Innovation • Compatibility • Success

STANDARDS UNIVERSITY

March 2016 | Volume 6, Issue 1
IoT, Cybersecurity and the related standards

IN THIS ISSUE

IoT Security Standards
Paving the Way For Customer Confidence

IEEE

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

ABOUT THE IEEE STANDARDS EDUCATION E-ZINE

Technical standards are formal documents that establish uniform engineering or technical criteria, methods, processes and practices developed through an accredited consensus process. The purpose of this publication is to help raise awareness of standards, show the importance of standards, present real-world applications of standards, and demonstrate the role you can play in the standards development process. Knowledge of standards and standards activities can help facilitate your professional engineering practice and improve technological developments to meet the needs and improve the lives of future generations.

Serving the community of students, educators, practitioners, developers and standards users, we are building a community of standards education for the benefit of humanity.

Join us as we explore the dynamic world of standards!

CONTENTS

Letter from the Editor

IoT and Security:

Do We Need Standards For Securing Your IoT Gadgets?

With all the rage (hype?) about Internet of Things (IoT) and Cybersecurity, it is important that we look into the standards at the intersection of these two technologies. As various sensors collect data about people and their surroundings, there is increasing concern about privacy and security along with safety and protection. This is known as the "Quadruple Trust" system within the technical community that addresses Cybersecurity issues.

Among the questions that are often raised in the cybersecurity context, need and use of technical standards are typically at the top of the list. How can systems trust each other without having a common security protocol? The need for trusted communication protocols may be obvious, but when the trust is breached – "if" is no longer a question. As we have seen frequent breaches, we must take steps to improve data security, system security, people's security, business security and national security. In some cases, common sense use is sufficient such as having a 'strong' password and not sharing it with others. In some cases, double verification may be considered sufficient. And, in many cases, significantly higher standards of security must be maintained because entire business or national interests may be at stake.

On the other hand, IoT gadgets are often used as personal devices by people who may not be sufficiently tech-savvy to realize if and when their devices have been compromised. Inherently, IoT gadgets are end-nodes in a large network, and one compromised device can open up the possibility of compromising the entire network. The device makers often restrict its users to be on the networks controlled by them, which may use private/proprietary protocol to ensure greater security. But, do proprietary protocols and security schemes inherently increase the data security? Does it compromise interoperability and possibly limit the business opportunity for the device maker?

Then there are questions about ethics and governance, often dealt in the judicial context. How aware and informed are the policymakers and how capable is our judicial system to deal with the privacy and security issues? Each government is responsible for the safety and well-being of its citizens, yet spying and espionage have been used for millennia in the interest of national security. Where is the balance and how does one define it?

If you believe that standards are important in this area, naturally the questions are who develops these standards, how can I participate in it and how do I become aware of such standards? It is also important to know which standards development organizations (SDOs) are focused on this area and how do they collaborate among themselves to create an ecosystem of and around such standards.

This brings me to the need for standards and education in this important field. I firmly believe that you are as secure as you are informed and aware. Just as one has to be aware of pickpockets and robbers in the real world, one has to be informed and aware of cybersecurity issues while using gadgets in the digital world. So in this quarterly issue of the IEEE Standards Education eMagazine, we have contributors from the industry and academia sharing insightful information. We also have a list of existing standards as well as those under development shared by IEEE Standards Association. As always, we have included student paper, funny pages and links to a number of public articles and other information that you may find useful.

Happy reading, and be safe in the digital world!

Yatin Trivedi
Editor-in-Chief, SEC eZine
Member, IEEE-SA Board of Governors
ytrivedi@ieee.org

Yatin Trivedi, Editor-in-Chief, is a member of the IEEE Standards Association Board of Governors (BoG) and Standards Education Committee (SEC), and serves as vice-chair for Design Automation Standards Committee (DASC) under Computer Society. Since 2012 Yatin has served as the Standards Board representative to IEEE Education Activities Board (EAB). He also serves on the Board of Directors of the IEEE-ISTO and on the Board of Directors of Accellera.

Most recently, Yatin served as Director of Strategic Marketing at Synopsys. In 1992, Yatin co-founded Seva Technologies as one of the early Design Services companies in Silicon Valley. He co-authored the first book on Verilog HDL in 1990 and was the Editor of IEEE Std 1364-1995™ and IEEE Std 1364-2001™. He also started, managed and taught courses in VLSI Design Engineering curriculum at UC Santa Cruz extension (1990-2001). Yatin started his career at AMD and also worked at Sun Microsystems.

Yatin received his B.E. (Hons) EEE from BITS, Pilani and M.S. Computer Engineering from Case Western Reserve University. He is a Senior Member of the IEEE and a member of IEEE-HKN Honor Society.

IoT Security Standards – Paving the Way For Customer Confidence

by Alan Grau

With the opening of the Consumer Electronics Show in Las Vegas, the IoT has moved beyond the initial hype phase and even past the phase of early deployments into what I call the "parental awareness phase". That is to say, my parents, both of whom first setup a Facebook account just a few months ago, have now heard of the IoT. This morning my mom asked me if I was going to the show in Vegas to learn about the "new IOT electronics".
However, if my mom were to ask an employee at BestBuy, "Is this new Internet of Things thermostat, garage door opener, or smart door lock, secure", I don't think she would get an accurate answer today.

In July of 2014, HP Labs did a study of 10 popular IoT devices and found that the security was shockingly bad. The researchers studied 10 devices, looking at the end-to-end security capabilities of these devices including privacy protection, authorization, encryption, user interface protection, and code security.
They found that 70% of the devices had at least one MAJOR vulnerability! By the time they completed their study, the researchers identified over 250 vulnerabilities, an average of 25 security vulnerabilities per device. Security was clearly an afterthought – or worse – for these devices.

An average consumer, or even a security savvy consumer, has little ability to know which brand of IoT device has better security or even any security. An OEM may claim "built-in security", but that phrase alone means little.

The Role of Security Standards
IoT standards groups are emerging to address issues of interoperability, communication protocols and, yes, security.
At the end of the day, if security standards for IoT devices are to be useful, they must help the average consumer evaluate the security of an IoT device. As these standards are being developed, they should maintain focus on this end goal.

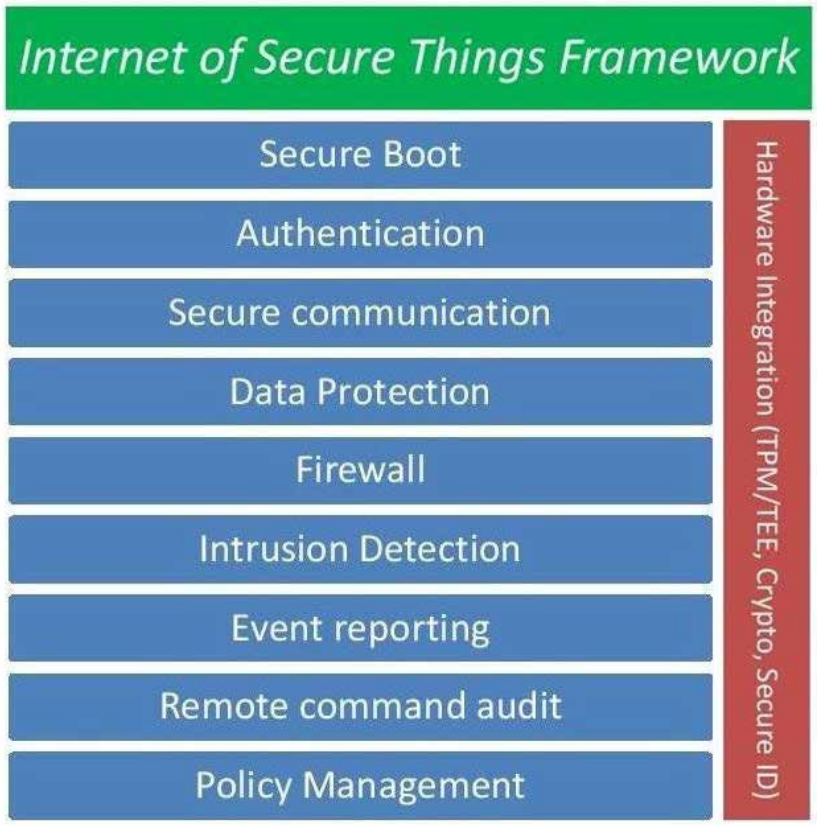
Achieving this will undoubtedly take time, but it is, in my mind, the only true measure of success. IoT security standards must aim to serve as the cyber equivalent of an Underwriters Laboratories (UL) or CE safety ratings. Standards groups should strive to create an IoT Security Standard (ISS) that is measurable and defines a minimum standard of security for devices. Consumers can trust that devices that are ISS rated provide a reasonable or acceptable level of security for common use.

