Principles, Practices and a Prescription for Responsible IoT and Embedded Systems Development

This document addresses security challenges related to the Internet of Things (IoT). As a working paper, it outlines ideas and approaches to improve the situation. Your perspective and participation would be helpful; our aim is significant and timely progress.[1] Please send any comments or related questions to **IoTiap** in care of IoTiapEmail@gmail.com. The document is available as HTML and PDF at:

https://www.iotiap.com/principles.html and https://www.iotiap.com/principles.pdf

The Immediate Challenge: Security and IoT

The Internet of Things, also known as IoT, has been a buzz in technical circles for several years now. In October 2016 a large scale cyber attack crippled a portion of the internet - the cause of this cyber attack was attributed to malware commandeered IoT devices. IoT Security made headline news.

After the October 2016 cyber attack some people asked, “What can we do to help avoid a recurrence of this event in the future?” This document seeks comments on that question from three audiences:

- Consumers (who provide economic incentives and real-world product understanding)
- Technologists (who develop and sell these products and components)
- Policy Makers (who can encourage, including business and technology standards)

This document grew from discussions of technologists who share concerns about the reliability and security of the internet and the worldwide web in this era of rapidly proliferating, powerful “things”. Our shared goal is lasting improvements in how the “Internet” **and** “Things” interact. It will take a coordinated, integrated effort of Consumers, Technologists and Policy Makers to achieve this.

We see this document as a starting point. The aim is to help educate Consumers; seek collaborative, support and standardization by Technologists; and invite Policy Makers’ appropriate advocacy.

Take The Toaster Test

On October 21, 2016, many of us observed “hiccups” in the internet and wondered if “the cloud”[2] was under attack. It was. This was the day the internet stopped working right - at least momentarily.

[1] Draft 16, 12/03/16 - See https://www.iotiap.com/principles.pdf and https://www.iotiap.com/principles.html

[2] Cloud computing refers broadly to digital devices connected via network and sharing data and computation. Wikipedia offers and expanded descrption at https://en.wikipedia.org/wiki/Cloud_computing.

If you have any doubt this is an immediate real-world security threat to you personally, then "**Take the Toaster Test**." *The Atlantic* has an October 2016 article describing the creation of a fake networked toaster which the author put online. In this clever experiment, more than 300 different IP addresses were recorded trying to hack this (fake) toaster within the first 12 hours of it being online.[3]

Rapid7 studied attack scans in a formal study of "the six largest clouds in the world—Amazon Web Services, Microsoft Azure, Digital Ocean, Rackspace, Google Cloud Platform and IBM SoftLayer."[4] In less than a month their honeypot "captured 100,000 unique IPv4 addresses behaving like Mirai", the IoT-based botnet implicated in the 10/21/16 attack. Their findings suggest the problem is bigger than commonly realized, as they observed "we did not expect to see the volume of Mirai that we have".

Here's a list of "Technical Prescriptions for Improving IoT Security" prepared by IOTiap. These represent easily implemented approaches which could rapidly improve today's IoT security shortcomings. The remainder of the document digs deeper, and takes on a broader exploration of this topic.

A Prescription for Improving IoT Security

1. **Documentation and Testing**. Users need to be educated. Product transparency reveals product capabilities and limitations (e.g., data, communication, encryption).
2. **Tools and Functionality**. Identification and information for all network devices is required. This includes module and component level inventory of software and hardware "ingredients". Approved devices appear on a whitelist[5]; unapproved or altered devices can be detected.
3. **Common Sense**. One example is this: "instead of hard-coding credentials or setting default usernames and passwords that many users will never change, hardware makers should require users to pick a strong password when setting up the device."[6] You can think of more!
4. **Technical Support**. Online and over-the-phone support including a security hotline.
5. **Product and Security Updates**. Routine, reliable updates from vendors providing firmware and software patches. Easily applied bug fixes with user ability to re-set installation to a known state.
6. **Diagnostics to Monitor and Manage**. "Always On" diagnostics automatically inform owners of security concerns, anomalies in product behavior, and cases requiring user attention.
7. **Technical Transparency**. Vendor product specifications disclose all ports, protocols, and technical standards used internal to these devices for any access to network resources.
8. **Consumer Advocacy**. Vendors must improve customer input, product warranties and life cycle maintenance for the wide range of IoT devices.
9. **Industry Associations**. Industry driven standardization efforts will help improve IoT Security for both local and international marketplaces.

---

[3] See "The Inevitability of Being Hacked" at http://www.theatlantic.com/technology/archive/2016/10/we-built-a-fake-web-toaster-and-it-was-hacked-in-an-hour/505571/

[4] Rapid7 Finds Certain Cloud Risks With Heisenberg Honeypot, http://www.eweek.com/security/rapid7-finds-certain-cloud-risks-with-heisenberg-honeypot.html

[5] Wikipedia provides a general description of this: https://en.wikipedia.org/wiki/Whitelist

[6] See "Who Makes the IoT Things Under Attack?" https://krebsonsecurity.com/2016/10/who-makes-the-iot-things-under-attack/

10. **A Multi-faceted Approach**. Meaningful participation of the three audiences addressed by this document (Consumers, Technologists and Policy Makers) will help improve IoT Security and chart pathways for IoT devices to become “good network citizens”.

Why is IoT Security a Concern?

A fundamental tenet of security is this: “A security system is only as strong as its weakest link.”[7] There is abundant evidence that a major weakness in systems today is the point where IoT devices connect to the network. Consequently, that “weak link” is the primary focus of this document. If we address and resolve one weak link at a time, before we know it we’ll have a super strong chain!

IoT security risks are real. They threaten global and local computer networks. The key question is not just “Will my internet connected devices be hacked?”, but rather “When will my network devices be hacked?” Because IoT Devices are often connected to real-world devices, there are added elements of safety and privacy that must be considered. (Burnt toast can have real-world consequences.)

IoT security risks not only apply to the whimsical WiFi Toaster described in *The Atlantic* article, but to a wide range of real devices operating in diverse, dispersed personal, business, and municipal environments. WikiPedia describes IoT broadly as follows:

> “The Internet of things (stylised Internet of Things or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. … The IoT allows objects to be sensed and/or controlled remotely across existing network infrastructure, creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit. When IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020.”[8]

On October 21, 2016 many people (initially on the East Coast, and eventually elsewhere) had difficulty accessing normally responsive sites like www.cnn.com. This was perhaps only an inconvenience for a short-period of time on that day. However, it was a clear indicator of fundamental, underlying weaknesses in our internet infrastructure exposing potentially billions of failure points.

