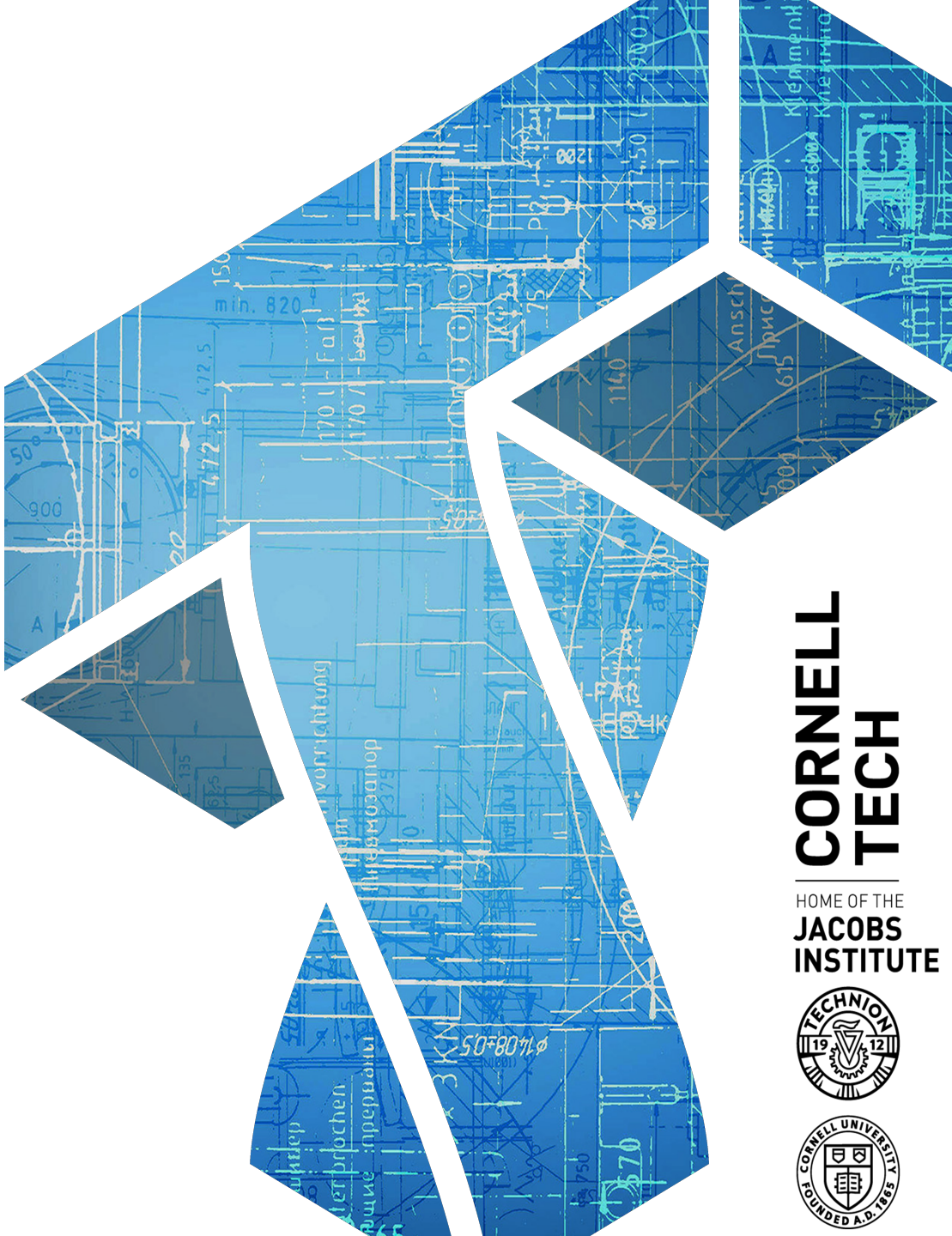
CS 5439:
Internet of things

Tom Ristenpart



CORNELL TECH
HOME OF THE
JACOBS INSTITUTE

Today’s topic

What is this “Internet of things”?

General security issues in IoT

IPV threat models

Internet of things (IoT)

“The interconnection via the Internet of computing devices embedded in everyday objects, enabling them to send and receive data.”