This security rating could one day be used by the insurance industry in evaluating cyber-insurance claims and big-box retailers could choose to only sell ISS rated products. Most importantly of all, consumers such as my parents would have some way to evaluate the security of products they purchase.

The electrical power infrastructure and industrial automation markets are already moving in this direction with the and IEC security standards that apply to their respective markets. NERC-CIP defines a set of security requirements for equipment operating within the North American power grid. IEC-62443 is a security standard for industrial automation and control systems. Each of these creates a baseline that device OEMs must meet when developing their products. If a device meets these security requirements the user can be assured that the device meets this baseline for security.

Creating a Security Standard
Cyber security is a difficult challenge and it would be naïve to think that we will see a security standard that will eliminate all risks of cyber-attacks against IoT devices anytime soon. Even so, a security standard can ensure that devices meet reasonable standards for security. There are a number of fundamental security capabilities that should be included in any IoT device.

We have defined a framework for IoT device security that provides a number of essential security features.
A security framework provides a foundation for evaluating and verifying the security capabilities of IoT devices.



A security framework provides a foundation for evaluating and verifying the security capabilities of IoT devices.

There are many elements that must be addressed in any IoT security standard. Hackers thrive by discovering the weak link in a security implementation. Systems or standards that fail to provide complete, end-to-end security are bound to fail.

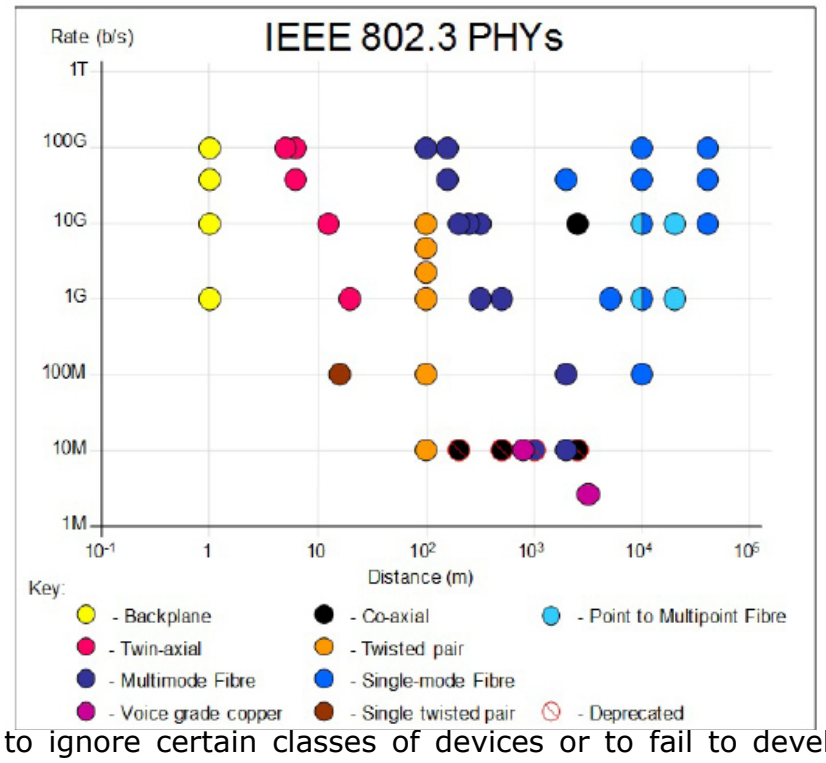
A successful security standard will provide:

- Protection for the device: by ensuring only authentic code from a trusted source is allowed to run on the device.
- Protection for data: by providing secure communication, data-at-rest protection and secure decommissioning of devices.
- Awareness of attacks: by including security monitoring, intrusion detection and integration with security management systems.
- Security management: enabling updates to security policies in response to emerging threats.
- Machine to machine authentication: ensuring that IoT devices are only communicating with other known, trusted entities.

Challenges for IoT Security Standards

In addition to the normal challenges of creating standards, an IoT security standard must address the challenge of scalability. IoT devices range from very small, very cost sensitive sensors using mesh networking technologies to sophisticated gateway devices and sophisticated endpoint devices such as cars, industrial automation controllers and weather satellites. The security requirements, potential attack vectors and computing resources available for security vary widely between these devices.

While this is a challenge, it must not become an excuse



to ignore certain classes of devices or to fail to develop a standard. The embedded computing industry has developed sophisticated hardware and software systems that scale to meet the computing and price challenges of this vast range of devices. I have no doubt the industry is also capable of developing security standards, and the corresponding implementations, that scale to meet these diverse requirements.

"IoT Security Standards need to provide broad protection from cyber-attacks"

Getting started

As shown by the HP Labs research study of IoT device security, we clearly have a long way to go, and we must get started today. Just because there are no standards in place, companies building IoT devices must not wait to start implementing security. Solutions exist today to help OEMs build security into their devices and if they begin building security into their devices today, they will have a head start as security standards are defined.

Better yet, companies can be proactive and help define the standards. This will allow them to align product development efforts with emerging standards, ensuring compliance as standards are released. Getting started today on adding security only benefits both the companies building the products and the consumers that use them.

Emerging standards for IoT security

As an emerging market, Security standards are still evolving for IoT devices. Many of the existing security standards are focused on a specific industry or sector. NERC-CIP security standards , for example, were developed specifically for the electric utility industry. A similar, but more encompassing security standard is the NIST Cybersecurity Framework which is applicable to financial, energy, healthcare and other critical systems, and is designed to help these industries better protect their information and physical assets from cyber-attack. In the medical arena, the U.S. Food and Drug Administration has provided recommendations to manufacturers for managing cybersecurity risks to better protect patient health and information.

In addition to these industry specific security standards, a number of new standards specifically for IoT services are beginning to emerge. These standards are beginning to address a wide range of security concerns including security protocols for communication between IoT devices, threat modeling, device protection requirements, security architectures, secure software development processes and security robustness testing.

In addition, a number of IEEE standards address security elements that are applicable to the Internet of Things. These include: IEEE P1363 a standard for Public-Key cryptography, IEEE P1619 which addresses encryption of data on fixed and removable storage devices, IEEE P2600 , a standard that addresses security of printers, copiers and similar devices, and IEEE 802.1AE and IEEE 802.1X which address Media Access Control (MAC) security.

Summary

The IoT has entered a phase of mass usage and it will nolonger be acceptable that 70% of IoT devices have a major security vulnerability. It will take time for security standards to reach a level where customers can feel confident in the security of a device based on a security rating, but we must start moving in that direction.

While security standards are being developed, OEMS can begin building security into their devices to get started in creating the Internet of Secure Things.

- Source: Mathew Sparks, The Telegraph.co.uk. Average Internet of Things device has 25 security flaws. http://www.telegraph.co.uk/technology/internet-security/11000013/Average-Internet-of-Things-device-has-25-security-flaws.html
- Source: HP Intenet of Things Research Study. http://fortifyprotect.com/HP_IoT_Research_Study.pdf

Alan Grau
President and co-founder of Icon Labs
alan.grau@iconlabs.com

Alan Grau is President and co-founder of Icon Labs, a leading provider of security software for IoT and embedded devices. He is the architect of Icon Labs' award winning Floodgate Firewall. Icon Labs was named a 2014 Gartner "Cool Vendor" and 2015 Gartner "Select Vendor", and is focused on creating The Internet of Secure Things by providing a security from for even the smallest IoT devices.

Alan has 25 years' experience in telecommunications and embedded software marketplace. On December 29, 1992 Alan co-founded Icon Labs, an embedded systems software development company whose clients include Motorola, Lucent Technologies, Intel and Tellabs. Prior to founding Icon Labs he worke for AT&T Bell Labs and Motorola. Alan has an MS in computer science from Northwestern University.

Security and IoT in IEEE Standards

by Marco A. Hernandez

Security elements have been included in numerous IEEE standards and standards projects over many years. If one searches the IEEE standards status report[1] by entering "security," and views the project scope, purpose and/or abstract, multiple references to security can be seen. These standards and standards projects cover topics as diverse as vehicle communications, smart grid technologies, personal health devices, networking, mobile devices, and storage devices. All these and more could conceivably be part of the Internet of Things (IoT). A number of these standards were developed before the term "Internet of Things" became widely used.

