Fox, whose testimony was presented as evidence to the federal court in Minnesota hearing the case.

https://threatpost.com/st-jude-faces-new-claim-heart-implants-are-hackable/121504/
Not so “smart” lock

- Set up iPad Pro in living room as central, voice-controlled HomeKit hub (à la Alexa)
- Better to set voice commands to lock only
- Alexa does this but Siri does not

https://www.reddit.com/r/technology/comments/532gmg/my_neighbor_just_let_himself_into_my_locked_house/
Hacking your TV, smartwatch, phone, etc.

But the operating system [Tizen] is riddled with serious security vulnerabilities that make it easy for a hacker to take control of Tizen-powered devices, according to Israeli researcher Amihai Neiderman.

"It may be the worst code I've ever seen," he told Motherboard in advance of a talk about his research that he is scheduled to deliver at Kaspersky Lab's Security Analyst Summit on the island of St. Maarten on Monday. "Everything you can do wrong there, they do it. You can see that nobody with any understanding of security looked at this code or wrote it."

Fridge-in-the-middle

“Whilst the fridge implements SSL, it FAILS to validate SSL certificates, thereby enabling man-in-the-middle attacks against most connections. This includes those made to Google's servers to download Gmail calendar information for the on-screen display.

So, MITM the victim’s fridge from next door, or on the road outside and you can potentially steal their Google credentials.”

http://www.pentestpartners.com/blog/hacking-defcon-23s-iot-village-samsung-fridge/
Phishing Fishing Attack

IoT Hall of Shame

Welcome to the IoT Hall-of-Shame

With the rise of internet enabled devices in the Internet of Things or IoT the need for software security is becoming even more important. Unfortunately many device makers seem to put security on the back burner or not even understand the basics of cybersecurity. Some call it the Internet of Evil Things.

https://codecurmudgeon.com/wp/iot-hall-shame/

#ITDEVCONNECTIONS  |  ITDEVCONNECTIONS.COM
IoT Security risks to address

1. Large number of new network endpoints (devices)
2. Mobility and Vulnerability of devices
3. Privacy and Security of data generated (by devices)
4. Compromised devices used to launch attack on IT
5. Compromised IT used to launch attack on devices
6. Compromised Network access points
Personal IoT Security

1. Many smart things support Wi-Fi so that you don’t have to plug them into your smartphone or computer every time you want to use them. If your home Wi-Fi router allows you to create separate guest networks to keep untrusted visitors off your regular network, make a special guest network for your “things” and connect them there.

2. Many devices, such as video cameras, try to talk to your router to open up inbound holes so they can accept connections from outside. This makes it easier to access them from the internet, but it also exposes your devices to the rest of the world. Turn off Universal Plug and Play (UPnP) on your router, and on your IoT devices if possible, to prevent this exposure. Don’t assume that “no one will notice” when you hook up your device for the first time. There are specialised search engines that go out of their way to locate and index online devices, whether you wanted them to be found or not.

3. Keep the firmware up to date on all of your IoT devices – patching is just as important as it is on your PC. It can be time consuming to figure out whether updates are available, but why not make a habit of checking the manufacturer’s website twice a year? Treat it like changing your smoke detector batteries: a small price to pay for safety and security.

https://nakedsecurity.sophos.com/2016/03/07/7-tips-for-securing-the-internet-of-things/
Personal IoT Security

4. **Choose passwords carefully and write them down if needed.** Complexity is important, but so is uniqueness. Many IoT devices have been found to have bugs that let attackers trick them into leaking security information, such as giving away your Wi-Fi password. Remember: one device, one password.

5. **Favor devices that can work without the cloud.** IoT “things” that require a cloud service are often less secure, and potentially give way more information, than those you can control entirely from within your home. Read the packaging carefully to determine whether permanent internet access is needed for the device to function. If it’s “all-or-nothing,” then you can’t try out the device on your own network first.

6. **Only network devices as much as you need to.** If all you want from your TV is to watch broadcast television, you don’t need to connect it to the network at all. If you only want to control it or stream to it from your home network, it doesn’t need access to or from the outside. Eliminate unnecessary internet connections when possible.

7. **Don’t take your IoT devices to work or connect them to your employer’s network without permission from IT.** Insecure devices could be used by attackers as a foothold into the organisation, and used to assist with data stealing and illicit surveillance. You could put your company and your job at risk.

https://nakedsecurity.sophos.com/2016/03/07/7-tips-for-securing-the-internet-of-things/
Additional Reading

https://stage.securityintelligence.com/media/ibm-x-force-research-weaponizing-the-internet-of-things/
IoT Security Vulnerability Testing

https://www.ibm.com/security/services/penetration-testing/

#ITDEVCONNECTIONS | ITDEVCONNECTIONS.COM
Thank You!

Jeff Crume, CISSP-ISSAP
Distinguished Engineer
Master Inventor
IBM
crume@us.ibm.com