National Aeronautics and Space Administration

Ames

Discovery Innovations Solutions

The Lighter Side of Things: The Inevitable Convergence of the Internet of Things and Cybersecurity

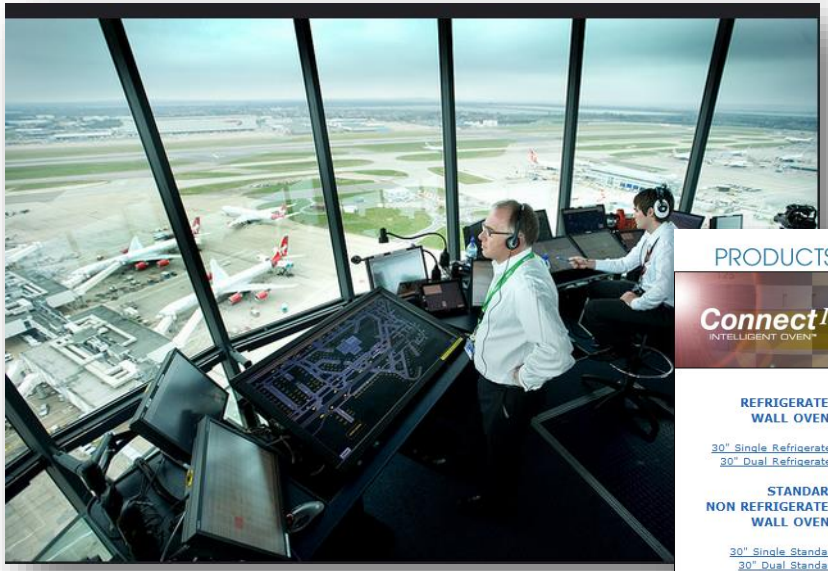
Jerry Davis, Director, Information Technology and CIO
NASA Ames Research Center

GITEC
April 2, 2017

Agenda

- NASA In the Mix of Things
- Of Things to Come!
- IoT and the Inevitable Convergence of Cybersecurity
- Why IoT in Cyberspace will Flourish as a “Contested” Environment
- The Cybersecurity Professional Hiring Dilemma
- What needs to Happen on the Educational Front
- Graphics Credits

NASA In the Mix of Things….



PRODUCTS: PROFESSIONAL COOKING SOLUTIONS for your KITCHEN

Connect Io™ INTELLIGENT OVEN™

REFRIGERATED WALL OVENS

30" Single Refrigerated
30" Dual Refrigerated

STANDARD NON REFRIGERATED WALL OVENS

30" Single Standard
30" Dual Standard

Refrigerated Ovens

COOL › CONNECT › COOK

PS301SS00 30" Refrigerated Single Wall Oven

(Zoom Image)

PS302SS00 30" Refrigerated Dual Wall Oven

(Zoom Image)

Standard Ovens

CONNECT › COOK

PS301SS01 30" Non Refrigerated Single Wall Oven

(Zoom Image)

PS302SS01 30" Non Refrigerated Dual Wall Oven

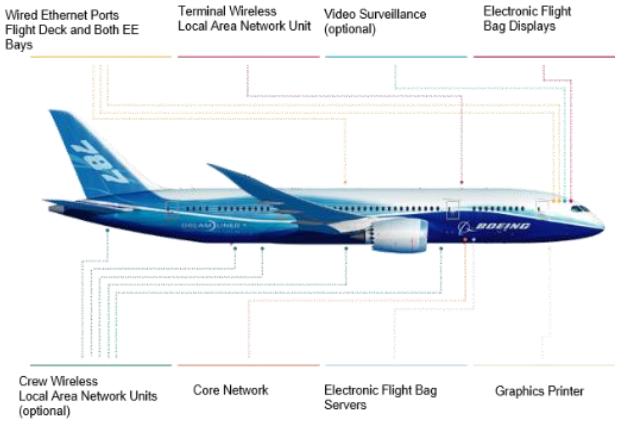
(Zoom Image)

The World's Finest Professional Cooking Ovens. Telephone, Cell Phone, and Internet Command & Control. Modern space age convenience finally arrives in your home with the Connect Io Intelligent Oven, Professional Series: The world's finest cooking oven, and first appliance that allows you to refrigerate foods for cooking later, then connect remotely via phone or Internet—delivering the great taste of traditional cooking at home whenever you are ready. State-of-the-art cooking, luxury conveniences, exceptional performance, and beautiful design are the hallmark of Connect Io wall ovens that households and professional chefs insist on, and that we deliver.

Of Things to Come!

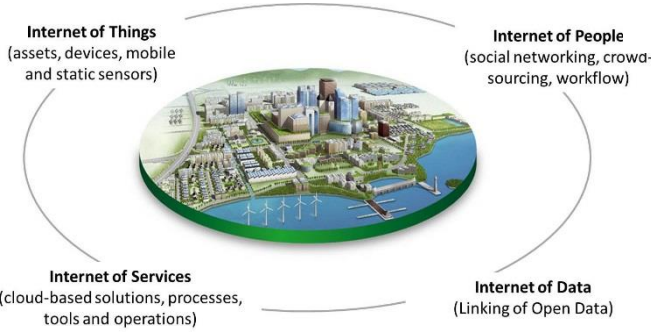
According to a 2011 Cisco white Paper "*The Internet of Things: How the Next Evolution of the Internet is Changing Everything*", there will be 50 BILLION connected to the Internet by the year 2020!