IoT Architecture

IEEE has a specific initiative (one of IEEE's important, multi-disciplinary, cross-platform Initiatives) for the Internet of Things (IoT). The IEEE IoT website includes a link for educational resources such as webinars, other videos, and podcasts. The link to the IEEE-SA IoT website is for standards and related information. In particular, the project IEEE P2413 , Standard for an Architectural Framework for the Internet of Things (IoT), has a subworking group focused on Quadruple Trust i.e. "Protection, Security, Privacy and Safety". This involves a holistic end-to-end approach, including development of a threat model for IoT.[2] This considers the various vertical applications for IoT and documentation of architecture needs to address the threat model. The participants in IEEE P2413 include representatives from major corporations involved in IoT from regions around the world and provide expertise in all aspects of IoT including security and compliance. To involve startup companies, IEEE-SA hosts a number of events where the companies can present their projects for evaluation as well as learn about the IEEE's activities in IoT.

The following are examples of IEEE standards and projects related to security and IoT.

Cryptography

- The IEEE 1363 series of standards for public key cryptography beginning with IEEE 1363-2000, IEEE Standard Specifications for Public-Key Cryptography, and including IEEE 1363a-2004, IEEE 1-2008, IEEE 1363.2-2008, IEEE 1363.3-2013 is developed by 1363 WG.
- The IEEE 1619 series of standards for encryption in storage media beginning with IEEE 1619-2007, IEEE Standard for Cryptographic Protection of Data on Block-Oriented Storage Devices, and continuing with IEEE 1619.1-2007, IEEE 1619.2-2010 is developed by SIS-WG, Security in Storage Working Group.
-

Devices and sensors/actuators

- Within the IEEE 1451/ 21450[3]/21451 series of standards for transducers for sensors and actuators including IEEE 21451-1-2010, IEEE21451-2-2010, IEEE 21451-4-2010, IEEE 21451-7-2011, a new project IEEE P24151-1-4, Standard for a Smart Transducer Interface for Sensors, Actuators, and Devices – eXtensible Messaging and Presence Protocol (XMPP) for Networked Device Communication, being developed by the XMPPI – XMPP Interface Working Group, specifically addresses issues of security, scalability, and interoperability in session initiation and protocol transport.
- IEEE 2410-2015, IEEE Standard for Biometric Open Protocol, provides "Identity assertion, role gathering, multilevel access control, assurance, and auditing"[4] and was developed by the BOP – Biometrics Open Protocol working group.
- A new project approved in 2015, IEEE P1912, Standard for Privacy and Security Architecture for Consumer Wireless Devices, being developed by the P1912 WG will describe a common communication architecture and approaches for end user security including device discovery/recognition, user authentication, and user control of tracking items/people and sharing of information.
- IEEE 2600-2008, IEEE Standard for Information Technology: Hardcopy Device and System Security, covers printers, copiers and multifunction devices. It defines security requirements such as authentication, authorization, privacy, integrity, device management, physical security and information security.

Networking for IoT

- IEEE 802.1X-2010, IEEE Standard for Local and metropolitan area networks–Port-Based Network Access Control, covering common architecture, functional elements, and protocols for mutual authentication and secure communication between the clients of ports attached to the same LAN and its amendment IEEE 802.1Xbx-2014 were developed by 1 – Higher Layer LAN Protocols Working Group.
- IEEE 802.1AE-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security, specifies "how all or part of a network can be secured transparently to peer protocol entities that use the MAC Service provided by IEEE 802 LANs to communicate."[5] Its amendment IEEE 802.1AEbw-2013 expands its security capabilities. These were developed

by 1 – Higher Layer LAN Protocols Working Group.

- IEEE 802.1AR-2009, Standard for Local and metropolitan area networks – Secure Device Identity, enables the secure association of locally significant device identities with manufacturer provisioned identities for use in provisioning and authentication protocols and was developed by 1 – Higher Layer LAN Protocols Working Group.
- The latest editions of IEEE 11-2012, IEEE Standard for Information technology–Telecommunications and information exchange between systems Local and metropolitan area networks–Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications developed by WG802.11 – Wireless LAN Working Group and IEEE 802.15.4-2015, IEEE Standard for Local and metropolitan area networks–Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs) developed by WG802.15 – Wireless Personal Area Network (WPAN) Working Group include extensive sections on security.
- IEEE project 15.9, IEEE Draft Recommended Practice for Transport of Key Management Protocol (KMP) Datagrams, developed by WG802.15 – Wireless Personal Area Network (WPAN) Working Group provides guidelines for support of key management in IEEE 802.15.4.
- IEEE 802.21a-2012, IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services – Amendment for Security Extensions to Media Independent Handover Services and Protocol was developed by 21 – Media Independent Handoff Working Group.
- The IEEE 1888 series beginning with IEEE 1888-2014, IEEE Standard for Ubiquitous Green Community Control Network Protocol, and including IEEE 1888.1-2013, IEEE 1888.2-2014 has a specific standard for security IEEE 1888.3-2013, IEEE Standard for Ubiquitous Green Community Control Network: Security was developed by UGCCNET-SEC/P1888.3 WG – Ubiquitous Green Community Control Network: Security Working Group/UGCCNET-SEC/P1888.3. It includes security requirements, architecture, authentication, authorization, and security procedures and protocols.

Infrastructure systems (note – intranets may incorporate IoT while not necessarily connected to the public internet.)

- IEEE 692-2013, IEEE Standard for Criteria for Security Systems for Nuclear Power Generating Stations, developed by WG 3.2 – Security Systems Working Group addresses security system equipment for "detection, assessment, surveillance, access control, communication, and data acquisition".
- The numerous IEEE smart grid systems standards[6] include a number focused on security, e.g. IEEE C37.240-2014 – IEEE Standard Cybersecurity Requirements for Substation Automation, Protection, and Control Systems developed by 240 WG – PC37.240 Cyber Security Standard and IEEE 1686-2013 – IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities developed by WGC1 – Substations Working Group C1.

Other Considerations

It should be noted that IEEE P2413 includes in its definition for properties of the "thing" in the Internet of Things, virtual properties such as might be derived from big data analysis. The IEEE Big Data Initiative includes standards development as a key focus area. Privacy and security remains a concern for Big Data.

While not official IEEE standards, the documents "Building Code for Medical Device Software Security", and "Avoiding the Top 10 Software Security Design Flaws" provide guidance for software designers including those involved in software for IoT. They were developed as part of the IEEE Cybersecurity Initiative.

In addition to IEEE, other organizations are also involved in standards for IoT and security. Another article "IoT Interoperability Requires Security" includes along with IEEE, descriptions of the work in several of these organizations.

[1] http://standards.ieee.org/develop/project/status.html

[2] http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf

[3] http://standards.ieee.org/findstds/standard/21450-2010.html

[4] http://standards.ieee.org/findstds/standard/2410-2015.html

[5] http://standards.ieee.org/findstds/standard/802.1AE-2006.html

[6] http://smartgrid.ieee.org/resources/standards

Cherry Tom
Emerging Technologies Intelligence Manager, IEEE Standards Association
c.tom@ieee.org

Cherry Tom is Emerging Technologies Intelligence Manager for the IEEE Standards Association. In her role, she is seeking to establish IEEE communities in emerging technologies for standards and/or standards related projects. This involves collaboration with experts from other parts of IEEE, notably Technical Activities and IEEE societies, as well as organizations outside of IEEE including corporations, universities, government agencies, and consortia. Among current topics of interest are Big Data and Artificial Intelligence. Prior to joining IEEE, she worked for a large telecommunications company and a wireless startup where she managed standards and regulatory strategies, and participation in US and global standards developing organizations.

New Approaches by Colleges and Universities in Cyber Security Education

by William Butler, William "Vic" Maconachy, Helen G. Barker

The Evolving Internet of Things (IoT) Requires New Approaches by Colleges and Universities in Educating All Students in Cyber Security

Abstract

The Internet of Things (IoT) is quickly evolving with 2016 predicted to be a critical year for the growth of connected devices, the sheer volume of data captured, and the types of 'things' connected (human-to-machine, machine-to-machine). The machine-to-machine category is growing at an exponential rate along with the data captured and communicated to databases for categorization and analysis. Colleges and universities are challenged to educate students across curriculum to understand the underlying technologies and the application of this technology to solve everyday problems. Students must learn that the IoT surrounds them and is already a critical aspect of their daily lives. Business, engineering, computer science, and cyber security departments across the country must plan to address student awareness through revamped departmental curricula and interdisciplinary opportunities across departments. It is this generation of future workers who will be tasked to solve the issue of security within the IoT. This article does not advocate a new degree, but, rather, a comprehensive interdisciplinary systems approach.

