November 2015
Federal Internet of Everything Summit Report

December 15, 2016

Tim Harvey and Tom Suder
The Advanced Technology Academic Research Center

Karen Caraway, David Crabtree, Casey Creech, David Keppler, Nancy Ross
The MITRE Corporation[1]

[1] The authors' affiliation with The MITRE Corporation is provided for identification purposes only, and is not intended to convey or imply MITRE 's concurrence with, or support for, the positions, opinions or viewpoints expressed by the authors.
Approved for Public Release; Distribution Unlimited. 16-1770

Contents

1 Executive Summary

The inaugural installment of Federal Internet of Everything (IoE) Summit, held on November 10th, 2015, included three MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions. These collaboration sessions allowed industry, government, academic, and MITRE representatives an opportunity to collaborate and discuss challenges the government faces in Internet of Things (IoT)/IoE). The working definition for the summit and collaboration sessions was: An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react. The goal of these sessions is to create a forum to exchange ideas and develop recommendations to further the adoption and advancement of the Internet of Things techniques and best practices within the government.

Participants representing government, industry, and academia addressed three challenge areas in federal IoT/IoE: IoT and Security, Architecting IoT Ecosystems, and IoT Driving Changing Dynamics.

This white paper summarizes the discussions in the collaboration sessions and presents recommendations for government and academia while identifying orthogonal points between challenge areas. For the sake of clarity, the term IoT is used throughout the paper when referring to IoT/IoE or IoE as used and defined above.

2 Introduction

During the inaugural Federal Internet of Everything Summit, held on November 10th, 2015 three MITRE-ATARC (Advanced Technology Academic Research Center) Collaboration Sessions gave representatives of industry, government, academic and MITRE the opportunity to discuss challenges the government faces in IoT. Experts who would not otherwise meet or interact used these sessions to identify challenges, best practices, recommendations, success stories, and requirements to advance the state of the Internet of Everything/Internet of Things and research in the government.

It also proposes a community built around government and industry collaboration with academia to leverage previously untapped academic resources. The proposed community will be fostered by MITRE and the ATARC to enable communications between the different participating communities. This community's outcomes include:

- Academia produces higher quality, better-prepared, and "industry-ready" graduates for hire;
- Government leverages graduate and undergraduate level research to help solve critical IoT challenges; and,
- Government organizations have an integrated research and advisory capability made up of commercial companies, academic institutions, and federally funded research and development centers (FFRDC)

The MITRE Corporation is a not-for-profit company that operates multiple Federally Funded Research and Development Centers (FFRDCs). ATARC is a non-profit organization that leverages academia to bridge between Government and Corporate participation in technology. The invited collaboration session participants across government, industry, and academia worked together to address challenge areas in the Internet of Everything/Internet of Things, as well as identify courses of action to be taken to enable government and industry collaboration with academic institutions. Academic participants used the discussions as a means to help guide research efforts, course development, and to help produce graduates ready to join the workforce, advance the state of the Internet of Everything research, and work in the government.

This white paper is a summary of the results of the collaboration sessions and identifies suggestions and recommendations for government, academia, and industry while identifying crosscutting issues between the challenge areas.

3 Collaboration Session Overview

Each of the three MITRE-ATARC collaboration sessions consisted of a focused and moderated discussion of current problems, gaps in work programs, potential solutions, and ways forward regarding a specific challenge area. At this summit, sessions addressed:

- IoT and Security;
- Architecting IoT Ecosystems; and,
- IoT Driving Changing Dynamics.

This section outlines the goals, outcomes, and findings of each of the three collaboration sessions.

3.1 IOT and Security Session

The *IoT and Security* session focused on examining the impacts and challenges on IoT security, as they relate to end points (hardware), applications and software, and IPv6 and networks. The goal of the joint session was to outline recommendations for addressing security impacts and challenges based on viewpoints from government, industry, and academia.

3.1.1 Session Goals

The goals of this session were to identify:

- Lowest trust level for devices in an IoT;
- Solutions for lowering the acceptable trust levels to accommodate non-traditional devices;
- Solutions for building in software assurance whereby reducing the "attack surface" of an IoT ; and,
- Required changes in "consent and knowledge" practices to protect security (and privacy) yet enable the IoT.

