MEETING RECAP

IEEE Trust and Security Workshop for the Internet of Things (IOT) Washington, D.C.

4 February 2016

IEEE

IEEE | 3 Park Avenue | New York, NY 10016-5997 | USA

Trademarks and Disclaimers

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

To order IEEE Press Publications, call 1-800-678-IEEE.
Find IEEE standards and standards-related product listings at: http://standards.ieee.org

Notice and Disclaimer of Liability
Concerning the Use of IEEE-SA Documents

This IEEE Standards Association ("IEEE-SA") publication ("Work") is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the Industry Connections IoT activity that produced this Work. IEEE and the Industry Connections IoT Activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the Industry Connections IoT members disclaim any and all conditions relating to: results; and workmanlike effort. This Industry Connections IoT document is supplied "AS IS" and "WITH ALL FAULTS."

Although the Industry Connections IoT members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR Industry Connections IoT MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so. IEEE and the Industry Connections IoT members make no assurances that the use of the material contained in this work is free from patent infringement. Essential Patent Claims may exist for which no assurances have been made to the IEEE, whether by participants in this Industry Connections IoT activity or entities outside the activity. The IEEE is not responsible for identifying essential patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents claims, or determining whether any licensing terms or conditions, if any, or any licensing agreements are reasonable or non-discriminatory. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at http://standards.ieee.org/about/sasb/iccom/.

This Work is published with the understanding that IEEE and the Industry Connections IoT members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

Contents

IEEE Trust and Security Workshop for the Internet of Things

Executive Summary

Estimates run as high as 50 to 200 billion Internet of Things (IoT)-connected devices will be in the world by 2020-2025—everything from home appliances to health monitors to countless devices in our environment making sure that crops are growing, that power is flowing, that things are working and safe.

Essential to reaching this future, however, is that the public trusts it—that they believe that their privacy is protected and their security is not compromised. The End to End Trust & Security Workshop for the Internet of Things held in February 2016 in Washington, DC included dozens of presentations on aspects of these questions, developed and presented by thought leaders in academia, industry, not-for-profits, technical organizations, consortiums, and governments from around the world.

IEEE, Internet2, and the National Science Foundation (NSF) as well as a host of other sponsors worked together to gather industry technologists for this workshop who can help drive the Internet of Things (IoT) conversation and contribute to the development of an open architectural framework. The focus of the workshop submissions and discussions was to address the TIPPSS elements of IOT: trust, identity, privacy, protection, safety, and security.

The presentations enabled rich discussions focused in the following broad areas:

End to End Trust and Security

Depending on where you are definitions of privacy and security differ and sometimes significantly, yet the challenge will be to make the IoT's architecture as universal as possible to meet those expectations while enabling broad system level interoperability and eliminate vulnerabilities. Different solutions to aspects of this question range from creating an architectural model, to secure, self-monitoring fiber optic and wireless networks, to changing the way devices are developed to make TIPPSS – trust, identity, privacy, protection, safety and security - a primary objective from the start.

Access Control & Identity Management

With new devices coming on to the network constantly, how they are verified and what they are allowed to do is essential to not allowing them to introduce vulnerabilities. At the same time, not every device has to be identified in the same way, and in fact doing so presents privacy risks if every interaction identifies the user fully. In the highly interconnected world users gain access to the information that may reside in the neighboring application domains. Biometrics as a secure form of identification, the Semantic Web as a way to standardize definitions for privacy and security, secure ways to bring new devices into use, and new schemes such as Virtual Organizations for security were all discussed in these sessions.

Architectural Framework

TIPPSS elements are important to be built in with defense in depth, which can be baked in at the hardware, firmware, software and service level of the device and application —but it's also important that it be done in an efficient way that doesn't have a high resource cost. Approaches to improving security while keeping its cost low were discussed. This included a layered approach to security, hardware approaches such as deterministic photonic packet switches, an improved taxonomy of error control, and a centralized authority to manage security issues so that every device doesn't have to on their own. The opportunity to provide an ability for device democracy for applications and use cases that require in-situ real time trust, identity and security was also discussed. The application of these TIPPSS ideas in an architectural framework that would apply in multiple scenarios was explored, including how all these concerns interact with the dynamic environment of intelligent highways, connected vehicles and connected healthcare.

Policy & Standards

The IoT's future depends on acceptance of standards for privacy and security; it also requires knowing what authorities can and will establish such standards in order to make norms accepted. Policy issues begin with agreement as to where governance is coming from, making it technologically possible in low power environments, while providing transparency from all parties, incentivization for manufacturers, and application to new areas that open up new law and policy such as drones and brain-digital interfaces. The discussion also touched the subject of the gap that exists between policies and technologies and how this gap can be closed through the collaborative efforts of policy makers and technology developers.

