Tuck School of Business at Dartmouth

CENTER FOR DIGITAL STRATEGIES:
MBA FELLOWS PROGRAM

Securing the Internet of Things

Mandakini Saroop

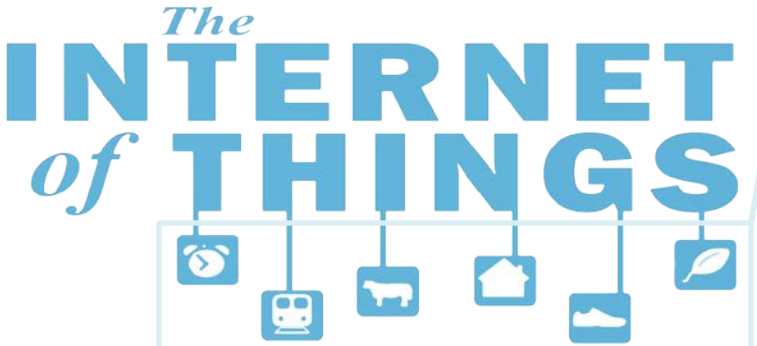
Agenda

- Overview of the Internet of Things
- Major security concerns and vulnerabilities
- Securing the internet of things
- Conclusion and summary

Internet of Things: an overview

"The Internet of Things (IOT) refers to uniquely identifiable objects and their virtual representations in an Internet-like structure."

- Wikipedia



Applications of the Internet of Things

Home and Safety

- Kitchen and home appliances
- Lighting and heating/HVAC
- Safety monitoring (video cameras, sensors)

Health and Fitness

- Fitness wearables like FitBit
- Pulse, blood pressure, blood sugar monitoring
- Fitness data collection like Nike Fuel and Runkeeper

Transportation

- Smart transportation solutions (traffic signals, smart parking)
- Streamlined operations at airports, railroads, roadways
- Fleet service management, including maintenance, monitoring, navigation, etc.

Industrial

- Connected industries to control flow of materials
- Oil & gas to check for flow interruptions
- Cost control by monitoring and controlling electricity usage

Security concerns and vulnerabilities

"Yet as we connect more and more devices to the Internet, everything from the thermostat to the toilet to the front door itself may create a potential new opening for electronic intruders." – MIT Technology Review, August 2013

- Data about usage can reveal whether a person is present at home or not
- Automated home system can be cracked into, allowing intruders entry into the home
- Video feeds of homes allow attackers access to private information about individuals

More security concerns and vulnerabilities

"Even with current campaigns, attackers are able to relatively easily penetrate enterprise defenses. Now imagine the volume of attacks increased by [ten-fold]... and no one could turn off the sending devices." – Kevin Epstein, Proofpoint

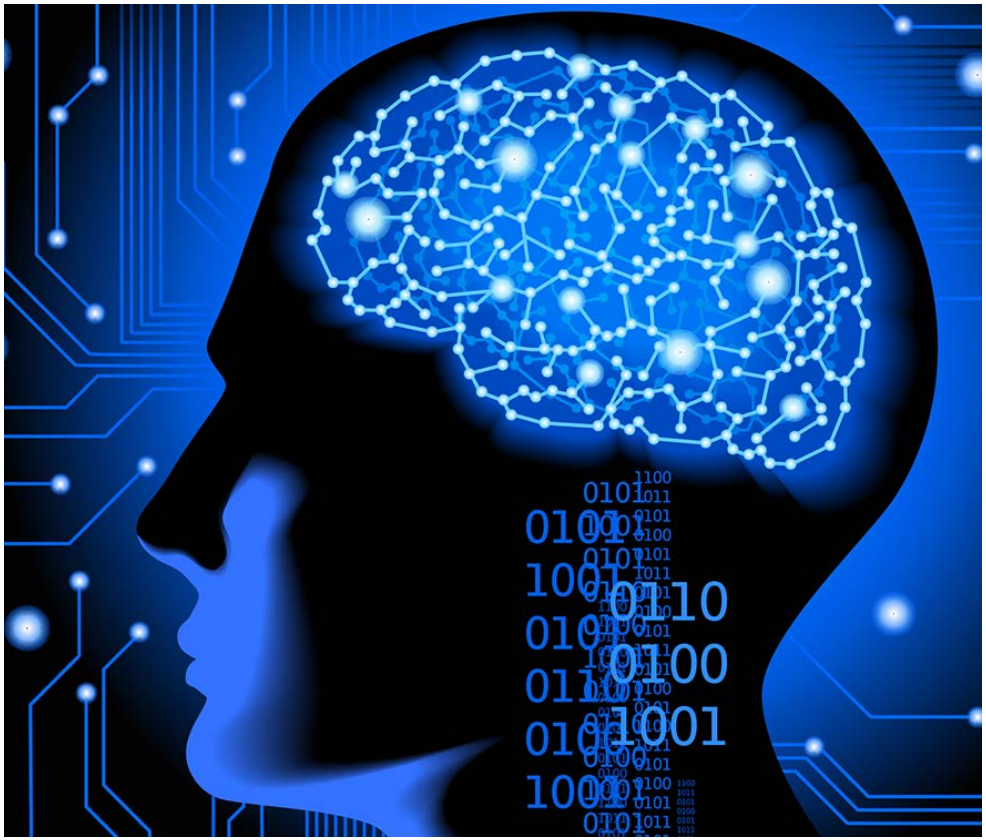
- Proliferating number of endpoints gives attackers multiple points of entry into previously tightly controlled industrial systems
- Even attacking home systems to drive up electric consumption can bring down a grid
- Hacking remote sensors in oilfields can bring flow of oil and gas to a halt
- Commercial espionage will become much easier