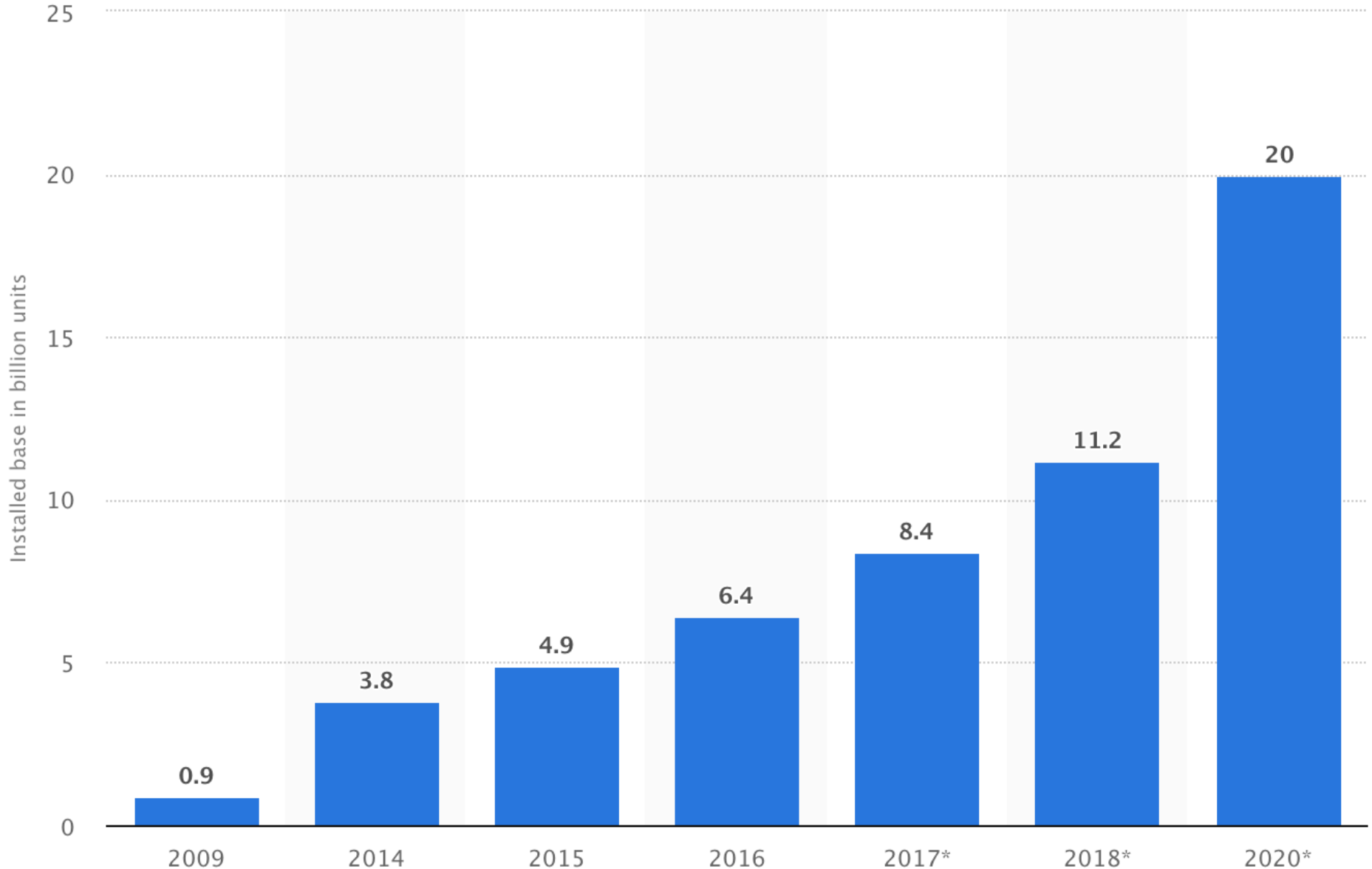
-Google

Embedded systems Cyberphysical systems Sensor networks


nest
Nest Protect:
Smoke + Carbon Monoxide™
PUSH TO DEMO


nest
COOLING
75


nest



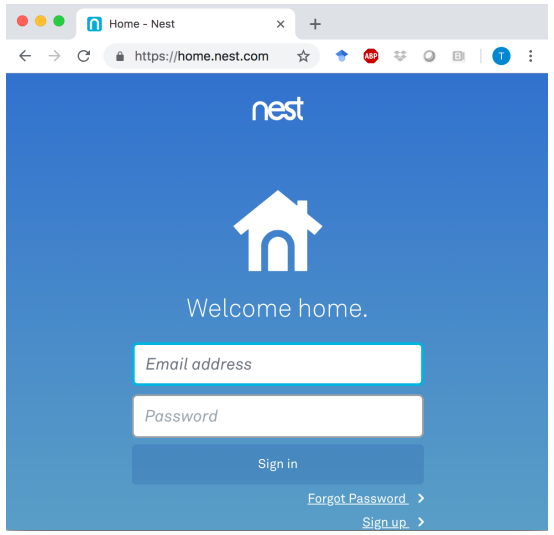
https://www.statista.com/statistics/764026/number-of-iot-devices-in-use-worldwide/

Embedded systems have:

- 1 or more low power microcontroller
- Ex: ARM Cortex-M3 with 128KiB of flash storage and 16KiB of RAM
- Sensors (camera, temperature, etc.)
- Actuators (motors for swiveling)
- Displays (LED, LCD)

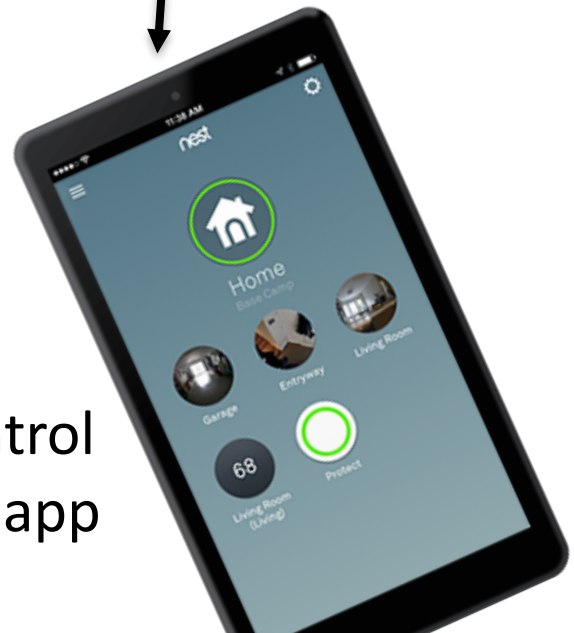
Example basic architecture of home IoT device

Data sent to cloud service operated by manufacturer



Sync & control via web

Cloud service



Sync & control via mobile app

Connect to internet via home WiFi

Some security issues (non-IPV setting)

Cloud account compromise

IoT device security (remote)

- open ports
- default account logins / passwords
- software vulnerabilities

IoT device security (local area network)

- Open WiFi network
- Lack of WiFi encryption such as WPA2
- WPA2 vulnerabilities
- Bluetooth vulnerabilities

IoT device security (physical access)

- Unprotected USB
- JTAG debugging ports
- Disabling LED indicators?

Don't panic, but your baby monitor can be hacked into a spycam

Researchers confirm hardware vulnerable to remote attacks

By Shaun Nichols in San Francisco 22 Jun 2018 at 06:30 34 SHARE ▼

"The security shop's researchers decided to look into the matter, and they found that the P2P service connects directly to the cloud and can be accessed with no more than an 8-digit device number and a shared default password. In other words, someone could go to the online portal and enter random numbers with the default password to pull up camera feeds."

https://www.theregister.co.uk/2018/06/22/baby_monitor_hacked/

(IoT) botnets

Botnets are networks of compromised computers

Include command & control (C&C) functionality to allow “botmaster” to marshal bot resources

Used for:
spam, DDoS, SEO, traffic generation, ...