Scenarios and Use Cases

In the real world, consumers don't think about security enough, and they often consider it the manufacturer's responsibility. ,Many of the systems that are being implemented such as the Smart Grid are vulnerable to attack or present privacy concerns. Connected vehicles won't sell if they're seen as reporting every time you speed to authorities. Privacy needs call for privacy mediators who advocate for users and anonymize the minor details of our daily lives. The DIY (Do It Yourself) and "maker" culture calls for wide education on the issues of trust, identity, privacy, protection, safety and security, leading to a discussion of IoT Ethics and education.

Invited Speakers

Florence Hudson, Internet2
Rosio Alvarez, US Department of Energy
Oleg Logvinov, IEEE (IEEE Internet Initiative and IEEE P2413 Working Group)
Robert Martin, MITRE, Industrial Internet Consortium (IIC) Steering Committee
Anita Nikolich, NSF
Sarah Cooper, M2Mi
Alan Karp, Earth Computing
Ira Kovalinka, DSPOmnia Inc.
Rob Gingell, Resilient Network Systems
Prof. Scott Streit, Jason Braverman and Hector Hoyos, Hoyos Labs
Ken Klingenstein, Internet 2
Brian Scriber, Cable Labs
Dr. Wenjia Li, New York Institute of Technology
Dr. Craig A. Lee, The Aerospace Corporation
Dr. Erfan Ibrahim, Maurice Martin, National Renewable Energy Lab
Ted Szymanski, McMaster University
Cleon Rogers, LRDC Systems LLC
Yiorgos Makris, Dr. Angelos Antonopolous, Kiruba S. Subramani, Aria Nosratinla, Trela, University of Texas at Dallas
Margaret Lyell, Explorations Minerva LLC
Vamsi Gondi, David L. White, Jill Gemmill and Christopher W. Post, Clemson University
Vyacheslav Zolotnikov, Semen Kort, Ekaterina Rudina, Kaspersky Labs
William J. Miller, ISO/IEC/IEEE P21451-1-4 (Sensei-IoT*)
William Woodward, SAE International
Glenn Fink, Pacific Northwest National Laboratory
Karen O'Donoghue, Internet Society
Lillie Coney, chair, IEEE PAR 1912 Privacy and Security Architecture for Consumer Wireless Devices Working Group
Juan Carlos Zuniga, InterDigital Labs
John Murray, SRI International
Dr. Bertrand Cambou, Paul Flikkerma, Constantin Ciocanel, Northern Arizona University
Edward Aractingi, Marshall University/Internet2 CINO-IoT Working Group
Michael A. Eisenberg, University of Colorado - Boulder
Martin Murillo, University of Notre Dame
Mark Cather, UMBC Chief Information Security Officer
Pamela Gupta, OutSecure Inc.
Carl Hewitt, Standard IoT Foundation
Luke Russell, Carleton University
Dr. Reza Arghandeh, Florida State University
Nigel Davies, Lancaster University
Dr. George Corser, Saginaw Valley State University
Dr. Rabindra Chakraborty, Senslytics
Ron Winward, Radware
Ulf Lindqvist, SRI International
Steve Wallace, Indiana University

Opening Remarks

Oleg Logvinov, Director, Special Assignments, Industrial & Power Conversion Division, STMicroelectronics; Chair, IEEE Internet Initiative and IEEE P2413 Standard

This event was born at the intersection of two IEEE Initiatives:

- IEEE Internet Initiative (internetinitiative.ieee.org)
- IEEE IoT Initiative (http://iot.ieee.org/)

IEEE Internet Initiative

The mission of the IEEE Internet Initiative is to raise IEEE's influence and profile in global technology policy in the areas of Internet governance, cybersecurity and cyberprivacy policy development by providing a consensus of sound technical and scientific knowledge and guidance to the process.

The IEEE Internet Initiative is a cross-organizational, multi-domain community that connects technologists and policymakers from around the world to foster a better understanding of, and to improve decisions affecting, Internet governance, cybersecurity, and privacy issues. Regardless of the specific areas of Internet-related technology and policy you work in, nearly everyone has a stake in the future of Internet governance and the related issues of cybersecurity and privacy. Both technologists and policymakers can derive practical benefits from learning more about each other's perspectives, challenges and opportunities. For technologists, an advanced awareness of public policy issues should lead to the development of sound technical solutions and best practices. For policymakers, access to technologists and an improved grasp of technology will help clarify the trade-offs inherent in related public policy choices and decisions.