Devices connected to IoT are not very secure

"How many of those net-connected doodads are secure? The answer: none of them" – Jason Bloomberg

- Too many endpoints to monitor
- Passive devices like RFID tags and sensors can be read easily
- Low-energy devices do not have power or storage to negotiate complicated handshake protocols or store encryption keys
- Machine-to-Machine communication dictates a certain level of trust
- All devices have IP addresses which means they can be discovered and hacked
- Very few countries have regulations for internet-compatible devices
- Ease-of-use is preferred over security when designing IoT compatible devices
- No identity or permissions management

Threat intelligence and business model awareness to control security for IoT



Threat Intelligence

- Too many devices to monitor, especially with growing number of cheap sensors
- Being aware of attack patterns and taking measures to secure beforehand will be key
- Being aware of attack patterns will also help design future devices with vulnerabilities in mind

Business Integration with IoT

- Being aware of the business strategy and using it to intelligently design integration with Internet of Things will prove key to security
- Easy to get carried away with connecting everything to the internet
- Managing business processes so that information flow is carefully handled when transmitting over a network (especially from device-to-device for IoT)

Managing devices and vendors will also help control security vulnerabilities in IoT

Vendor Management

- The vendors and suppliers of IoT devices need to be tightly controlled to maintain quality and security standards
- Streamline vendors in order to reduce risk of improperly designed or compromised devices

Device Management

- Too many devices to monitor, especially with growing number of cheap sensors
- Better to implement security protocols now and build devices compliant with security protocols than to retrofit devices
- Build in basic permissions management to revoke permissions to a device not authorized to the network any longer

Integrating security measures into the application itself will also help control security

Application Security Measures

- Building security measures into the application itself that leverages IoT will go a long way towards controlling security issues
- This includes:
  - Secure handshake protocols between communicating devices
  - Identity and access management
  - Secure connection protocols between all devices
  - Storing all identifiable information on servers instead of devices
- Making decisions that allow applications to be user-friendly while remaining secure

Case study of a secure network protocol: ZigBee

ZigBee Alliance

ZigBee offers green and global wireless standards connecting the widest range of devices to work together intelligently and help you control your world.

COMCAST freescale Itron Kroger Landis+Gyr manage energy better legrand PHILIPS Schneider Electric SILICON LABS Texas Instruments iControl Time Warner Cable IntelligentHome

ZigBee Alliance – Security Standards

- Integrated AES 128 encryption for sensitive information (PII)
- Server driven – no information on handheld devices
- Automatic and secure network registration using pre-installed keys or standard public-key cryptography
- Regional regulatory compliance for healthcare applications
- Device authentication supported

Conclusion

- Security for IoT is still in its infancy, but definitely a concern
- Secure protocols like ZigBee need to be followed stringently to allow a secure IoT experience
- Device authentication and access management is a big issue
- With protocols like ZigBee and commercial solutions like Cisco's, IoT security should ramp up to same levels as computer security

Thank you!

Questions?

Sources and citations

- http://en.wikipedia.org/wiki/Internet_of_Things
- http://www.businessinsider.com/heres-how-people-will-actually-use-the-internet-of-things-2014-4
- http://www.businessinsider.com/growth-in-the-internet-of-things-2013-10
- http://www.digi.com/blog/healthcare/connecting-your-body-with-the-internet-of-things/
- http://www.cisco.com/web/strategy/transportation/intelligent_trans.html
- http://www.technologyreview.com/news/517931/more-connected-homes-more-problems/
- http://cloudcomputing.sys-con.com/node/2868551#.UoPMJ0ljnNY.twitter
- http://www.ecommercetimes.com/rsstory/79438.html
- http://www.cbronline.com/news/security/how-the-internet-of-things-is-life-endangering-4206796
- http://www.computerworld.com.au/article/542300/6_ways_internet_things_will_transform_enterprise_security/
- http://www.vidyo.com/wp-content/uploads/The-Internet-of-Things-A-Study-in-Hype-Reality-Disruption-and-Growt....pdf
- http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in-the-internet-of-things.pdf
- https://www.zigbee.org/
- Personal interview with Adam Mayer, Time Warner Cable IntelligentHome: http://www.youtube.com/watch?v=-aRTGtS5sRk