[7] Page 5 in Cryptography Engineering: Design Principles and Practical Applications by Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno, Wiley Publishing, 2010.
[8] Wikipedia entry for Internet of things, https://en.wikipedia.org/wiki/Internet_of_things

Since this October 2016 hack attack, politicians (including a new *Senate CyberSecurity Caucus*[9]) and journalists[10] have taken steps to speak out on the topic. This open document offers a starting point for technologists to help provide solutions. These three audiences together can take collaborative steps to improve the circumstances which led to the October hack attack. Action is needed to prevent similar incidents from happening on a recurring (though unpredictable) basis. The longer that flaws in the underlying technology remain accepted as the "norm", the greater the likelihood that future cyber attacks will be of a larger scale and longer duration than what occurred in October 2016.

However, security concerns surprisingly stretch beyond unknown, malicious attackers.

At the November 2016 O'Reilly Security Conference, Cory Doctorow, of the EFFF, issued a clarion call on risks not only from unknown malicious attackers, but also from actions of established corporations.[11]

The Doctorow keynote, titled "Security and feudalism: Own or be pwned", described ways that well-known product vendors handle security matters as part of their "business model" in the device and IoT arena. In the video made available on YouTube, Doctorow identified examples of commonly used products and how vendors handle security updates as part of their business model. He described a "future of the internet of vulnerable, illegal to audit things-on-fire".[12] One of the instances Doctorow described involved a printer update by a leading manufacturer. You can read full details on that in the letter Doctorow sent to the company's CEO[13], and the company's public statement about this incident.[14]

Doctorow offered two of his own principles including

Doctorow posed the question: "So how do we fix this? We're not going to do it in onsies, twosies. No one of you is going to be able to solve this problem. Just like no one of you can recycle your way out of climate change. It's not a matter of individual choices. It's a matter of collective action that can make deep structural changes in the way that our information economy works."[15] At EFF, Apollo 1201 is a multi-year project aimed towards making progress. Doctorow proposed two simple, near-term principles which all participants in this product/service space should abide by: 1) Devices obey their owners; 2) Security facts are legal to disclose.

---

[9] Senator Warner's letter to the FCC - http://www.warner.senate.gov/public/index.cfm/2016/10/sen-mark-warner-probes-friday-s-crippling-cyber-attack and a recent article descibing te senator's concerns: "Senator Prods Federal Agencies on IoT Mess", https://krebsonsecurity.com/2016/10/senator-prods-federal-agencies-on-iot-mess/

[10] "Hacked Cameras, DVRs Powered Today's Massive Internet Outage" https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[11] Doctorow posted information about his keynote at https://boingboing.net/2016/12/01/my-keynote-from-the-oreilly.html

[12] Doctorow posted information about his keynote at https://boingboing.net/2016/12/01/my-keynote-from-the-oreilly.html

[13] September 26, 2016 letter from Cory Doctorow to HP President and CEO, https://www.eff.org/deeplinks/2016/09/what-hp-must-do-make-amends-its-self-destructing-printers

[14] September 28, 2016 HP Newsroom posting, "Dedicated to the best printing experience", http://www8.hp.com/us/en/hp-news/blog/Small-Business-Printing/best-possible-printing-experience.html

[15] 26:30 of video at https://youtu.be/duG55M8t0sc

Beyond this, what kind of “collective action” does Doctorow suggest? His talk closed with a plea of sorts: “Find two deep nerds … who already understand all that stuff…. We have a lot of people who are ready to understand what … this stuff means. People who you don’t have to give the technical education to. We can build a movement by bringing those people along… Have that conversation with two people in the next week. And one week later call them up and ask them if they’ve thought about it and if they are willing to have this conversation with two more people.”

Since that talk, www.deepnerds.com was established as an independent platform to coalesce a common cause effort and accelerate collective action towards solutions for digital era challenges like this.

Companies Share some Operational Research and Strategies

AT&T has made a significant effort to research and share information broadly related to Cybersecurity. They have available the following three documents:

> “What Every CEO Needs to Know About Cybersecurity”
> https://www.business.att.com/cybersecurity/archives/v1/
>
> “The CEO's Guide to Securing the Internet of Things”
> https://www.business.att.com/cybersecurity/archives/v2/
>
> “The CEO's Guide to Cyberbreach Response”
> https://www.business.att.com/cybersecurity/archives/v3/

Beyond corporate concerns there are also far-reaching issues across our government and in the public interest, such as national security. Jill Singer, Vice President-National Security, AT&T Global Public Sector Solutions described it this way: “IoT, like the internet before it, offers benefits beyond what we can currently imagine at this time,” Singer’s comments to www.washingtonexec.com elaborated on IoT:

> “It can bring cost efficiencies, speed, data-driven insights and actions, automation and so much more to agency systems and processes. Properly regulated – with the appropriate pro-growth incentives and cooperation across government and industry – IoT will result in a highly-effective environment that benefits everyone.”[16]

That article estimated that the global IoT market would reach $1.7 trillion by 2021. AT&T - which is just one of many technology vendors in this marketspace - “added 1.3 million new connected devices in the third quarter of [2016]” bringing their total to “30 million connected devices on its network”.[17]

[16] What the Government Stands to Gain – and Lose – from IoT, by Ben Wicker, 11/30/16, https://www.washingtonexec.com/2016/11/government-stands-gain-lose-iot
[17] What the Government Stands to Gain – and Lose – from IoT, by Ben Wicker, 11/30/16, https://www.washingtonexec.com/2016/11/government-stands-gain-lose-iot

In “The CEO’s Guide to Securing the Internet of Things”[18], AT&T provides “a four-part framework to help you identify IoT-related risks and put the proper controls in place.” The main components of this framework, also summarized in a brief abstract[19], are as follows:

1. Assess your risk
2. Secure both information and connected devices
3. Align IoT strategy and security
4. Identify legal and regulatory issues

AT&T summarized observations from their own *Security Operations Center*, and also incorporated the findings from others (notably PWC[20]) to make the following observations as part of an October 1, 2015 from their Newsroom[21], including the following information from that report:

1. a 62% increase in the number of Distributed Denial of Service attacks over a two year period
2. A 458% increase in the number of times hackers searched Internet of Things connections for vulnerabilities
3. Nearly 75% of businesses do not involve their full board of directors in cybersecurity oversight.
4. Approximately 51% of organizations are not re-evaluating their information security as a result of high-visibility data breaches
5. Roughly 78% of all employees do not follow the security policies set forth by their employer
6. AT&T believes that sharing its security insights and expertise will help others stay protected.