To help technologists and policymakers accomplish these and other goals, the IEEE – recognized for its open, transparent, collaborative processes – is convening neutral platforms to support mutually beneficial dialogue and engage other pertinent stakeholders. The IEEE Internet Initiative website, for instance, offers a one-stop destination for current news, upcoming events, recent publications, and a growing trove of rich resources. Other key related activities, include:

- supporting and facilitating the development of open standards to address cybersecurity and privacy challenges;
- working to identify societal implications of alternative technology policy solutions;
- monitoring the technology policy landscape;
- supporting, collaborating and partnering with Internet ecosystem entities, and
- connecting stakeholders to a comprehensive framework of conferences, educational programs, and standards.

Dialogue with all interested stakeholders is an essential element of IEEE Internet Initiative's mission.

IEEE IoT Initiative

The mission of the IEEE IoT Initiative is to serve as the gathering place for the global technical community working on the Internet of Things; to provide the platform where professionals learn, share knowledge, and collaborate on this sweeping convergence of technologies, markets, applications, and the Internet, and together change the world.

The IEEE Internet of Things is one of IEEE's important, multi-disciplinary, cross-platform Initiatives. The Internet of Things (IoT) is one of the most exciting technological developments in the world today and the global technical community is coalescing around the thought-leading content, resources, and collaborative opportunities provided by the IEEE IoT Initiative.

More information is revealed daily about the Internet of Things and its potential to transform how we communicate with machines and each other. To bring clarity to and disseminate information globally, IEEE Future Directions launched the IEEE IoT Initiative in 2014. It serves as a home for the global community of engineering and technology professionals in industry, academia, and government working in related technologies. Here, professionals learn, share knowledge, and collaborate on this sweeping convergence of technologies, markets, applications, and the Internet. Participants in the community have access to the most trusted resources developed including publications, videos, articles, and interviews, as well as webinars, Hangouts, presentations, workshops, and conferences, this web portal, and much more.

Opening Panel: The Needs and Challenges in Trust, Security, and Privacy for the IoT

Panelists:

Rosio Alvarez, Chief Information Officer, Lawrence Berkeley National Laboratory

Sarah Cooper, Chief Operating Officer, M2Mi

Oleg Logvinov, Director, Special Assignments, Industrial & Power Conversion Division, STMicroelectronics; Chair, IEEE Internet Initiative and IEEE P2413 Standard

Bob Martin, Senior Principal Secure Software & Technology Engineer, MITRE Corporation; Steering Committee, Industrial Internet Consortium

Anita Nikolich, Cybersecurity Program Director, National Science Foundation

Moderator: Florence Hudson, Senior Vice President & Chief Innovation Officer, Internet2

The opening panel presented perspectives from multiple leaders from across the public and private sector on TIPPSS – Trust, Identity, Privacy, Protection, Safety and Security – in IoT. From industrial applications, to government assets, to consumer applications, cybersecurity and TIPPSS are prime areas of required focus.

The discussion included architectural frameworks already being developed by the Industrial internet Consortium, IEEE, the National institute of Standards and Technology (NIST) along with the need to ensure interoperability and safe, secure systems whether in brownfield or greenfield applications. There is research, development and discovery yet to be done in IoT and those areas need to be explicitly enunciated and addressed. From defense in depth strategies in an IoT device, to the process of ensuring trust and identity of users and devices, to ensure we protect the data and privacy of the individual or entity to which the data pertains, to increasing the safety and security of the application and device, there is much more to do. There is critical infrastructure that requires the utmost safety and security, which can also be in an organization with an open collaborative culture, requiring an ambidextrous management paradigm.

The panel agreed the potential value of IoT is indeed driving the development of use cases and devices, requiring all of us to work together to ensure the diligence of architecting trust, safety, security, and privacy into the IoT technologies and processes today and into the future.

Presentations on Trust and Security for the Internet of Things

Trust And Security Draft Standard Using The Semantic Web – W.J. Miller

One important goal is to provide an IoT approach that meets differing definitions of privacy for personal data around the world. ISO/IEC/IEEE P21451-1-4 offers Semantic Web 3.0 capabilities that include unique identification, access control and identity management, device sharing, built-in Transport Layer Security (TLS), a common reference architecture for data exchange that is technology agnostic and protocol independent. Privacy is protected by use of "Thing Registries" limiting access to those authorized and trusted by the owner of the Thing.