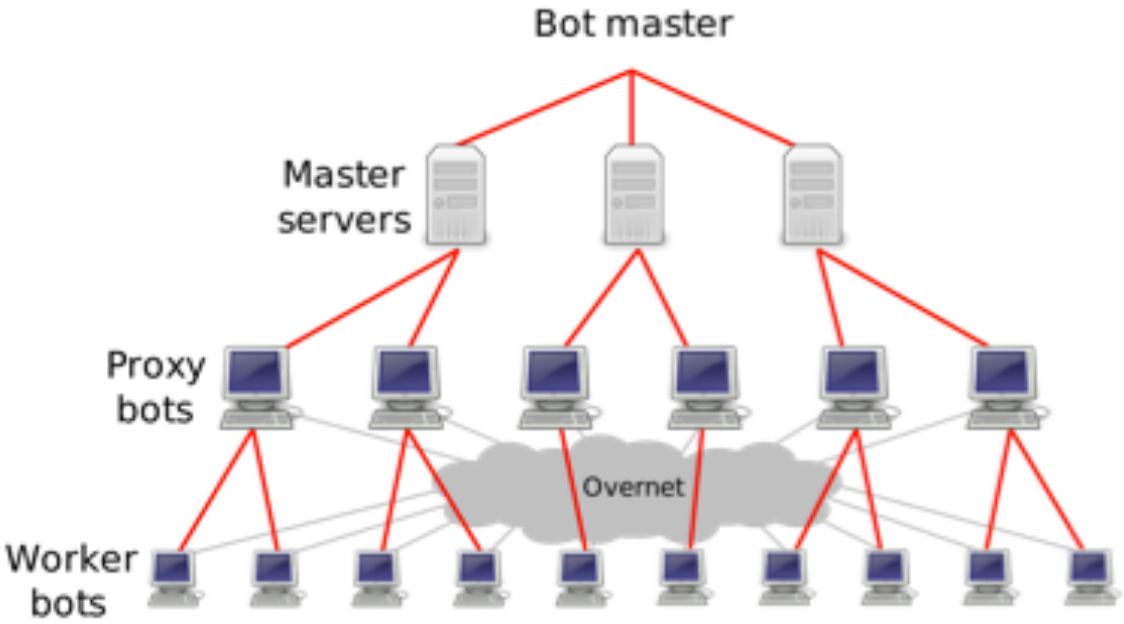


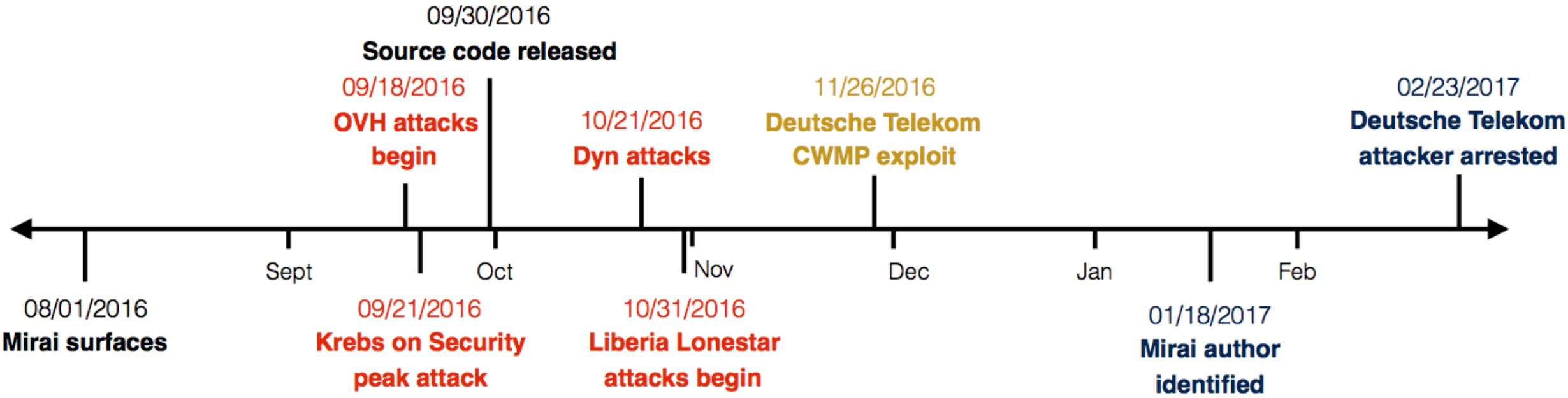
Figure 1: The Storm botnet hierarchy.

