

Exploiting Smart Devices

A PRIMER ON IOT ATTACKS



Agenda

EXECUTIVE OUTBRIEF

Introduction/Background

- What is the Internet of Things?

The New Wireless

- ZigBee, Z-Wave, Bluetooth
- Demo

Exploiting “Smart” Devices

- Organization
- Approaches

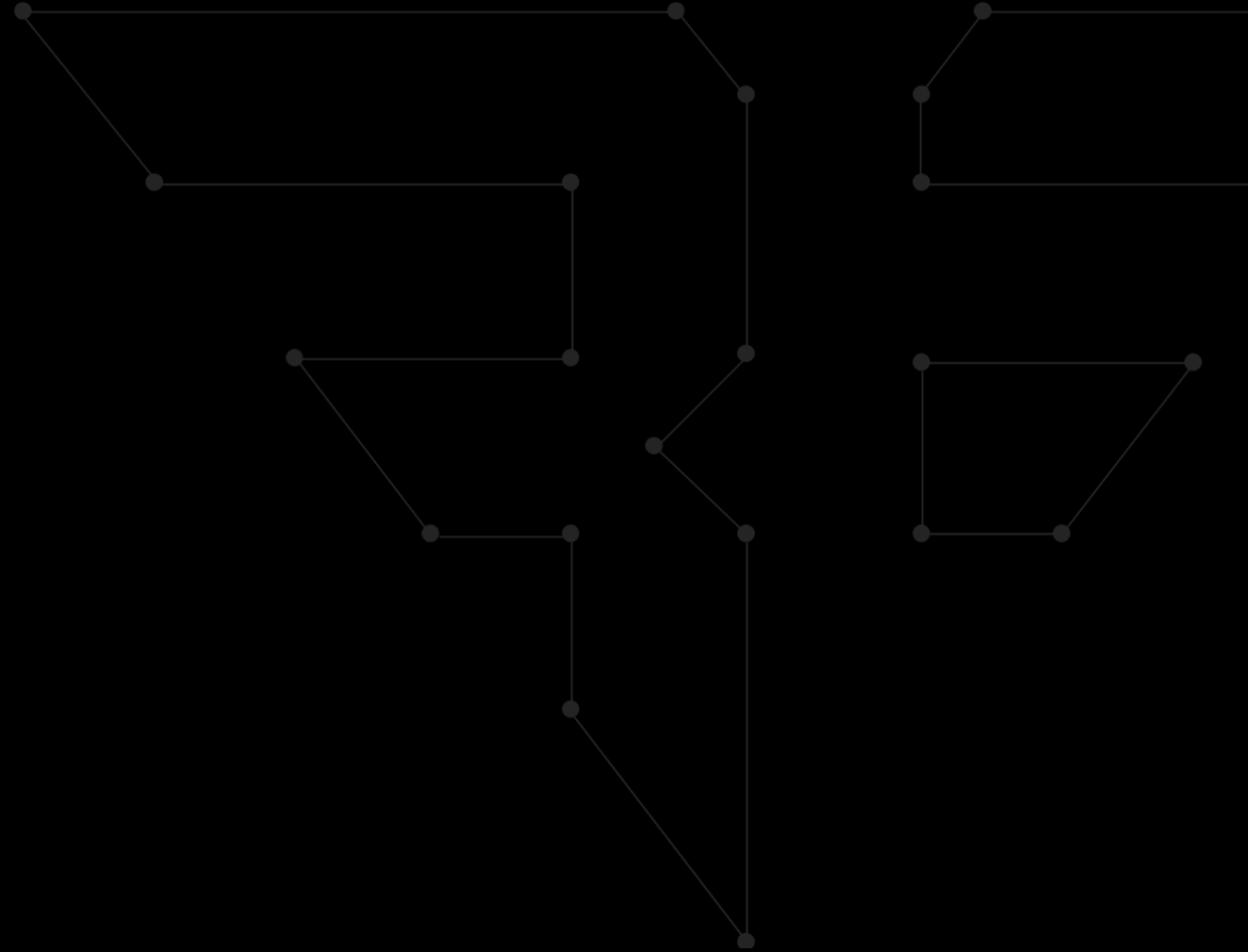
Going the Distance

- IoT hacking in the news
- Bonus demo
- Where to go from here

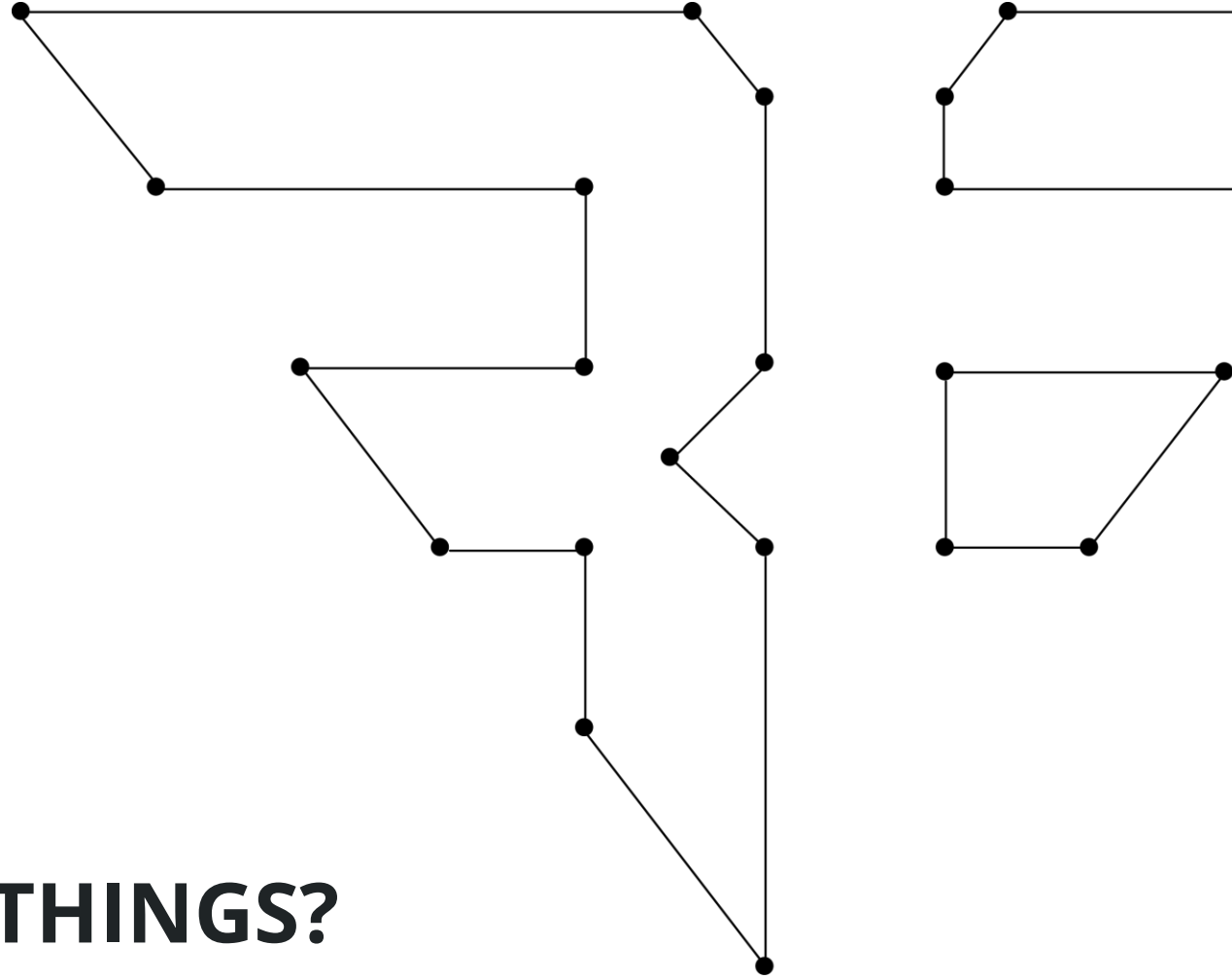


INTRODUCTION

GETTING UP TO SPEED



WHAT IS THE INTERNET OF THINGS?



