RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: SBX1-W07

Hacking the IoT: When Good Devices Go Bad

Jesus Molina
@verifythentrust

Joe Gordon

Balint Seeber
@spenchdotnet

Bastille

#RSAC

What is the IoT?

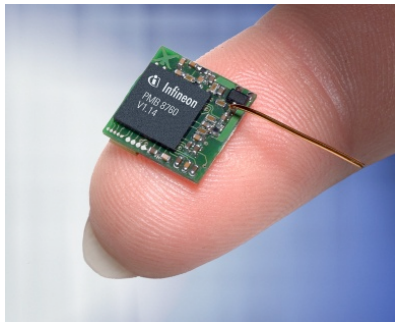
- The “**I**nternet **o**f **T**hings” is a broad buzz phrase:
  - Imagine any one of the many devices/objects you (knowingly/ unknowingly) interact with on a daily basis
  - Embed communications module for control and/or telemetry
  - Commonly connects to Internet (‘Cloud’), or to Smart Phone

IoT Communications

- IoT enabled by cheap communications hardware
- Wireless - portable, cheaper than installing cabling (copper)
- Commodity Wi-Fi chips, Bluetooth Low Energy & embedded processors
- Optimised proprietary, IoT-specific protocols in development
  - Long-life, low power consumption

SIGFOX
One network A billion dreams

LoRa



ibelium

IoT Playroom

Future IoT Trends

- Various predictions based on current production & low cost, reuse of IoT-enabling hardware/software/firmware
- 50 billion connected devices by 2020
  - Just a few years away!
- Smallest, insignificant devices will be able to communicate wirelessly

IoT Playroom

Ubiquity of the IoT

- In the home
  - Security, lighting
- In the enterprise
  - HVAC
- In Smart cities
  - Traffic flow, lighting
- In infrastructure

IoT Playroom

The Good, The Bad & The ???

Daniel Gasienica @gasi · Feb 10

Begun have the IoT Wars: My Roomba™ just destroyed my Philips Hue™ bulb 😭

6

TECHNOLOGY

SmartyPans: World's First Smart Cooking Pan

Tracks nutrition in real time and teaches you how to cook with it's temperature and weight sensors.

$31,133 USD

104% 20 hours left

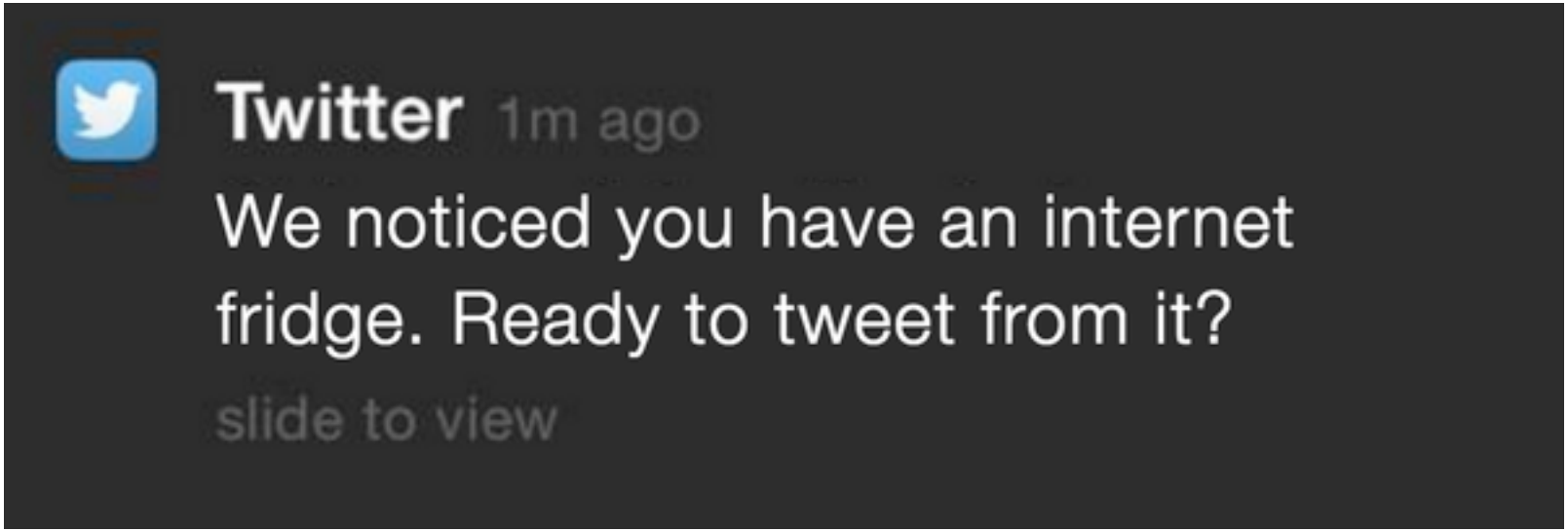
The Good, The Bad & The ???