IIRA Meta-Reference Architecture For Diverse Applications – Robert Martin

The Industrial Internet Consortium's IIRA (industrial internet reference architecture) defines and supports a wide and diverse set of system types in many configurations, connected in many different ways across a wide range of industries, sectors and use case contexts. It supports and guides any creation of solutions for architectural needs, and its open architecture and interoperability and the use of allied testbeds helps advance innovation and best practices.

Network End to End Data Link Evaluation System (NEEDLES) For Optical Cable Monitoring – William Woodward

Originally developed for the Navy, NEEDLES is a standard for detecting impairment in fiber optics. It consists of one main document and several slash sheets. Designed to be non-intrusive and non-destructive, it provides a 24/7-condition status of the entire fiber optic network, detecting faults and isolating them in real time.

Report on 2015 IoT Security and Privacy Keynotes Workshop – Glenn Fink

At the 2015 IoT Security and Privacy Keynotes Workshop, held in conjunction with the IoT World Forum in Milan, participants identified six key areas where security and privacy improvements were needed for the IoT's future growth: data privacy, data provenance, lifecycle data encryption, scalable infrastructures, standard protocols and standardized risk metrics. Top issues that were identified include analysis and use of data while encrypted to ensure confidentiality and integrity, standardization of vendor protocols, sensor identity verification and data security, and policies for data sensitivity and privacy in a world of sophisticated data analysis.

IoT: Issues And Challenges Of A More Connected World – Karen O'Donoghue

Devices on the Internet are not new, but their abilities and the scale of the IoT will be. The key challenges of the IoT include security, privacy, interoperability/standards, legal and regulatory issues and rights, and issues related to the emerging economy and economic development. Security challenges include not only the scale but also the invisibility of internal workings and the relative lack of physical security for everyday objects. Similarly, privacy issues must be dealt with in a context whose ubiquity makes it hard to keep privacy. The IoT presents amazing opportunities but also serious challenges that must be solved collaboratively.

Defending Against The Silent Intruder – Lillie Coney

IEEE PAR 1912 is working to develop a standard for a common privacy and security architecture for consumer wireless devices, making it easier for consumers to integrate those technologies into their lives and have greater control over devices and technology. Recommendations include rethinking operating systems from a security and privacy perspective, making them fail-safe or fail-secure, reference libraries for software reflecting higher levels of security, greater transparency for apps, and accountability regarding the chain of custody for both the digital and physical IoT.

Access Control and Identity Management

A New Model For IoT Sharing And Access Control – Vyacheslav Zolotnikov, Semen Kort, Ekaterina Rudina

An effective sharing system has six aspects—it's dynamic, attenuated (can't be shared further without your permission), chained (tied to the person who shares), composable (you set the terms for each transaction). accountable, and it works across domains. At present you rarely have any of these levels of control while sharing electronic files or permissions, and IoT may well make the problems worse. A new model built on tokens avoids those problems.

Private Biometric Verification In IoT Authorization - Ira Konvalinka

Existing one-to-many models for biometric verification have multiple points of vulnerability. Spoofing can occur at any of these points, the most vulnerable of all being also the most common, handheld personal devices such as cellphones. A new one-to-one model shifts key parts of the process outside the reach of these vulnerabilities to an encrypted domain, using a revocable hardwired key and PUF (Physical Unclonable Function) that authenticates devices as surely as iris scans authenticate humans.

No T In The IoT Is An Island - Rob Gingell

At least that's the goal. Right now we are still in the island phase where Things are relatively isolated on the network, but soon there will be a dynamic network of interconnected devices forming trust relationships quickly and with low overhead. To get there, though, we need efforts to preserve privacy through better use of trust relationships, and explicit policies for connections between authorities. Systematic trust maximizes IoT utility and helps protect the network as a whole.

IoT Security: "A Nightmare In Progress" - Prof. Scott Streit, Jason Braverman, and Hector Hoyos

A wide-ranging list of the security problems in the IoT was presented: "Usernames and passwords are broken," there's no two-factor authentication for connected devices, Oauth-type logins have a large surface of attack, mobile apps stay logged in, hackers leverage mobile devices to attack others, unencrypted data is everywhere, and few devices use two-way TSL connections. Open Sesame™ offers a smarter, biometric-based way to lock connected devices. Together with BOPS—Biometrics Open Protocol Standard—it secures physical access through biometric authentication and encrypts all data to protect the user.

Lessons from the Internet of People - Ken Klingenstein

The Internet as it exists now for human users has lessons to teach about the shape of the IoT. Internet identity evolved with the rise of federated authentication. Metadata came to play a

critical role in authentication and access control. Different forms of trust came to work together in different circumstances. In all, there are emerging tools on the people side that can address the privacy, personalization and security needs for the P to T interface, though the IoT has other issues as yet unexplored.