Enright 2007

Mirai botnet

Infected Linux IoT devices such as webcams and WiFi routers

Used for DDoS: >**600 GB/s** attack against Krebs on Security one of largest ever



[Antonakakis et al. 2017] https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46301.pdf

Mirai botnet

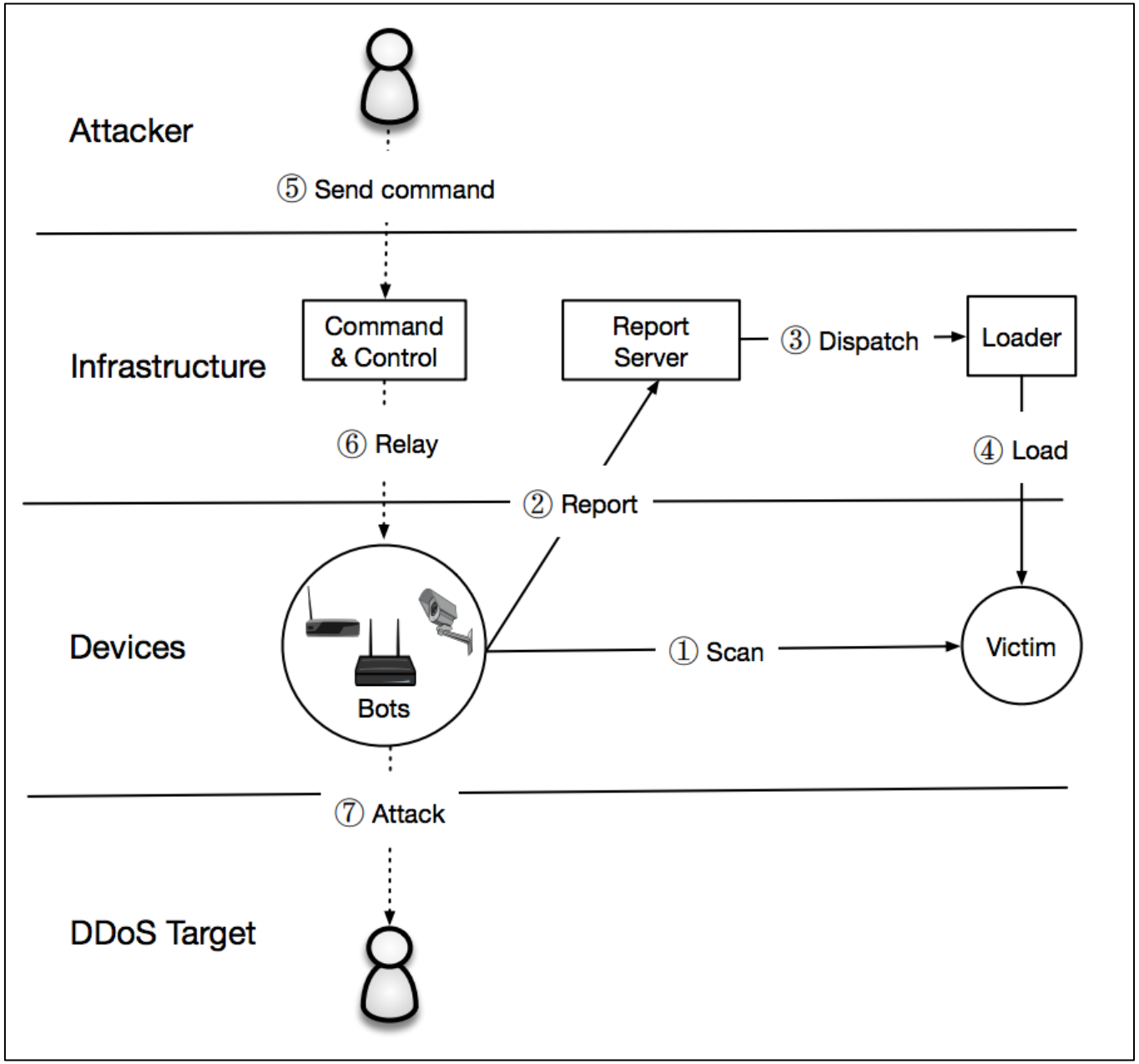
Infected Linux IoT devices such as webcams and WiFi routers

Ping random IPv4 addresses to see if running on telnet / ssh

Try to logging with known default IoT username, passwords

Download exploit to IoT device

Max size: 600,000 devices



[Antonakakis et al. 2017] https://static.googleusercontent.com/media/research.google.com/en//pubs/archive/46301.pdf

Some security issues (non-IPV setting)

Cloud account compromise

IoT device security (remote)

- open ports
- default account logins / passwords
- software vulnerabilities

IoT device security (local area network)

- Open WiFi network
- Lack of WiFi encryption such as WPA2
- WPA2 vulnerabilities
- Bluetooth vulnerabilities

IoT device security (physical access)

- Unprotected USB
- JTAG debugging ports
- Disabling LED indicators?