Everything is connected

SMART HOME

IRL = URL



Everything is connected

FRIDGE



SHOPPING LIST



Everything is connected

HEALTH MONITORS

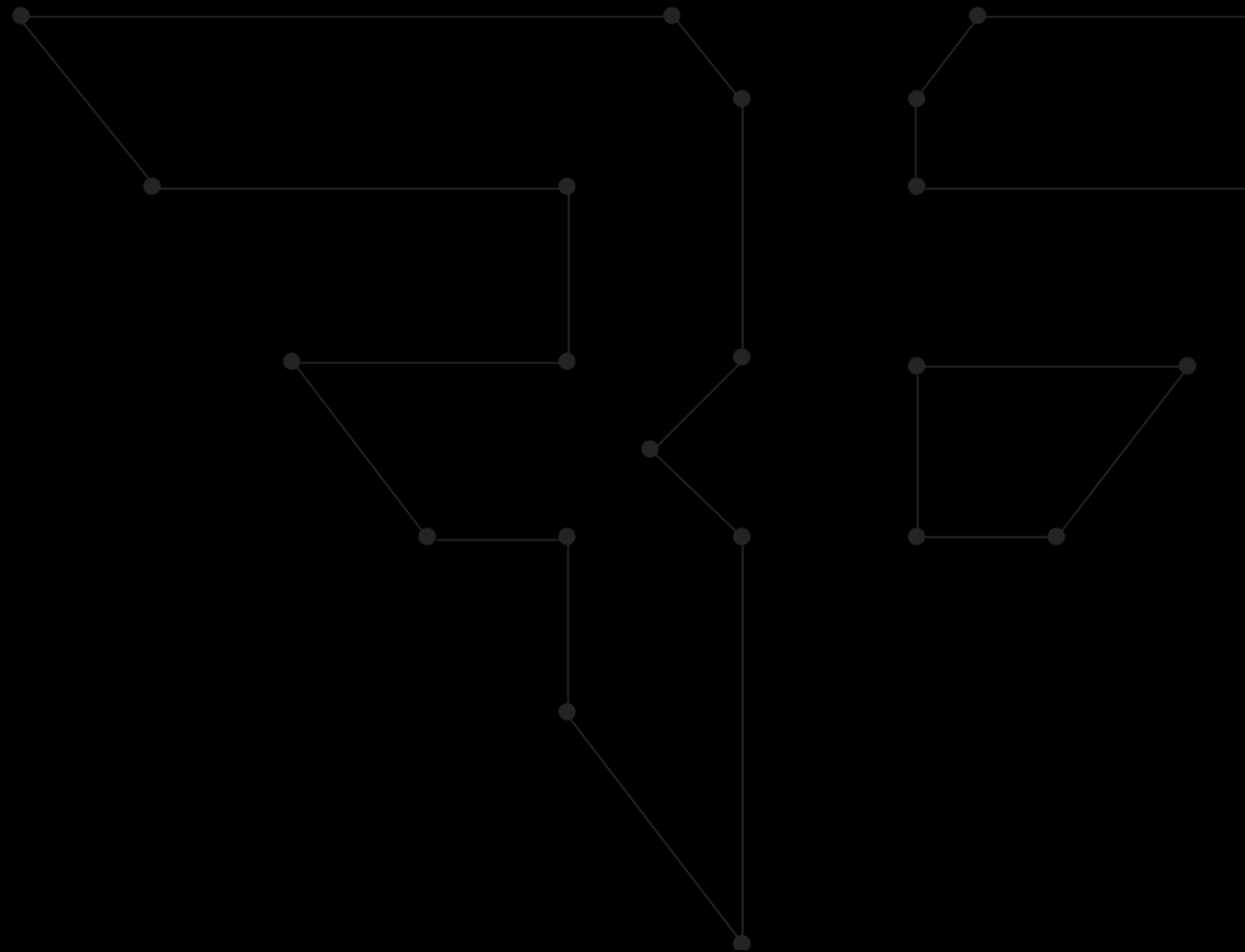


Everything is connected

EVERYTHING ... EXCEPT SECURITY

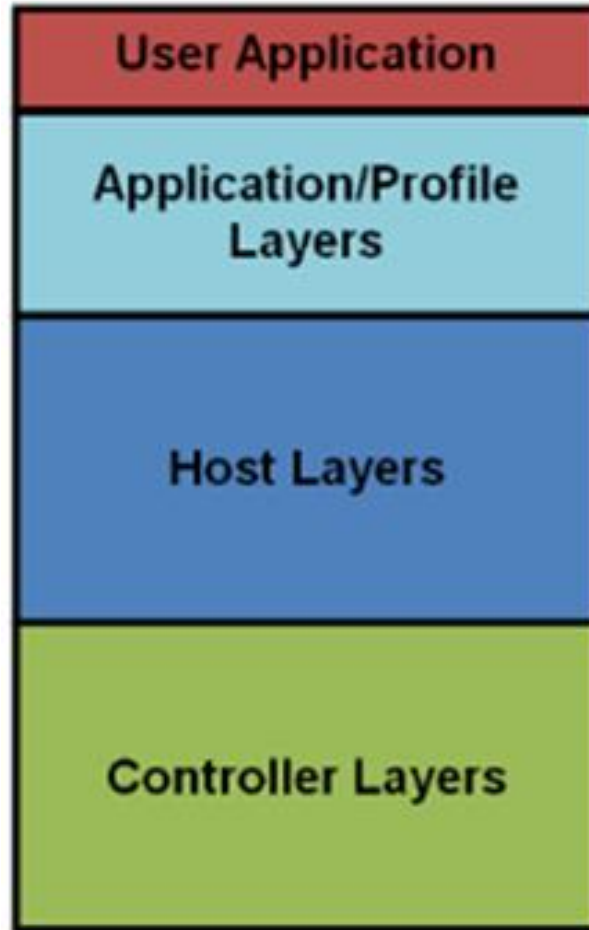


THE NEW WIRELESS

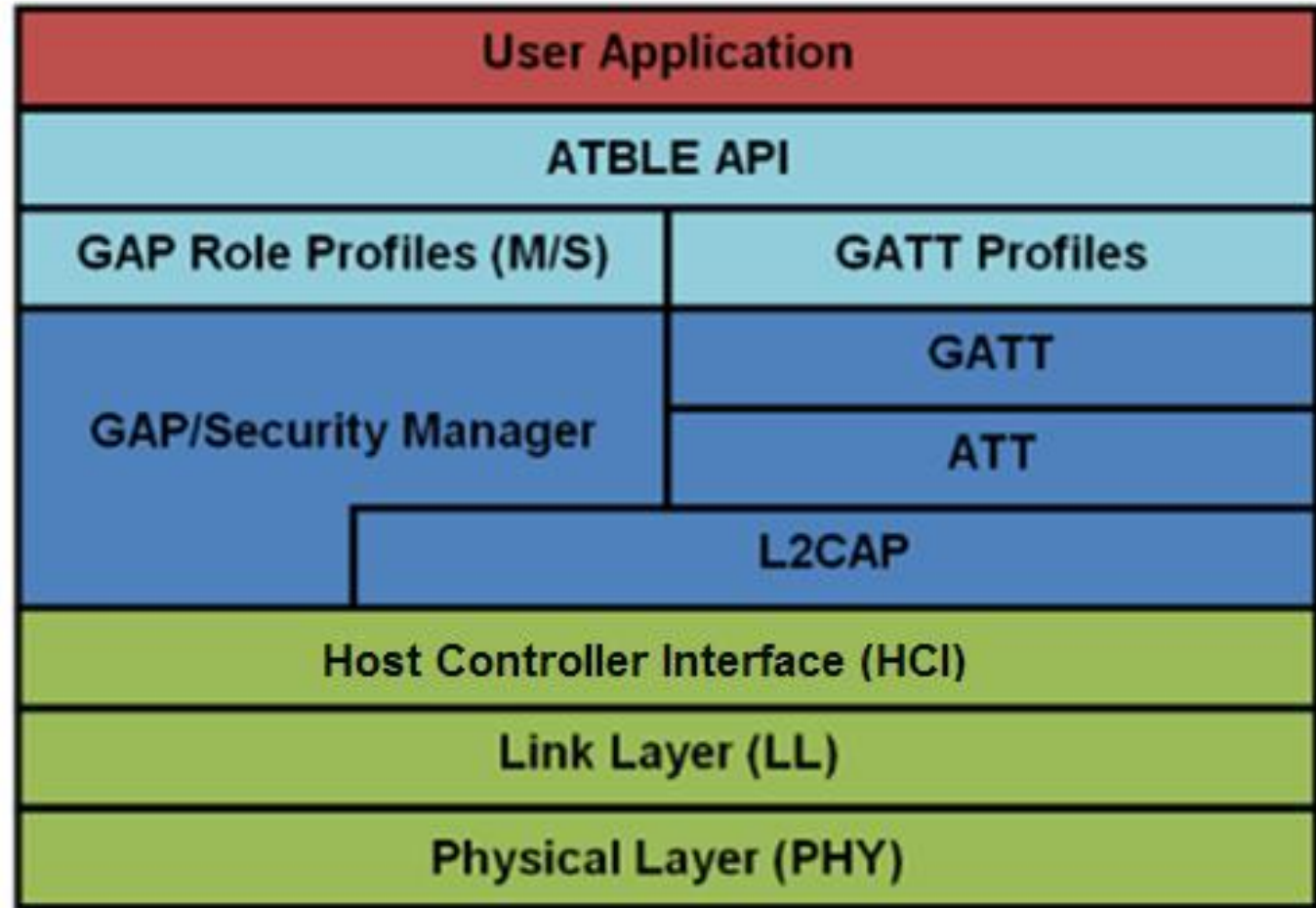


Bluetooth 4.0 /BTLE

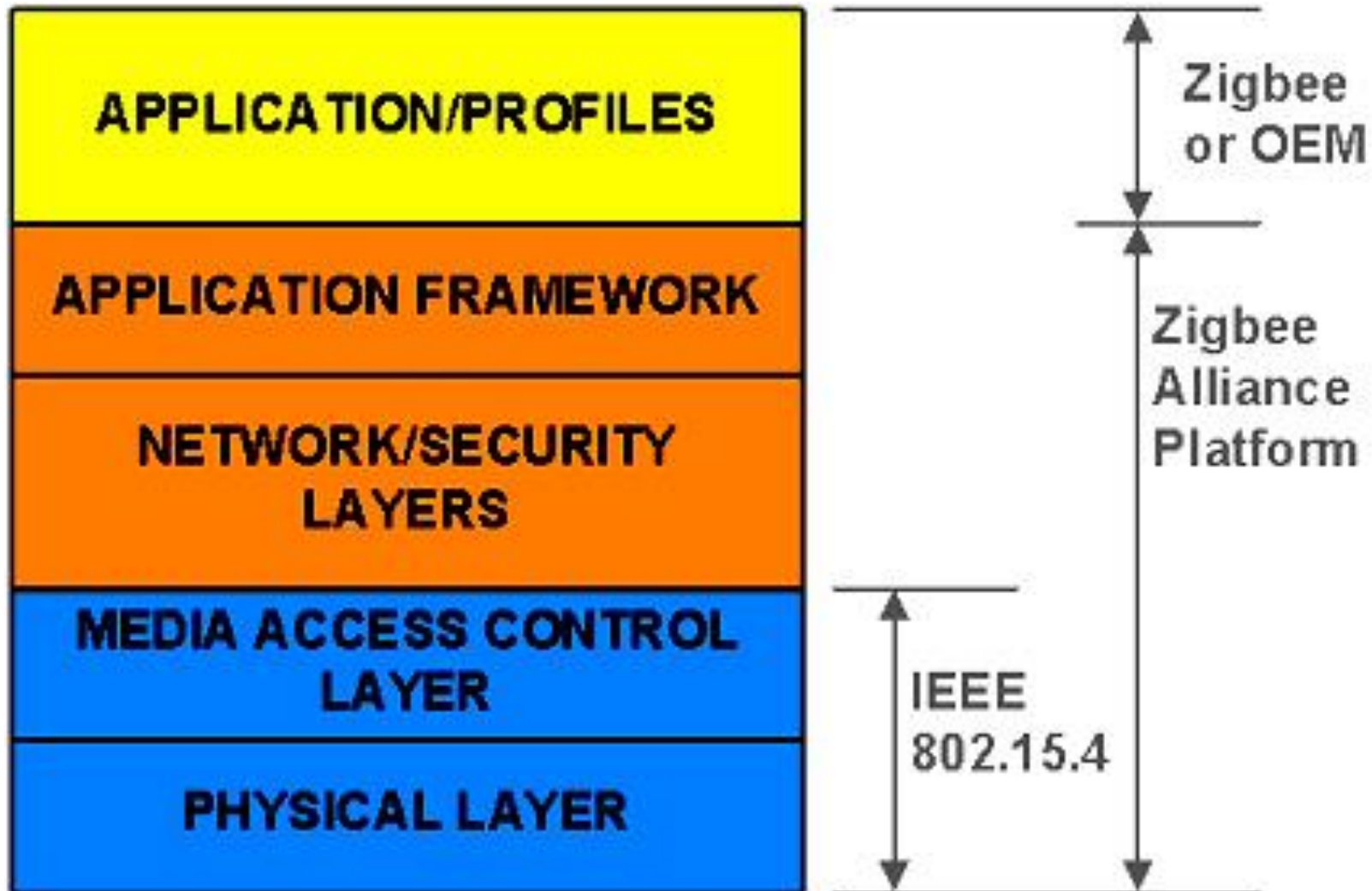
Simplified Stack



Detailed Stack

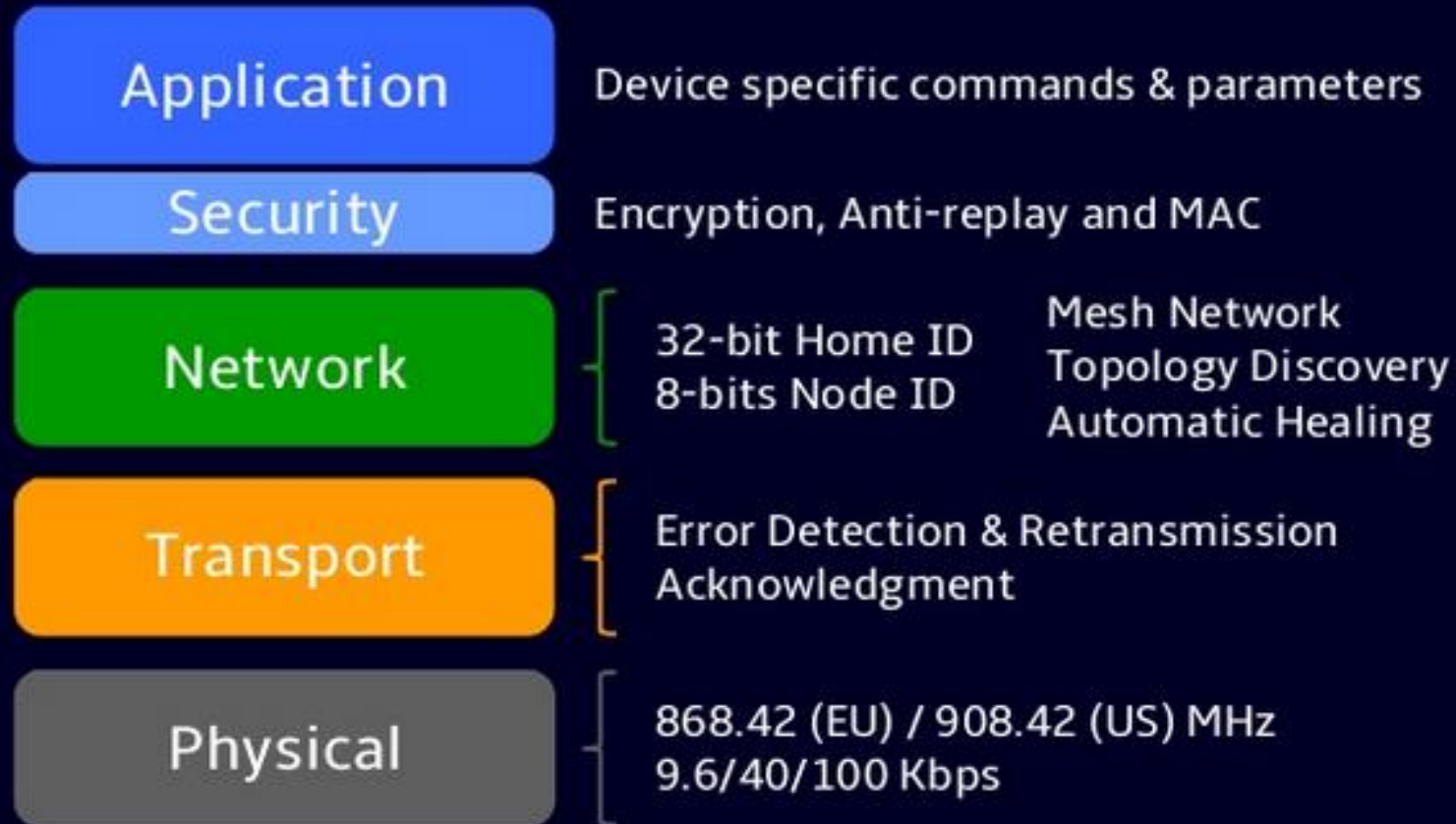


ZigBee



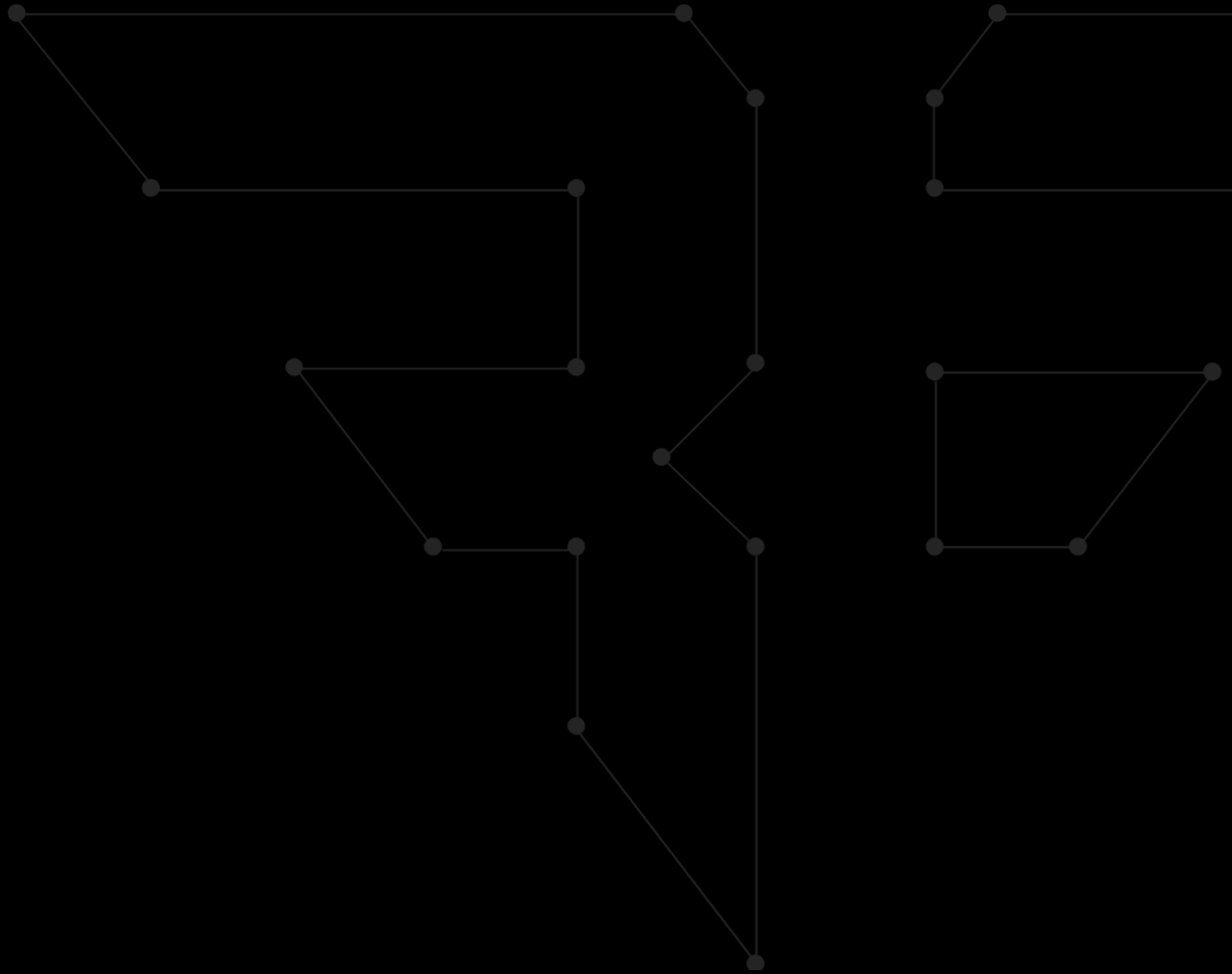
Z-Wave

Z-Wave Protocol Stack



Name	Bluetooth Classic	Bluetooth 4.0 Low Energy (BLE)	ZigBee	Wi-Fi
IEEE Standard	802.15.1	802.15.1	802.15.4	802.11 (a, b, g, n)
Frequency (GHz)	2.4	2.4	0.868, 0.915, 2.4	2.4 and 5
Maximum raw bit rate (Mbps)	1-3	1	0.250	11 (b), 54 (g), 600 (n)
Typical data throughput (Mbps)	0.7-2.1	0.27	0.2	7 (b), 25 (g), 150 (n)
Maximum (Outdoor) Range (Meters)	10 (class 2), 100 (class 1)	50	10-100	100-250
Relative Power Consumption	Medium	Very low	Very low	High
Example Battery Life	Days	Months to years	Months to years	Hours
Network Size	7	Undefined	64,000+	255



