ISC 2015 中国互联网安全大会

360互联网安全中心

ISC 2015

数据驱动安全

2015 中国互联网安全大会 China Internet Security Conference

# 智能设备安全漏洞研究和防护
# Smart vs. Security: IoT Security and Protections

**Yier Jin**

Department of Electrical Engineering and Computer Science

University of Central Florida

yier.jin@eecs.ucf.edu

Security in Silicon Lab (SSL)

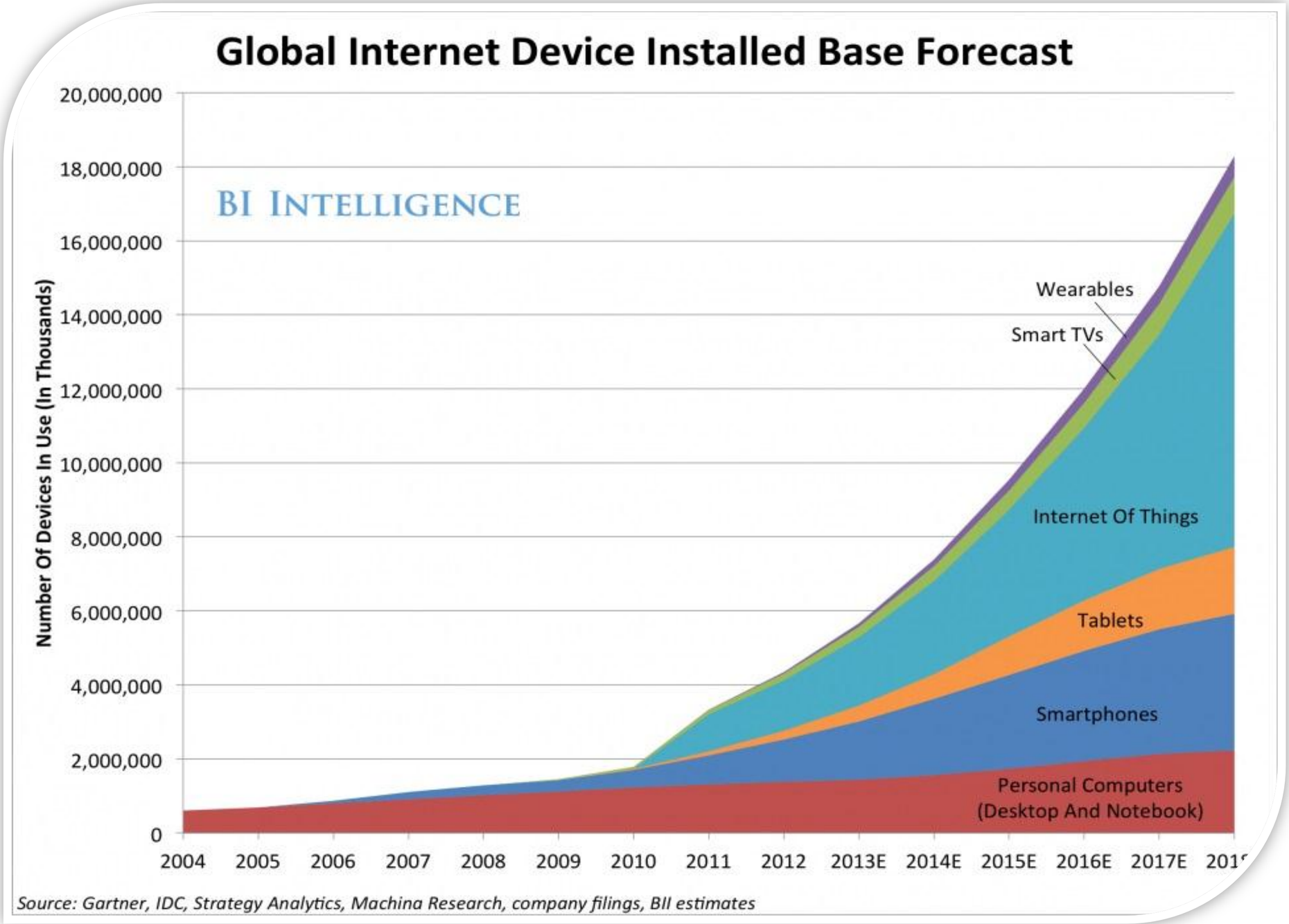
# IoT and Wearable Devices

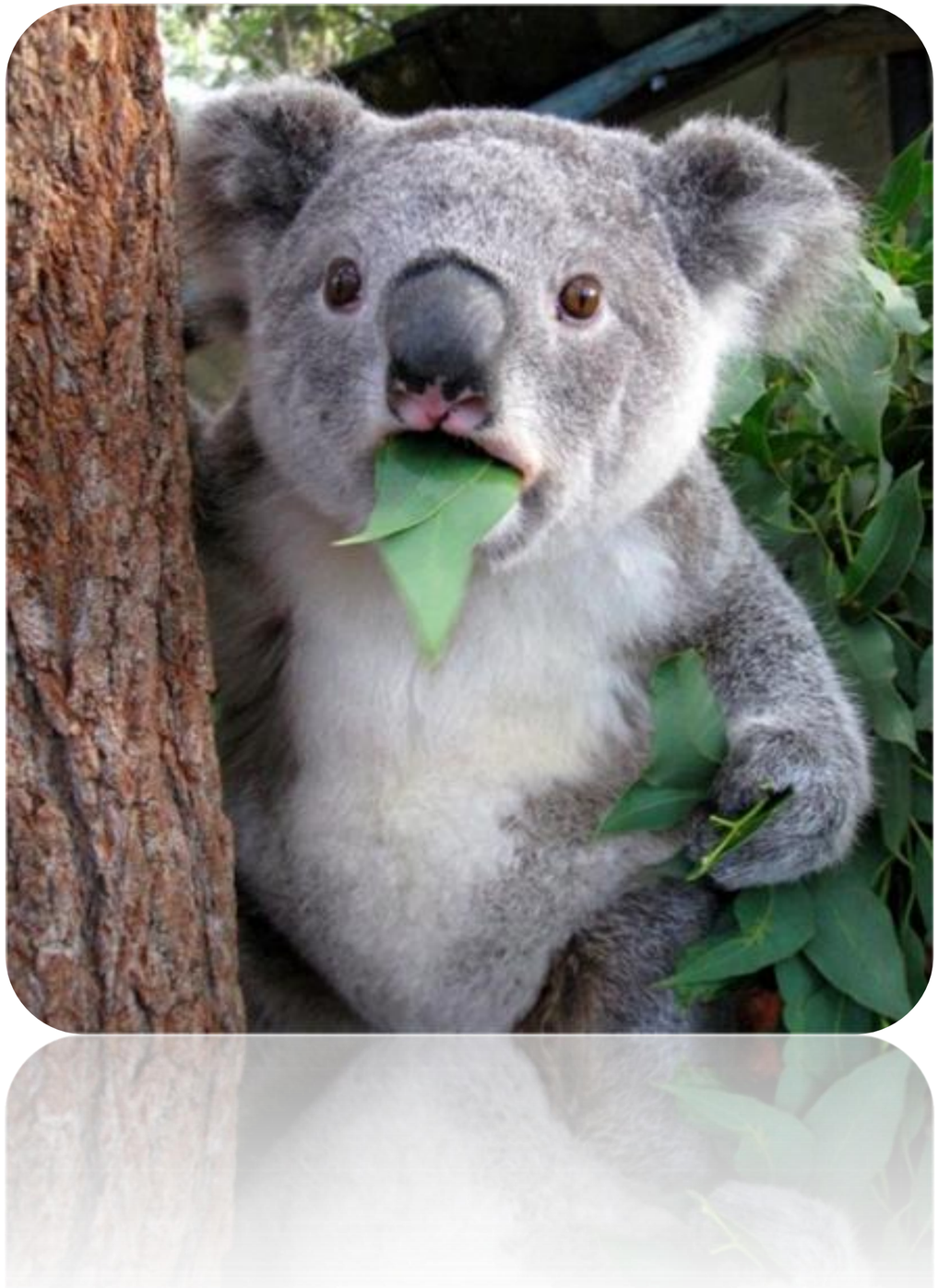




Assorted images found online.