PRIVACY AND SECURITY

This Nest Security Flaw Is Remarkably Dumb

Adam Clark Estes
3/22/17 1:06pm • Filed to: LESS THAN NEST

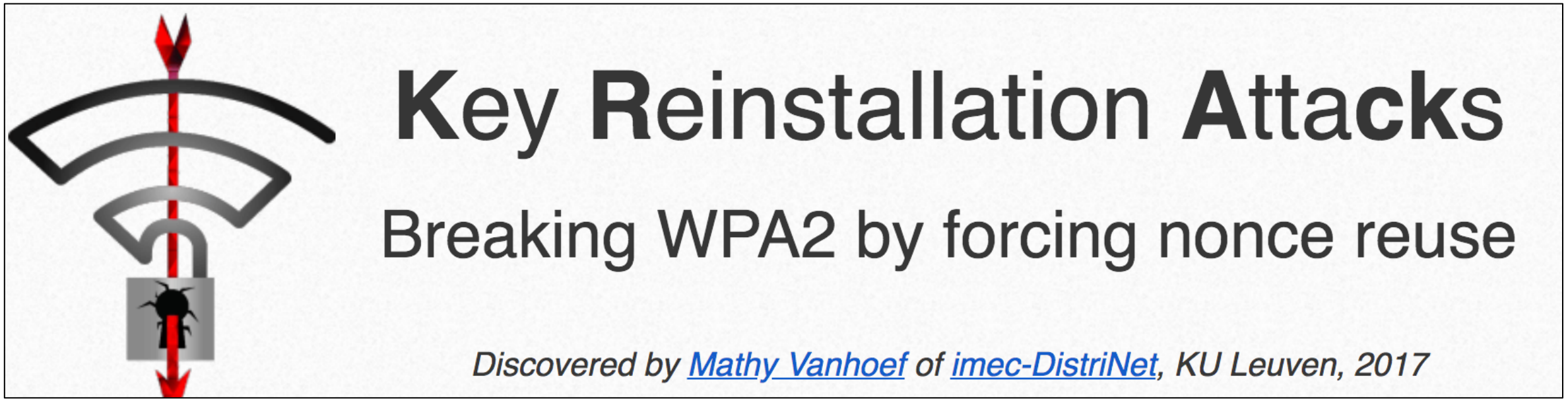
68.5K 50 5

https://gizmodo.com/this-nest-security-flaw-is-remarkably-dumb-1793524264

Send simple-to-construct Bluetooth commands to device, cause it crash and reboot --or-- log off WiFi

Either way disables camera feed

https://github.com/jasondoyle/Google-Nest-Cam-Bug-Disclosures/blob/master/README.md



https://www.krackattacks.com/

- Logical vulnerability in WPA2 spec allows replacing encryption keys with all zeros, or previously used keys
- Breaks WiFi encryption, allowing decryption of local network content

Some security issues (non-IPV setting)

Cloud account compromise

IoT device security (remote)

- open ports
- default account logins / passwords
- software vulnerabilities

IoT device security (local area network)

- Open WiFi network
- Lack of WiFi encryption such as WPA2
- WPA2 vulnerabilities
- Bluetooth vulnerabilities

IoT device security (physical access)

- Unprotected USB
- JTAG debugging ports
- Disabling LED indicators?

Smart Nest Thermostat: A Smart Spy in Your Home

Grant Hernandez[1], Orlando Arias[1], Daniel Buentello[2], and Yier Jin[1]

[1]Security in Silicon Laboratory, University of Central Florida
[2]Independent Researcher
yier.jin@eecs.ucf.edu

https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf

BlackHat paper:
Show how to install new software via a USB port in Nest thermostat

Look for the light

- Nest Cam is on.
- Blinking green means someone's watching.
- Blinking blue means someone's talking through the speaker. You'll also hear a little chime before and after.

Speaker

Hear a chime if someone is about to speak. Then listen to what they have to say.