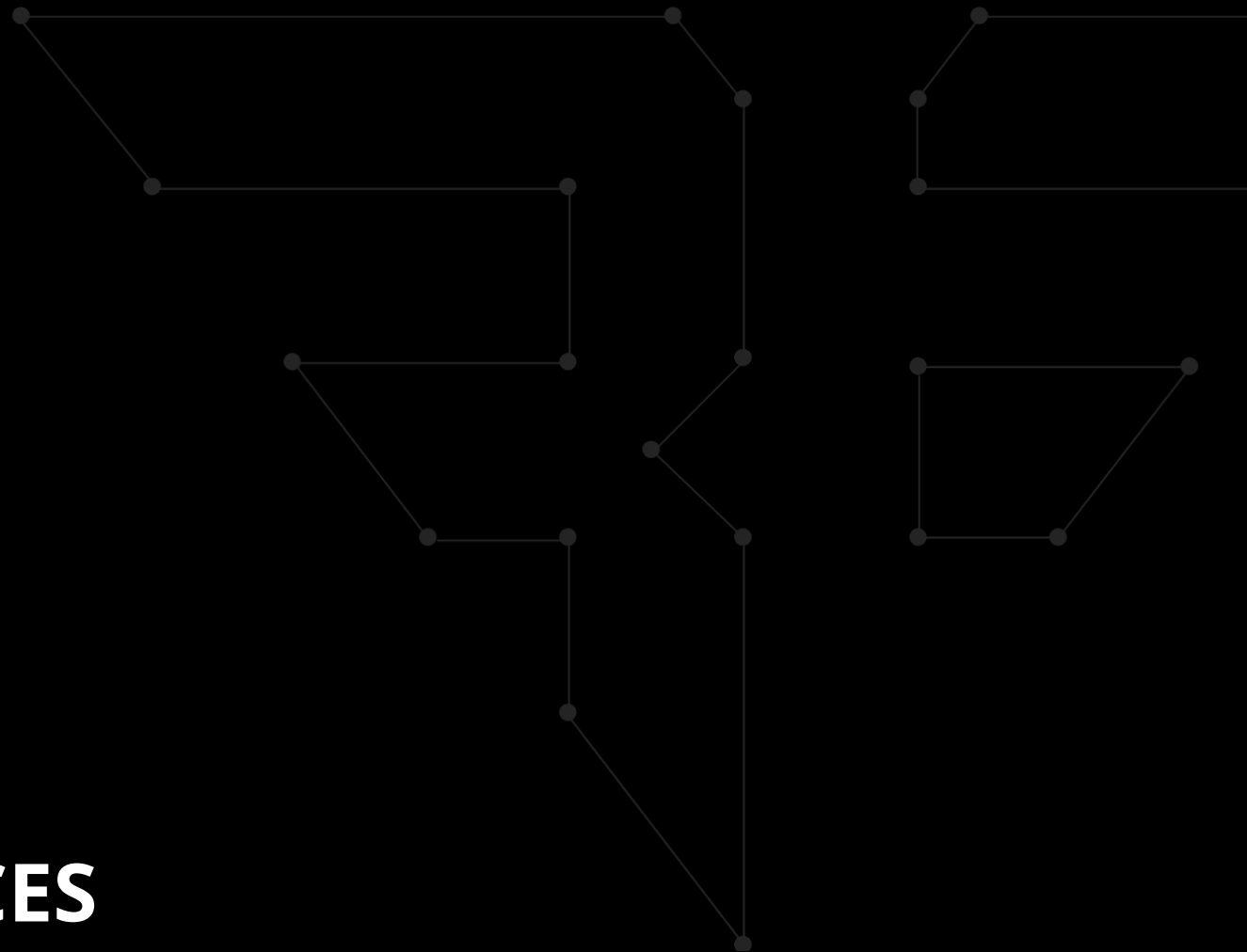


ILLUSTRATIVE FOOTAGE

A VIDEO FOR YOUR ENJOYMENT



EXPLOITING SMART DEVICES



Identification

WHOAMI

Wi-Fi/Physical Network

- Networking protocols
- Connect to a test network
- Inspect DNS requests
- Proxy requests

BLE/ZigBee/Z-Wave

- Pairing
- Encryption



Tools

MUCH TOOLS

ZigBee

- KillerBee Framework - <https://github.com/riverloopsec/killerbee>
- RaspBee - <https://www.dresden-elektronik.de/funktechnik/solutions/wireless-light-control/rasabee/>

Z-Wave

- KillerZee - <https://github.com/joswright/killerzee/>
- Z-Force - <https://code.google.com/archive/p/z-force/>

Bluetooth LE

- Ubertooth One - <http://ubertooth.sourceforge.net/hardware/one/>
- GATTacker - <https://github.com/securing/gattacker>

Tools

MORE TOOLS

Logic Analyzer

- Saleae Logic Analyzer- <https://www.saleae.com/>

JTAGs

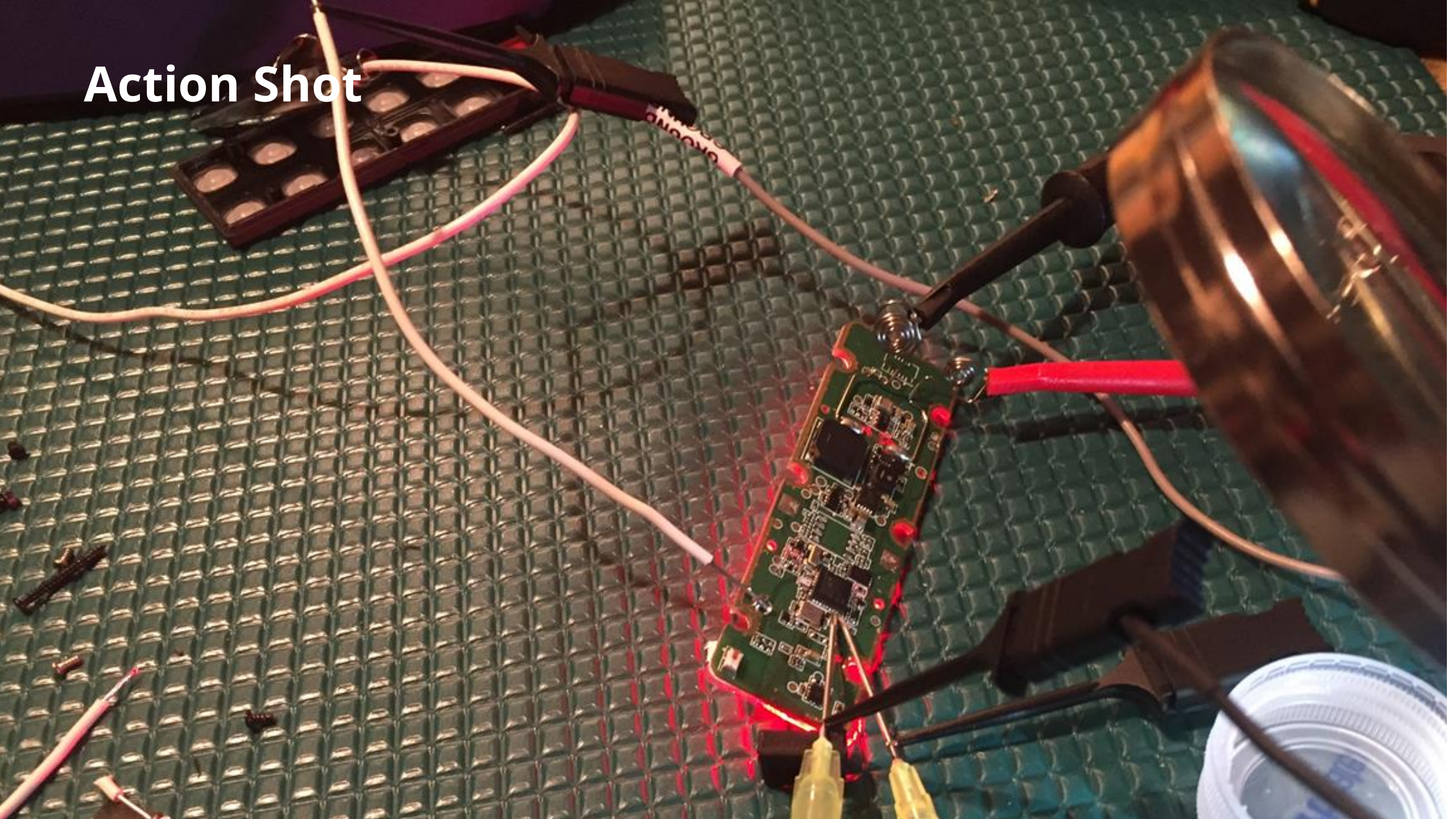
- JTagulator- <http://www.grandideastudio.com/jtagulator/>

Software Defined Radios (SDR)