IoT Playroom

The Good, The Bad & The ???

IoT Playroom

The Good, The Bad & The ???



IoT Playroom

IoT Security

- History shows that security is never implemented correctly
  - Time-to-market pressure
  - Lack of understanding of good security
  - Poor code quality & reuse
  - Upgrade later
- Vulnerabilities persist and propagate from reference designs

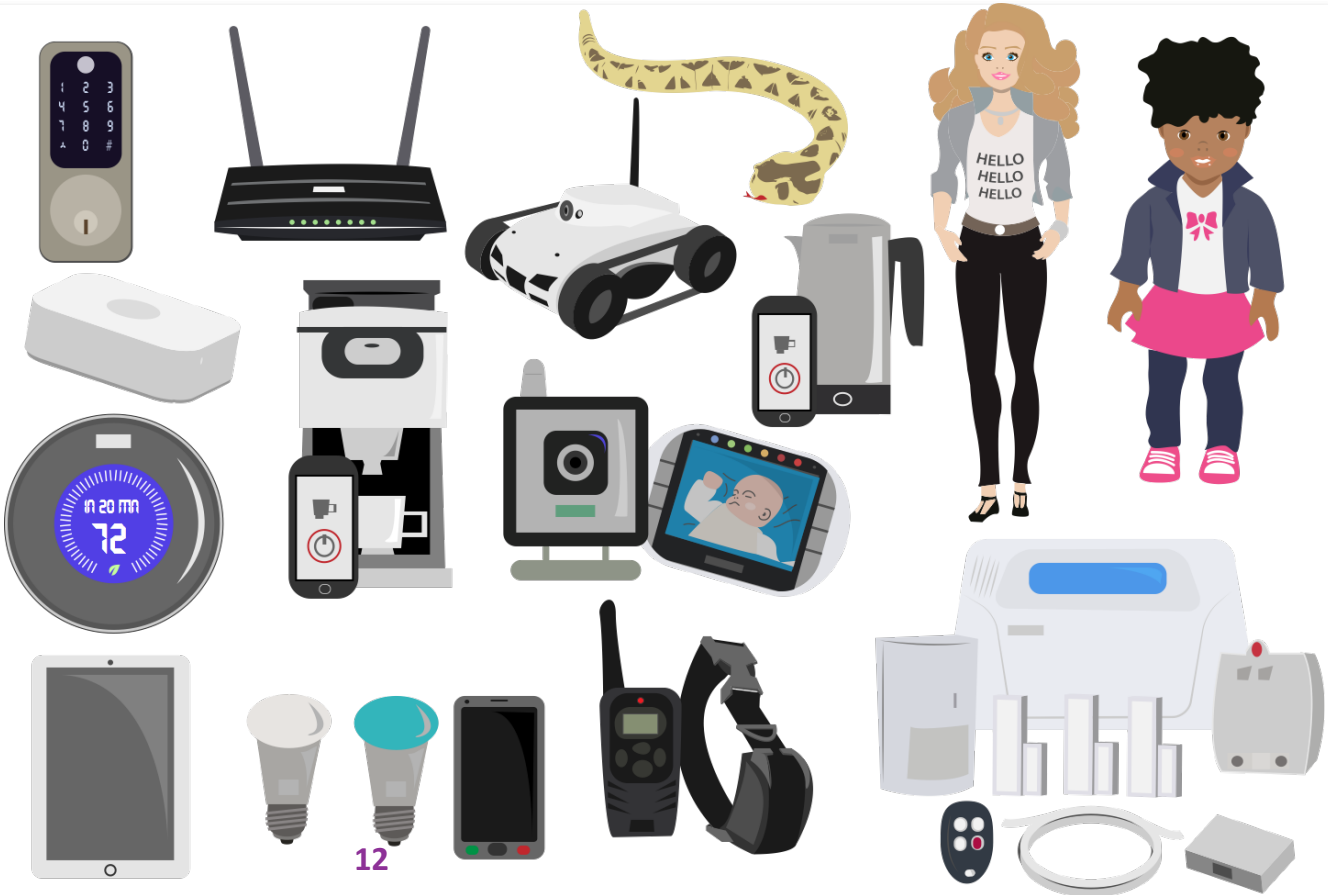
Our IoT Devices

- Home automation
  - ZigBee-enabled door lock (open from your Smart Phone)
- Home security
  - Wireless alarm system (no more wires to install!)
- Toys
  - iSpy Tank

IoT Playroom

Our IoT Devices

- NEST
- Hello Barbie
- Cayla
- Baby Monitor
- Dog Shock Collar
- Light Bulbs



IoT Playroom

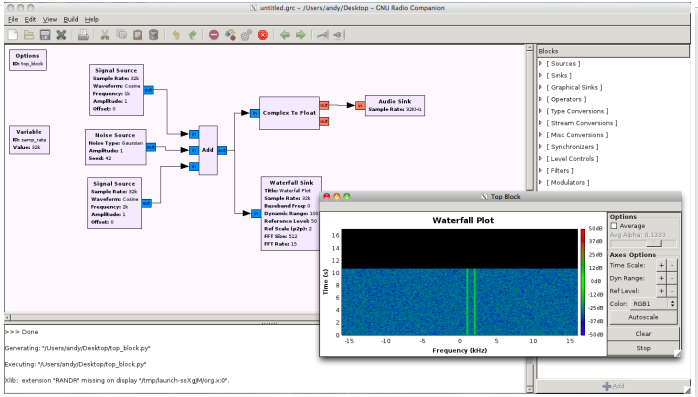
Communications Hardware

- **S**oftware **D**efined **R**adio
  - Re-configurable, programmable radio
  - Signals decoded & generated on computer
  - SDR hardware provides RF front-end

IoT Playroom

Communications Software

- GNU Radio
  - Free Open Source Software