Introduction

In January 2016, a panel of experts discussed IoT security and privacy issues at the Consumer Electronics Show (CES) in Las Vegas, NV and drew attention to the rapid spread of devices connected to the net. The panel cited the following facts:

- There are 25 billion connected devices;
- There are more devices than humans on earth;
- Devices exchange data without human intervention and can be remotely activated;

90 percent of connected devices are sharing personal information with more than 70 percent of those devices sharing information on unencrypted networks (Mansell, 2015).

With that degree of proliferation, cyber criminals are viewing the spread of unprotected Internet-connected devices throughout the world as a welcome target in end-point device compromise. Compromising these Internet-connected devices is the first step in infiltrating the enterprise networks of major corporations and governments.

Business leaders, cyber security and network design professionals, as well as software and hardware vendors, face new challenges in protecting their network infrastructures and the Internet-connected devices. Colleges and universities must step up and address these new security challenges within their curricula to better prepare students for the security challenges they will face in the workplace. This paper discusses the Internet of Things (IoT) security challenge and some actions educators can take to begin to address this growing problem.

The IoT Defined

There are many definitions for the Internet of Things (IoT). The IEEE definition of the IoT is, "A network of items — each embedded with sensors — which are connected to the Internet" IEEE, 2015. The IoT has also been referred to as Cyber Physical Systems (CPS), M2M (machine to machine), and simply Industrial Internet and Connected devices. Figure 1 depicts the generic topology of the IoT viewed in layers to include the Datacenter, Gateway, IoT Devices and Sensors. Figure 1 also depicts that within the IoT architecture, data is acquired by smart devices, aggregated at the gateway and categorized and analyzed at datacenters in order to present the data as useful information to the consumer. Figure 1 also accounts for legacy devices (brown field) and new devices (green field), which when deployed on the same network present complex integration challenges to network and security operations.

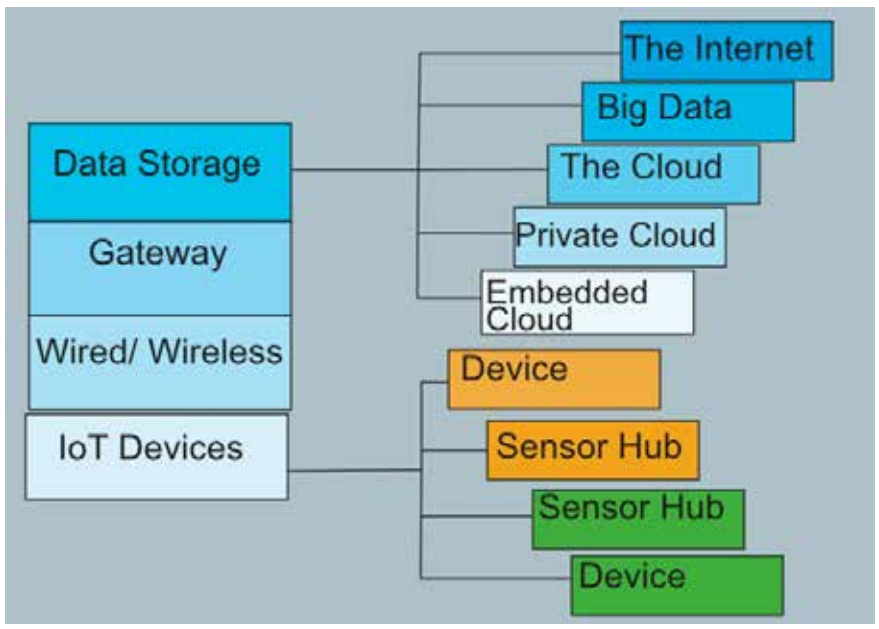


Figure 1: IoT Topology. Michael Strittmatter (2016). Based on diagram in Internet of Things Topology, Wind River (2015).

Internet-Connected Devices

As mentioned by the Cloud Security Alliance (CSA, 2015) the major stakeholders in the IoT ecosystem are banking and finance, public services, manufacturing, smart city, retail, health and energy. IEEE, 2015 also identified additional stakeholders such as consumers, regulators, and insurance companies. In the healthcare sector Internet-connected devices range from fitness watches to heart pacemakers. In the energy sector utilities have implemented smart meters connecting our homes to our utility company via a wireless Internet connection.

According to the World Semiconductor Trade Statistics, automobile safety systems are equipped with a swarm of 28 sensors (WSTS, 2013). These automobile sensors detect conditions such as tire air pressure, air bag pressure, and collision detection. These sensors also control the critical road-to-vehicle and vehicle-to-vehicle communications systems.

In the retail sector stores are using automated checkout, proximity advertising and smart vending machines. Smart cities have implemented smart meters, traffic management systems, and video surveillance for public safety. In the manufacturing sector factories are using robotics to assemble cars, and RFID sensors are used for inventory control and tracking the movement of goods (CSA, 2015).

While the list of stakeholders and industry examples are not all-inclusive, it does offer significant evidence of the need for cross-field training and awareness. Auto manufacturing provides a good example of multiple stakeholder involvement. Potential system vulnerabilities must be minimized in the R&D phase. Failure to do so ultimately affects the end users, which will then return to impact the business operation through events such as recalls and lawsuits. Awareness through training and education will help mitigate these issues.

The Threat Is Real

The threat to these Internet-connected devices is very real and continues to evolve quickly as public reliance on these devices increases. On September 10, 2015, the U.S. Federal Bureau of Investigation (FBI) issued Internet Crime Complaint Center (IC3) Alert # I-91015-PSA which alerted the public to the emerging threat to the IoT presented by cyber criminals (FBI, 2015). FBI Alert #I-91015-PSA not only defined IoT devices but also discussed the risks posed to these devices by cyber criminals.

FBI Alert #91015-PSA also discussed several reported incidents worth noting in this article. First, cyber criminals exploited gaps in a closed circuit TV system rendering this countermeasure useless to security officers. Second, criminals can exploit unsecured wireless connections for automated devices, such as security systems, garage doors, thermostats, and lighting. Third, cyber criminals can originate e-mail SPAM attacks from home-networking routers, connected multi-media centers, televisions, and appliances. Lastly, cyber criminals can exploit security weaknesses in monitoring systems embedded in our control networks in power generating and distribution systems (FBI, 2015).

In 2015, hackers exploited the vehicle control system of a Jeep Cherokee driven by *Wired Magazine* reporter Andy Greenberg by compromising these same communications systems while the reporter drove the vehicle down the highway in St. Louis (Grenoble, 2015). In February 2015, during a CBS *60 Minutes* episode, Defense Advanced Research Projects Agency (DARPA) scientists demonstrated a similar compromise of automobile systems such as brakes and wiper systems of a vehicle driven by 60 Minutes reporter Leslie Stahl (CBS, 2015). In July 2015, these two much-publicized incidents may have prompted U.S. Sens. Edward Markey (D-Mass.) and Richard Blumenthal (D-Conn.) to introduce a bill forcing automobile makers to offer more protections (Grenoble, 2015).

The Challenge

The challenges in protecting Internet-connected devices such as those in automobiles from threats are many. Cyber security experts protect these Internet-connected devices by applying the three pillars of cyber security: confidentiality, integrity, and availability, also known as CIA. One issue with such IoT devices is the generally limited processing power, memory, storage, communications capabilities, and power built into the systems, all of which are required at a more enhanced level than exists to support the use of encryption, strong authentication mechanisms, and virtual private networks (VPN) (CISCO, 2015). Protecting these devices will require some new thinking from hardware and software vendors as well as current and future cyber security experts. In addition, there needs to be a focus on partnerships between future technical (e.g. engineers) and cyber security experts. The first step in this new partnership should be with educational institutions of higher education. Interdisciplinary communication on associated topics offers the potential of greater understanding to properly address these issues. Cooperation in solving these developmental issues will go a long way towards reducing the vulnerabilities, which currently exist in IoT devices and systems.

An additional challenge is protecting millions of legacy devices currently in use, which do not have the capability to implement the latest countermeasures. Similar to systems in automobiles, these devices fall short of the required technical capabilities that would allow the implementation of stronger encryption standards, or any encryption for that matter, and are limited by the devices processing power, power, memory, and storage and communications capability. These limitations also affect the device's ability to support strong authentication. The use of VPN connectivity is a possible countermeasure which provides device-to-network confidentiality. Another threat lies in the chips at the center of IoT devices, which are globally sourced requiring the supply chain be assured against counterfeit chips and other inserted components (Leef, 2015).