Security Improvements In New Device Onboarding - Brian Scriber

Bringing new devices onboard poses, and exposes, common security risks, that can make the device the entry point to future attacks. Anonymous devices are most vulnerable but PIN-based ones are nearly as risky, not least because they seem to offer more security than they really do. We need new systems rooted in securely stored keys and manufacturer-based certificates.

Trust and Security for the IoT - Wenjia Li

Trust and security are real and severe challenges that threaten the wide deployment of IoT—they can even be life-threatening. The majority of current trust management schemes model trust in one single scalar or value, which is too crude for sophisticated systems. A new model of trust management would collect and evaluate prior behavior of other nodes and build a trust value for each node based on the behavior assessment, identifying harmful players more quickly. At the same time, evaluating the trustworthiness of the data itself can be as important as evaluating individual nodes.

Virtual Organizations For Managing Trust And Collaboration - Dr. Craig A. Lee

Federations are a way to manage collaborations utilizing the cloud, and can be done at any level in the system stack to securely manage collaborations and the sharing or resources across a wide spectrum of application and administrative domains. This vastly expands the applicability and potential impact of what cloud federation could mean, all the way to a global intercloud of things. For this to be realized, certain things will be needed including semantic interoperability, a standard federation gateway or agent and modular trust components. Such Virtual Organizations already run under the Interoperable Global Trust Federation, and the next step is creating a Keystone-based, General Federation Agent.

Goals of the IEEE Cyber Security Initiative - Ulf Lindqvist

The IEEE Cyber Security Initiative has three primary goals—to become the go-to online presence for security and privacy, to improve understanding of the issues at the student level, and to improve designs and implementation at the professional level. To that end IEEE has a number of secondary initiatives in process. The Try Cyber Security Initiative focuses on raising awareness of a “Top 10” of security flaws, while the Center for Secure Design (CSD) brings together software security expertise from industry, academia and government to devise “building codes” for software.

Key Points from Access Control & Identity Management Breakout Session

- Identity vs. Identifiers:
  - Establishing identity requires authentication and can work against privacy concerns in many cases. There are, of course, circumstances where Identity has to be established, but an extensible IoT environment won't be able to do this effectively.
  - Identifiers can be used to show authorization to perform some action or access some resource, but can be deployed in a privacy-protecting manner.

- Biometrics have the potential to address questions of strong authentication and allow users/entities to control access to their data by binding the authentication to data or other resources.

- Standards are needed to allow for interoperability, heterogeneity, common semantics, etc. The sooner these can be put into place, the easier it will be for a broad-based IoT ecosystem to develop that supports security, trust, and privacy.
  - Many of the actual issues have technical solutions.
  - The need is for standards to layout how solutions work together in a coherent/cohesive whole.

- Access control: There needs to be a mechanism to keep devices separated. Simply because a light bulb is on the network doesn't mean it should be able to access anything else on the network.

- In order to preserve privacy, anything should only be challenged to authenticate where needed. It's not needed everywhere or to everything. That is, device-to-device interactions shouldn't necessarily require authentication when they can show that they are authorized.

- There does not yet seem to be a meaningful definition of the lifecycle of an IoT device and what are the requirements at each stage. Specific stages that need attention: on-boarding, normal operation, end of life or transition.

- Authorization: architecture design with policies stored elsewhere for examination.

Architectural Framework

A Layered Solution To Cybersecurity - Dr. Erfan Ibrahim, Martin, Maurice

The National Renewable Energy Laboratory (NREL) has demonstrated end to end security using off the shelf technology, tested on NREL's Distribution Grid Management (DGM) testbed. The key is choosing technology to cover 9 system layers: 7 logical layers in the OSI Basic Reference Model, 1 semantic layer and 1 business layer. The technology challenge of securing DGM has been largely solved with off the shelf products today. The more important matter is sound network design, proper technology integration, strict security policies on routers and firewalls, well defined security patch management processes in the organization, regular employee training on security awareness, and defeating social engineering schemes for data exfiltration and insider threat.

A Secure, Lower Overhead "Industrial Internet Of Things" (IIoT) - Ted Szymanski

Security is critical in industrial IoT applications, but will also require huge resources. Deterministic photonic packet switches offer a way to design a secure IIoT at a lower resource cost, by embedding millions of secure virtual networks in layers 2 or 3, using low-energy-usage field-programmable gate arrays with Optical I/O. This allows for a significant increase in cyber-security, as VN packet transmissions can be encrypted and decrypted in FPGAs, while reducing congestion (and efforts to combat it).