  - Flow-based DSP framework
  - Active developer community, many Out Of Tree modules
  - Supports variety of SDRs



IoT Playroom

GNU Radio

THE FREE & OPEN SOFTWARE RADIO ECOSYSTEM

ZigBee Door Lock

- Keypad for electronic control
- Wireless module to connect to Home Automation hub
  - Control/monitor from Smart phone
- ZigBee & Z-Wave options
- ‘Uses encryption’

IoT Playroom

ZigBee Door Lock

- “Zigbee Exploited: The Good, the Bad and the Ugly”
  - Tobias Zillner
- https://cognosec.com/blackhat-defcon-2015/

IoT Playroom

cognosec
A UC GROUP COMPANY

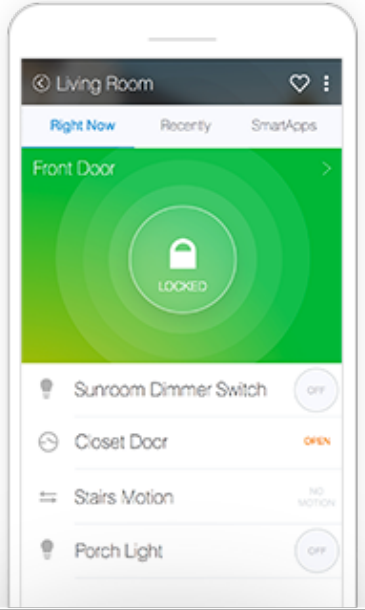
ZigBee Door Lock

Encrypted

Control & Status

Sniff Link Key

Encrypted ‘Unlock’



IoT Playroom

Wireless Home Alarm System

- Avoids wired installation
- Uses simplistic communications protocol between controller & security sensors

IoT Playroom

Wireless Home Alarm System

- "Home Insecurity: No alarm, False alarms, and SIGINT"
  - Logan Lamb
- https://media.defcon.org/DEF%20CON%2022/DEF%20CON%2022%20presentations/Logan%20Lamb/