From an enterprise network perspective, managing and protecting potentially millions of devices that are constantly connecting and disconnecting from the enterprise network is a huge challenge and concern. Such devices require logical and physical security integration. The physical security of a device can be easily compromised if cyber criminals gain physical access to that device and overcome whatever security measures happen to be implemented. New countermeasures such as *kill switches* (permanently

disable the device), and *remote wipe* (remote erasure of contents of memory and storage) must be implemented to prevent compromise of collected data on the device, user credentials and more importantly the enterprise network via the compromised device.

Countermeasures

In addition to noting vulnerabilities in IoT devices, FBI Alert #91015-PSA also lists viable countermeasures which can be implemented to protect these Internet connected devices. These countermeasures are routinely applied to more capable network devices by cyber security professionals; however the physical limitations of IoT devices will limit the viable security options. We previously mentioned measures such as encryption, strong authentication and VPN's exceed the ability of the IoT device to implement security measures due to limited memory, power, storage and CPU power. With that said the FBI offers some very basic common sense measures that are often overlooked and not implemented. For example consumers should purchase devices for the intended purpose, change the default passwords, and update the software when patches become available.

IoT device security must be evaluated under a risk management framework so that threats and vulnerabilities can be systematically identified and appropriate countermeasures devised and implemented by cyber security professionals. The application of a formal risk management process by the organization will help identify measures, which effectively address each vulnerability. While protecting IoT devices is far from business as usual for cyber security professionals, using a systematic approach to address the threat is the best course of action to achieve IoT-related security.

Conclusion

While the Internet of Things promises added convenience and efficiency, it also brings a new dimension of cyber and physical security issues. With the current rush to market mentality of device and network developers, future retroactive security solutions will be left to the next generation of security solution providers. Colleges and universities will be challenged to address IoT security via traditional departmental curricula and approaches. Solutions to the IoT security challenges are both multidimensional and interdisciplinary. Business and educational leaders must assure the supply chain of chips and other vital components, protect consumer privacy, and understand that their future success will be based on how well they harness the power of IoT technology to provide new sources of immense amounts of data about their customers and the business environment. Engineers and computer scientists must understand cloud computing and design IoT devices and supporting networks which can be protected utilizing best practices in secure coding, tamper resistant hardware and more secure networks utilizing strong encryption and authentication, and VPNs. Cyber security academics and other professionals are challenged to identify best security practices to be applied throughout IoT and supporting networks lifecycle (from concept to disposal) using an interdisciplinary systems approach. As Chris Rouiland, founder and CTO of Bastille, a provider of threat detection software for IoT devices recently noted, "Enterprises will start to find that compromises are entering their networks through things like wearables, m2m communications and industrial control systems" (All, 2016). While the IoT presents the promise of helping people, especially those with disabilities to lead more productive lives, the threats posed by IoT insecurity will emerge as the number one cyber challenge in the very near future. America's higher education system must be prepared to provide the next generation multi-disciplined cyber security solution providers.

References

CBS (2015). CBS News 60 Minutes Program (video) 6 Feb 2015. Retrieved from http://www.cbsnews.com/news/car-hacked-on-60-minutes/

CISCO (2015). Securing the Internet of Things: A Proposed Framework. Retrieved from http://www.cisco.com/web/about/security/intelligence/iot_framework.html

Cloud Security Alliance (2015). Security Guidance for Early Adopters of the Internet of Things – April 2015, https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

All, A. (2016). eSecurity Planet. Webcam Hack Shows IoT Security Threat. Retrieved from: http://www.esecurityplanet.com/print/network-security/webcam_hack. January 12, 2016.

Federal Bureau of Investigation (FBI) (2015). Internet Cyber Crime Center (IC3), Alert Number I-091015-PSA (September 10, 2015). Retrieved from http://www.ic3.gov/media/2015/150910.aspx

Grenoble, R. (2015). Hackers Hijacked A Jeep With A Reporter Inside, And 5 Other Scary Hacks. Retrieved from http://www.huffingtonpost.com/entry/hackers-hijacked-a-jeep-with-a-reporter-inside-and-5-other-scary-hacks_55ae9091e4b0a9b94852b44f

Institute of Electrical and Electronics Engineers (IEEE) (2015). Towards a definition of the Internet of Things. Retrieved from http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf

Leef, S. (2010). Internet of Things meets Hardware Cybersecurity. Retrieved from http://www.oregontechtalks.org/speakers/2015Files/SergeLeef.pdf

Mansell, W. (2015). Policy Makers Try To Define Security, Privacy With The IoT. Retrieved from http://www.idigitaltimes.com/policy-makers-try-define-security-privacy-iot-501712

Sorrell, S. (2015). Juniper Networks: The Internet of Things: Consumer, Industrial & Public Services 2015-2020, http://

www.juniperresearch.com/researchstore/key-vertical-markets/internet-of-things/consumer-industrial-public-services

Wind River (2015). Security in the Internet of Things. Retrieved from http://www.windriver.com/whitepapers/security-in-the-internet-of-things/wr_security-in the-internet-of-things.pdf

World Semiconductor Trade Statistics (WSTS) (2013). The smart and connected vehicle and the Internet of Things San Diego CA. Retrieved from http://tf.nist.gov/seminars/WSTS/PDFs/1-0_Cisco_FBonomi_ConnectedVehicles.pdf

Dr. William "Vic" Maconachy
VP for Academic Affairs, Capitol Technology University
wvmaconachy@captechu.edu

In October, 2007, Dr. Maconachy assumed the position of Vice President for Academic Affairs/Chief Academic Officer at Capitol Technology University, Laurel, MD. Dr. Maconachy is charged with sustaining and enhancing the academic quality of programs of study ranging from Business Administration through Engineering, Computer Science and Information Assurance. He also oversees the operations of Distance Learning Services, the Library, The Cyber Battle Lab, and the Space Operations Institute. He is the liaison officer for the university to the Middle States Association. Dr. Maconachy holds the rank of professor, and teaches graduate and undergraduate research courses in Information Assurance.

Prior to Joining Capitol College Dr. Maconachy served at The National Security Agency. While there he held several leadership positions. He was appointed by the Director of the NSA as the Deputy Senior Computer Science Authority where he built a development program for a new generation of Cryptologic Computer Scientists. Prior to this position, Dr. Maconachy served as the Director of the National Information Assurance Education and Training Program (http://www.nsa.gov/ia/academia/acade00001.cfm). He was responsible for implementing a multidimensional, interagency program, providing direct support and guidance to the services, major DoD components, federal agencies, and the greater national Information Infrastructure community. This program fosters the development and implementation of Information Assurance training programs as well as graduate and undergraduate education curricula. In this capacity, he served on several national level government working groups as well as in an advisory capacity to several universities. Dr. Maconachy was the principal architect for several national INFOSEC training standards in the national security systems community. During Dr. Maconachy's time at the National Security Agency he held many different positions, including work as an Information Assurance Operations Officer, Information Assurance Analyst and a Senior Manager.

Prior to joining the NSA, Dr. Maconachy worked for the Department of Navy. He developed and implemented INFOSEC training programs for users and system maintainers of sophisticated cryptographic equipment. He also served as the Officer In Charge of several INFOSEC-related operations for the Department of Navy, earning him the Dept. of Navy Distinguished Civilian Service medal. Dr. Maconachy holds a Ph.D. from the University of Maryland. He has numerous publications and awards related to Information Assurance, and is the recipient of the prestigious National Cryptologic Meritorious Service Medal. Dr. Maconachy is also the Co-Founder and current Chairman of the Colloquium for Information Systems Security Education (WWW.CISSE.info) CISSE is an international organization of professionals dedicated to advancing Information Assurance Higher Education.

Professor William Butler
Chair Cyber Security, Capitol Technology University
whbutler@captechu.edu

Bill Butler is Chair of the Cyber Security Program at Capitol Technology University. Bill has over twenty years' experience in the networking and engineering industries as an engineer and consultant. Bill served in the U.S. Marine Corps Reserves and retired as a Colonel. Bill is active in working groups such as the National Institute of Standards and Technology, Cloud Security Alliance, and the National CyberWatch Center. Bill holds degrees from Brenau University, U.S. Army War College, National Defense University, and the University of Maryland. Bill is currently completing his DSc in cyber security at Capitol focusing on preserving cell phone privacy.