# IoT Forecast





数据驱动安全

# IoT in Commercials

- How About Security?

**Wireless**

**Remote Control**

**Constant Access**

**Machine Learning**

**Big Data**

**Cloud Computing**

**Security**

# Security and Privacy

- Security Concerns
  - “ThingBot”: More than 750,000 phishing and SPAM emails launched from “ThingBots” including televisions, fridges
  - WeMo “Light Switch” firmware can be remotely controlled
- Privacy Concerns
  - Personal data is often collected without users’ awareness
  - The “big personal data” includes too much information

**When industrial-level damages can be caused through device-level hacking, can we still ignore the issues of IoT security threats?**

# CASE study - World

- How secure are current IoT/networked devices?

# Power Grid


*数据驱动安全*

# Vehicle

*数据驱动安全*

# Weapon


*数据驱动安全*

# CASE study – my lab

- How secure are current IoT/networked devices?

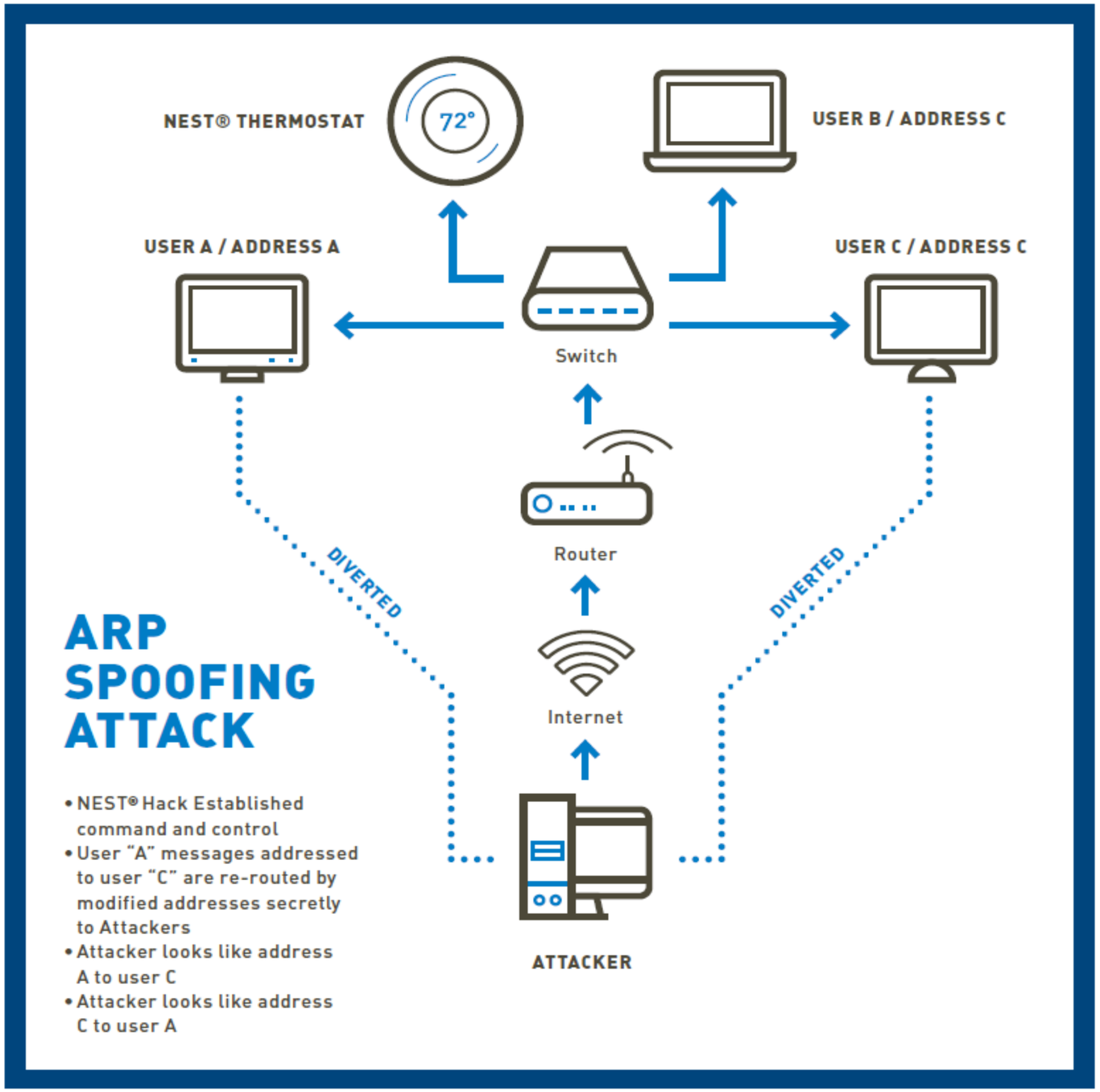
# Google Nest Thermostat


- Functionality
  - Smart thermostat (self-learning, auto-away, Nest app, Nest leaf)
- Exploitation and Payload
  - Bypass firmware verification and install customized userland
  - Remote control and user privacy collection
- Security Impact
  - Through the backdoor, remote access capability can be inserted for hackers to exploit the device and the local network remotely


数据驱动安全

# TrapX

- ARP Spoofing
  - Compromised Nest
  - Collect user data in other devices
  - Local network compromise
  - Attack interface to infrastructure



# Company A - Protect

- Functionality
  - Smart smoke detector
  - An important home automation component
- Exploitation and Payload
  - End-user can modify the software core
- Security Impact
  - Physical damage (attackers may turn off the Protect)
  - Inconvenience (high quality becomes a burden)

# Company B – Smart Band

- Functionality
  - Smart band for health tracking
    - Wireless Chip
    - ARM-based Microcontroller
    - USB – charge only
    - LED Matrix Display
    - Bluetooth 4.0 pairing to smart phones
- Exploitation and Payload
  - Bypass firmware integrity
  - Boot any firmware
- Security Impact
  - Learn user’s health information
  - Privacy breach

# Roku

- Functionality
  - Streaming media player
- Exploitation and Payload
  - Telnet root shell spawned on boo
  - Enable U-Boot shell