IoT Playroom

Wireless Home Alarm System

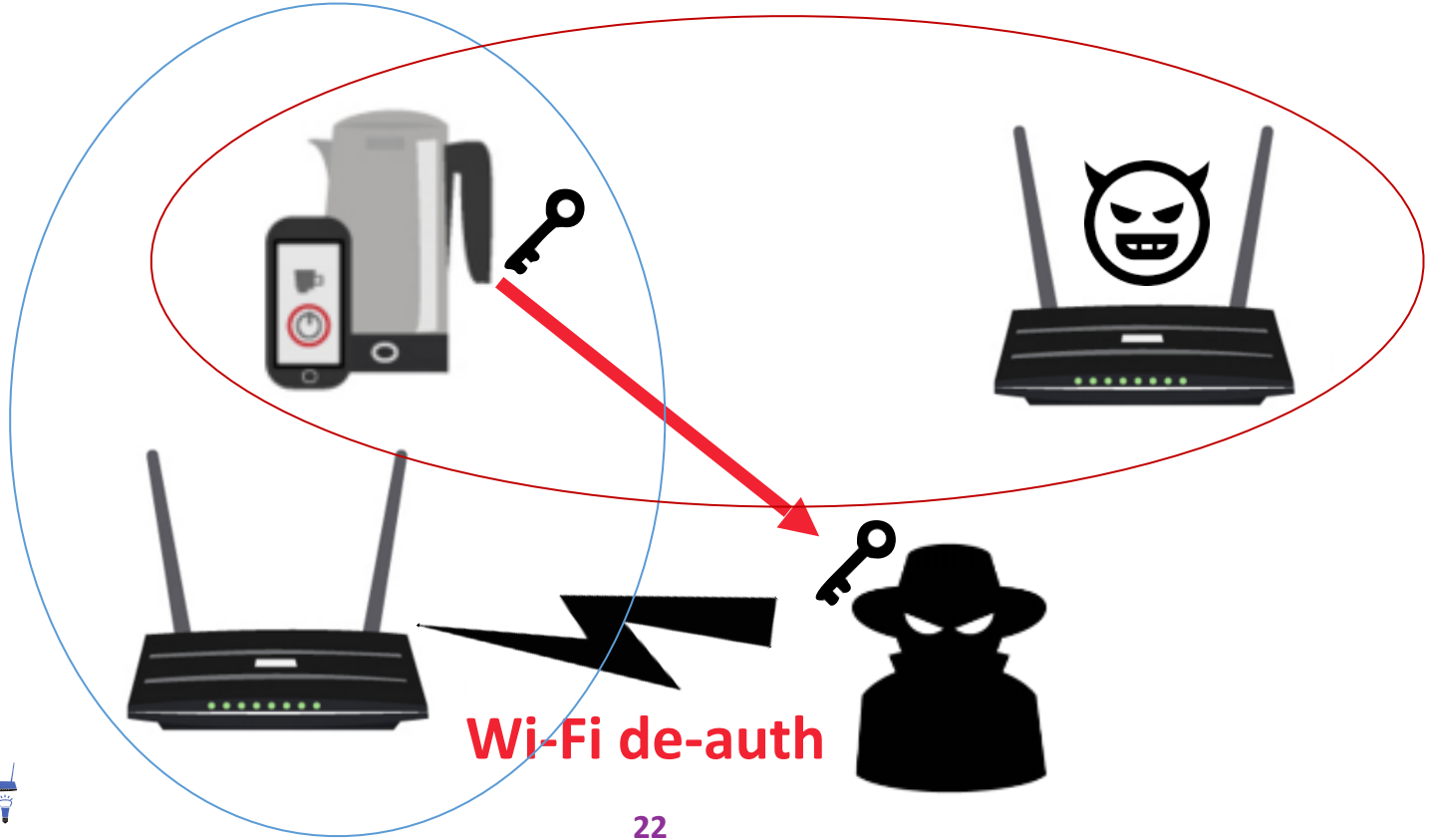
IoT Playroom

iKettle

- Leaks Wi-Fi network credentials to attacker
- Compromises security of private network