Dr. Helen G. Barker
Dean of Academics,
Capitol Technology University
hgbarker@CapTechU.edu

Dr. Helen Barker serves as Dean of Academics with Capitol Technology University. Before joining Capitol in 2000, Dr. Barker worked in the private sector as a management analyst and resource training specialist in the Washington, DC area and a research analyst in child welfare and economic development in Northern Virginia. Dr. Barker received a B.S.B.A. from Thomas Edison State College, M.S.B.A. from Strayer University, M.S. in Information Telecommunications Management from Capitol Technology University, and doctorate from University of Phoenix in Organizational Leadership. Current research interests include pedagogy relating to online learning and integration of cyber security into business curriculum.

Internet of Things Requirements and Protocols

by Kim Rowe

Introduction

More and more protocols are being added for the Internet of Things (IoT) as large vendors address the deficiencies of their products. These higher level IoT protocols are suitable for a broad range of applications. For example, MQTT has been used for many years to manage messaging between server applications and has now been updated to address secure small client usage. DDNS has been used to provide browser access to web devices and CoAP has been extended with other protocols to provide security management and more robust operation. All of these protocols can be used for managing and configuring a plethora of home devices. A deeper understanding of these protocols, their security and configuration options and the applications requirements is required to properly select the best protocol for the application at hand.

Knowing the correct protocol or set of protocols for a given application which cover the communication, security, management and scalability is the first design consideration. After this, the best implementation of each of the protocols must be understood. From this understanding, the designer can select the optimal implementation of each protocol for the system and then from these, select the best set of protocol implementations for the system. This decision will be impacted by requirements decisions related to the supporting hardware which has been selected.

The protocol set selection problem is closely tied to the implementation of the protocol, hardware requirements specifications and the additional hardware and software components that support the protocol set. This makes the decision a very complex one. All aspects of deployment, operation, management and security must be considered as part of the protocol selection including the implementation environment and must be done within the requirements specifications.

For the IoT protocol space, standards are not yet converged for particular applications and the market ultimately decides which of these standards are most relevant. This is a problem and an opportunity. The protocol that is selected today may become obsolete in the future and may need to be replaced. Conversely, the protocol selected today could become the standard in the future. As a developer, predicting the converged protocol is usually the prudent path but implementation costs and risk must always be considered. Also using specific features of the hardware and operating system to implement the protocols and then using specific protocol, operating system and hardware features for application implementation can make future migration to a new protocol or porting the application to a completely new environment very difficult.

This article examines the range of protocols available, the specific requirements that drive the features of these protocols and considers the implementation requirements to build a complete system.

Protocols and Vendors

Most higher level IoT protocols were developed by specific vendors which typically promote their own protocol choices, don't clearly define their assumptions, and ignore the other alternatives. Higher level protocols for IoT do offer choices of different capabilities and features but relying on vendor information to select a specific IoT protocol or protocol set is problematic. Most comparisons which have been produced are insufficient to understand the tradeoffs due to the vendor's obfuscation and omissions.

IoT protocols are often bound to a business model; for example, Azure-IoT is linked to Microsoft analytics offerings primarily for large enterprises and Thread is linked to a consortium of hardware vendors and Google which want to dominate home automation. Other times these protocols are incomplete and/or used to support existing business models and approaches or they offer a more complete solution but the resource requirements are unacceptable for smaller sensors. In general, the key assumptions behind the use of the protocols are not clearly stated which makes comparison difficult.

The fundamental assumptions associated with IoT applications are:

- various wireless connections will be used,
- devices will range from tiny MCUs to high performance systems with the emphasis on small MCUs,
- security is a core requirement,
- operation may be discontinuous,
- data will be stored in the cloud and may be processed in the cloud,
- connections back to the cloud storage are required,
- and routing of information through wireless and wireline connections to the cloud storage is required.

Assumptions made by the protocol developers in addition to this list require deeper investigation and will strongly influence the features of the protocol they designed. By looking at the key features of these protocols and looking at the implementation requirements, designers can develop a clearer understanding of exactly what is required in both the protocol area and in the supporting features area to improve their designs. Before we look at this, let's review the protocols in question.

IoT or M2M Protocols

There is a broad set of protocols which are promoted as the silver bullet of IoT communication for the higher level machine to machine (M2M) protocol in the protocol stack. Note that these IoT or M2M protocols focus on the application data transfer and processing although some such as SNMP are focused more on remote node management. The following list summarizes the protocols generally considered.

- Azure-IoT
- CoAP
- Continua – Home Health Devices
- DDS
- DPWS: WS-Discovery, SOAP, WSAddressing, WDSL, & XML Schema
- HTTP/REST
- MQTT and MQTT-SN/S
- SNMP
- Thread
- UPnP
- XMPP
- ZeroMQ

These protocols have their features summarized in the following table. Several key factors related to infrastructure and deployment are considered separately below.

Key Protocol Features

Communications in the Internet of Things (IoT) is based on the Internet TCP/UDP protocols and the associated Internet protocols for setup which means either UDP datagrams of TCP stream sockets. Small device developer claim that UDP offers large advantages in performance and size which will in turn minimize cost. It is not significant in many instances.

Stream sockets suffer a performance hit but they do guarantee in-order delivery of all data without errors. The performance hit on sending sensor data on an STM32F4 at 167MHz is less than 16.7% (measured with 2KB packets, smaller packets reduce the performance hit). By using stream sockets, standard security protocols can also be used. Similarly, the difference in memory cost for an additional 20K of flash and 8K of RAM to upgrade to TCP is generally small.

Messaging the common IoT approach is very important and many protocols have migrated to a publish subscribe model. With many nodes connecting and disconnecting, and these nodes needing to connect to various applications in the cloud, the publish/subscribe request/response model has an advantage. It responds dynamically to random on/off operation and can support many nodes.

Two protocols: CoAP and Http/REST are both based on

Protocol	*Transport*	*Messaging*	*2G,3G,4G (1000's)*	*LowPower and Lossy (1000's)*	*Compute Resources*	*Security*	*Success Stories*	*Arch*
Azure-IoT	AMPQ or Https/TCP	Rqst/Rspnse	Excellent	Good	10K-100Ks RAM Flash	High-Manditory	Weraables	Client-Server
CoAP	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	Medium - Optional	Utility field area ntwks	Tree
Continua HDP	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	None	Medical	Star
DDS	UDP	Pub/Subsrb Rqst/Rspnse	Fair	Poor	100Ks/RAM Flash +++	High-Optional	Military, Industrial	Bus
DPWS	TCP		Good	Fair	100Ks/RAM Flash ++	High-Optional	Web Servers	Client Server
HTTP/ REST	TCP	Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	Low-Optional	Smart Energy Phase 2	Client Server
MQTT & MQTT-SN/S	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	Medium - Optional	IoT Msging	Tree
SNMP	UDP	Rqst/Response	Excellent	Fair	10Ks/RAM Flash	High-Optional	Network Monitoring	Client-Server
Thread	UDP	Rqst/Rspnse	Excellent	Excellent	10Ks/RAM Flash	High-Manditory	Nest?	Mesh
UPnP	UDP	Pub/Subscrb Rqst/Rspnse	Excellent	Good	10Ks/RAM Flash	None	Consumer	P2P Client Server
XMPP	TCP	Pub/Subsrb Rqst/Rspnse	Excellent	Fair	10Ks/RAM Flash	High-Manditory	Rmt Mgmt White Gds	Client Server
ZeroMQ	UDP	Pub/Subscrb Rqst/Rspnse	Fair	Fair	10Ks/RAM Flash	High-Optional	CERN	P2P

Using a POSIX/Linux API makes implementation of IoT protocols simpler because many of these protocols run above the transport layer. In the case of the Unison OS, it has most IoT protocols off the shelf providing a tiny, fast and simple multi-protocol option.

request response without a publish and subscribe approach. In the case of CoAP the use of 6loWPAN and the automatic addressing of Ipv6 is used to uniquely identify nodes. In the case of Http/REST the approach is different in that the request can be anything including a request to publish or a request to subscribe so in fact it becomes the general case if designed in this way. These protocols are being merged to provide a complete publish/subscribe request/response model with Thread as an example.

System architectures are varied, including client server, tree or star, bus, and P2P. The majority use client-server but others use bus and P2P approaches. A star is a truncated tree approach. Performance issues exist for these various architectures with the best performance generally found in P2P and bus architectures. Simulation approaches or prototype approaches are preferred early in design to safeguard against surprises.