Taxonomy Of Error Control Requirements – Author???

Two recent papers questioned the adequacy of CRC Standards in modern software development, and recommended new research on error control in critical software-intensive systems. The resulting proposal is for a taxonomy to classify and aid the specification and verification of error control solutions, followed by implementation of the standards by training and authorizing the appropriate authorities globally. The model for this effort would be the advanced practices already used to ensure a high level of error control in the aviation sector.

Vulnerabilities That Begin With The Hardware - Vamsi Gondi, David L. White, Jill Gemmill and Christopher W. Post

Do you trust your IoT hardware? Insecure network services (UPnP), cloud services, and insecure wireless communications all represent vulnerabilities. Hardware trojans at the device or network level can steal sensitive information by exploiting gaps between wireless standards, and these gaps can be amplified in the presence of multiple intropperable communication protocols, links and devices. We need to address the ability of devices to be sensitive to data misuse, and to alert the user.

Preparing For The Era Of Connected Vehicles And Intelligent Roadways - Margaret Lyell

The Intelligent Transportation System (ITS) and Connected Vehicle (CV) provide a systems level exemplar of the Internet of Things. ITS/CV will make use of wireless technologies and embedded devices and algorithms to control a vehicle's behavior while in traffic, even if overriding driver instructions. Providing for safety, security, privacy and reliability is a must, and the interface of ITS/CV with current business/ societal structures (car dealerships, embedded device manufacturers, insurance companies, etc.) must be carefully worked through.

Centralized Authority To Manage Security Issues With IoT Installations – Author ???

Resource constrained CPUs, memory and communication capabilities coupled with low energy consumption result in limited security using low-end algorithms. Add in the physical risk to monitors and data, the risks of things like denial of service attacks, and vulnerabilities on the communication and application layers, and the IoT is vulnerable in many ways. There is a need for a centralized federated management authority to generate, distribute and manage the credentials across security layers in the IoT framework and across multiple application environments.

The Security To Safety Model - Vyacheslav Zolotnikov, Semen Kort, Ekaterina Rudina

Cyber physical systems exist in at least two types of environment: the **informational** environment and the **physical** environment. Issues may arise from both types of environment and affect physical aspects, informational aspects and the system itself. Conducted research helps us simplify determining of significant threats in IoT systems, identify the possible weaknesses in security solutions, and reasonably enhance the approach to the security and safety enforcement using the principles of secure architectural design.

Secure Data Architecture: Ensuring data integrity at the beginning of the scientific workflow; a Mini-ScienceDMZ1 (Mini-DMZ) for instruments - Steven Wallace

Key Points from Architectural Framework Breakout Session

While many have been talking about "End to End Security," the real issue to be discussed for enterprise use of IoT is "End to End Security and Safety" which is not just a network issue really, rather it is about the security and safety of each of the elements, each of the components, their connections, how they are maintained, how they are used. We need to make sure we don't get fixated on the "network" part of IoT only.

- The first thing we came up with is that for IoT, safety needs to be considered along with the privacy and performance types of issues (reliability and resiliency), and of course security for these systems.
- The next thing that needs to be addressed is the liability of software development and the software driven capabilities of the devices themselves.

  That leads us into a more rigorous, holistic systems approach and developing that process. More specifically, what is the role of policy, both public and private policy, and defining some general guidelines and rules for IoT type systems?

  A. Issues of scale – both scale up and scale down

  B. Professionalism of the software workforce is really an open question that is almost the other side of the liability issue. Every other engineering trade has licensing, certifications, and it has a history of failures and what you do to resolve those and avoid them

  C. The need for standardization of best practices and really knowing that things are not going to fall over when the first "wrong" thing comes at them or something malicious.
- IoT is going to be extremely disruptive to today's policy regimes. In any industry in any area, because there are very entwined groups driving policy, there is going to be a lot of resistance and a lot of misunderstanding

Policy & Standards

Developing Ethics For A Data-Driven World - John Murray

Privacy and security have been much in the news, and have raised awareness not only of how much data is collected but how analytics use it without our permission, resulting in profiling, surveillance, and social discrimination. The effect of a data-centric approach can be harmful to humans, and we need a new approach in which the collection and end use of data are both driven by an ethical, honest approach.

