Internet of Things and Physical Vulnerabilities

By

Michael Goltz

System Security 6930

University of South Florida

Fall 2016

Internet of Things and Physical Vulnerabilities

- What are IoT's?
- How are they connected?
- What is at risk?
  - People, companies, cities, nations, …?
- Reports
- Solutions

What are IoT's?

Kevin Ashton at MIT’s AutoID lab

1999 article for the RFID Journal, Ashton wrote:

> “If we had computers that knew everything there was to know about things—using data they gathered without any help from us -- we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers to observe, identify and understand the world—without the limitations of human-entered data.”

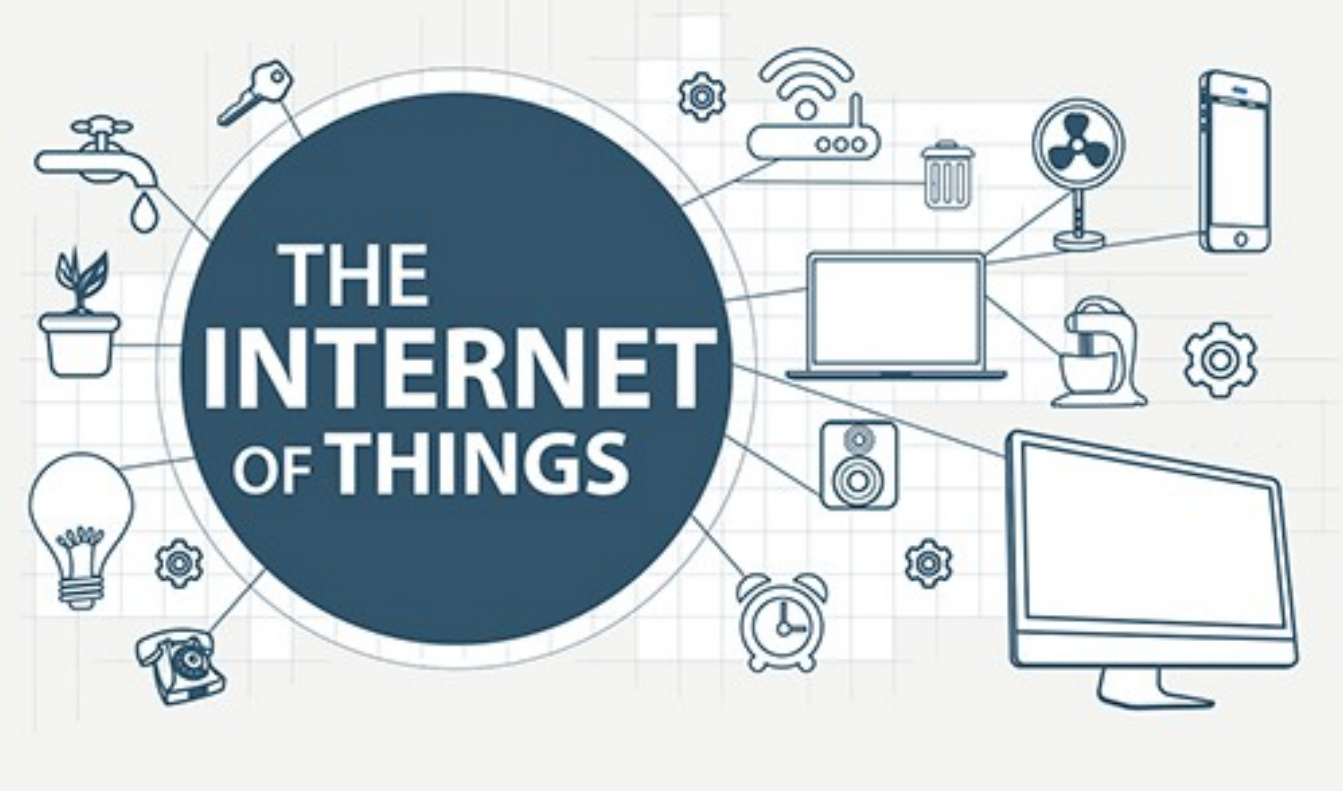
What are IoT's?

Under the Internet of Things Global Standards Initiative, IoT can be defined as:

> “A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.”

What are IoT's?

Can you think of any?