Scalability depends on adding many nodes in the field, and having the cloud resources easily increased to service these new nodes. The various architectures have different properties. For client server architectures, increasing the pool of available servers is sufficient and easy. For bus and P2P architectures, scale is inherent in the architecture but there is no cloud services. In the case of tree or star connected architectures, there can be issues associated with adding extra leaves on the tree which burdens the communication nodes.

Another aspect of scalability is dealing with a large number of changing nodes and linking these nodes to cloud applications. As discussed, publish/subscribe request/response systems are intended for scalability because they deal with nodes that go off line for a variety of reasons, allows applications to receive specific data when they decide to subscribe and request data resulting in fine data flow control. Less robust approaches don't scale nearly as well.

Low Power and Lossy Networks have nodes that go on and off. This dynamic behaviour may affect entire sections of the network so protocols are designed for multiple paths dynamic reconfiguration. Specific dynamic routing protocols found in Zigbee, Zigbee IP (using 6loWPAN) and native 6loWPAN ensure that the network adapts. Without these features, dealing with these nodes becomes one of discontinuous operation and makes the resource requirements of the nodes much higher.

Resource requirements are key as application volume increases. Microcontrollers offer intelligence at very low cost, and have the capacity to deal with the issues listed above. Some protocols are simply too resource intensive to be practical on small nodes. There will be limitations around discontinuous operation and big data storage unless significant amounts of serial flash or other storage media are included. As resources are increased, to reduce overall system costs, aggregation nodes are more likely to be added to provide additional shared storage resources.

Interoperability is essential for most devices in the future. Thus far we have seen sets of point solutions but ultimately users want sensors and devices to work together. By using a set of standardized protocols as well as standardized messaging, devices can be separated from the cloud services that support them. This approach could provide complete device interoperability. Also, using intelligent publish subscribe options, different devices could even use the same cloud services, and provide different features. Using an open approach, application standards will emerge, but today, the M2M standards are just emerging and the applications standards are years in the future. All the main protocols are being standardized today.

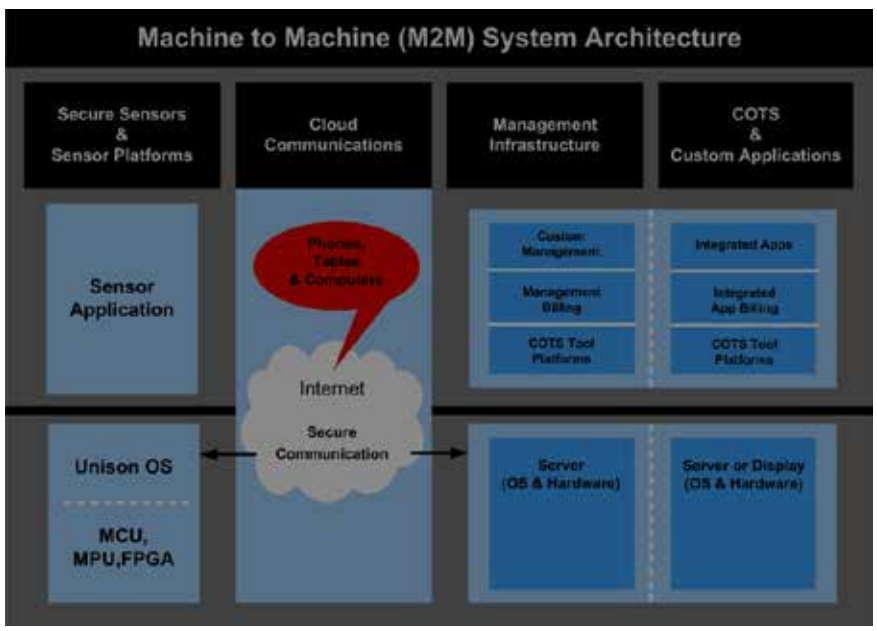
Security using standard information technology security solutions are the core security mechanisms for most of these protocols which offer security. These security approaches are based on:

- TLS
- IPSec / VPN
- SSH
- SFTP
- Secure bootloader and automatic fallback
- Filtering
- HTTPS
- SNMP v3
- Encryption and decryption
- DTLS (for UDP only security)

As systems will be fielded for many years, design with security as part of the package is essential.

Implementation Requirements

Privacy is an essential implementation requirement. Supported by privacy laws, almost all systems require secure communication to the cloud to ensure personal data cannot be accessed or modified and liabilities are eliminated. Furthermore, the management of devices and the data that appears in the cloud need to be managed separately. Without this feature, user's critical personal information is not protected properly – available to anyone with management access.



Separation of management and user data is a preferred solution to guarantee privacy for users. By using separate cloud solutions for management and user data this isolation and therefore improved security is provided.

Separation of management and user data is a preferred solution to guarantee privacy for users. By using separate cloud solutions for management and user data this isolation and therefore improved security is provided.

In the system architecture diagram we show the two separate components inside the cloud required for system management and application processing to satisfy privacy laws. Both components may have separate billing options and can run in separate environments. The management station may also include:

- system initialization
- remote field service options (ie field upgrades, reset to default parameters, remote test, …)
- control for billing purposes (account disable, account enable, billing features, …)
- control for theft purposes (the equivalent of bricking the device)

Given this type of architecture, there are additional protocols and programs which should be considered:

- Custom developed management applications on cloud systems.
- SNMP management for collections of sensor nodes.
- Billing integration programs in the cloud.
- Support for discontinuous operation using SQLite running on Unison OS to store and selectively update data to the cloud.

Billing is a critical aspect of commercial systems. Telecoms operators have demonstrated that the monthly pay model is the best revenue choice. In addition, automatic service selection and integration for seamless billing is important. Also credit card dependence creates issues including over the limit issues, expired cards and deleted accounts.

Self Supporting Users are a key to implementation success too. This includes things like remote field service so devices never return to the factory, intelligent or automatic configuration, online help, community help, and very intuitive products are all key.

Application Integration is important too. Today point systems predominate but in the future the key will be making sensors available to a broad set of applications that the user chooses. Accuracy and reliability can substantially influence application results and competition is expected in this area as soon as standard interfaces emerge. Indirect access via a server ensures security, evolution without application changes, and billing control.

Discontinuous Operation and Big Data go hand in hand. With devices connecting and disconnecting randomly, a need to preserve data for the sensors and update the cloud later is required. Storage limitations exist for both power and cost reasons. If some data is critical, it may be saved while other data is discarded. All data might be saved and a selective update to the cloud performed later. Algorithms to process the data can run in either the cloud or the sensors or any intermediate nodes. All of these options present particular challenges to the sensor, cloud, communications and external applications.

Multiple connection sensor access is also a requirement to make sensors truly available to a broad set of applications. This connection will most likely happen through a server to simplify the sensors and eliminate power requirements for duplicate messages.

IoT Protocols for the Unison OS

The Unison RTOS is targeted at small microprocessors and microcontrollers for IoT applications. As such it offers many of the things that you would expect are required. Unison has:

- POSIX APIs
- Extensive Internet protocol support
- All types of wireless support
- Remote field service
- USB
- File systems
- SQLite
- Security modules

and much more. This is in addition to off the shelf support and factory support for the wide set of protocols discussed here.

By providing a complete set of features and modules for IoT development along with a modular architecture, developers can insert their protocols of choice for IoT development. Building protocol gateways is also possible. This approach minimizes risk by eliminating lock in and shortening time to market.

Unison is also very scalable, which allows it to fit into tiny microcontrollers and also provide comprehensive support on powerful microprocessors. The memory footprint is tiny which leads directly to a very fast implementation.

Summary

Many protocols are being touted as ideal Internet of Things (IoT) solutions. Often the correct protocol choices are obscured by vendors with vested interests in their offerings. Users must understand their specific requirements and limitations and have a precise system specification to make sure that the correct set of protocols is chosen for the various management, application, security and communications features and make sure that all implementation specifications are met.

1. Internet of Things Requirements and Protocols[1], Embedded Computing, 2015, Kim Rowe

[1]This is an update from the article provided in Embedded Computing.

Kim Rowe
Founder, RoweBots Limited
pkr@rowebots.net

Kim is a serial entrepreneur in the areas of computer systems and electronics. With over 30 years in companies doing technology product development, Kim has extensive experience in embedded systems, product development, general management, marketing, sales and finance. For the past decade, Kim has been managing RoweBots, an Internet of Things / Machine to Machine product development company. Kim holds a BESc from The University of Western Ontario, an MBA from The University of Ottawa and an MEng, from Carleton University.