3.1.2 Challenges

The IoT and Security session identified several challenges or needs:

- Protect and harden the endpoint devices in IoT Systems
- Maintain the integrity and confidentiality of aggregated and raw data
- Identify and manage the unintended consequences created by conversion of personal, municipal, ambient, and enterprise controlled IoT systems co-existing in same physical and wireless area
- Address impacts to industry-wide systems and critical infrastructures
- Standardize security requirements and compliance
- Educate decision makers and practitioners regarding the challenges and definition of IoT

3.1.3 Session Summary

The participants discussed several use cases, associated challenges and impacts on adoption including industrial control and sensing and uses of mobile and IoT technology to support data collection. However, industry expressed the need for more efficient and affordable processes for government standards compliance.

The collaboration session discussions focused on several topics including risk management as well as other areas of concern.

3.1.3.1 Risk Management

Modeling and simulation were identified as a tools for understanding security risk in complex, large-scale IoT systems with many components. In particular, these models must be strongly rooted in real operational models to be useful.

3.1.3.2 Policy Making

The attendees next discussed how to proactively manage security problems before non-secure practices become entrenched, and importantly, before major incidents occur. The discussion next centered on the policy making process. The group concluded the process needs to begin as early as possible, include experts that understand the technical issues at hand, avoid the “checklist” mentality of the past, and avoid overregulation of the technology.

To support these goals, IoT practitioners will need better tools to help identify the real threats to their systems at a technical and mission level, such as the modeling and simulation techniques discussed earlier.

The group next turned to the problem of end-user education and awareness of IoT security issues, such as the privacy, operational security (OPSEC), and pattern-of-life concerns raised by some devices.

Finally, the group considered the intersections of personal and enterprise use of IoT including concerns with personally-owned devices operating in government spaces. Existing blanket bans and waiver processes may not scale with the increasing use of devices such as medically prescribed wearables.

The group next talked about how to build more secure IoT systems to mitigate these risks. The difficulties posed by legacy systems was raised early on.

Another significant challenge identified was how to operate or accept the vulnerabilities from existing application security, as many of the developers assemble IoT devices from sub components or modules that already contain vulnerabilities. One partial solution proposed was to create better tools that can at least identify well-known vulnerabilities in those building blocks and make developers aware of their presence.

Another challenging area discussed was the explosion of complexity present in IoT systems and the additional difficulties that it imposes. The discussion also touched on the conflicting incentives at play that can exacerbate the problem, including the view expressed by some industry attendees that government approval processes can be overly cumbersome and expensive. Members of the group also raised the point that there are numerous applicable security technologies already in existence and government could do more to engage with industry to identify and make use of them.

The session also looked at what future trends and directions in IoT technology will have an impact on security. For one, hardware constraints will ease over time as technology improves. For example, cryptography is often not present in legacy designs as it was considered too expensive to fit into low-resource, low-power devices of the past. Newer chips that are faster, cheaper, and have lower power requirements will steadily enable more and more security techniques to be applied to IoT devices. The group also explored how the proliferation of small, dedicated devices might benefit from a reduced attack surface, and in general, the market may tip towards single purpose devices that are generally considered to be easier to secure than general purpose computing systems.

Finally, the group discussed technical approaches to harden IoT endpoint devices. One major challenge identified is the often locked-down, “black box” nature, of these devices which makes it difficult if not impossible to retrofit security. The group then examined several approaches to adding security in light of this limitation. Diversity was mentioned as a technique for limiting the scope of vulnerabilities across a deployment. Sandboxing, isolation, network segmentation (including various features of 5G networks), and other defense-in-depth measures are expected to play a significant role. Lastly, the group believed there is a role for self-healing and resilience technologies for defending IoT devices and networks.

3.2 Architecting IoT Ecosystems Session

The *Architecting IoT Ecosystems* session focused on defining what makes up an IoT ecosystem. What differentiates an IoT ecosystem from a cloud, mobility or big data was also explored. Recommendations were also developed on how to address these issues, taking into account viewpoints from government, commercial, and academia.

3.2.1 Session Goals

The goals of this session were to identify:

- Risk management factors that are unique to IoT;
- The role of business rules in the IoT; and,
- The role of governance with regard to architecting IoT ecosystems.

3.2.2 Challenges

The session identified several challenges or needs:

- Governance and businesses adaption to a world, where traditional means of power and control seem to be decaying;
- Potential impact to people’s ability to make a living;
- Security and privacy implications for IoT;
- Minimize technologies from being used against us by criminals and hostile adversaries;

- Governments and industry align their bureaucracies to take good and bad data to make improved decisions; and,
- Minimizing overload of data.

