nebgnahz / awesome-iot-hacks

Watch 75 Star 644 Fork 165

Code Issues 0 Pull requests 0 Projects 0 Insights

A Collection of Hacks in IoT Space so that we can address them (hopefully).

awesome iot security hack

47 commits 1 branch 0 releases 4 contributors MIT

Branch: master New pull request Find file Clone or download

nebgnahz committed on Aug 28, 2017 Add the 2015 Rifle hack … Latest commit 2e0b81a on Aug 28, 2017

LICENSE	Initial commit	3 years ago

README.md	Fix typo	9 months ago

README.md

Awesome IoT Hacks

A curated list of hacks in IoT space so that researchers and industrial products can address the security vulnerabilities (*hopefully*).

The table of content is generated with doctoc. Make sure you run it and update the table of content before making pull requests.

Contents

- Cameras
- Traffic Lights
- Automobiles
- Airplanes
- Light Bulbs
- Locks
- Smart Scale
- Smart Meters
- Pacemaker
- Thermostats
- Fridge
- Media Player & TV
- Rifle (Weapon)
- Toilet
- Toys

Analysis, Reports and Slides

- Internet of Things Research Study (HP 2014 Report)
- The Internet of Fails, (video)
- Cameras, Thermostats, and Home Automation Controllers, Hacking 14 IoT Devices
- Hack All The Things: 20 Devices in 45 Minutes - (wiki, video)
- Careful Connections: Building Security in the Internet of Things (FTC)

Communities

- IoT Village^{TM}
- BuildItSecure.ly
- Secure Internet of Things Project (Stanford)
- The Open Web Application Security Project (OWASP)

IoT Hacks

Thingbots

- Proofpoint Uncovers Internet of Things (IoT) Cyberattack

RFID

- Vulnerabilities in First-Generation RFID-enabled Credit Cards
- MIT Subway Hack Paper Published on the Web
- Tampered Card Readers Steal Data via Bluetooth

Home Automation

- IOActive identifies vulnerabilities in Belkin WeMo's Home Automation
- Cameras, Thermostats, and Home Automation Controllers, Hacking 14 IoT Devices
- Popular Home Automation System Backdoored Via Unpatched Flaw

Connected Doorbell

- CVE-2015-4400: Backdoorbot, Network Configuration Leak on a Connected Doorbell, (video)

Hub

- TWSL2013-023: Lack of Web and API AuthenticationVulnerability in INSTEON Hub

Smart Coffee

- Reversing the Smarter Coffee IoT Machine Protocol to Make Coffee Using the Terminal

Wearable

- How I hacked my smart bracelet

Smart Plug

- Hacking the D-Link DSP-W215 Smart Plug
- Reverse Engineering the TP-Link HS110
- Hacking Kankun Smart Wifi Plug
- Smart Socket Hack Tutorial

Cameras

- Trendnet Cameras - I always feel like somebody's watching me
- Hacker Hotshots: Eyes on IZON Surveilling IP Camera Security
- Cameras, Thermostats, and Home Automation Controllers, Hacking 14 IoT Devices
- Hacker 'shouts abuse' via Foscam baby monitoring camera
- Urban surveillance camera systems lacking security

- TWSL2014-007: Multiple Vulnerabilities in Y-Cam IP Cameras
- Say Cheese: a snapshot of the massive DDoS attacks coming from IoT cameras
- Samsung SmartCam install.php Remote Root Command Exec

Traffic Lights

- Green Lights Forever: Analyzing The Security of Traffic Infrastructure
- Hacking US (and UK, Australia, France, etc.) Traffic Control Systems

Automobiles

- Hackers Remotely Attack a Jeep on the Highway
- Comprehensive Experimental Analyses of Automotive Attack Surfaces

Airplanes

- Hackers could take control of a plane using in-flight entertainment system

Light Bulbs

- Hacking into Internet Connected Light Bulbs
- Hacking Lightbulbs: Security Evaluation Of The Philips Hue Personal Wireless Lighting System
- IoT Goes Nuclear: Creating a ZigBee Chain Reaction
- Extended Functionality Attacks on IoT Devices: The Case of Smart Lights

Locks

- Lockpicking in the IoT

Smart Scale

- Fitbit Aria Wi-Fi Smart Scale

Smart Meters

- Solar Power Firm Patches Meters Vulnerable to Command Injection Attacks

Pacemaker

- Pacemakers and Implantable Cardiac Defibrillators: Software Radio Attacks and Zero-Power Defenses

Thermostats

- Cameras, Thermostats, and Home Automation Controllers, Hacking 14 IoT Devices
- Google Nest: Exploiting DFU For Root
- Smart Nest Thermostat, A Smart Spy in Your Home
- TWSL2013-022: No Authentication Vulnerability in Radio Thermostat

Fridge

- Proofpoint Uncovers Internet of Things (IoT) Cyberattack - Spam emails from fridges.
- Hacking Defcon 23'S IoT Village Samsung Fridge

Media Player & TV

- Breaking Secure-Boot on the Roku
- Google TV Or: How I Learned to Stop Worrying and Exploit Secure Boot
- Chromecast: Exploiting the Newest Device By Google

- Ransomware Ruins Holiday By Hijacking Family's LG Smart TV on Christmas Day

Rifle (Weapon)

- Hacking a IoT Rifle - BlackHat 2015 - 36 slides
- Hackers Can Disable a Sniper Rifle—Or Change Its Target - Wired 2015

Toilet

- TWSL2013-020: Hard-Coded Bluetooth PIN Vulnerability in LIXIL Satis Toilet

Toys

- TWSL2013-021: Multiple Vulnerabilities in Karotz Smart Rabbit
- Fisher-Price smart bear allowed hacking of children's biographical data (CVE-2015-8269)
- Hello Barbie Initial Security Analysis
- Security researcher Ken Munro discovers vulnerability in Vivid Toy's talking Doll 'Cayla'
- Data from connected CloudPets teddy bears leaked and ransomed, exposing kids' voice messages