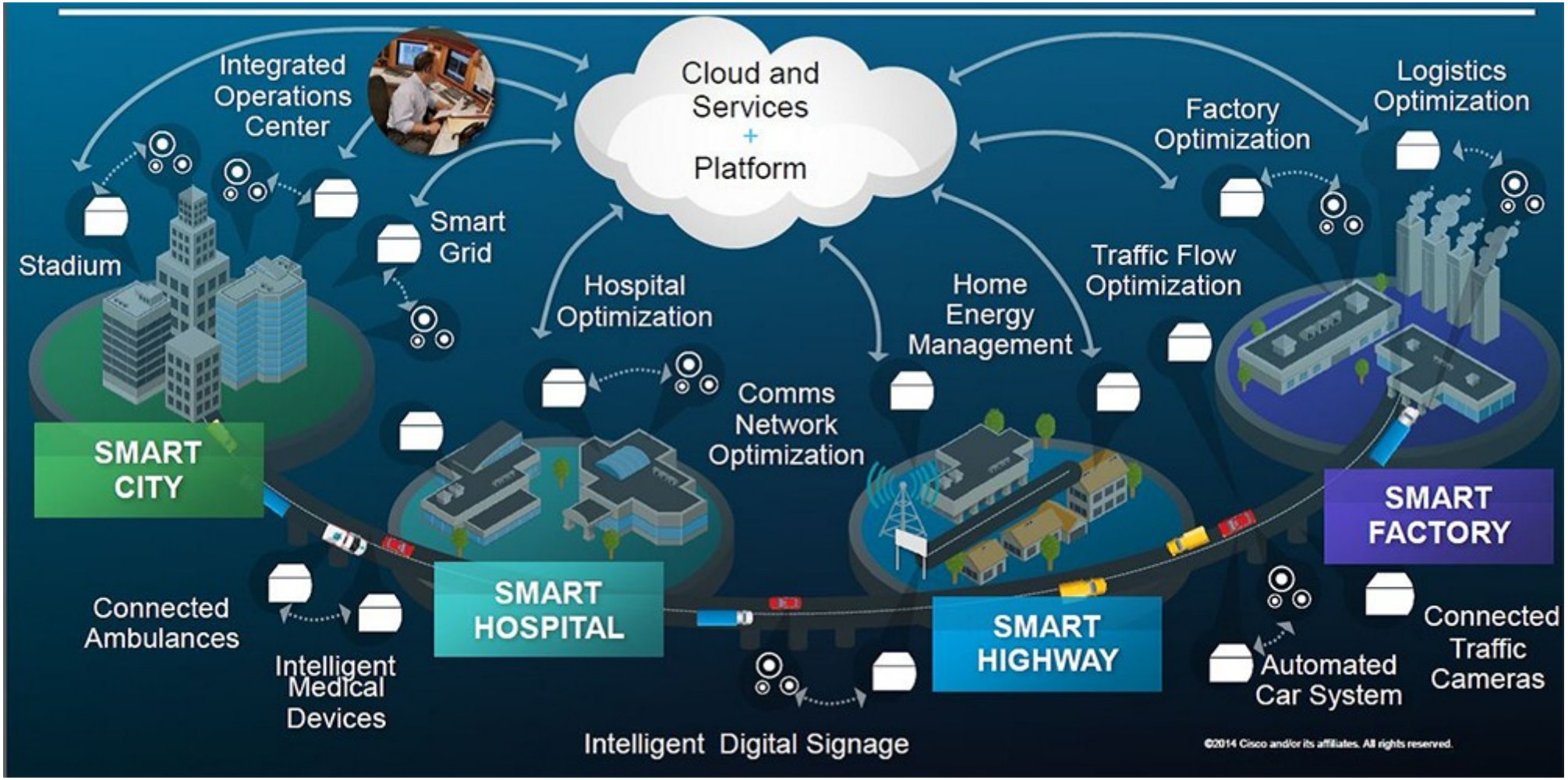


What are IoT's?