AT&T further identified[22] the primary security threats they believe to be facing businesses as follows:

1. Corporate espionage: Spies looking to steal intellectual property
2. Nation States: Groups looking to access information for their own benefit or cause
3. Organized cybercrime: Digital criminals that act using malware and hacking to extract information for financial gain
4. Hacktivists: Groups of hackers that use cyberattacks to promote social change or impact public policy
5. Malicious insiders: Employees or those with internal access that use company information for their own

[18] See “Exploring IoT Security”, AT&T Cybersecurity Insights Volume 2, at https://www.business.att.com/cybersecurity/docs/exploringiotsecurity.pdf
[19] See “The CEO’s Guide to Securing the Internet of Things Executive Abstract” | AT&T Cybersecurity Insights | Volume 2 https://www.business.att.com/cybersecurity/docs/vol2-exploringiotsecurity-abstract.pdf
[20] See PWC, "Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey" 2015 at http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf
[21] http://about.att.com/story/cybersecurity_insights_report.html
[22] http://about.att.com/story/cybersecurity_insights_report.html

Technologists Share Their Thoughts

The scale and importance of this concern is huge. Symantec's comprehensive report notes "In the USA, for example, there are 25 online devices per 100 inhabitants, and that is just the beginning. Gartner forecasts that 6.4 billion connected things will be in use worldwide in 2016… Over the last year, Symantec has seen an increase in proof of-concept attacks and growing numbers of IoT attacks in the wild. In numerous cases, the vulnerabilities were obvious and all too easy to exploit. IoT devices often lack stringent security measures."[23]

This document is based on discussions and shared experience of technologists who themselves have many decades of experience building computational and networking products at the cutting edge of innovation in various product areas. In some ways, the overall objective here is to make sure products are built for others in a way these technologists might build their own products. A technologist's concept of product ownership implies cost-effective usefulness, quality, reliability, security, ease of use, hackability (i.e. good customizability) and transparency of operation.

Remarkably and ironically, a big "player" in the 10/21/16 attack on the internet has now been identified as "security" cameras. Imagine that, security cameras crippling the security of the internet!

In this event, security cameras and DVRs were reportedly infected by malware which was then used to launch a sizable denial of service attack. These low-cost, useful and powerful devices are used but perhaps little understood. Risks increase with the growth of multi-functional, computational devices connected to the internet, including security risks of various sensors providing input for processing. This growth is happening so rapidly it is difficult to track or keep up with the evolving technology.

October 21, 2016 was a wake-up call to all internet users: we can no longer allow "business as usual" to take place on the internet, or with devices that connect to the internet. One device vendor took the step of recalling thousands of devices.[24] Some people have acknowledged some devices - especially older ones - can't be fixed. Smaller devices may have a relatively short life and be considered almost as disposable. However, larger devices connected to networks - televisions, refrigerators, and increasingly automobiles - are big investments expected to operate for years or even decades.

As the underlying technology of IoT has become extremely powerful, communication bandwidth has also increased, network access has become nearly ubiquitous, even as the cost of component parts and products have fallen. This creates a host of interesting economic issues not seen during the Personal Computer revolution. Security researcher Bruce Schneier offered his view of the unique challenges in an October 10, 2016 blogpost: "the economics of the IoT mean that it will remain insecure unless government steps in to fix the problem. This is a market failure that can't get fixed on its

[23] Page 16, Symantec's "2016 Internet Security Threat Report", VOLUME 21, APRIL 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf
[24] "IoT Device Maker Vows Product Recall, Legal Action Against Western Accusers" https://krebsonsecurity.com/2016/10/iot-device-maker-vows-product-recall-legal-action-against-western-accusers/

own."[25] Schneier returned to that topic one month later, with a post titled "Regulation of the Internet of Things"[26].

Market participants must take significant steps to 1) protect consumers: 2) safeguard resources commonly shared, like the internet; 3) and strive to maximize the innovation and productivity gains from IoT and related technological advances.

Today, good people can cause unintended harm to others as a consequence of "using" IoT. Something as simple as not changing a gadget's default password can expose devices to the malicious mayhem of others. To put it in the context of the "Toaster Test", someone (remotely) could burn your toast, just as easily as your "Toaster" might be the cause of their burnt toast. Intrusions into private networks are also possible, including the potential for data loss or threat of ransomware.

Security is a big topic. It includes a study of threats - ranging from simple traffic analysis to tampering. It requires security services to address authentication, access control, and data integrity. Encryption and various cryptographic techniques play a role in keeping information secure if it is accessed.[27] Security is a simple word that oversimplifies the challenges we face, but it is a useful simplification. Security is a huge challenge for IoT. A related topic is privacy. The legal landscape and lessons learned from practices with privacy policies might be beneficially applied in strengthening IoT security policies. Some corporate policy examples include:

- Apple - http://www.apple.com/privacy/
- Facebook - https://www.facebook.com/policy.php
- Google - https://privacy.google.com
- Verizon - http://www.verizon.com/about/privacy/privacy-policy-summary

International considerations may be key factors in this discussion. Privacy and security are global concerns and technology is widely influenced by political constraints. Even though these are global issues, they also often are further shaped by - and subject to - local legislative or watchdog groups.[28]

The "prescription" provided above attempts to address the types of general considerations which arise in general security discussions. Here's a list of ten core security services identified by security researchers Christof Paar and Jan Pelzl in their text book: *Understanding Cryptography*[29]:

1. Confidentiality
2. Integrity

---

[25] "Security Economics of the Internet of Things" https://www.schneier.com/blog/archives/2016/10/security_econom_1.html

[26] See "Regulation of the Internet of Things", posted on 11/10/16 at https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

[27] See "Wireless Security and Cryptography" by Nicolas Sklavos and Xinmiao Xhang (CRC 2007).

