THE INTERNET OF INSECURE THINGS
Getting Connected
Getting Connected
TODAY’S DISCUSSION

- 30,000 Foot View of the Law
- IoT Case Studies
- Policy Activity
- Business Best Practices
30,000 FOOT VIEW OF THE LAW

U.S. Federal Laws and Regulations
Representative Sample

International Laws and Regulations
Representative Sample

U.S. State Laws and Regulations
Representative Sample

Industry Standards and Self-Regulatory Frameworks
Representative Sample
PROMISES TO CONSUMERS

What do you communicate to the public about privacy and security?

What do you actually do?
GUIDANCE ON REASONABLE SECURITY

- Sensitivity and volume of consumer data
- Size and complexity of data operations
- Cost of available tools to improve security and reduce vulnerabilities
Wireless Internet Camera Server

- Secure your home or office with wireless streaming video
- Mount this compact stylish Internet camera on most surface areas
- Advanced complimentary software supports up to 16 Internet cameras
- Optimal wireless encryption for secure wireless transmissions

“secure wireless transmissions”
Setting to require PW/UN to access live feeds

Setting didn’t function correctly for 20 camera models – live feeds were publicly accessible.
Somebody's watching: how a simple exploit lets strangers tap into private security cameras

By Katie Notopoulos on February 3, 2012 12:10 pm

FTC: TrendNet failed to use reasonable security to design & test the software

Hackers posted live feeds of hundreds of IP cameras
ASUS

“protect computers from any unauthorized access, hacking, and virus attacks”

“SPI intrusion detection”

“DoS protection”
1. On your web browser such as Internet Explorer, Firefox, Safari, or Google Chrome, manually key in the wireless router’s default IP address: **192.168.1.1**

2. On the login page, key in the default user name (**admin**) and password (**admin**).

**Default user name:** (admin)
**Default password:** (admin)
enable the [router’s] firewall to protect your local network against attacks from hackers

Router software susceptible to cross-site scripting, etc.
Notified & took no action for years
ASUS: AiCloud

Plug in a USB device to router to access files & share files through a secure URL

“the most complete, accessible, and secure cloud platform”
Authentication bypass vulnerability: allow access to AiCloud account w/o login credentials

Password disclosure vulnerability in AiCloud application: allowed retrieval of router’s login credentials (& modify firewall, etc.)

ASUS notified in 6/2013 – emailed customers in 2/2014 about firmware updates
ASUS: AiDisk

Remotely access files on USB storage device attached to router via FTP

“safely secure and access your treasured data through your router”
“limitless access rights”

Anyone w/ the router’s IP address could access consumer’s USB storage
Hackers placed text files on thousands of USB devices: “This is an automated message being sent out to everyone effected [sic]. Your Asus router (and your documents) can be accessed by anyone in the world with an internet connection.”

Hackers posted list of IP addresses of over 12,000 vulnerable ASUS routers & login creds for over 3,000 AiCloud accounts.

FTC: ASUS failed to provide reasonable security in the design & maintenance of the software developed for its routers & related “cloud” features.
D-Link

“EASY TO SECURE”

“ADVANCED NETWORK SECURITY”
D-Link

“HARDCODED USER CREDENTIALS”

“COMMAND INJECTION FLAWS”

“FAILED TO TAKE REASONABLE STEPS TO MAINTAIN CONFIDENTIALITY OF PRIVATE KEY”
Breathometer

“Breathometer is a law enforcement grade breathalyzer.”
Sensors deteriorated significantly over time & allegedly did not accurately detect a consumer’s BAC.

Company had no way to recalibrate products in the field.

Eventually stopped selling products but didn’t notify consumers until FTC investigation.
• **Security**: build reasonable security into device at the outset
• **Data Minimization**: limit data collect/retain & dispose of it when no longer need it
• **Notice & Choice**: is data collected/used in way inconsistent w/ the interaction?
• **Legislation**

Workshops

Ransomware
September 7

Drones
October 13

Smart TV
December 7

Workshops

PrivacyCon 2017

https://www.ftc.gov/news-events/events-calendar/2017/01/privacycon
• FTC & NHTSA workshop to examine consumer privacy & security issues posed by automated and connected cars

• https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected
• **Challenge**: Create tool consumers can use to guard against IoT security vulnerabilities & protect against out-of-date software
  • **IoT Watchdog**: Scan home network inventory connected devices & flag out-of-date software & other common vulnerabilities & provide instructions to update the software
• **Prize**: $25,000
• **More info**: https://www.ftc.gov/iot-home-inspector-challenge
Business Education

- Implement “security by design” and “defense in depth” approach
- Design your product with authentication in mind.
- Protect the interfaces between your product and other devices or services.
- Consider how to limit permissions.
- Test the security measures before launching your product.

**CAREFUL CONNECTIONS**

- Select the secure choice as your default setting.
- Establish an effective approach for updating your security procedures.
- Innovate how you communicate.

QUESTIONS?

Steve Wernikoff
T: 312.701.9380
swernikoff@honigman.com