The Principles of IoT Security
A Hands-on Course

Class 1: Intro to IoT Security

January 30, 2017

Charles J. Lord, PE
President, Consultant, Trainer
Blue Ridge Advanced Design and Automation

Presented by:

DesignNews

Blue Ridge Advanced Design and Automation
Asheville, North Carolina

CEC CONTINUING EDUCATION CENTER

Digi-Key ELECTRONICS

This Week’s Agenda

1/30 Intro to IoT Security

1/31 Hardware Security Challenges

2/1 Data Security

2/2 Network Security

2/3 Other Security Issues in the IoT

Ericsson:

- “We have a vision of 50 billion connected devices by 2020”

- “Anything that benefits from being connected will be connected”

- IoT Devcon, 2014

Main Markets

- Building Automation
- Industrial Automation
- Lighting
- Commercial Transportation / Fleet Mgmt
- Enterprise Asset Management
- Smart Cars
- Test and Measurement
- Energy Grid (Smart Grid)

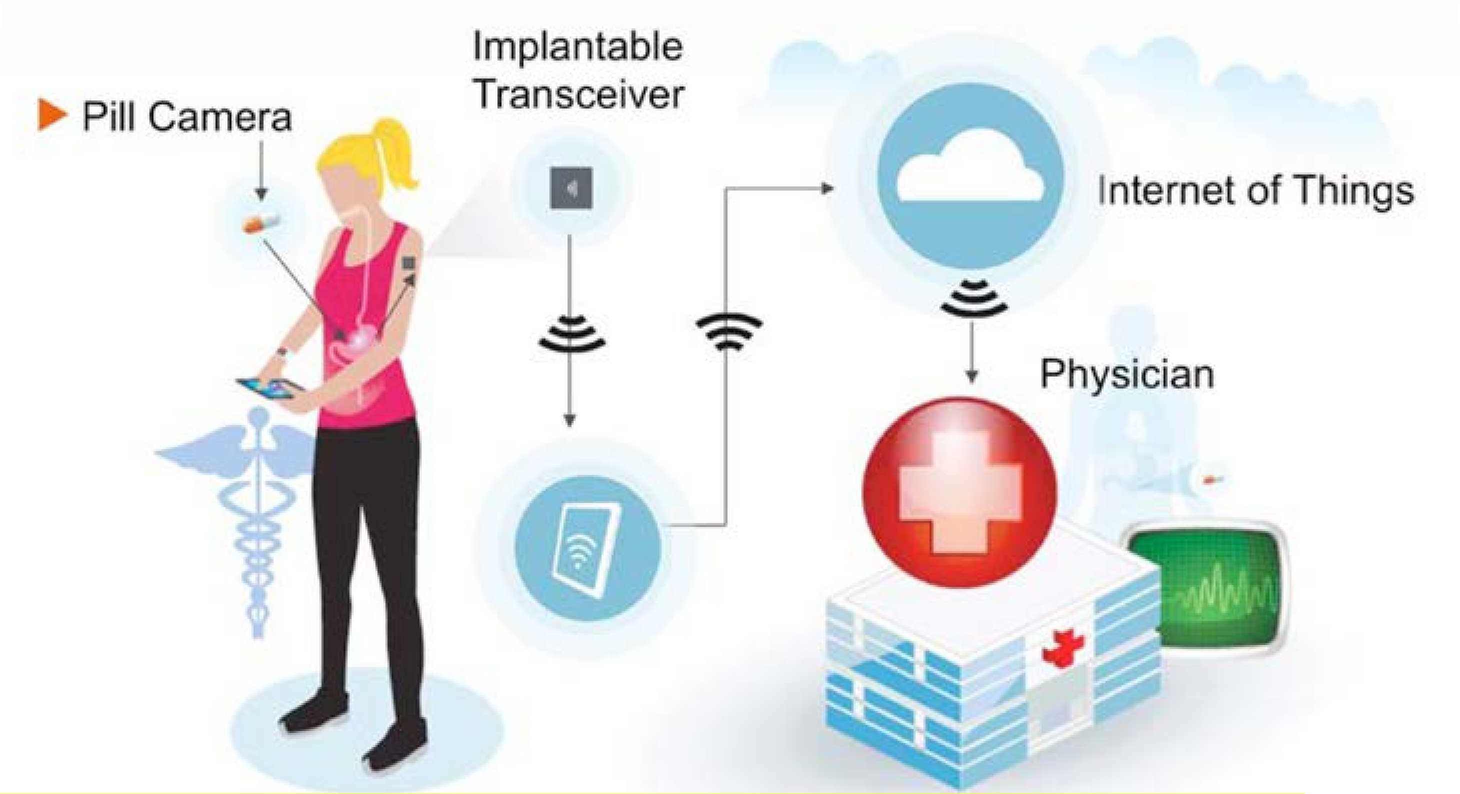
What to do with all this data??