[28] See "WhatsApp-Facebook privacy U-turn now being probed by EU data watchdog" at https://techcrunch.com/2016/10/28/whatsapp-facebook-privacy-u-turn-now-being-probed-by-eu-data-watchdog/ and "Europe Tried to Rein In Google. It Backfired.", , http://www.nytimes.com/2016/04/19/technology/google-europe-privacy-watchdog.html

[29] Understanding Cryptography: A Textbook for Students and Practitioners, Christof Paar/Jan Pelzl, Springer 2010.

3. Message authentication
4. Nonrepudiation
5. Identification/entity authentication
6. Access control
7. Availability
8. Auditing
9. Physical security
10. Anonymity

The creativity and skills to produce IoT products has flourished, but there needs to be corresponding attention placed on keeping these devices safe and secure. Some chip vendors are actively working to address today's challenges. ARM announced new product offerings targeted at IoT end points. You can find an informative technology description, with video published by ARMDevices.net, discussing steps toward a smart, secure future of IoT:

https://plus.google.com/+charbax/posts/fNneTsLrHF1

This document covers a wide range of concerns which have generally been categorized under the umbrella of *"security for IoT"*. However, we are only scratching the surface as we seek to strengthen the weakest link in the chain of IoT Security.

Technological Evolution

Powerful, connected technologies are embedding themselves into our daily lives - often in places and in ways that consumers are only partially aware of. Today's technology can greatly improve the quality of life without much expense or effort on the part of the beneficiary. As a result, these technologies are increasingly hidden and invisible and don't always get the attention or mindshare required to pay attention to the possibility of unintended consequences.

New technologies evolve out of a confluence of economic, market, social, engineering, entrepreneurial, and political forces. Consider automobiles for instance. People drove automobiles before they had windshields. After creating windshields, people drove many miles before the invention of windshield wipers. (Mary Anderson invented the windshield wiper in 1903.) Intermittent wipers, now a common convenience, weren't invented until some 50 years after windshield wipers. How about seatbelts? They were first used in airplanes! A 1955 article in the Journal of the American Medical Association advocated[30] for action against the hazards of automobile accidents. By 1966, the Crash Test Dummies had been invented and the National Traffic and Motor Vehicle Safety Act passed[31]. These improvements in automobile safety and security took place over many decades

Airbags and other safety elements have greatly improved the technology of transportation. Today, a tiny illuminated indicator can appear on your dashboard indicating air pressure in your tires - even the

[30] "Prevention, the only cure for head injuries resulting from automobile accidents", in http://jamanetwork.com/journals/jama/article-abstract/302856 and Wikipedia on seat-belts at https://en.wikipedia.org/wiki/Seat_belt

[31] https://en.wikipedia.org/wiki/Samuel_W._Alderson

spare tire - is low. Sensors and wireless radio technologies make this possible. Other advanced technologies utilize camera sensors and radar for safe driving assist features. We need to advocate and accelerate similar innovative progress and improvements for IoT.

In the aftermath of the October 2016 hack attacks, some described the practical reality of the state-of-the-art situation and costs: “That leaves the victims to pay. This is where we are in much of computer security. Because the hardware, software and networks we use are so unsecure, we have to pay an entire industry to provide after-the-fact security. … Buy mitigation if you need it, but understand its limitations. Know the attacks are possible and will succeed if large enough. And the attacks are getting larger all the time. Prepare for that.”[32]

It is the firm belief of **IoTiap**, we need to work collaboratively and proactively to research and find technologies, techniques and solutions to prevent and curtail these kinds of costs in advance.

Sharing Ideas and Creating Prototypes

In February 2014, a number of us organized an “IoT Festival”[33] where many security issues were raised. One of the presentations “Security in IoT cannot be an afterthought!” focused on routers. The hack of the internet on 10/21/16 was a “burning platform”[34]. The following month, some 900,000 Deutsche Telecom customers experienced service problems, attributed to a “a failed hacking attempt to hijack consumer router devices for a wider internet attack.”[35]
Today, the three audiences this document targets - Consumers, Technologists and Policy Makers - can take steps to facilitate rapid progress on improving the state of security in IoT. It needn’t take decades to address the security shortcomings we are seeing with IoT today.

Security is hard (and can be expensive) and it requires shared principles to get right. But there is hope as a number of companies have made initial efforts. TechCrunch described tamper-resistant components and secure booting environments. You can read about “the Internet of Things Security Foundation, a non-profit body that will be responsible for vetting Internet-connected devices for vulnerabilities and flaws.”[36]

This document invites your shared effort to address these challenges directly. A productive approach could include collaboration, in-person and remote interaction, and the sharing of prototypes and presentations on improved methods for operating and managing IoT devices.

[32] See “Lessons From the Dyn DDoS Attack” at https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html
[33] Some of the slides and information from the 2014 IoT Festival can be found at http://www.iotfestival.com/agenda-2014-02-22.html.
[34] See a “burning platform” moment described at https://hbr.org/2012/12/how-to-anticipate-a-burning-platform
[35] November 28, 2016, “German internet outage was failed botnet attempt”, http://www.reuters.com/article/us-deutsche-telekom-outages-idUSKBN13N12K
[36] Why IoT Security Is So Critical, https://techcrunch.com/2015/10/24/why-iot-security-is-so-critical/

Call to Action

The so-called Internet of Things appears to be under development with little or no attention to issues like safety, reliability, and security. These are critical issues because IoT systems are designed to surround us and be infused into our daily lives. IoT will be observing us as well as acting with - and on - us every day with virtually ubiquitous global connection over the Internet to cloud-based business entities.

The engineers acting as designers and implementers of these systems lack a framework for thinking about systems-level engineering problems introduced by these new systems. In fact, they are not even integrating solutions historically available to simpler, yet still difficult problems, from nearby domains like communications, cyber security, fault tolerant systems, etc.

The Engineering profession in particular needs to step up its game to meet these new challenges.

How can we get this started?

Proposal Ideas

As mentioned earlier, www.deepnerds.com was established as a platform to bring together people and talent who have the ability to propose and implement. (To help, send email to deepnerds@gmail.com)

One idea from that is to see that every IoT product or system provide a standard Software Developer Kit (SDK) and Application Program Interface (API). These toolkits would provide standard, well-defined ways to interconnect and monitor networks of IoT devices. For instance, network owners should have the right to require every device on their networks to identify itself. Thus, the standard toolkit could standardize the process of sharing “identifying” messages upon “entering” their network (“Hello, Network”) and a message upon “leaving” the network (“Goodbye, Network”).