IoT Playroom

iKettle



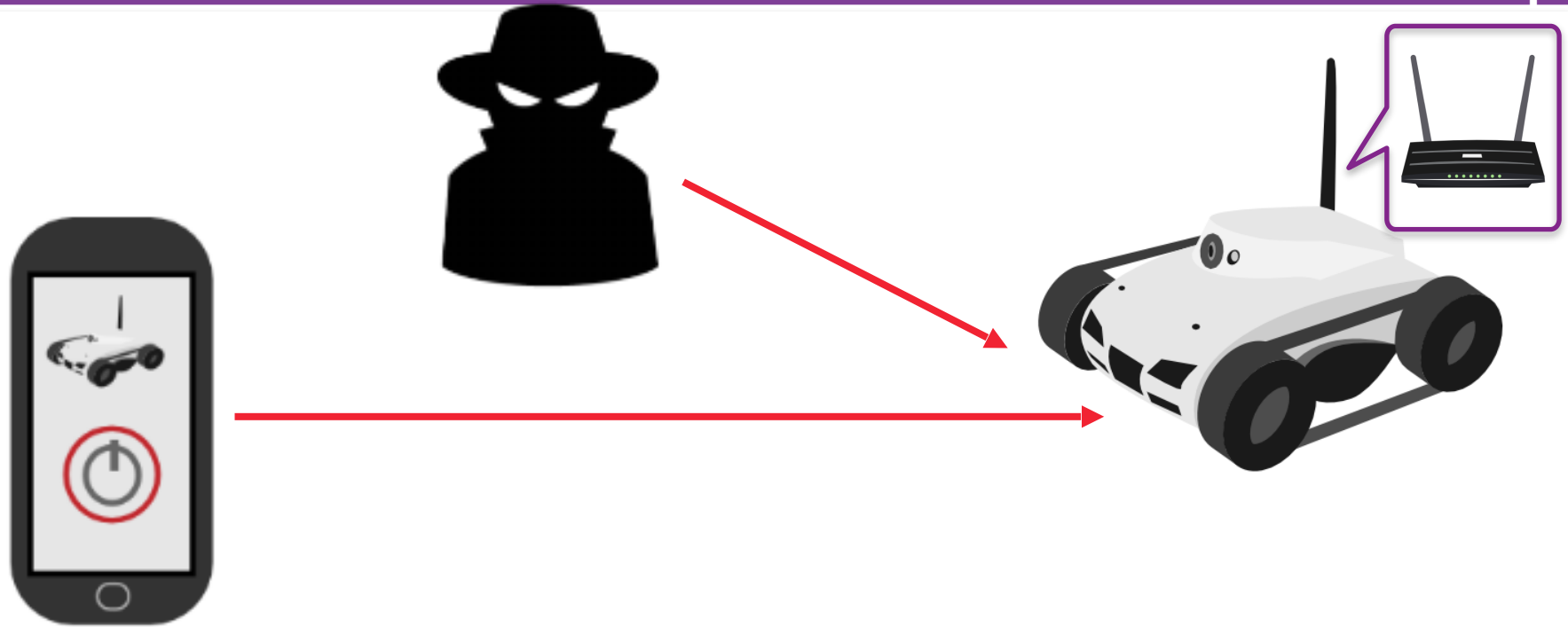
IoT Playroom

iSpy Wi-Fi Tank

- Re-purpose toy to sniff traffic on connected Wi-Fi network
- No access control
- Hard-coded passwords

IoT Playroom

iSpy Wi-Fi Tank



Cayla

- Bluetooth headset
- No PIN
- Eavesdropping
- Play any audio

IoT Playroom

Apply: Preparing for the IoT

- Next week: Be fully aware of all wireless capabilities of devices
  - Infrastructure radio capabilities
- 3 months: Minimize wireless attack surface
  - Attacks via RF domain are cheap
  - Do not rely on Security Through Obscurity
- 6 months: Understand security implications
  - Design security in from the beginning
  - Hire talent that understand good security practice/protocols

IoT Playroom

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

Hacking the IoT: When Good Devices Go Bad

Jesus Molina
@verifythentrust

Joe Gordon

Balint Seeber
@spenchdotnet

Bastille

#RSAC