Reducing The Threat And Enhancing The Opportunities Of Drones - Dr. Bertrand Cambou

UAVs, unmanned aerial vehicles—better known as drones—make illegal activities easier; they also offer enormous benefits to society, much like cars, telephones, or many other things we've grown used to and for which we have made policies. Five technological changes were suggested for helping us adapt to a new drone world: connect UAV's wirelessly to the internet, add a secure element such as a SIM card, personalize them using secret keys, host authentication on a secure server using PKI, and require flight planning and registration via the web.

Three new technology advancements were also suggested: increased security technology that prevents their being hijacked, sensing of aerial vehicles so warnings can be issued, and safer power sources in the form of structural super capacitors.

A Model For IoT Assurance - Edward Aractingi

The IoT did not have security as a focus in its developmental stages. Due to low power, minimal computing resources and slow networks, the overhead of encryption was a barrier to development, and underlying protocols such as HTTP and MQTT lack built-in security. It's true that not all IoT applications need the same level of protection. But there is a need for a standard system of security levels for different applications.

Recommendations include using IP whitelisting and low overhead network ACL, considering the use of session tokens in ReST, using MAC addresses for device authentication, using JSON & XML encoding, and using Certificates when possible. There's a need for collaboration between organizations like IEEE, Internet2, NIST and others to solidify and certify the IoT assurance model.

Is IoT Governance Creating As Well As Solving Problems? - Michael A Aisenberg

The proliferation of organizational bodies where IoT norms are being debated and created reflects important attention being paid to an important process. But the absence of standard processes for engagement, collaboration or even communication threatens development of inconsistent or conflicting norms in some areas, or the absence of norms altogether. Developing norms will provide certainty to stakeholders, enhance utility and availability of technology, and guide organizational and individual behavior.

Open Solutions For Maintaining Privacy And Security Across Devices, Networks And More - Mark Cather

The Internet of Things could grow to 50 - 200 billion devices by 2020, in many different areas of life. Open multi-vendor solutions will be necessary to meet these needs. But there are often subcontractors behind the subcontractors behind the lead vendors, and open communication between all of them is essential, especially on sensitive subjects such as privacy. Openness in how data is used and protected will be a key issue. Tagging to maintain and share consumer preferences will be another, and a data ownership and management framework will be needed to ensure data owners retain control of their data. And the maintenance of such security on different networks—or while unconnected—is also a crucial concern that must be consistent across manufacturers and devices.

Privacy And Security Standards Ensure IoT Viability - Pamela Gupta

What are the problems that the IoT faces? It is not viable or scalable without trust, yet developers are trained to focus not on those issues but on functionality and time to market. We've already seen these issues in products that turned out to have security problems, like Samsung smart TVs or Z-Wave enabled door locks. We need standards for authentication, device security, web interfaces, cloud interfaces, 3rd party APIs, updates and other aspects of devices, but most of all, we need a culture of approaching the ecosystem holistically to ensure security and privacy from the beginning.

Security Without IoT Mandatory Backdoors - Carl Hewitt

It sounds like science fiction—and for the moment it still is, but DARPA is developing an implantable neural interface for data transfer between the human brain and the digital world. Long before we reach such a level of medical IoT, however, the issues of backdoors into the private information IoT devices collect presents itself. Backdoors help devices interoperate, but they also necessarily decrease security, and run the risk of harming economic development of IoT, hampering exports and imports, as well as creating civil liberties issues when so much data about individuals is available without warrants to government.

Key Points from Policy & Standards Breakout Session

What is the IOT?

- IOT is everything and scale and interconnectedness must be considered up front.
- 50 - 200 Billion Devices in 2020 - 2025
- Trust will be essential to IOT growth. 40% of consumers would avoid IOT without Trust.
- Vendor-Neutrality, Openness and International Standards will be necessary to ensure that everyone's devices can work together and protect TIPPSS together.
- Devices in themselves are not risky. A device's risk is related to how it is used. A lightbulb in a home poses less of a risk to life than the light over an operating table. You must understand the device within its entire system.
- Key principles: Trust, Identity, Privacy, Protection, Safety, Security

With billions of devices across the IOT, the volume of devices and data will drown centralized architectures and traditionally rigid frameworks will break. The TIPPSS concepts will need to be pushed down to the devices in order to scale.

All parts of the entire IOT device must be integrated across TIPPSS from the perspective of privacy and security. The device hardware, firmware, cloud, mobile application, interfaces, software, encryption, authentication, service, everything.

Open Data Control, Ownership, and Device Organization

An association layer must be overlaid on the open transport network to provide TIPPSS, data ownership, compliance, and control. The Association layer will allow devices to relate to each other in a similar manner to the way that people relate to each other.

Consumers and IOT data owners need to retain control of their data regardless of where the data goes.