- Secuirty Impact
  - Allows a user to execute commands as a root user

# Belkin Wemo

- Functionality
  - The device is able to turn electronics on and off remotely
- Exploitation and Payload
  - Root shell can be accessed
- Security Impact
  - Electronic equipment may be remotely controlled by attackers
  - Physical damage

# Epson Artisan 700/800

- Functionality
  - All-in-one printer
  - Wi-Fi connection
- Exploitation and Payload
  - Feature a shell through serial port
  - Controller menu is available
- Security Impact
  - Information leakage

# Amazon Fire TV Stick

- Functionality
  - Stream media to the TV using the HDMI port
- Exploitation and Payload
  - User can gain root access
- Security Impact
  - The device can be rooted for any modifications

# Amazon Fire TV Box

- Functionality
  - Stream media to the TV using the HDMI port
- Exploitation and Payload
  - Copy over the SuperSU APK
  - Copy “su” binary to “bin”
  - Get root access
- Security Impact
  - Amazon released a firmware update that will brick the device if it discovers that it has been rooted
  - For unpatched devices, root access can be gained

# Company G – Smart Meter

- Functionality
  - Power consumption collection
  - Wireless transfer the measurement

# IoT Security Challenges

- Lacking Protection
  - Large amount of IoT devices
  - Time-to-market dominates
  - Lacking security standard and specification
- Solutions
  - Understand the IoT vulnerabilities
  - Develop rules to eliminate/migrate vulnerabilities
- Standard Testing Toolset
  - Automated trigger generation
  - Systematic device security analysis
  - Security report generation

# Attack Surface

- A description of the attack surface
- Threat agents
- Attack vectors
- Security weaknesses
- Technical impacts
- Business impacts
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid the issue
- Design-for-security

# Security Rule Check - IoT

*数据驱动安全*

# Conclusions

- Metrics and rules for the discussed vulnerabilities
- New vulnerabilities through smart device analysis
- SRC tools
- Low-cost mitigation techniques

**Goal: An automated IoT device security checking framework and toolset to validate the security of any IoT devices momentarily.**

# Questions?

## Thanks!

Yier Jin
University of Central Florida
Email: yier.jin@eecs.ucf.edu