- AirSpy SDR- <http://airspy.com/>



Action Shot

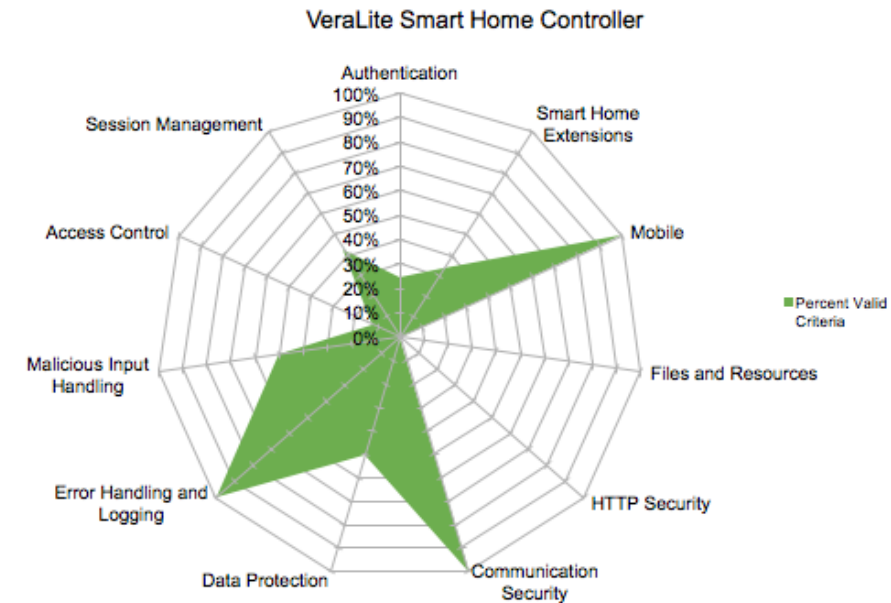


Organization

DETAILS MATTER

Requirements

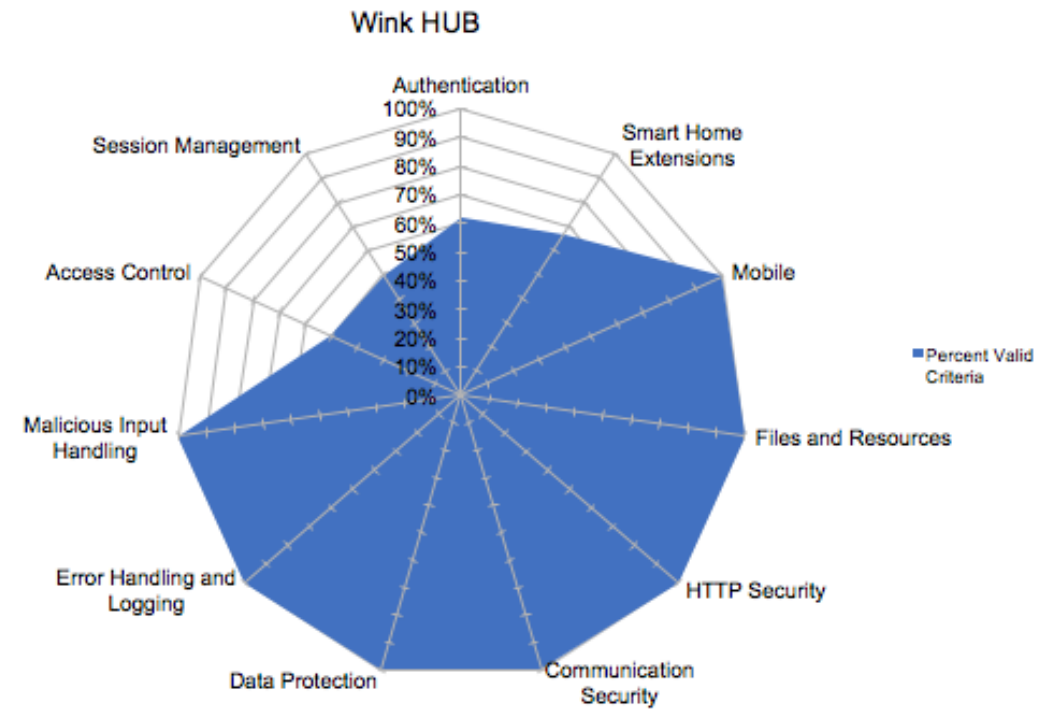
#	Description	1	2	3
2.1	Verify all pages and resources by default require authentication except those specifically intended to be public (Principle of complete mediation).	✓	✓	✓
2.2	Verify that all password fields do not echo the user's password when it is entered.	✓	✓	✓
2.4	Verify all authentication controls are enforced on the server side.	✓	✓	✓
2.6	Verify all authentication controls fail securely to ensure attackers cannot log in.	✓	✓	✓
2.7	Verify password entry fields allow, or encourage, the use of passphrases, and do not prevent long passphrases/highly complex passwords being entered.	✓	✓	✓



Organization

DETAILS MATTER

Category	Requirement Number	ASVS Level	Verification Requirement	Valid	Comment	Tool Used	Date Completed	Notes
Communications Channel	CC.1	3	Verify each communications channel used by the device implements the currently accepted strongest encryption available. For example: Wi-Fi should be secured using WPA2 and AES encryption, Z-Wave should use secure node authentication, Bluetooth 2.1+ should use security mode 4 with 3 as a fallback, Bluetooth Smart should use security mode 1 level 3, and ZigBee should use the encryption security service.	Valid	WiFi supports WPA2 encryption with AES. HTTP uses TLS 1.2 with AES_128_GCM and uses ECDHE_RSA for key exchange. ZigBee is using encryption, but I have no way of telling what type of encryption.	SSLScan, Manual testing, killerbee framework with the RZUSBSTICK	4/24/15	Unable to test Z-Wave as no working sniffing device was available. No compatible Bluetooth devices available.
	CC.2	3	Verify each communications channel used by the device implements some type of encryption.	Valid	HTTP is using SSL/TLS. WiFi is using WPA2. ZigBee uses encryption.	Burp Suite, Manual testing, killerbee framework	4/24/15	Unable to test Z-Wave as no working sniffing device was available. No compatible Bluetooth devices available.
	CC.3	3	Verify that previously paired devices authenticate each other upon reconnecting.	Not Applicable	Unable to test with ZigBee without a channel hopping device and updated firmware for the RZUSBSTICK	killerbee framework	4/28/15	Unable to test Z-Wave as no working sniffing device was available. No Bluetooth devices available.
	CC.4	3	Verify that no services are listening on undocumented ports.	Valid	Nmap scan report for 192.168.246.4 Host is up (0.00013s latency). Not shown: 65534 closed ports (nmap -sT 192.168.246.4) Valid for Bluetooth, ZigBee	NMAP	4/24/15	No documentation to go off of, but the only services are one on port 80.
	CC.5	3	Verify the device is undetectable with regard to wireless protocol pairing except as needed for pairing.	Valid		Android phone	4/24/15	Unable to test Z-Wave as no working sniffing device was available.
	CC.6	3	Verify that fallback settings for any protocol are at least as secure as default settings to prevent downgrade attacks.	Non-valid	Still accepts RC4 suite. Unsure how to test this using ZigBee and the killerbee framework	SSLScan	4/24/15	Unable to test Z-Wave as no working sniffing device was available. No compatible Bluetooth devices available.
Data Backup/Restore	DB.1	3	Verify that a user can backup and retain a copy of the device configuration.	Non-valid	No observable way to make a backup of the device configuration.	Manual testing, Android emulator.	4/24/15	It is possible that the company is backing up the device configuration automatically, but nothing is communicated to the user. Also, if this is the case, there is still no way to restore to a previous version.
	DB.2	3	Verify that any credentials stored in backups are encrypted.	Not Applicable	No observable way to make a backup of the device configuration.		4/24/15	
	DB.3	3	Verify that backups are encrypted and protected with a passphrase or key.	Not Applicable	No observable way to make a backup of the device configuration.		4/24/15	
	DB.4	3	Verify that a user can restore a previously backed up configuration.	Not Applicable				
	DB.5	3	Verify that a user can reset the device to factory defaults, either via a hardware button or through software.	Non-valid	No observable way to perform a factory reset.	Manual testing, Android emulator.	4/24/15	When the SSL certificate expired, no factory reset was possible. I had to use their DNS resolvers which, I assume, backdated the time and thereby allowed them to load a new, valid SSL certificate.
Updating/Patching	UP.1	3	Verify that there is a secure method to update or patch the system. This may be in the form of user-initiated update functionality protected by authentication, or automatic updates over a secure channel such as HTTPS.	Valid	The hub checks for updates automatically. They are delivered over SSL, which was confirmed by their certificate expiration problem.	Manual testing, Android emulator.	4/24/15	
	UP.2	3	Verify that patches or updates are integrity-checked (for example with a cryptographic checksum) and delivered over a secure channel.	Not Applicable				No way to check this with my current level of access.
	UP.3	3	For patches delivered using HTTPS, verify that the application uses SSL pinning.	Valid	The application does use SSL pinning, as it was necessary to bypass this to observe traffic.	Burp Suite, Android emulator	4/24/15	
	UP.4	3	Verify that patches or updates are cryptographically signed and verified before being applied. Signature and verification should be done with a public/private key pair to mitigate the risk of key extraction if a symmetric key were used.	Not Applicable				No way to check this with my current level of access.