Mic

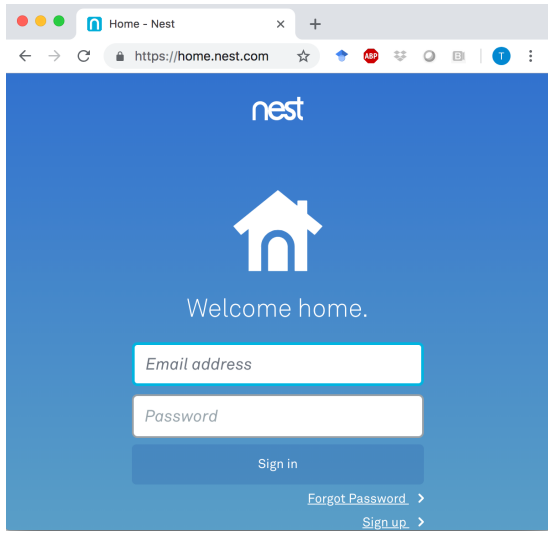
Pick up sounds clearly up to 20 feet away.

https://nest.com/cameras/nest-cam-indoor/tech-specs/

https://checkoway.net/papers/iseeyou2014/iseeyou2014.pdf

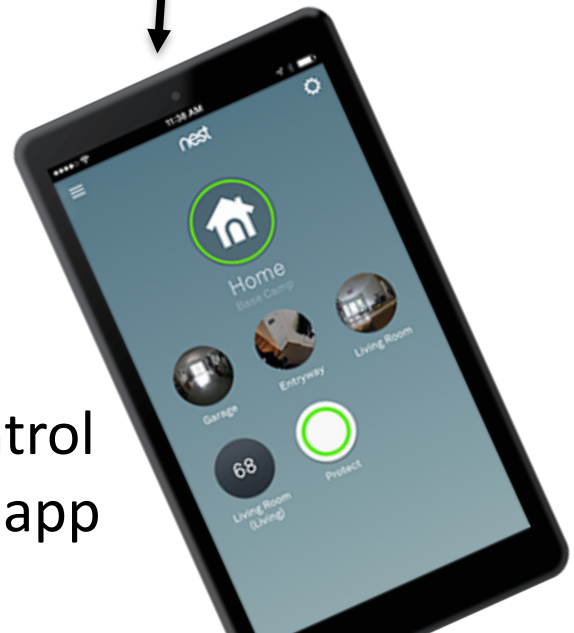
IPV threat models?

Data sent to cloud service operated by manufacturer



Sync & control via web

Cloud service



Sync & control via mobile app

Connect to internet via home WiFi

Roles of users for Nest products

The Owner

- You're the Owner if you created an account in the Nest app and added the first Nest product to it.

- The Owner can control all products with the app, manage subscriptions, change billing, view account and activity history, change settings, invite people to the home with the app, and more.

Full Access

- People who have Full Access can control all products, change settings, view account and activity history, and invite people to your home with the app.

- Up to 10 people including the Owner.

Some security issues (IPV setting)

IoT devices setup (owned) by abuser

IoT accounts can be broken into by abuser

- guessable passwords / compelled disclosure

With access:

- monitor victim
- control physical environment (temperature, lights, locks)
- disclose information online (setup a public feed)
- gaslighting
- ...

How to deal with IoT issues in IPV settings?

> "I have a specific exit plan that I'm in the process of implementing, and one of my fantasies is to be able to say, 'O.K. Google, play whatever music I want,'" she said. Her plan with the smart thermostat, she said, was to "pull it out of the wall."
>
> - Anonymous (from NYT story)

How to diagnose compromise of these devices?

Detection of web camera compromise?

From a webcam vendor (reolink.com):

1. Check Out Strange Noises from Your IP Camera, Baby Monitor
2. See If Your Security Camera Rotates Abnormally
3. Check If the Security Settings Have Been Changed
4. Find Out If There's a Blinking LED Light
5. Pay Attention to an Illuminated LED Light
6. Check the Data Flow of Your Security Camera

https://reolink.com/how-to-tell-if-your-security-camera-has-been-hacked/

How to deal with IoT issues in IPV settings?

> "I have a specific exit plan that I'm in the process of implementing, and one of my fantasies is to be able to say, 'O.K. Google, play whatever music I want,'" she said. Her plan with the smart thermostat, she said, was to "pull it out of the wall."
>
> - Anonymous (from NYT story)

How to diagnose compromise of these devices?

Better how-to guides for taking back control of IoT devices

Same account security guides (setting up 2FA, etc.)

Legal issues: orders of protection should prevent IoT access