The British Standards Institution “has published PAS 212, Automatic resource discovery for the Internet of Things” which claiming to “make it much easier to discover Internet of Things data”. The PAS 212 standard covers: “A mandatory file format for representing a catalogue of linked-data resources, annotated with metadata” and “Recommendations for catalogue access in file transport; security mechanisms to protect access and to prove provenance; search functions; subscription mechanisms; well-known entry-points and machine-readable hints to ease usability.”[37]

A requirement of IoT devices is that their software be updated - in order to add features as well as plug security holes. This pathway into routers became the avenue for some 900,000 routers supported by Deutsche Telecom to be attacked and infected. One of the comments suggests a software solution. Is

[37] See “Internet of Things interoperability specification is published” http://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2016/july/Internet-of-Things-interoperability-specification-is-published/

this feasible for routers and light-switches and such? This Deutsche Telecom router attack cuts right to the heart of the technical requirement for auto-updating - so a solution is needed.

Another suggestion posted anonymously by a commenter in response to the viral attack on Deutsche Telecom German routers offered this:

> "Instead of using telnet – they could of used an IPSEC SSH tunnel with a cipher signature based login. Each router could have a string cipher that can be used to get a password and username combination.
>
> So the initial SSH knock would say hello — I am tretR^$#rtfs54w^#$ please enter credentials now.
>
> The credentials are derived from the knock string.
>
> However, it will only allow limited SUDO-ing of a user so that input would cannot be put in one after the other and executed like ROOT can do. So, a user would be in the sudoers – allowed one command execution at a time. There is no sudo -s, or sudo -i, Only sudo . sudo and so on.
>
> Which then allows a remote connection from the ISP to push updates securely.
>
> The cipher key could be leaked, broken, and so on. But at this point its better than turning it off or blocking or dropping.
>
> These routers also need some intelligence. It needs to have some advanced firewall features so that when it detects a scan that would put it off line – it can just turn the wan port off for 15 minutes – and notify the users via the gateway. Something like comcast was doing -"Brand firewall model xxx has detected an aggressive scan on – temporarily shut down service for 15 minutes.. 12 minutes left.. if you want to reactivate the wan port, please click here…"
>
> Then there should be a scan log sent to a department at the ISP so they can make adjustments to block at the network level – and protect all its assets...."[38]

Finally, it's clear that ISP organizations have a duty to address this. As one network expert observed, "In a lot of the recent DDoS attacks, the return address of the offending packets were in private internet address space (you know, 192.168.X.Y). There is absolutely no reason that an ISP should not filter out packets entering its network that has such a return address. But many don't bother. ISPs need to demonstrate the three C's: C – Care; C – Competence; C – Capability."

There are good ideas circulating now - but they need to be acted on. The required action includes prioritizing, gathering, coordinating, standardizing and implementing feasible engineering solutions.

[38] "New Mirai Worm Knocks 900K Germans Offline", November 30, 2016, https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline

IoT Supervisor

A prototype under development to demonstrate some of these point capabilities is called the "**IoT Supervisor**"[39] (http://www.iotsupervisor.com/). This is server technology that runs on a low-powered device dedicated to monitoring and manage network IoT traffic and device activity. The "IoT Supervisor" shares some feature attributes with a DHCP server, but is designed specifically with the operational needs of IoT in mind. This could include automatic discovery of devices and services.

For instance, the "**IoT Supervisor**" is able to exchange a stream of key / value pairs via remote procedure calls (RPC)[40] with the network owner. This allows the network owners to identify any new IoT devices that want to join their networks. All new devices can be scanned - if they are on an approved "whitelist" they could be approved for interacting with network resources.

The "**IoT Supervisor**" prototype demonstrates how the following types of information can easily be gathered and shared to provide better monitoring and management of a digital environment:

1. Device Identification (e.g., password, serial/model number, vendor reference links)
2. Device Type, Name, Feature, and Descriptive Identifiers (all provided by vendor)
3. Device Hardware Information (including MAC address for any network/radio device)
4. Device Component Inventory (reports on hardware and open source used)
5. Device Service Descriptors (sensors, transactions, resources)
6. Device "Hello, Network" initiation time
7. Device "Goodbye, Network" closing time
8. Device Pulse (e.g., frequency of "**IoT Supervisor**" check-ins)

This kind of information can be programmatically searched and incorporated into self-monitoring networks. Automated self-monitoring can tirelessly search for rogue or malfunctioning IoT devices. This approach appears feasible for a wide range of low-powered IoT devices, in corporate, industrial, municipal and residential configurations.

RPC connections can be used to continually monitor network activity, while a connected browser with appropriate credentials can view information via HTTP connections. Making opaque network activity transparent will go a long way towards improving IoT Management. Automated inspection of network activity could be constantly running in the background, under the control of the network owner, to effortlessly improve the security and reliability of today's devices and networks.

These types of functionality exist today, but typically this only on large, institutional networks comprising powerful servers, desktops and laptops. Security needs to be re-thought and applied on a smaller, broader scale across a variety of IoT devices in non-institutional settings.

[39] More details on the "IoT Supervisor" are available at www.iotsupervisor.com.
[40] See https://en.wikipedia.org/wiki/Remote_procedure_call

General History

Multi-million dollar mainframes of the 1970s and 1980s operated in climate and access-controlled rooms about the size of a small hockey rink. Data storage devices stood as tall as a full-sized refrigerator. Those compute capabilities have been far surpassed by today's low-cost computing and communication devices.

Local area networks and the internet migrated from business, government, and academia into personal use by the late 1990s. The World Wide Web revolutionized how people could consume information and transact commerce. The dot-com revolution changed life in numerous beneficial and irreversible ways.

Not long after this, smart phones were introduced and suitable for everyday use - with voice, data and applications all packed into a tiny little rechargeable device. Today, the "Internet of Things" and embedded devices appear to be re-shaping our future in similar ways.