3.2.3 Session Summary

Covering the small conference room's walls with thoughts about the future, this passionate group envisioned the IoT-enabled world of 2025, where web headlines like the following are common:

- *A High School class wins major Government acquisition contract*
- *A government agency is as agile as Netflix; releases 100 code updates a day*

Getting there requires understanding current trends, potential barriers, and needed behaviors to creating a healthy and safe architecture and ecosystem for the Internet of Everything. Specifics of the group's discussion include:

- Creating a climate and culture shift in the relationships between government and industry for adapting to the velocity of change, while providing an acquisition level playing field for incumbents, prime government contracts, and new contractors;
- Building trust, with constituents and customers for people and the IoT devices and processes to address privacy issues, improve online attribution, while taking a holistic view of capabilities and realizing just because we can do something, should we do it; and
- Establishing IoT protocols through industry and government collaboration and crafting system-of-system frameworks intended to decrease complexity. This may require:
    - Red teaming checks and balances on portals, processes, and new capabilities;
    - Opening government data; and
    - Increasing education across government and industry of IPv6 benefits.

Highlighting some possibilities, big problems, and barriers to overcome, the group took pictures of the notes spread across the walls and emailed them to each other. What follows is a breakout of their discussion with some potential huge IoT successes and the barriers that may prevent potentially disastrous events from occurring.

Looking into the future the group believed IoT could potentially enable the following ideas:

- Agile and predictive systems that reduce traffic congestion and improve commutes;

- A virtual world that coincides in perfection with the physical world, enhancing training, monitoring infrastructure, and enabling timely maintenance and response;
- Ability to monitor of systems and services that improve energy efficiency;
- Improved medical monitoring and smarter drugs through the use of ever smaller-and-smaller sensors and processors; and,
- A better-educated world supported through online schooling and services.

In the Washington DC area, few people would argue about the need for a better commute. As with improved commutes, all the items on the group's lists could provide real benefit for the world. None of ideas are small changes. Preparing for the velocity at which these changes may occur requires understanding potential challenges and building partnerships between industry and government to prepare for them.

With everything having potential to be connected to everything else[1] the group focused on identifying problems that may exist as IoT grows. What follows are concerns about governance, business rules, and risks. Because research shows that experts are good at estimating base rates but weak at making predictions, the group's predictions are backed with projections of current and historic trends.[2]

3.2.3.1 Assessing IoT Governance and Business Rules as Disruption Occurs

With IoT having potential to enable billions of people to lead fuller lives, the resulting loss of power and control will be hard from some social structures, governments, and leaders to understand and adapt to.

Another emerging trend dealing with the shifting of power and control is sometimes referred to as the "uber-ization" of the world, where existing jobs and services convert into discrete, repeatable on-demand tasks. Today a driver of a combine harvester can clear a wheat field faster than dozens of men from the early 20th century. In the 2025 IoT-enabled world, advances in self-driving vehicles, wireless systems providing access to 1 gigabit per second bandwidth, and companies like Skybox Imaging providing near real-time space-based imagery and video, may enable an individual to operate a fleet of combines from anywhere in the world.

3.2.3.2 Assessing Risk Management in an IoT-Enabled World

Gene Roddenberry, creator of the Star Trek television series, envisioned a pristine world 40 years ago, with devices that resemble our smartphones of today. Now, 3D printers, self-driving cars, and hover boards[3] are also shifting out of the world of

[1] D. Burrus. *The Internet of Things is Far Bigger Than Anyone Realizes.* http://www.wired.com/insights/2014/11/the-internet-of-things-bigger/, 2014.

[2] C. Heath and D. Heath. *Decisive: How to Make Better Choices in Life and Work.* Crown Publishing, 2013.

[3] S. Curtis. *Lexus has created a real, riddle hover board.* The Telegraph, 2015.

fiction to reality. IoT has the potential to connect all these systems. Large complex systems sometimes exhibit emergent behavior and do things you did not predict.

In 2003, 50+ million people in the Northeast United States and Canada lost power because a minor fault caused ripples through the power grid. With IoT bring trillions of connections across its billions of sensors and devices, disruption on a worldwide scale may be possible. To protect constituents and customers, government and industry need to understand how and where emergent behavior can exist when everything and everyone have potential to be connected.

When everything is connected, privacy concerns exist. Given today's trends, imagining an immediate future in which everyone you know is on Facebook and all your movements are tracked via mobile devices, this is feasible. With advances in facial recognition software and the potential for connected sensors everywhere, and IoT's exponential growth potential, tracking and anonymity-reducing technologies may grow faster than initially perceived. This initial perception may accelerate beyond the point where anonymity no longer exists.

3.3 IoT Driving Changing Dynamics Session

The *IoT Driving Changing Dynamics* session focused on four primary subtopics in addressing IoT Dynamics: Data, Lessons Learned, Use Cases, and Security. The session concluded the discussion with the Way Ahead.