- "to the Cloud!!"
- Big Data principles
- Privacy, security will be huge areas for development
- Regulatory issues that must be met today and in the future
- Sampling and Monte Carlo
- Trends, patterns

Growth Areas

- Sensors
- Product tracking from supply chain to end-of-life
- Medical
- Auto
- Protocols and bridging between protocols
- What to do with data overload – communications, analysis, storage

Medical Example



Question 2 – What are some other medical devices for the IoT?

The ‘Ten’

- The following nine slides are from Bill Montgomery’s LinkedIn blog, “The 10 Most Terrifying IoT Security Breaches you aren't aware of (so far)”
- There are only nine as one was later proven incorrect…

Nuclear Facilities

The US National Nuclear Security Administration who are responsible for managing and securing their nation's nuclear weapons stockpile, experienced 19 successful cyber attacks during the four-year period of 2010 - 2014. Also as many of you are aware, in June 2010, Stuxnet, a nasty computer worm designed to attack industrial programmable logic controllers (PLCs), was discovered. PLCs allow the automation of electromechanical processes like centrifuges (which are used separating nuclear material). The Stuxnet attack was purportedly launched to sabotage the uranium enrichment facility in Natanz, Iran, and many experts believe that Stuxnet destroyed up to 1,000 centrifuges (10%) before it was discovered and removed. Stuxnet, in the view of many, set the template for future attacks not only on nuclear facilities, but on everything that uses PLCs, from factory assembly lines to amusement park rides. *(The wild rollercoaster rides that dot amusement parks worldwide just got a whole lot scarier...)*

Steel Mills

Germany’s Federal Office for Information Security (BSI) recently issued a report that confirmed that hackers had breached a steel plant in their country and compromised numerous systems, including components on the production network. As a result, mill personnel were unable to shut down a blast furnace when required, resulting in “massive damage to the system.” The BSI report stated, “The know-how of the attacker was very pronounced not only in conventional IT security but extended to detailed knowledge of applied industrial controls and production processes.” *(Makes one wonder if this breach was perpetrated by a former, disgruntled employee. That would bring a whole new [chilling] meaning to the term “going postal...”*)

Energy Grid

According to a June 2015 Congressional Research Service (CRS) report, attacks on the U.S. power grid system are “increasing,” with hackers stepping up efforts to penetrate critical systems and to implant malicious software that could compromise the power grid and result in a nationwide crisis. Attackers successfully compromised U.S. Department of Energy computer systems more than 150 times between 2010 and 2014. (*What really took down the Northeast power grid in Canada and the US back in 2003? The blackout was attributed to software bug in the alarm system. Was it really a “bug?” Or, could it have been a virus embedded by a dangerous cybercriminal?)*