Typical issues

GET USED TO IT

- **Authentication**
- **Session Management**
- **Access Control**
- **Malicious Input Handling**
- **Error Handling and Logging**
- **Data Protection**
- **Communication Security**
- **Cryptography**
- **Business Logic**

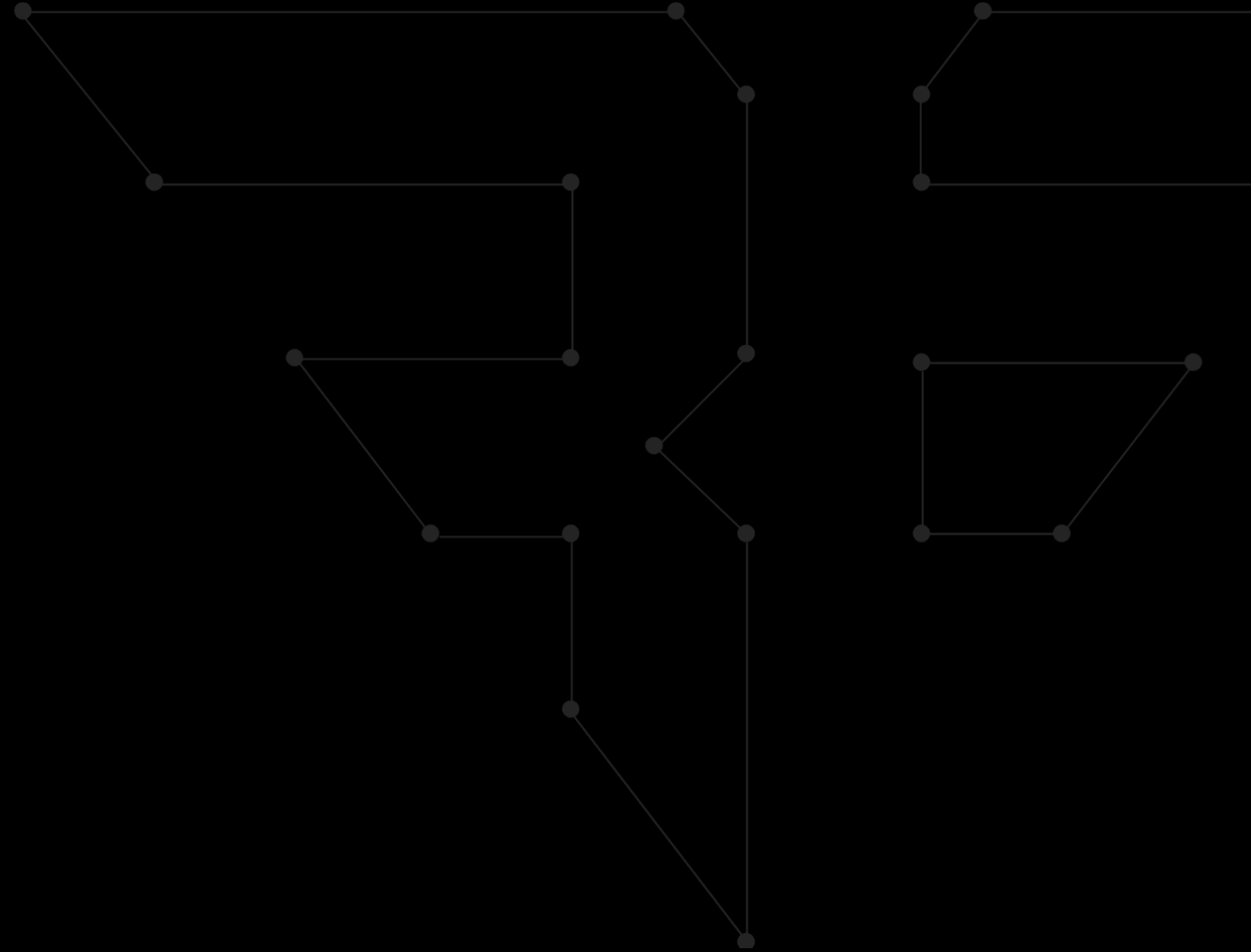


Tailoring Attacks

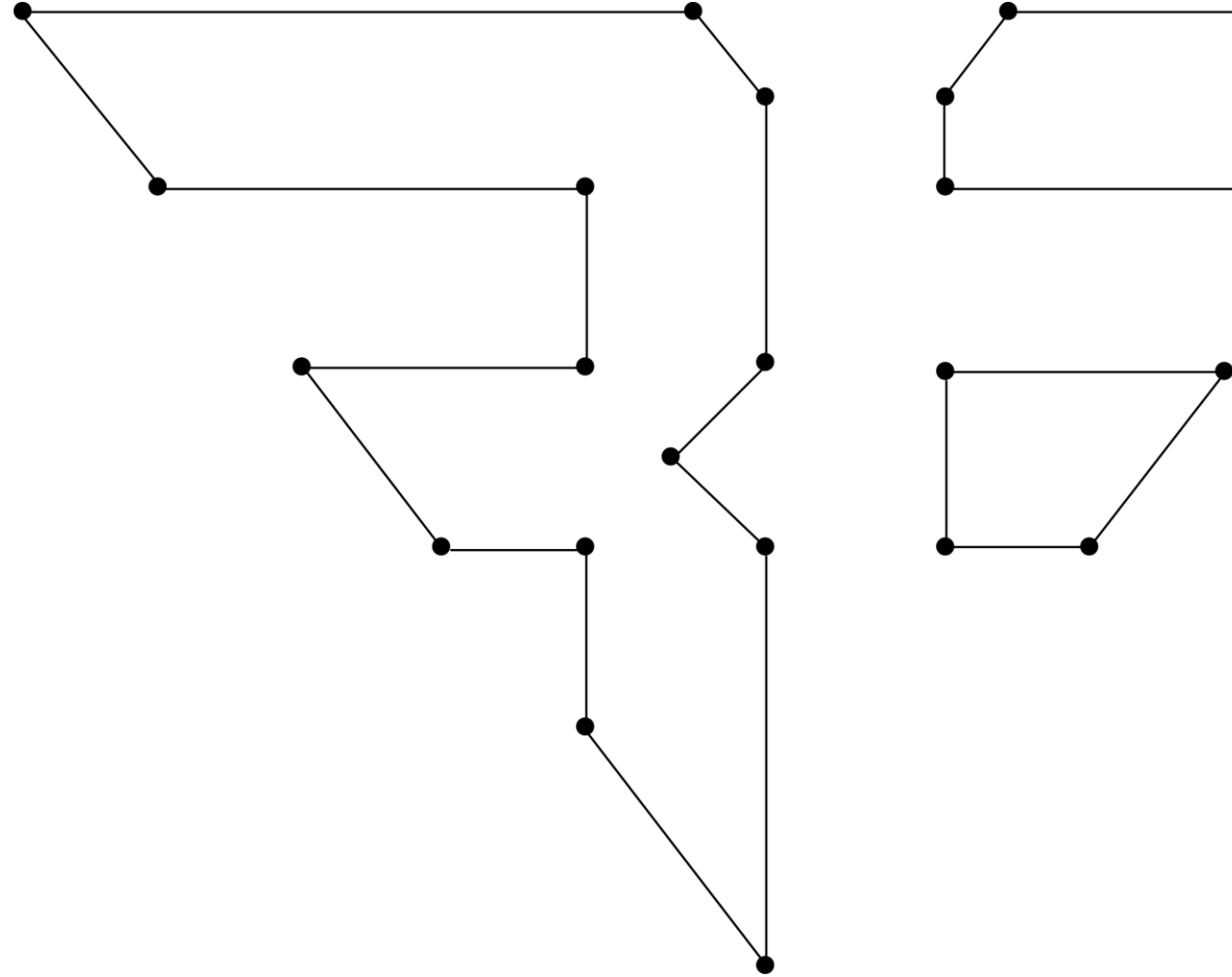


GOING THE DISTANCE

WHAT DOES IT ALL MEAN?



IN THE NEWS



Twitter Feed Webcams

#CAUGHTONNESTCAM


nest Nest Netherlands  @NestNL · Sep 17

De eerste stapjes, #caughtonNestCam.
Heb jij onbetaalbare momenten vastgelegd met je Nest Cam?



GIF 

   3 

Home About  Have an account? Log in

#caughtonnestcam


Top Live News Photos Videos More options

New to Twitter?
Sign up now to get your own personalized timeline!
[Sign up](#)

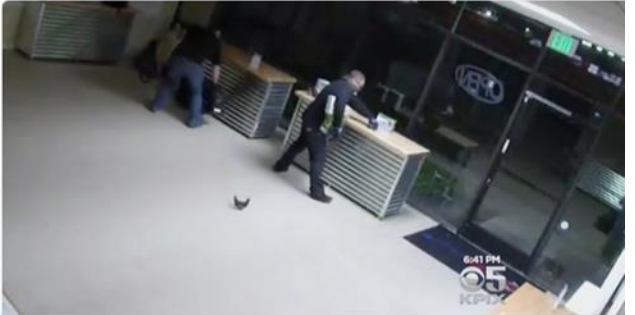
Trends

- #BeersWith Promoted by Let's Grab A Beer
- #MarsAnnouncement
- #CamsOldPhotos
- #UNGA
- #wakeupjames
- #DuragHistoryWeek
- George Zimmerman
- Ronnie Pickering
- August Alsina
- Arctic
- #mondaymotivation





© 2015 Twitter About Help Terms Privacy Cookies Ads info


nest Nest  @nest · Sep 23

Drone theft? Drone theft. Santa Clara drone store burglary
#caughtonNestCam: sanfrancisco.cbslocal.com/2015/09/14/dro...



Santa Clara Drone Store Burglary Caught On Camera
A break-in at a drone store in the South Bay was caught on camera, and this isn't the first time it's happened. At least three drone stores up and...
sanfrancisco.cbslocal.com

  8  8 

 **funnypranks4u** @funnypranks4you · Sep 22

Baby Webcams

#CAUGHTONNESTCAM



Ashley Carman, Reporter

[Follow @ashleyrcarman](#)

February 03, 2015

Hacker commandeers baby monitor, terrifies nanny

Share this content:



A Houston nanny got an IT security wake-up call this past week when an anonymous voice came through the baby monitor of the child she was watching.

A hacker took over the internet-connected device to say to the nanny, Ashley Stanley: "That's a really pooppy diaper."

He then went on to warn Stanley to "password protect" her camera. The nanny told [a local news station](#) she thought it was the child's parents playing a joke on her, but that turned out not to be the case.

The baby monitor maker, Foscam, [had a similar incident in April](#) and now provides information on how to keep the monitors secure.

Topping the list is the need for parents to change the monitors' default username and password. Newer devices require users to do so, but older versions might require a firmware upgrade.

Samsung smartTVs don't encrypt voice and text data

February 22, 2015 By Pierluigi Paganini



Samsung smartTV send unencrypted voice recognition data and text information across the Internet without encrypt it, allowing hackers to capture them.

A few days ago I was one of the first to publish the news about the [Samsung privacy policy](#) that reports smartTV are sending user voice data to third parties.

