Hacking and Abuse
IoT

Kim Jonatan Wessel Bjørneset
Institutt for informatikk
Universitetet i Oslo

Book:

Abusing the Internet of Things

Nitesh Dhanjani

Presentation overview:

- Philips Hue Lightbulbs
- Assaults on Baby Monitors
- Attacking Smart TVs
- Car Security Analysis
- Summary

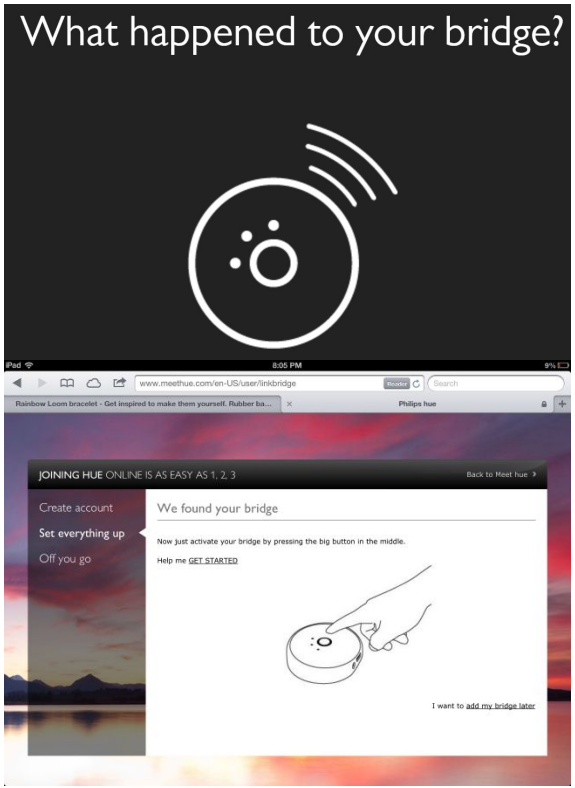
Philips Hue Lightbulbs - Website Interface

- Information Leakage
  - Web server at the hue website header: Access-Control-Allow-Origin set to: *
- Drive-By Blackouts
  - Web server runnning on the bridge has Access-Control-Allow-Origin set to: *

- Weak Passwords and Leaks
  - 6 characters
  - Reuse of credentials

Philips Hue Lightbulbs - iOS App

- Stealing the Token from a Mobile Device
  - Needs physical access to the phone
  - Specific file stored on the phone
- Malware can cause Perpetual Blackouts
  - Username token created from MAC address hash
  - Can’t deregister a whitelist token
- IFTTT
  - IF This Then That
  - Light fit to colors on a photo
  - Account compromised



Philips Hue Lightbulbs - Siri (not from the Book)

- SiriProxy - https://github.com/plamoni/SiriProxy
- The Three Little Pigs - https://github.com/interstateone/The-Three-Little-Pigs-Siri-Proxy

- Hue API - Philips SDK?
- Install the proxy on a Mac and/or a Raspberry Pi

Assaulting Baby Monitors

- The Foscam Incident
  - IP address as part of the URL -> http://[IP]/proc/kcore
  - Open the file to obtain username and password
  - Control of the camera
- Using Shodan
  - shoddanhq.com
- Belkin WeMo
  - WiFi and one-time access gives full control of the device

Attacking Smart Televisions

- TOCTTOU
  - Time Of Check To Time Of Use
- Samsung LEXXB650 Series
  - Exploit
  - Change the image file
  - Forcing the TV to read the image again
- Samsung Smart LED Encryption Exploit
  - XOR
  - “Encraption”
  - Applications
  - With other IoT Devices

Car Security Analysis

- Tire Pressure Monitoring System
- Eavesdropping and Privacy Implications
- Spoofing Alerts
- Exploiting the Wireless Connectivity
- Tesla Model S

Summary & Questions