3.3.1 Session Goals

The goals of this session were to explore the current state of IoT implementation and planning for various government agencies and to identify whether the government requires better resourcing versus outsourcing adoption.

3.3.2 Challenges

The session identified several challenges or needs:

- Security of data
- IA policy reform
- Data Standardization
- Increased Partnership with Industry

3.3.3 Session Summary

The participants discussed the impact of IoT on Data Analytics, Security of Data and Lessons Learned. In particular, the discussions address the following targeted areas within each domain of impact:

- Data Analytics
    - "As is" resourcing
    - "Required" recourses required
    - Value added in data analytics
- Lessons Learned
    - Best practices

  - Case Studies
  - Paradigm shifts
- Security of Data
  - Level of security
  - Cost analysis
  - Data ownership

3.3.3.1 Data Analytics

The group had a valuable discussion on multi-modal data acquisition and the subsequent analysis of the data. Several methodologies of data acquisition were explored:

- *Human to Human* - Data recorded during interviews into an electronic device;
- *Human to Machine* - Self servicing entry via the internet; and,
- *Machine to Machine* - Remote sensors such as through weather monitors, seismic monitors, intentional and unintentional telematics such as through everyday automobile telematics, airlines engine interaction, to agricultural equipment sensing livestock health and or combine locations.

The group also focused a segment of the session on how to respond to and manage this data. The consensus was to establish large data centers where multiple agencies could share the information and leverage data analytic algorithms to fuse the information.

Additional items that we discussed in this arena were:

- Utilizing a single or even multiple data centers that are all interconnected; and,
- Government agencies were not presently in a position to manage or system engineer the IoT growth and that there needs to be a change to the acquisition/contracting process to allow for a better partnership with industry in order to keep pace with technology

3.3.3.2 Lesson Learned

The following items were the most actively discussed in this context:

- In order to keep pace with technology, the government agencies would need to rely on partnerships with industry including migrating to shared resources such as Data Centers;
- Security of the data was paramount for maintaining the trust of the public; and,
- IA policy was far behind technology and that reform is needed.

3.3.3.3 Way Ahead

The Way Ahead, although a separate subtopic, was sporadically discussed throughout the session. Key points discussed were:

- Data Centers shared by multiple agencies;
- Cross-agency algorithm development that leverages data from multiple agencies (e.g., synchronizing weather data with traffic sensors for emergency routing of citizens);
- Development of predictive algorithms;
- Partnership with industry;
- Development of new business models that optimize Operational Expenditure (OPEX) and reduce Capital Expenditure (CAPEX); and,
- Reliance on utilizing National Information Exchange Model (NIEM) for the data standardization for interoperability.

3.4 Summary

The November 2015 Federal Internet of Everything Summit highlighted several challenges facing the Federal Government's adoption of IoT. The highlighted challenges were not unique to this Summit's challenge areas, but span across the discussions by the government, commercial IoT practitioners and early adopters.

Based on the recommendations made in the Collaboration Sessions, government should participate in working groups and special interest groups; partner with Industry and academia to leverage research; and influence security and data standards. These activities will alleviate Internet of Things challenges cited by the practitioners.

4 Recommendations

While Government and Industry believe that IoT provides opportunity for efficiencies, they recognize the disruptive nature of the technology. Therefore, in order to increase adoption and gain efficiencies, it is important to establish Industry partnership, resolve security and compliance concerns, identify acquisition reform and establish protocol and data standards.

As IoT connects more endpoints together, it provides a greater opportunity for risks or threats to the overall environment. Therefore, it is very important to protect and harden the endpoint devices in the IoT ecosystem, maintain the integrity and confidentiality of the aggregated and raw data, and standardize security and compliance requirements.

The current federal acquisition process does not provide sufficient flexibility to support the dynamic nature of IoT. Therefore, government should look for creative methods for supporting a rapidly changing and more dynamic environment.

The lack of IoT protocol and data standards will stifle adoption if not appropriately addressed. Therefore, the government should participate in working groups with Industry and academia to drive and influence the adoption of standards.

Academia can provide technical resources and visions to support the discussed challenge areas. In order to lessen the burden on government resources, Academia should be included in planning and research processes to help provide technical input and supplement government knowledge. With an emerging technology, qualified resources are difficult to acquire and are in high-demand. Therefore, government should partner with university researchers to prepare graduates for IoT employment.

Based on the challenges and concerns made in the Collaboration Sessions, government practitioners should participate in special interest groups and working groups to influence standards development; continue to partner with academia to leverage research and career enrichment for the government workforce; and continue to identify dynamic acquisition models that support IoT adoption.