Hospitals

Recently a news bulletin revealed that hackers had broken into the massive hospital network of the University of California, Los Angeles, accessing computers with sensitive records of 4.5 million people. That is worrisome, but it seems that the public reaction is akin to news about other reported cybercrimes that have led to the extraction of personal records. Joe Public said, “It feels like a daily occurrence, and unless I’m personally impacted, I don’t really care.” *(I get that, and maybe it takes something even more personal to raise Joe’s concern level when it comes to a hospital being hacked. How about this, Joe?)* In an unprecedented move, last month the US FDA directed hospitals to stop using Hospira's Symbiq Infusion System because it can be remotely accessed by hackers, allowing the unauthorized user "to control the device and change the dosage the pump delivers, which could lead to over - or under-infusion of critical patient therapies.” *(Imagine resting in a hospital bed and being attacked by an invisible enemy thousands of miles away...)*

Building Infrastructure

The Department of Homeland Security recently disclosed a 2012 breach in which cybercriminals managed to penetrate the thermostats of a state government facility and a manufacturing plant in New Jersey. The hackers exploited vulnerabilities in industrial heating systems, which were connected to the Internet and then changed the temperature inside the buildings. *(On the surface, that might seem harmless, but think about the damage that cybercriminals could do with unfettered access to the controls that govern most major buildings today. The smart building might not seem so smart if for example, the bad guys activate the water sprinkler systems in a data centre or mess with the elevators.)*

Oil Rigs

According to a 2014 Reuters report, hackers shut down a floating oil rig, by tilting it, while another rig was so riddled with computer malware that it took 19 days to make it seaworthy again. The report notes that while the number of known cyber attacks at sea is currently low, the industry is likely to become a serious target due to its size and scale: 90 percent of global trade is estimated to be sea-bound, and increased container ship size means that company losses could exceed $1 billion for a single vessel. *(Picture a cruise ship being hacked and sent on a direction that would leave its passengers "lost at sea" with no way of returning to port under their own power).*

Firearms

TrackingPoint makes a smart rifle that lets you digitally "tag" a target, and then locks the trigger until the gun is perfectly positioned to hit it (from up to a half mile away). It also connects to smart phones or tablets so a buddy (or accomplice) can view what the shooter sees in the scope. Now, security researchers have discovered software flaws in the computerized rifle. Anyone near enough for a Wi-Fi connection to a rifle can remotely tinker with its controls. In the worst case, a hacker could force a police sniper to miss while shooting directly at a hostage-taking criminal -- and hit the hostage instead. Or a hacker could simply lock the rifle's controls, rendering it useless. *(Now, imagine all law enforcement weapons connected in the emerging IoT world - and all easily hacked by the bad guys because the manufacturers embedded dated [or no] security. It's not a pretty picture.)*

Airplanes

I did refer to the serious breach of an airplane while in flight earlier in this post and hadn’t intended to provide much more insight into this breach as I referred to it in an earlier blog. But something is bugging me, so I have to throw it out there. Debris from the wreckage of Malaysian Air Flight MH370 has now being discovered, indicating that the plane and its 239 passengers went down in the Indian Ocean. What’s still unknown is what caused the plane to alter its flight path. The investigations into the pilot, co-pilot and other crew members turned up nothing to suggest that they were responsible for the crash. So, what then? (*Could this be a case where somebody hacked into the aircraft controls while on the flight or from afar, and took the plane down? That is a terrifying scenario that nobody is talking about. Well, maybe Chris Roberts - the guy who commandeered the United Airlines Flight after hacking into the flight control system through the entertainment system and who also claims to have altered the temperature on the International Space Station.)*

The Kitchen

Yes, one might argue that this is not as big a threat as the first 9 breaches on this list, but I just couldn’t resist adding it. After all, we are talking about a place associated with one of the key components of the physiological layer in Maslow’s Hierarchy of Needs – food. This breach that recently occurred in the UK boggles the mind. Hackers attacked IoT-connected devices in kitchens across the country, with almost comical outcomes. Smart toasters are forcing consumers into reconsidering eating habits by refusing to toast any bread that isn’t considered ‘healthy’. Smart Fridges and freezers across the UK are shutting down as soon as ice cream is detected. *(The message is abundantly clear. Leave that white bread on the grocery store counter and stock up on whole wheat, and while you’re there, put down those high-fat/high-calorie frozen goodies in favour of good old wholesome fruit).*