“

*“Samsung SmartTV transmits data to a third party, be aware that if your spoken words include personal or other sensitive information.”
I wrote in my previous post.*

Vehicle Attacks

GONE IN 60 SECONDS

Chrysler just launched the first-ever hacking recall for cars

1.9k
SHARES

Share on Facebook

Share on Twitter



IMAGE: JOHN BAZEMORE/ASSOCIATED PRESS



BY HEIDI MOORE

JUL 24, 2015

Fiat Chrysler said it will pull 1.4 million cars off the road "out of an abundance of caution" after some were found vulnerable to hacks in an elaborate magazine stunt.

The recall is the first-ever involving fear of hacking, a source familiar with the matter suggested, showing the potential trouble that looms as cars become more and more digital and veer from mechanical machines into the technological "smart car" category.

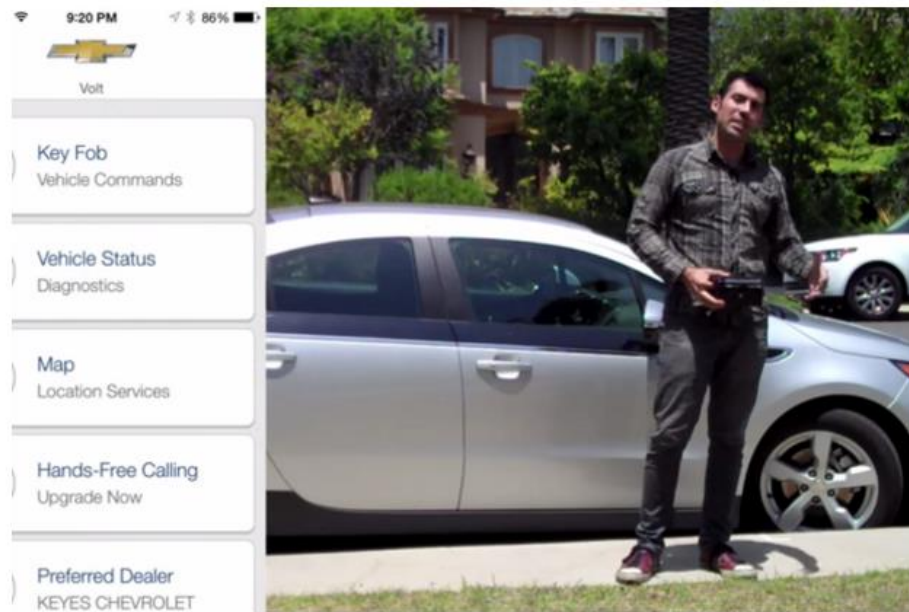
Vehicle Attacks

GONE IN 60 SECONDS

NEWS

Hacker shows he can locate, unlock and remote start GM vehicles

GM is working on a fix



Samy Kamkar stands next to a Chevy Volt that he used to demonstrate how he could hack into the GM's OnStar mobile app in order to unlock and start the car. Credit: Samy Kamkar



By Lucas Mearian

FOLLOW

Computerworld | Jul 30, 2015 1:50 PM PT

MORE LIKE THIS



Update: Chrysler recalls 1.4M vehicles after Jeep hack



Senators call for investigation of potential safety, security threats from...



10 scary hacks from Black Hat and DEF CON

on IDG Answers →

How to prove an individual is stealing my data through smstracker he installed...

Vehicle Attacks

BECOMING A FIELD OF RESEARCH

WIRED

The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse

SUBSCRIBE

NEWS

CULTURE

DESIGN

GEAR

SCIENCE

SECURITY

TRANSPORTATION

SHARE

2630

TWEET

PIN

20

COMMENT

31

EMAIL

THE JEEP HACKERS ARE BACK TO PROVE CAR HACKING CAN GET MUCH WORSE



FBI warning - PSA

IOT IS DANGEROUS



September 10, 2015

Alert Number
I-091015-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field

INTERNET OF THINGS POSES OPPORTUNITIES FOR CYBER CRIME

The Internet of Things (IoT) refers to any object or device which connects to the Internet to automatically send and/or receive data.

As more businesses and homeowners use web-connected devices to enhance company efficiency or lifestyle conveniences, their connection to the Internet also increases the target space for malicious cyber actors. Similar to other computing devices, like computers or Smartphones, IoT devices also pose security risks to consumers. The FBI is warning companies and the general public to be aware of IoT vulnerabilities cybercriminals could exploit, and offers some tips on mitigating those cyber threats.

What are some IoT devices?

- Automated devices which remotely or automatically adjust lighting or HVAC
- Security systems, such as security alarms or Wi-Fi cameras, including video monitors used in nursery and daycare settings
- Medical devices, such as wireless heart monitors or insulin dispensers
- Thermostats
- Wearables, such as fitness devices
- Lighting modules which activate or deactivate lights
- Smart appliances, such as smart refrigerators and TVs
- Office equipment, such as printers
- Entertainment devices to control music or television from a mobile device
- Fuel monitoring systems

Breaking all the things

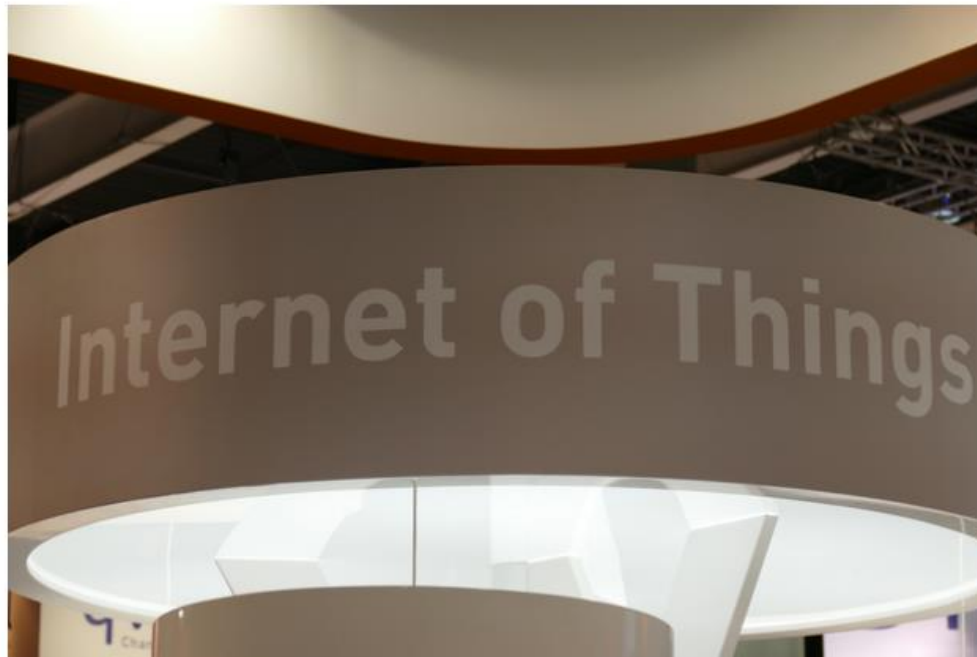
NO SECURITY

COMPUTERWORLD
FROM IDG

INSIDER

Hackers found 47 new vulnerabilities in 23 IoT devices at DEF CON

The results from this year's IoT hacking contest are in and it's not a pretty picture



Credit: Stephen Lawson

MORE LIKE THIS



How to secure your router and network



This tiny device can infect point systems and unlock hotel rooms



Hackers demonstrated first for IoT thermostats at DEF CON

on IDG Answers →

How to set network location in Windows 10 so can be seen by other...

CCTV Botnet

ONE VULNERABILITY TO RULE THEM ALL

IoT Botnet – 25,000 CCTV Cameras Hacked to launch DDoS Attack

Tuesday, June 28, 2016 Swati Khandelwal

91 Like 3.2K Share 1500 Tweet 362 Share 150 share 2211



The [Internet of Things \(IoT\)](#)s or Internet-connected devices are growing at an exponential rate and so are threats to them.

Due to the insecure implementation, these Internet-connected embedded devices, including Smart TVs, Refrigerators, Microwaves, Set-top boxes, Security Cameras and printers, are routinely being hacked and used as weapons in cyber attacks.

Your Devices, too

NOT JUST PUBLIC DEVICES



CLOUD

INNOVATION

SECURITY

APPLE

MORE ▾

NEWSLETTERS

ALL WRITERS

MUST READ [THE BIG GOOGLE PIXEL SMARTPHONE QUESTION: WHAT'S GOOGLE'S HARDWARE BRAND WORTH?](#)

Hackers in the house: Why your IoT devices may have already joined a botnet

Hackers are taking advantage of lax security attitudes around connected devices to hijack them for malicious means, researchers have warned.



By [Danny Palmer](#) | September 22, 2016 -- 10:57 GMT (03:57 PDT) | Topic: [Security](#)

KrebsOnSecurity DDoS

POWER OF IOT BOTNETS

How Hacked Cameras Are Helping Launch The Biggest Attacks The Internet Has Ever Seen



Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.
FULL BIO



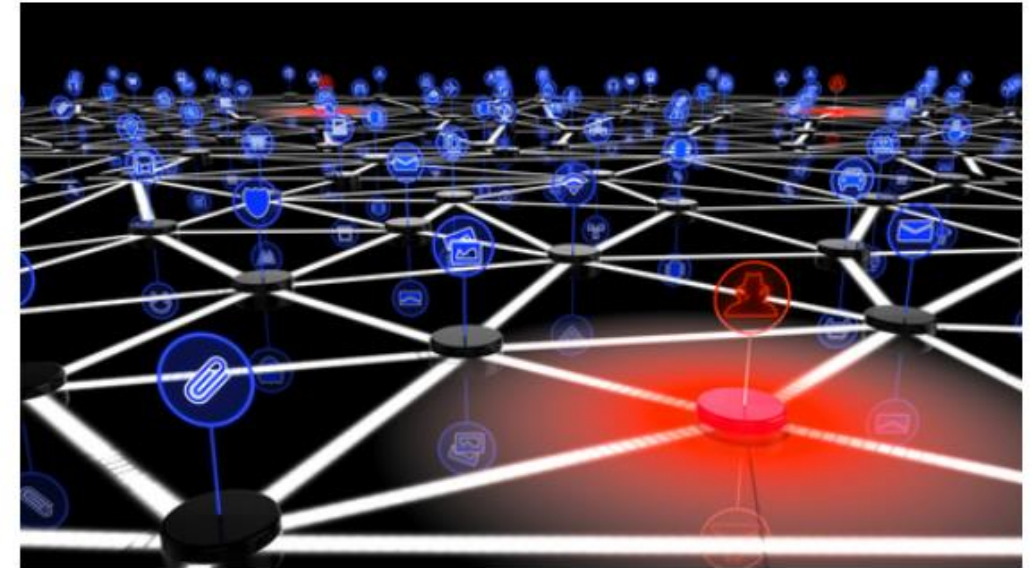
The Rio Olympics was targeted with epic DDoS attacks, but shrugged them off. But attacks are getting bigger, sites are falling and voices being silenced. / AFP / Odd ANDERSEN (Photo credit should read ODD ANDERSEN/AFP/Getty Images)

Brian Krebs knows what it's like to face intimidation from hackers. The independent reporter has had a SWAT team called to his house by subjects of his investigations.