Data Ownership and Transparency

In order to build and maintain trust in the IOT, the government and private sector must act with ethics and openly and transparently communicate with consumers. Transparency comes in many ways, such as how the data and systems will be used as well as changes in access to data and systems.

Centralized Open Cross-Vendor Tools

People don't currently patch and maintain their devices. Management of configuration, security and privacy factors related to billions of devices will overload people if not automated and centralized.

Policy / Standards / Law / Litigation

Better policies and standards around cyber safety, cyber profiling, cyber privacy are needed. Data Centric approach may be necessary. More communication and coordination between standards bodies.

How do you incentivize manufacturers and companies to put resources behind TIPPSS? Vendors need to bake security into the solution from the very beginning, but what will motivate them to do so?

Assurance at Scale will be challenging. Mutual agreement is needed to assure parties about the security of a particular IOT implementation. Industry wide assurance standards could be a way to standardize and provide a point of reference to the industry and consumer. Level 0 barbie doll (basic auth and encryption -> Level 5 pacemaker 2048 bit keys / multifactor device / user auth, session control).

Snowden's statements about the National Security Agency's (NSA) activities are only a drop in the bucket compared to the whistle-blower statements that could come in the future if we don't address TIPPSS right up front.

Scenarios and Use Cases

Users Don't Consider Security Their Problem - Luke Russell

Security is often an afterthought in a field where the barrier of entry is low. The example was made of a smart living room where the homeowner creates a build that is distributed to others; the security flaws are thus spread widely. We may give too much data to our connected systems through personal tools; yet the public expects easy accessibility, and regards security as the developer's problem. Privacy and security must be built-in early in the development process.

Consumer-Oriented, Closed-Loop Systems Are Vulnerable - Martin Murillo

As consumer systems in areas like power and communication move from industrial control to being IoT-based, they are vulnerable in new ways, from technical failure to attacks. The Northeast blackout of 2003 is an example where a software bug led to vulnerability, with no alert system in place.

Smart Grid Security Challenges Come From Many Directions - Reza Arghandeh

Software, IT hardware, power systems, and not least humans all represent potential security risk points. As a result, there's a need for system-wide security that reflects both cybersecurity and cyber-physical systems security; there was an example in Turkey in March 2015, where the attempt to shut down two substations knocked out power for an entire region. Answers will include a vulnerability assessment to identify key risk points, and algorithms to create situational awareness to detect new forms of attacks.

Privacy Needs Call For Privacy Mediators - Nigel Davies

Privacy concerns about the centralization of IoT systems are a growing threat to IoT adoption, which carry the possibility of stalling its acceptance by a wider marketplace. One key principle is that users should be able to control the release of their own data. Privacy mediators would advocate on behalf of users and create a layer between personal data and the cloud called cloudlets, while tools would enable users to control anonymization and deletion.

Vehicles Provide A Unique Set Of Privacy Concerns - Dr. George Corser

Vehicles are out in the open and so is the data they create. We need standards and guidelines for how that data is linked back to individuals and used. Yet some degree of open identity is needed to ensure vehicle safety. We need new metrics for privacy in driving situations, and definitions of location privacy and continuous precise location privacy.

Role Of IoT Analytics-Driven Warning Of Accidents And Other Events - Rabi Chakraborty

IoT analytics can be used for safety management, environmental protection and resource preservation, warning where incidents are most likely to happen based on observed noncompliance data. Where forewarning is based on past experience (i.e., that failure can be expected after a certain amount of time), event-driven prediction is based on observed data (that a specific device being monitored is close to failing). This data can also be used to inform public policy and regulation; examples include oil and gas (pipeline and storage monitors), agriculture (tracking chemical usage data), and smart water (predictive analytics protecting against waste, leakage and sabotage).

Defining Ourselves By Our Data - Ron Winward

Our online presence defines who we are not only to our friends, but also to business and industry. We are defined by our data. Yet our privacy is weakly defined in U.S. law, in contrast to many others. And we have grown comfortable with allowing a great deal of data collection—and even risk of things like ransomware—in return for the convenience of online life. In the end, automation is both the threat and the solution.

Key Observations from Brainstorming Sessions

- Policy moves slowly and in response to interest groups and positions; products are being created more and more quickly.
- Developers need to know they have responsibility for privacy, security and trust.
- Different industries need to work toward common goals within different regulatory frameworks and with different governmental bodies.
- Makers and do-it-yourselfers have to be educated as to privacy/security needs without impeding innovation.
- Can security, privacy and ethics be built into systems and developer tools?
- Technologists need to lead the creation of definitions, while reflecting local cultures/legal systems.