- The IoT brings great promise to the lives of mankind:
  - Promotes efficiency in our day-to-day lives through data analytics collected by IoT sensors;
  - Underpins the realization of *sustainability* by the creation of smart cities that use IoT technologies and;
  - Will bring about a new level of safety as connected vehicles provided greater awareness and avoidance of potentially hazardous situations.



eConnected Aircraft

IoT enabled Sustainable Cities



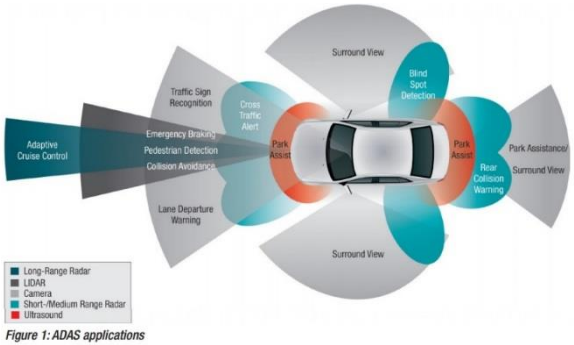


Figure 1: ADAS applications

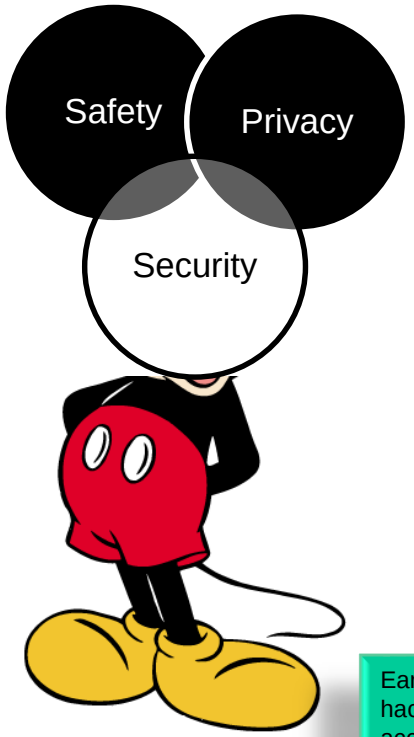
eConnected Cars

IoT and the Inevitable Convergence of Cybersecurity

Just as the IoT brings with it the promise of improving the lives of people everywhere, it also brings with it convergence of cyber insecurity and potentially catastrophic implications to safety and privacy anywhere.

July 2015, two security researchers remotely took over a Jeep Chrysler from a distance of 10 miles. The researchers access the vehicle over the cellular system and controlled the vehicle through its onboard infotainment system.

August 2015, FDA issues an alert that certain infusion pumps were vulnerable to remote hacking.



April 2015, security researcher Chris Roberts detained by FBI after tweeting about taking over the flight controls of a commercial aircraft during flight. Roberts was subsequently banned by United Airline from flying on their aircraft.

Early 2013, Iranian hackers remotely accessed a small flood control damn 20 miles north of NY City

Why IoT in Cyberspace Will Flourish as a "Contested Environment"

By the year 2020, the cyberspace will be a completely contested environment. Contested meaning that hostile individuals or groups will have the explicit intent and the means to disrupt, degrade or destroy activities that take place in, or connect through, cyberspace.

- The more connected things that move into the cyberspace domain without appropriate safeguards built in, the more susceptible to compromise they will become;
- 60 years of poor software development processes continues to be the primary attack vector;
- The security skills required to keep up with innovation and the speed to market is significantly behind:
  - Security engineers – Those who can "bake" security into the system development process (proactive);
  - Software Assurance engineers – Those who can implement secure coding practices into software (proactive) and;
  - Cyber Defenders – Those who have know how to identify, protect, detect, respond and recover from security events and incidents (reactive).

The Cybersecurity Professional Hiring Dilemma

The demand for cybersecurity professionals at every level is high, yet the supply pipeline is dribbling:

- According to the Bureau of labor statistics, between 2012-2022 the growth rate for cybersecurity professionals will be 37%;
- Mike Brown, CEO of Symantec suggested in 2015 that the global demand for cybersecurity professionals will grow to 6 million by 2019, but there will be a shortage of 1.5 million professionals;
- Competition is stiff in many markets. Companies regularly “poach” cybersecurity professionals from their competitors
  - Professionals can earn anywhere from $90k per year with just a year or two of experience to $300k per year with less than 10 years of experience.
  - In rare cases, some professionals are making nearly $1M per year.
- The federal government has a particularly tough time competing from a salary perspective
  - NASA is not immune. While our brand is arguably one of the most recognizable and strongest, keeping solid performers in this market is extremely challenging and;
  - We can’t compete with salaries, so we have to be creative to attract and retain good candidates.

What Needs to Happen on the Educational Front

Education that produces top-shelf cybersecurity professionals will be the pervasive underpinning to ensuring a secure IoT and cyber environment.

- STEM courses are paramount. While cybersecurity policy based education is needed, it alone won't ensure secure systems;
- Security engineering, Security software assurance, computer science, mathematics (the hard stuff) and the like are gaps in skills that need to be filled from here to fore;
- Cyber principles must be taught earlier (kindergarten) in the education ecosystem. Hands on education should follow shortly there after and continue throughout the post secondary educational years and;
  - Follow the National Centers for Academic Excellence model at the middle school and high school level.


NIST Special Publication 800-160
Initial Public Draft

Systems Security Engineering
An Integrated Approach to Building Trustworthy Resilient Systems

RON ROSS
JANET CARRIER OREN
MICHAEL McEVILLEY

NIST
National Institute of Standards and Technology
U.S. Department of Commerce