Global Trade and Collaboration on Big Systems

by Frans Vreeswijk

Standards are more important than ever

A couple of years ago, whenever I talked to business people or regulators, I was often disappointed by how little they knew about Standards and the role they play for governance, business and in daily life. However, more recently I find that awareness and understanding are increasing. I believe that this is due to two major factors that are related to global trade and increasingly big challenges that can only be addressed through big systems that require broad collaboration. In this context, the IEC and IEEE are developing joint-standards that provide solutions industry needs and avoid unnecessary duplication.

Profound changes in global trade

Over the past years we have seen profound changes in trade dynamics. On the one side, trade tariffs are lower than ever. The average tariff applied by WTO (World Trade Organization) members in 2013 was just 9%. At the same time the failure of the Doha round has sparked an unprecedented number of bi-lateral and regional trade agreements. Those have the potential of endangering previous multilateral agreements by excluding other trade partners and especially developing countries. In this context non-tariff measures such as Standards and regulations are increasingly important to overcome potential technical barriers to global trade. This is particularly significant in electrotechnology where offshoring and outsourcing has resulted in global value chains which can only work if every participant applies the same harmonized rules.

Today, electrical and electronic devices and their subassemblies transition through many countries before they are consumed by the end-user in a given market. The fact is that electrotechnical products are no longer "made in a country," they are now "made in the world." Raw materials, components and parts have to be exported, imported, and re-exported multiple times before the final product is assembled and shipped to that end-user. With this, the interoperability of products along the value chain becomes extremely important. Standards that ensure quality and compatibility are therefore more important than ever before.

Second biggest trade good

Electrical and electronic devices and components are the second largest group of goods traded globally. According to UN trade statistics, global trade in electrotechnology represents more than 12% (USD 2,382 trillion) in value and this doesn't even include lighting, optical electronic and photo devices, medical devices and aircraft. In comparison, raw energy – the biggest trade good – represents 16% (USD 3,209 trillion). Automotive and fashion, which are by most people perceived as very big, really only represent 7,2% respectively 2,5% of total trade value.

Increasing consumption of electricity

But changes in trade are not the only driver for the increasing importance of International Standards. The penetration of electrical goods and with it the consumption of electricity is steadily increasing everywhere in the world. According to OECD (Organisation for Economic Co-operation and Development) projections, by 2050 developing countries will use double the amount of electricity developed countries use today. With the huge integration of electrotechnology in traditional and many new and innovative applications, the number of industry sectors that can benefit from International Standards is growing exponentially.

Cooperation more important than ever

Another trend that directly correlates with the need for International Standards can be seen in the increasingly fierce way companies compete today in the electrical and electronic industries. It may sound counter intuitive, but despite of this competitiveness, companies now have to collaborate more than ever before in order to deliver the technology solutions that are needed for the Smart Grid, Smart Cities, Smart Transportation and other increasingly big integrated systems. In reality, the speed of innovation has accelerated to a point where individual companies are no longer able to develop everything alone. Complex systems require large integrated technology solutions beyond borders. International Standards are a key enabler of this cooperation…across industries and national frontiers.

Collaboration in standards development

The same is true for standardization work. Today, no single standards developing organization can develop all that is needed for increasingly complex systems. Instead we all need to bring our specific proficiency to the table to maximize resources. We have to combine our know-how beyond traditional boundaries to create a bigger whole.

The IEC works closely with many organizations, including IEEE. This ensures coordination of standardization work and helps avoid duplication of effort. The IEC and IEEE have jointly issued 50 dual logo publications and another 16 joint development projects are currently in progress. Collaboration is ongoing at all levels of the two organizations. The aim is to achieve optimal outcomes and deliver what

the end-users really need. The simple fact is: the pool of experts is limited and the companies that participate in standardization work expect clarity in order to contribute effectively and efficiently.
In this context IEC has invited IEEE to participate and support the first www.worldsmartcity.org online community dedicated to moving cities to greater smartness.

IEC (International Electrotechnical Commission)

- Founded in 1906
- 167 countries – 83 Members, 84 Affiliates (developing countries who participate free of charge in the IEC Affiliate Country Programme). 98% of global population and 96% of energy generation
- <20 000 experts from industry, test & research labs, government, academia and consumer groups
- <170 Technical Committees
- <9 000 International Standards in catalogue
- >1 million Conformity Assessment Certificates issued
- Headquarters: Geneva Switzerland. Regional offices: USA, Australia, Brazil, Kenya, Singapore

The IEC covers a broad range of technical areas, developing International Standards in support of safety, efficiency and compatibility of electrical, electronic and communications devices and systems.

The IEC uses a process to produce voluntary consensus International Standards. Each Member country, no matter how big or small, has a single vote in the IEC.

The consensus based process that is the foundation for IEC documents is a careful balance between speed in addressing market needs and consensus to build meaningful and useful results.

Globally leading multinationals, but also many, many small companies actively participate in IEC work via their National Committee.

The IEC is the only organization in the world that provides an international standardized form of testing, verification and certification. The IEC Conformity Assessment (CA) Systems are the largest and most successful multilateral recognition agreement.

Certificates of the IEC Conformity Assessment Systems are widely accepted, well beyond member countries.

Thousands of testing labs participate in the IEC CA Systems. Each of them accepts the certificates and conformity assessment reports of the other Members of a System. The ultimate aim is to reach one test that results in one certificate, which is accepted everywhere.

Frans Vreeswijk
General Secretary & CEO, IEC
info@iec.ch

Mr. Frans Vreeswijk became IEC General Secretary and CEO on 1 October 2012, having served as Deputy General Secretary since 1 March 2012. Prior to joining IEC Central Office, he worked for 30 years for Philips in the Netherlands, Austria and the USA, notably in research, healthcare and consumer electronics areas. Previously he was President of the Dutch National Committee of the IEC (NEC) and has served on the IEC CB and SMB as well as representing the Netherlands in CENELEC.

Protecting Against Cyber Threats

by Sangeeta Kodukula

In today's digital age we cannot argue with the idea that the evolution of technology has contributed to many conveniences in our day-to-day life. Online banking, the ability to access corporate data from smart phones, and e-commerce are just a few examples of how the digital evolution has changed the landscape of how we operate on a daily basis. While these conveniences have contributed to simplifying our daily operations, have we taken a moment to think about the possible repercussions of exposing sensitive data on the internet? Similar to how the landscape of technology has changed, so has the evolution of cyber threat.

Today's hackers are more sophisticated than ever, and can make over $1 million a year! Methodologies such as leveraging exploit kits to deliver malware, ransomware, Distributed Denial of Service (DDoS) attacks, and phishing attacks are just a few examples of how these hackers infringe on their victims. Industry and the public sector are just as vulnerable as consumers who post sensitive data on the internet. As a result, regulations such as PCI (Payment Card Industry) compliance, HIPAA (Health Insurance Portability and Accountability), and FIPS (Federal Information Processing Standard) are all examples of guidelines companies in these various verticals must adhere to in order to protect sensitive data from being compromised. These regulatory compliances consist of a comprehensive checklist of requirements companies must align with in order to pass their compliance audits. These standards evolve as threats evolve. These compliances require the industry to invest in IT security in order to protect and reassure their customers' sensitive data cannot be accessed from an unauthorized source. IT departments must invest in various layers of security by implementing Next-Gen Firewalls, Next-Gen Intrusion Prevention System (IPS) solutions, encryption technologies, and VPN technologies, to name a few solutions. Why should companies care to invest in these technologies? The cost of a potential breach can not only cost a company millions of dollars, it can bruise their overall brand reputation and can cause their stock price to go down.

From a consumer standpoint we can take necessary precautions in order to minimize our risk as well. Measures that can be taken include creating strong passwords, changing passwords frequently, not openly distributing bank account details, and checking credit card statements thoroughly. These measures will help prevent one from becoming the next victim of cyber-crime.

Further reading:

PCI Compliance Standards: https://www.pcisecuritystandards.org/

HIPAA Compliance Standards: http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

FIPS Compliance Standards: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

Sangeeta Kodukula
Security Consulting Systems Engineer, Cisco Systems
sakoduku@cisco.com

Sangeeta Kodukula is currently a Security Consulting Systems Engineer at Cisco Systems. Other roles over her 10 year tenure at Cisco include supporting network management applications as a Customer Support Engineer in the Technical Assistance Center and selling Cisco's technologies in the Dallas/Ft. Worth area as a PreSales System Engineer. She is a graduate of the University of Texas (B.S. in Electrical Engineering) and is a member of Women in IT, IEEE, and Society of Women in Engineering. She also mentors girls in high school and college to promote STEM development and careers for women in IT.

Funny Pages

Dilbert

by Scott Adams