The phrase "Internet of Things" was suggested in 1999[41], but the IoT applications we see today are far more advanced than anything possible at that time. Cell phones evolved to "smart phones" in what now seems like a technological blink of an eye. At the same time, there was tremendous innovation in the semiconductor industry leading to ever more powerful (yet progressively more energy efficient) chip designs. The first two decades of the 21st century unleashed remarkable progress in software and hardware development (with software propelled by the Open Source movement and hardware release accelerated by a global manufacturing push.) By 2012, China was aiming to be a global leader in IoT[42]. By late 2016, the going price of $20 per unit of quad-core 64 bit connected devices was a new norm.[43]

IoT presents many kinds of applications which, by design, are intended to blend into daily living activities. IoT solutions are often designed to not require much human attention, hands-on interaction or intelligence to operate. (After decades of hiding in research projects, artificial intelligence has now become headline news and integral to new product releases.) Consequently, all kinds of "compute" technologies pose a growing - but largely hidden - risk at work, at home, and in the municipal environments around us. As IoT products become more powerful and more complex, the situation only grows more challenging.

New devices are appearing daily from producers all over the world - smart thermostats, doorbells, light bulbs, and - yes - security cameras. Televisions now include ethernet connections and WiFi. Your refrigerators, washing machines, entertainment devices, and automobiles all want to talk to you - and to each other. This growing complexity poses new, real, risks. If we want to avoid recurrences of October 21st, we need to mitigate the risk of unintended harm from today's technologies. We need to make today's technologies more reliable, responsible, secure and powerful for all users.

---

[41] The first use of the phrase ties to activity at the MIT Media Lab, http://www.rfidjournal.com/articles/view?4986
[42] See "China looks to lead the Internet of Things" by Kevin Voigt, CNN, December 3, 2012
[43] Hackerboards have fallen below $20 for 64 bit, quadcore processing, and less than $10 for devices incorporating WiFi and ethernet - http://hackerboards.com/headless-orange-pi-zero-sbc-has-wifi-and-ethernet-for-7/ and https://techcrunch.com/2016/11/06/the-new-64-bit-orange-pi-is-a-quad-core-computer-for-20/

The legal landscape has also evolved in a way that is now more favorable to researching and seeking improvements in the Security of IoT. In an October 28, 2016 blogpost, the FTC described details of the "DMCA security research exemption for consumer devices".[44] This welcome development was reported by a number of media channels and will likely result in an uptick in security research and learning: "For years, the DMCA has been used to stifle legitimate research into the security of embedded systems. Finally, the research exemption to the DMCA is in effect (for two years, but we can hope it'll be extended forever)."[45] This new "Freedom to Tinker" will afford improved understanding and research into the security of devices and technologies that impact our lives.

IoT In A Connected World

Rogue devices and malicious actors exist today while the frequency and sophistication of botnet attacks is growing[46]. The processing power of connected IoT devices has been harnessed to use cumulative computing power to disrupt the internet. We have seen these activities have large regional impacts in various regions. The diversity of powerful IoT devices now capable of going rogue, presents a growing challenge. These devices are complex - consisting of sophisticated hardware and software, developed by innovators around the world and produced in mass market quantities at consumer-friendly prices.

In a November 2016 posting, security expert Bruce Schneier calls for regulation, echoing a theme that seems to have carried across several of his posts. His short article titled "Regulation of the Internet of Things" describes IoT-induced security problems to be "a form of invisible pollution", whereby the problems caused by one individual might primarily affect others:

> "And, like pollution, the only solution is to regulate. The government could impose minimum security standards on IoT manufacturers, forcing them to make their devices secure even though their customers don't care. They could impose liabilities on manufacturers, allowing companies like Dyn to sue them if their devices are used in DDoS attacks. The details would need to be carefully scoped, but either of these options would raise the cost of insecurity and give companies incentives to spend money making their devices secure."[47]

Meanwhile, many are outright opposed to regulation and some take a more balanced approach.

The IEEE provided a thoughtful and balanced write-up in an article titled "Wanted: Smart Public Policy for Internet of Things Security". The article takes a balanced approach to weighing pros and cons of regulatory solutions.

---

[44] See the FTC blog post at https://www.ftc.gov/news-events/blogs/techftc/2016/10/dmca-security-research-exemption-consumer-devices

[45] See https://www.eff.org/deeplinks/2016/10/why-did-we-have-wait-year-fix-our-cars, https://www.schneier.com/blog/archives/2016/11/research_into_i.html, and https://www.wired.com/2016/10/hacking-car-pacemaker-toaster-just-became-legal/

[46] Botnets are connected networks of communicating computer processes. Historically these were used to deliver spam mail. During 2016, we saw multiple instances of botnets being used to launch Denial of Service attacks.

[47] Regulation of the Internet of Things, https://www.schneier.com/blog/archives/2016/11/regulation_of_t.html

> If Congress ever gets around to drafting IoT security legislation, the FTC's 2015 recommendations for reasonable IoT security practices could someday become law. Industry groups have also floated their own recommendations as a starting point. Rulemakers could also look to third-party certifications available through groups such as the Online Trust Alliance.
>
> [David Thaw, a law professor at the University of Pittsburgh who specializes in cybersecurity policy] says he recommends an approach known as flexible regulation. Rather than mandating technical security prescriptions that may soon be outdated, flexible regulation describes critical steps that companies must take such as performing a risk assessment, drafting a plan to minimize security risks, training staff in security protocols, and sticking to their cybersecurity plan. Regulators describe this set of steps they expect companies to take, and issue punishment if they fail to do so.[48]

The FTC published a 71 page report from their 2013 workshop was titled: "Internet of Things: Privacy & Security in a Connected World."[49] This was an effort to gather input from staff experts and practitioners to share best practices. Perhaps because of the sprawling size of the FTC (e.g. it includes a Division of Privacy and Identity Protection) "no single agency has been tasked with keeping tabs on the IoT. Instead, some agencies have found reason to cover parts of it. Currently, the Department of Health and Human Services protects personal health information stored on connected devices, while the Federal Reserve has published security guidance that covers devices linked to the financial industry. The National Highway Transportation Safety Administration also recently issued guidelines for connected cars."[50]

The following sections provide additional background, including many questions you might ask about specific IoT products, services, or vendors. There's no single "right" answer to these questions - but it's essential the three main audiences for this document (Consumers, Technologists, and Policy Makers) can articulate representative answers if the goal is to improve the state of IoT Security.

Design and Development: IoT Product Principles

Here are questions to help ascertain the "security" readiness of an IoT product. These are questions every Consumer could ask Vendors - and every Vendor should readily answer.