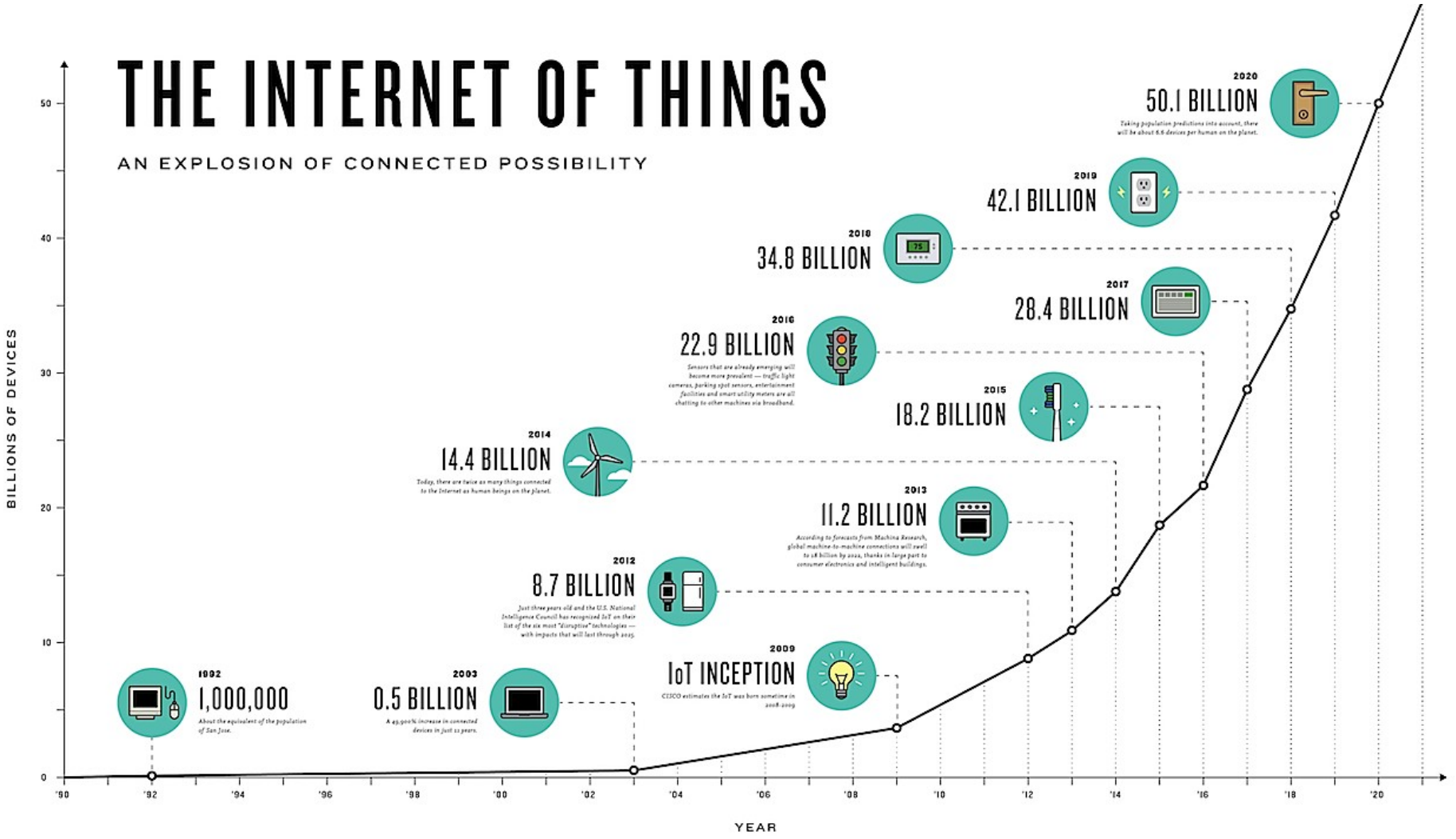
Can you think of any?

- Smart grids
- Smart cities
- Smart homes
- Intelligent transportation
- Devices
- Automated Houses
- Factories
- Businesses
- Autonomous Cars

What are IoT's?



What are IoT's



How are they connected?

Interconnecting things based on existing and evolving interoperable information and communication technologies