21 KrebsOnSecurity Hit With Record DDoS

SEP 16

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at **Akamai**, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.



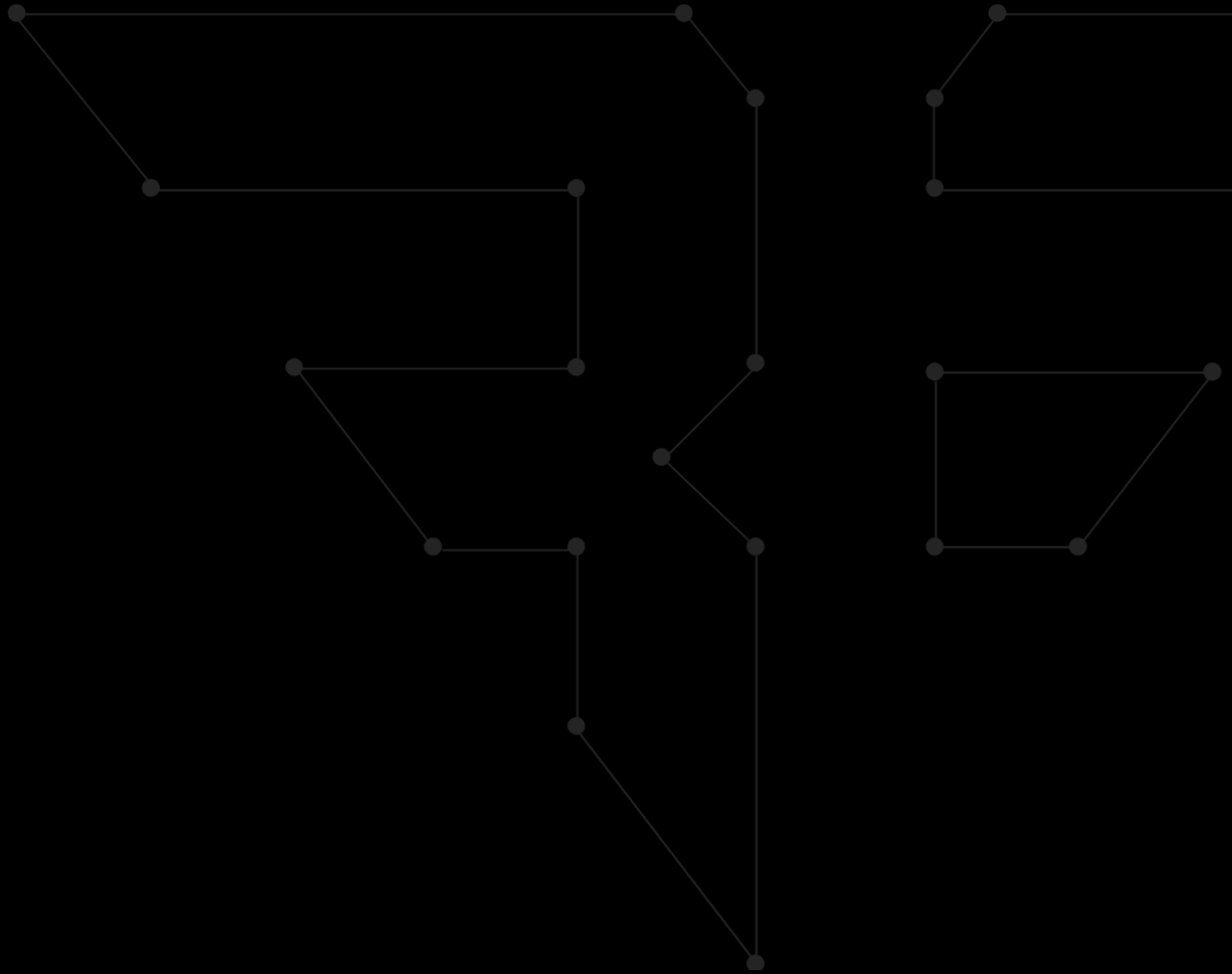
The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more traffic than is typically needed to knock most sites offline.

Brinks Smart Safes

PHYSICAL HACKING

The Brinks CompuSafe Galileo

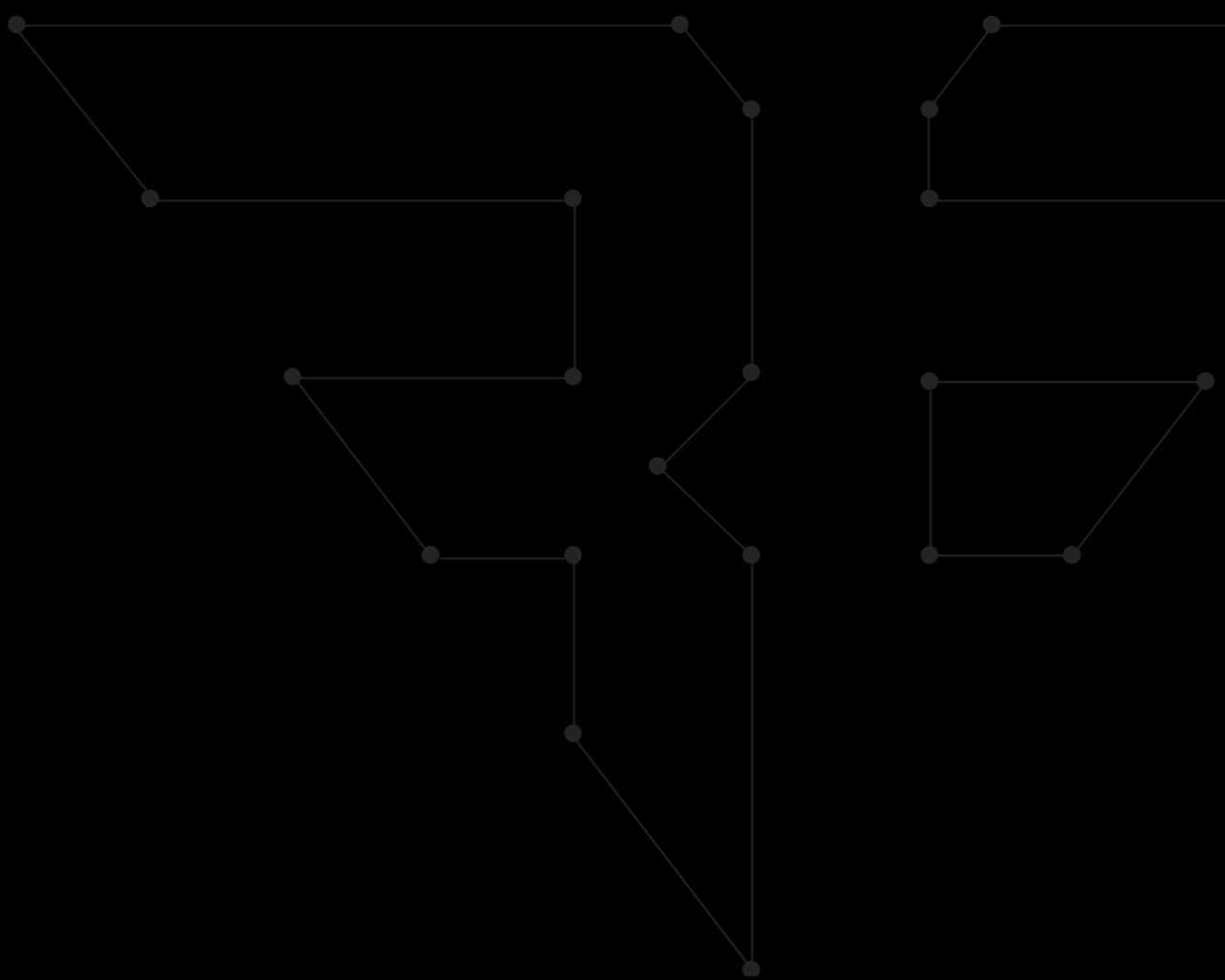
- Access to the USB port and 60 seconds is all a prepared attacker needs
- Adding “smarts” turned this safe into an unsafe



ILLUSTRATIVE FOOTAGE

A VIDEO FOR YOUR ENJOYMENT





DEFENSES

PROTECT YO NECK



Devices

PROTECTIONS: INTERNET

Buy devices that have update capabilities.

- Sign up for update notifications

Place untrusted devices on a separate network.

Use separate accounts for interacting with devices.

- Not your personal email address (iot-bob@gmail.com)

Trust but verify... Better yet, don't trust and verify.



Thank You



Attributions (Images)

[Smart Fridge image](#)

[Fitbits image](#)

[Garmin Watch image](#)

[Apple Watches image](#)

[IOT Cloud image](#)

[Apple Watch image](#)

[Smart Door Lock image](#)

[Samsung Lightbulb image](#)

[Panasonic Washing Machine image](#)

[Smart Fridge image II](#)

For further information:

[How to Engineer Secure Things: Past Mistakes and Future Advice – BF Blog](#)

Bishop Fox

www.bishopfox.com