1. Does the vendor publish a security contact? Who is it and what is the person's role?
2. What is the vendor's maintenance release schedule and process for issuing security updates? (These updates should occur on a regular basis.)
3. What is the vendor's current and past list of security issues and fixes? (Is this something the consumer finds acceptable?)

---

[48] Wanted: Smart Public Policy for Internet of Things Security, 10 Nov 2016 http://spectrum.ieee.org/tech-talk/telecom/security/wanted-smart-public-policy-for-internet-of-things-security

[49] See the FTC 2013 report at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[50] See "Wanted: Smart Public Policy for Internet of Things Security" http://spectrum.ieee.org/tech-talk/telecom/security/wanted-smart-public-policy-for-internet-of-things-security

4. What open source components are used in the product and where is the source available? (These lists should be well documented and widely and freely available.)
5. Are dates and history provided for any “forks” of open source modules? (This will be useful to communities of developers looking to identify and isolate problem areas.)
6. Does the vendor encourage bug bounties?
7. Does the vendor discourage legal action against ethical hacking?
8. What is the support plan - short-term and long-term - for the vendor’s product? How does this compare to other vendors in this product space? What is the vendor’s track record managing product life cycles, including end-of-life product transitions?
9. What is the vendor commitment to post information on confirmed customer reported bugs? (Transparency in this area is helpful to disclosing potential problem areas.)
10. Does vendor documentation spell out security claims in clear language? Under what circumstances will a vendor recall a product?
11. Where is product documentation and support information available online and offline? (This needs to be clear to each consumer prior to “powering up” their IoT device.)
12. What risk analysis / review did the vendor undertake prior to product release? (This should be part of the support information and should provide descriptive analysis of testing that was done.)
13. What test environments were utilized prior to product release (e.g., Networks, product interactions, duration of “burn in”, and volume of test data processed by device)?
14. Is there a "Warranty Log" of updates includes Statement of Product Support Policies documenting all known, outstanding Vendor Vulnerabilities with known user visible impacts? Where?

Software Features: IoT products could Include these

1. Is there a simple web interface to display device security status in real-time?
2. Is there a simple web interface to check for software and firmware updates?
3. What device monitoring functionality is available (to the user or a third party)?
4. Is the owner required to set a customer / owner password on first use?
5. What information does the device want to report outside the owner’s network? Is there a comprehensive log of this communication?
6. Is there a user visible interface to manage security (firmware updates, status)?
7. What functionality is built into the product to generate a real-time catalog and inventory update on module information and release dates for all included technologies?
8. What links / references are available to independent test labs and certifications? (e.g., FCC)?
9. What release notes are issued with each new software or hardware update?
10. What information is available to describe differences in various product versions in the market?
11. Does the product “play nice” on the network, “announcing” when it joins the network and when it leaves?
12. What information is the product able to communicate about its operating functioning? How is this information shared with the owner? What automated reporting is available to alert on possible security or other functional concerns?
13. How does the product alert the owner when new, security breaching bugs have been found?
14. How does the product alert the owner when required software and firmware updates are available to fix known bugs?

15. What “traffic reports” are available to allow user inspection of device activity (and identify traffic with other devices?)
16. The “**IoT Supervisor**” mentioned earlier addresses some of these desirable features.

Hardware Features: Recommended or Required

1. Is there a manual power on / off?
2. Is there a manual network connect / disconnect?
3. Can the device “operating system” be flashed with updates?[51]
4. Is the “flash update” process documented for third party use?
5. Does the device auto-restart after power outage? Is this re-configurable? (What data is lost during a power outage? What is the “reboot” sequence on first power-up and after a reboot?)

“Out of the Box” documentation

1. What is the process for reporting bugs and asking support questions?
2. Is the user able to access an SDK to programmatically display components which make up this device? This would include functionality to generate an inventory of hardware and software components and their descriptions along with verifiable vendor identification information (i.e. a technological version of an FDA ingredient listing for IoT).
3. Can the user install updates via stand-alone, air-gapped, off-line procedures? (e.g., fresh install from a signed USB stick)
4. Can the user carry out a complete reinstallation to original system settings, with inclusion of all updates?
5. What documentation exists to make the owners aware of the capabilities they buy/control/use so that they can understand the risks and security exposure incurred to themselves?

Liability Issues: Vendors should address these

1. What are the vendor’s policies for warranty repair?
2. What are the vendor’s policies for product liability related to data loss or security intrusion?
3. What disclosures have been made about vendor steps to reasonably mitigate product risk of using this product? Potential risks include those to both owner and risks to others.
4. Has the vendor issued any attestation that all known backdoors, trapdoors, and intrusion vectors have been secured?
5. What is the vendor’s committed “time to repair” or “time to work around” for different classes of bugs (e.g., network outage, data loss, security breach?) (Shorter is better!)

Industry Associations and Certification

1. Has a "Certified Public Security Officer" who "knows their stuff and can help evaluate the threats and risks" conducted a security audit?

[51] Software such as OpenWrt and devices like the Linksys WRT54G demonstrate there is a viable external development community willing to develop customizations and extensions to “factory” settings on devices.

2. Does the product respect the "principle of least privilege" - giving only the minimum power/privilege to do what it needs to do, and maintaining that during updates and upgrades?
3. Has the vendor issued Summary Statements out of Focus Group, Participation Observations, or Case Studies describing reports of usability and deployment experience?
4. What monetary and technology contributions has the vendor made to the "Internet Network Sustainability Fund", for ongoing support of the internet and world wide web?
5. Is the vendor an active member of **IoTiap** and other industry organizations?
6. Does the vendor log software updates to the central "Cyber Notices Registry" of **IoTiap**?
7. Has the product received certification and a designation of the "**IoTiap** Seal of Approval"?
8. Some of the existing initiatives include:
    a. The Industrial Internet Consortium (IIC)[52] [53]
    b. IoT Security Foundation - “industry document .... 30 pages”[54]
    c. The Open Connectivity Foundation[55]
    d. The GSMA self-assessment[56]
    e. BITAG - Internet of Things (IoT) Security and Privacy Recommendations[57]
    f. The British Standards Institution (PAS 212)[58]
    g. **IoTiap - http://www.iotiap.com/**