Wireless and wired Internet connections

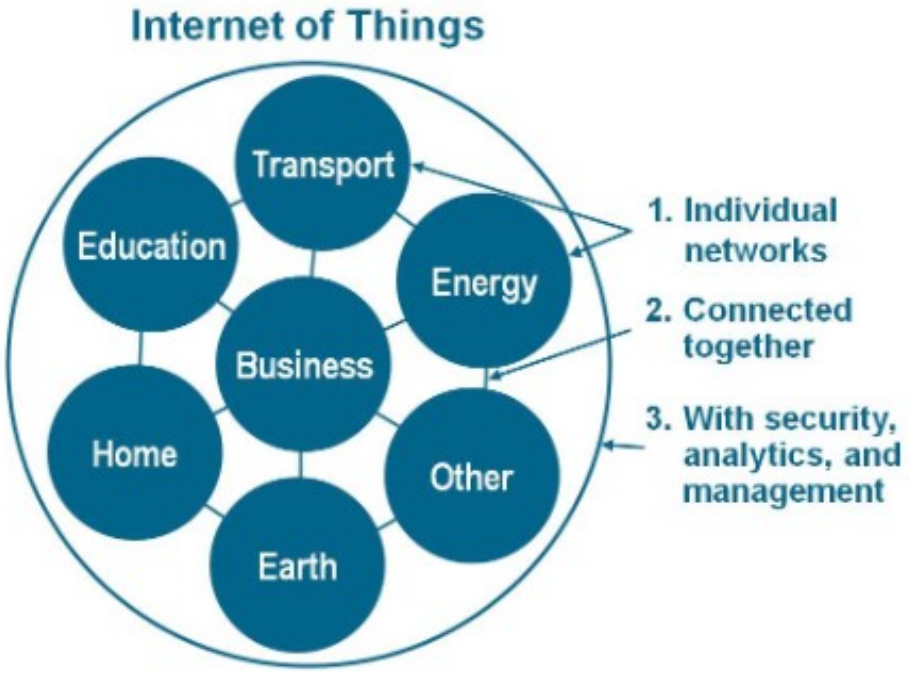
Local area connections: RFID, NFC, Wi-Fi, Bluetooth, and Zigbee

Wide area connectivity such as GSM, GPRS, 3G, and LTE

How are they connected?

IPv6 allows us to assign a communications address to billions of devices.

Electronic companies are building Wi-Fi and cellular wireless connectivity into a wide range of devices



Source: Cisco IBSG, April 2011

How are they connected?

Media - Big Data and Data Capture for targeting consumers

Environmental monitoring – remote sensing and monitoring spaning on a large geographical scale, i.e. water, atmosphere, soil quality. Wildlife tracking. Earthquake and tsunami early warning systems

Infrastructure management - Monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms. As well as control critical infrastructure like bridges to provide access to ships

Manufacturing - Digital control systems to automate process controls

How are they connected?

Energy Managment – electric company monitoring energy consumption and remotely control devices from AC, ovens, lighting conditions.

Medical and healthcare – wearable monitors and notification systems, Fitbit, pacemaker, blood pressure, heart monitors

Building and home automation – programmable and remote accessable cameras, dimmers, appliances, …

Transportation – electronic toll collection systems, vehicle controls, fleet management, inter and intra vehicular communication

What is at risk?

People, companies, cities, nations, …?

Traditional IT environments favor:

- confidentiality and availability

IoT environments favor:

- availability and integrity requirements

What is at risk?

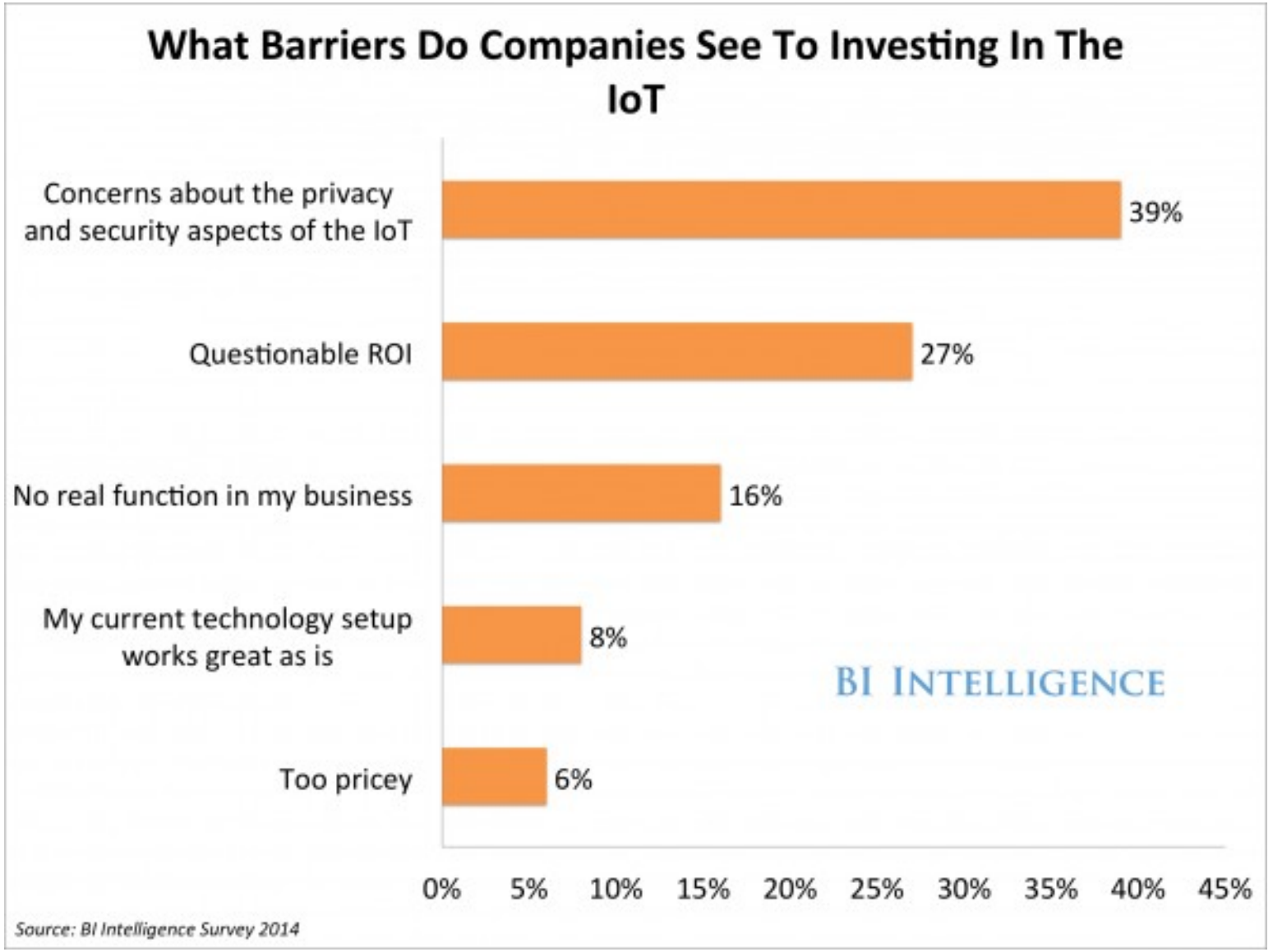
Physical and economic impact is a reality in IoT networks

Significant implications for IoT operators:

- Energy
- Manufacturing
- Smart-cities
- Transportation

Exploited networks can result in human injury and supply-chain disruption

What is at risk?



What is at risk?

Community impact at the federal, state, and local municipality levels

According to DHS, hackers could manipulate:

- the function of intersections, on ramps, toll plazas, interchanges and other critical components across a city.

Affecting a city's transportation grid for extended periods of time.

What is at risk?

Top 5 IoT Vulnerabilities:

- Insecure Web Interface
- Poor Authentication
- Poor network Services
- Lack of Encryption
- Poor Physical Security

Reports

January 2014 article in *Forbes*, by cybersecurity columnist Joseph Steinberg

Many Internet-connected appliances that can already "spy on people in their own homes" including televisions, kitchen appliances, cameras, and thermostats.

Reports

SANS 2014 survey: “Breaches on the Rise in Control Systems”

2014 – 27% of the respondents indicated a breach or infection in their control system environments

Up from 20% the previous year

Reports

DEF CON 2016

- 47 new vulnerabilities in 23 IoT devices

Types

- Hard coded passwords
- Buffer overflows
- Command injection

Reports

Door locks and padlocks

- Quicklock, iBlulock, Plantraco, Ceomate, Elecycle, Vians, Lagute, Okidokeys, Danalock

Vulnerable to:

- Password sniffing
- Replay attack

Reports

Solar array management device from Tigro Energy

- Hard coded password
- Command injection flaw
- Open access point connect
- Lack of network segmentation

Could lead to the shut down of a power plant!

Reports

Charlie Miller and Chris Valasek

Reports

2013, with a Ford Escape and a Toyota Prius connected to the onboard diagnostic port

- Disabled brakes
- Honked the horn
- Jerked the seat belt
- Commandeered the steering wheel

Reports

2015 Uconnect Web Flaw

Uconnect is a In-Car Internet connected service:

- wi-fi hot-spotwith a 150 foot range via a 3G EV-DO cellular network
- bluetooth for cell phones
- a hard drive
- Sirius TV and satellite
- GPS

Reports

At the time they thought they could exploit Uconnect:

- enable attacks over a direct Wi-Fi link, confining its range to a few dozen yards
- work only on vehicles on the same cell tower scanning using a cell phone a few dozen miles away
- It could be done anywhere, over the Internet

Reports

Uconnect’s cellular connection lets anyone who knows the car’s IP address gain access from anywhere in the country

- Dodge Ram, in Texarkana, Texas
- Jeep Cherokee driving around a highway cloverleaf between San Diego and Anaheim, California
- Dodge Durango, moving along a rural road somewhere in the Upper Peninsula of Michigan

Reports

Uconnect computers are linked to the Internet by Sprint's cellular network, and only other Sprint devices can talk to them.