According to an 11/8/16 article that appeared in the EE Times, the IIC is working across companies to and international borders to align standardization efforts:

> *Next on the list are deals in France, Chile, Kazakstan and other governments with national IoT programs. Beyond that, the IIC aims to add agreements making the deals multilateral so the IIC becomes an international hub of collaboration on IoT interoperability.*
>
> *“We don’t want to end up with a series of bilateral meetings, so everyone must agree with each other," said Richard Soley, executive director of the IIC and chief executive of the Object Management Group that oversees it and three other trade groups “It’s important our members don’t get stuck supporting multiple architectures and security frameworks,” he told EE Times in an interview.*

[52] Industrial Internet Consortium, https://www.iiconsortium.org/
[53] “China Signs IoT Interop Plan Deal expands network of global agreements”,
[54] See “”After cyberattacks, Internet of Things wrestles with making smart devices safer” at http://www.theglobeandmail.com/report-on-business/international-business/asian-pacific-business/after-cyber-attacks-internet-of-things-wrestles-with-making-smart-devices-safer/article32718232/
[55] The Open Connectivity Foundation has a variety of membership and participation arrangements, as you can see at https://openconnectivity.org/about/join
[56] GSMA IoT Self Assessment - http://www.gsma.com/connectedliving/iot-security-self-assessment/
[57] “Internet of Things (IoT) Security and Privacy Recommendations: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT”, November 2016, http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
[58] “Internet of Things interoperability specification is published”, 20 June 2016, http://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2016/july/Internet-of-Things-interoperability-specification-is-published/

In Closing

This effort was initiated by a group of technologists concerned about the impacts of IoT on the security and reliability of the internet and the worldwide web. Further updates to this document and ongoing discussions will take place in the future. (We'll be having an in-person meeting on this topic as part of the BLU meeting on 4/19/17 http://blu.org/cgi-bin/calendar/2017-apr)

The bottom line? We can no longer accept a design methodology or product development philosophy that says "We'll add security later" or "We'll make tradeoffs in security to get to market". Improved, usable network tools are required to make everyday intrusions more easily monitored and managed. We need to do security right from the start, and we need to get started doing it right now.

Are you interested in getting more involved in this discussion? Please email any comments, suggestions, or ideas you are willing to share. You can reach us at the following email address: IoTiapEmail@gmail.com. You can find this document and future updates at

https://www.iotiap.com/principles.html and https://www.iotiap.com/principles.pdf

Additional Articles / Related References

1. “Dan Geer’s 10 Cybersecurity Best Practices”, https://www.wired.com/brandlab/2015/06/dan-geers-10-cybersecurity-best-practices/ and http://geer.tinho.net/geer.lawfare.15iv14.txt
2. “Dirty COW and clean commit messages”, https://lwn.net/SubscriberLink/704231/93d90be96044c083/
3. “Keys Under Doormats: mandating insecurity by requiring government access to all data and communications”, https://www.schneier.com/academic/paperfiles/paper-keys-under-doormats-CSAIL.pdf
4. The Government and Recalls, http://www.recalls.gov/nhtsa.html and http://www.fda.gov/ForConsumers/ConsumerUpdates/ucm049070.htm
5. The FCC and Wireless, http://huchra.bufferbloat.net/~d/fcc_saner_software_practices.pdf
6. “Familiarity Breeds Contempt: The Honeymoon Effect and the Role of Legacy Code in Zero-Day Vulnerabilities”, http://x3.techzoom.net/Papers/Familiarity_Breeds_Contempt_(2010).pdf
7. “Moving Targets: Security and Rapid-Release in Firefox”, http://seclab.upenn.edu/sandy/movingtargets_acmccs14_340.pdf
8. “DHS Is Drawing Up ‘Strategic Principles’ for Internet of Things”, http://www.defenseone.com/threats/2016/10/internet-things-will-have-new-strategic-principles-soon-dhs-secretary-says/132611/
9. “I bought some awful light bulbs so you don't have to”, https://mjg59.dreamwidth.org/40397.html
10. “Dyn DNS DDoS likely the work of script kiddies, says Flashpoint”, https://techcrunch.com/2016/10/26/dyn-dns-ddos-likely-the-work-of-script-kiddies-says-flashpoint/
11. "Of course smart homes are targets for hackers", http://mjg59.dreamwidth.org/45483.html
12. GCHQ wants internet providers to rewrite systems to block hackers, Cara McGoogan 5 NOVEMBER 2016, http://www.telegraph.co.uk/technology/2016/11/05/gchq-wants-internet-providers-to-rewrite-systems-to-block-hacker/
13. “Worldwide market for military embedded computing to near-double over next five years”, October 24, 2016 http://www.militaryaerospace.com/articles/2016/10/military-embedded-computing-military-electronics.html
14. “Cyber security isn't just about big IT; it's about locks, lights, and even a child's plaything” October 11, 2016 By John Keller, http://www.militaryaerospace.com/articles/2016/10/cyber-security-information-technology-it.html
15. Industry consensus forming around cyber security as emerging new industry takes shape October 4, 2016 By John Keller, http://www.militaryaerospace.com/articles/2016/10/cyber-security-emerging-new-industry.html
16. WHY CHINA WILL RETAIN ITS M2M LEADERSHIP, ItU blog, June 30, 2016, https://itu4u.wordpress.com/2016/06/30/why-china-will-retain-its-m2m-leadership-new-report/

Industry Reports

1. “Internet of Things (IoT) Security and Privacy Recommendations: A BROADBAND INTERNET TECHNICAL ADVISORY GROUP TECHNICAL WORKING GROUP REPORT”, November 2016, http://www.bitag.org/report-internet-of-things-security-privacy-recommendations.php
2. Symantec’s “2016 Internet Security Threat Report”, VOLUME 21, APRIL 2016, https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Chronicle of News Stories

1. 11/30/16, Brian Krebs, New Mirai Worm Knocks 900K Germans Offline, https://krebsonsecurity.com/2016/11/new-mirai-worm-knocks-900k-germans-offline/
2. 12/2/16, 3:55 PM, by Dan Goodin, There’s a new DDoS army, and it could soon rival record-setting Mirai; For more than a week, someone has waged massive attacks on a daily basis. http://arstechnica.com/security/2016/12/theres-a-new-ddos-army-and-it-could-soon-rival-record-setting-mirai/
3.