Reports

Rewrote the chip’s firmware to plant their code

Allowing them to send commands through the car’s internal computer network known as a CAN bus

- vehicle bus standard (a message-based protocol)
- allows microcontrollers and devices to communicate with each other without a host computer

Control physical components like the engine and wheels

Reports

Brakes disabled

Reports

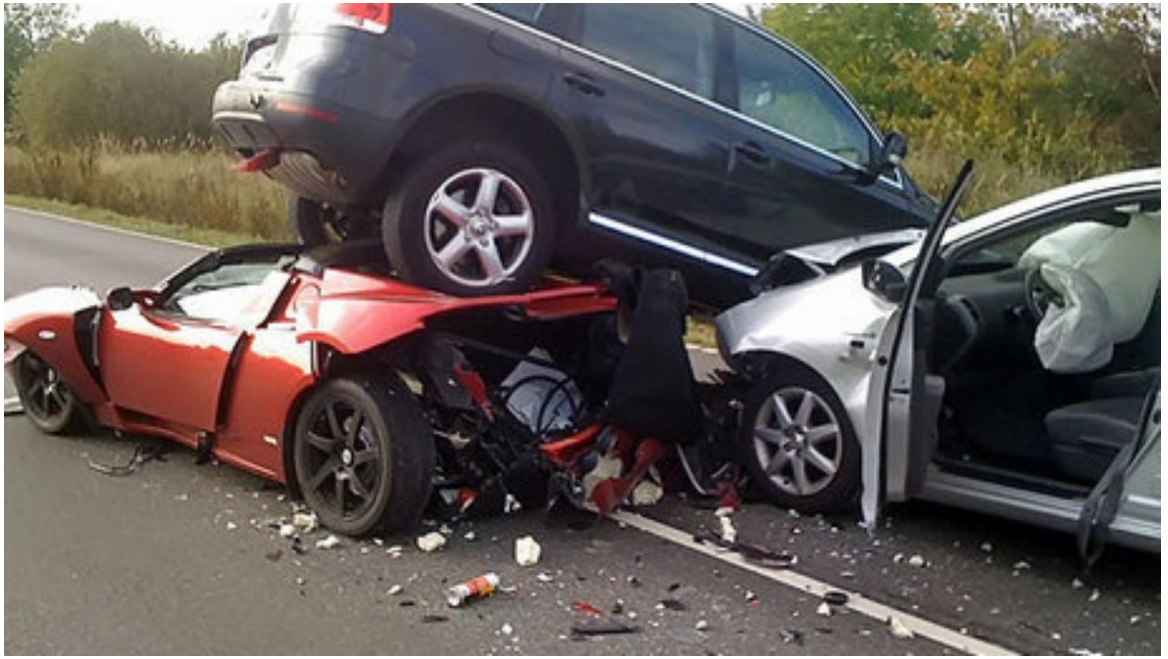
Full arsenal includes:

- at low speeds fully kill the engine
- abruptly engage the brakes, or disable them
- hijack the wheel when the Jeep is in reverse
- track a targeted Jeep’s GPS coordinates

Reports

Scanning is slow and random

- take over a group of Uconnect computers
- perform more scans by creating a wirelessly controlled automotive botnet



Solutions

Senators Ed Markey and Richard Blumenthal proposed a new digital security standards bill for cars and trucks

National Highway Traffic Safety Administration and the Federal Trade Commission

- federal standards to secure our cars and protect drivers' privacy
- → setting new security standards
- → creating a privacy and security rating system for consumers

Solutions

National Highway Traffic Safety Administration (NHTSA) released voluntary best practices on cybersecurity for automakers

- Well-documented penetration testing
- Encryption on all communication between the car and manufacturer
- Limited access to Engine Control Units

Solutions

Five Recommendations:

1) Safer design to reduce attack points
2) Third-party testing
3) Internal monitoring systems
4) Segmented architecture to limit the damage from any successful penetration
5) Same Internet-enabled security software updates

Questions or Comments

Internet of Things and Physical Vulnerabilities

By

Michael Goltz

System Security 6930

University of South Florida

Fall 2016