


Internet of Things (IOT) Security Best Practices

George Corser, PhD., Assistant Professor of Computer Science and Information Systems, Saginaw Valley State University

2017

IEEE
Advancing Technology for Humanity

Disclaimer

This document represents the considered judgement and personal views of the participating individuals listed on the following page with expertise in the subject field. It shall not be considered the official position of IEEE or any of its committees, and shall not be relied upon as a formal position of IEEE. It is produced by the IEEE Internet Initiative to enhance knowledge and promote discussion of the issues addressed.

Authors and Reviewers

Lead Author

- George Corser, PhD., Assistant Professor of Computer Science and Information Systems. Saginaw Valley State University.

Co-authors

- Glenn A. Fink, Ph.D., Cyber Security Researcher, Secure CyberSystems Group, Pacific Northwest National Laboratory
- Mohammed Aledhari, Doctoral Associate, Center for High PerformanceComputing and Big Data, Western Michigan University
- Jared Bielby, Independent Consultant; Co-chair, International Center forInformation Ethics
- Rajesh Nighot, Independent Consultant
- Sukanya Mandal
- Nagender Aneja, M.Engg in Computer Technology and Applications, UniversitiBrunei Darussalam
- Chris Hrivnak, Management Consultant, Marketing
- Lucian Cristache, Lucomm Technologies

Reviewers and Advisors

- Anna Slomovic, Independent Consultant; Expert on privacy and identity
- Greg Adamson, Chair, IEEE Ad Hoc Committee on IEEE Ethics Programs
- Jay Wack, President/CEO at Tecsec, Inc.
- Binit Sharma, Freelance Design Engineer, Nepal Innovation Center
- Geoffrey Beresford Hartwell, Independent, Engineer Arbitrator, Adjudicator,and ADR Practitioner
- David Richardson, Industrial Controls Engineer
- Sandhya Aneja, Assistant professor, Institute of Informatics andCommunication, University of Delhi
- Ali Kashif Bashir, Ph.D, Editor-in-Chief IEEE Internet Policy Newsletter
- John Laprise, Ph.D., Founder, Association of Internet Users;Internet Governance and Policy Strategist and Consultant
- Ina Wanca, Director of AI and Future Initiatives: x-MARS℠ and x-ENEA℠,Omnivest Consulting

Table of Contents

Introduction

The purpose of this paper is to present a set of well-investigated Internet of Things (IoT) security guidelines and best practices that others can use as a basis for future standards, certifications, laws, policies and/or product ratings. Most, if not all, of these guidelines would apply to any Internet-connected device; however, this paper focuses on security measures either peculiar to the IoT or especially relevant to the IoT. This paper assumes the end-to-end processing model of the Internet, in which application features such as security are handled by end nodes of the network, client and server hardware. It focuses on security mechanisms, including patching and updating, that should be considered at the manufacturing design phase rather than after devices have already been built or deployed.

This paper expands on the findings of a 2016 project by the IEEE Internet Initiative, the IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity and Privacy. Several ETAP events took place in 2015 and 2016 in various regions around the world, including Israel, China, India and the United States. These events brought together technologists, policy-makers and others with an interest and expertise in technology policy. One of the issues consistently brought up in these events was security of the IoT.

This paper is intended for an educated lay audience. The recommendations offered in this paper are generally intended for implementation by manufacturers of IoT products, however they are also designed to be readable by nontechnical but well-educated lawmakers, corporate and governmental policy makers, and participants in standard setting bodies.

Problem

Some manufacturers have produced and sold IoT devices that do not includesufficient security features. This has resulted in serious harm, both economicand otherwise, to specific parties and to the general public. A recent exampleof this include the DVRs and IP cameras now recalled by XiongMai Technologies [1]. As IoT devices proliferate, unless some action is taken to secure these devices, harm caused in the future may be even more severe.

Corporate and individual consumers of IoT devices may not currently possessthe technical expertise to evaluate the cost/benefit of purchasing perhaps more expensive properly secured devices. Further, if the dangers presented by the devices affect only parties other than the seller or purchaser of the devices, then there may be no financial incentive for seller or purchaser to worry about device security.

First step toward a solution to the problem

Some manufacturers have produced and sold IoT devices that do not includesufficient security features. This has resulted in serious harm, both economicand otherwise, to specific parties and to the general public. A recent exampleof this include the DVRs and IP cameras now recalled by XiongMai Technologies [1]. As IoT devices proliferate, unless some action is taken to secure these devices, harm caused in the future may be even more severe.

Corporate and individual consumers of IoT devices may not currently possessthe technical expertise to evaluate the cost/benefit of purchasing perhaps more expensive properly secured devices. Further, if the dangers presented by the devices affect only parties other than the seller or purchaser of the devices, then there may be no financial incentive for seller or purchaser to worry about device security.

Definition of IoT

The IoT overlaps other fields of study, including Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and Cyber Physical Systems (CPS) [2]. The IoT represents a growing and changing field with many definitions [3]. This paper defines the IoT as follows.

Internet of Things (IoT): a wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement.

Prior work on IoT security best practices

Several best practices papers targeted toward audiences similar to ours have been published in recent months. The Broadband Internet Technical Advisory Group (BITAG) produced a report focusing on consumer-oriented IoT devices [4]. The US Department of Homeland Security (DHS) published a document from a national defense perspective, omitting considerations such as personal privacy [5]. The Federal Trade Commission (FTC) released recommendations that emphasized privacy concerns: data security, data minimization, notice and choice [6]. The Automotive Information Sharing and Analysis Center (Auto-ISAC) created a set of cybersecurity best practices specifically for the automobile industry [6]. We considered suggestions from all of these sources when preparing our list.

Contributions of this paper

This paper offers a list of widely-accepted security techniques which may serve as a basis for creating future security standards. It prioritizes practices which might be most relevant to IoT and which might encourage standards and policies to improve IoT security. This is certainly not an exhaustive list of best practices. It is simply an attempt to help avoid some of the most serious and well known flaws in IoT practice today.

Organization of this paper

This paper begins with this Introduction and ends with a Conclusion. The Best Practices section is divided into three subsections: securing devices, securing networks and securing the overall system.

Best Practices

Securing Devices

1. Make hardware tamper resistant

Some IoT devices may operate continuously unattended and not subject to the security implied by this frequent, direct human observation. While it is best to keep devices relatively isolated so that only a few designated persons have physical access, especially for completely unattended devices, making them tamper-proof or tamper-evident may be advantageous. This form of endpoint hardening can help block potential intruders from reaching data. It may also defend against a hacker buying and then weaponizing devices.

The physical security of endpoints can include, for example, small simple plastic devices, port locks and camera covers, which lock out USB and Ethernet ports and cover webcam apertures. Port locks help prevent unwanted malware coming in. Some tamper-resistive approaches disable the device when it is tampered with. As a best practice, secure endpoint hardening likely implies a layered approach that requires attackers to circumvent a variety of obstacles designed to protect the device and its data from illicit access and use.

At the hardware/boot-software level, strong boot-level passwords or requiring the device to boot from local storage only may be sound approaches. Known vulnerabilities should be protected, such as open TCP/UDP ports, open serial ports, open password prompts, places to inject code such as web servers, unencrypted communications and radio connections. For shipping, tamper-evident packaging will enable the device owner to know if a device has been opened before it arrived. The number and strength of security at each layer depends upon the threat model, acceptable levels of risk, and desired convenience.

2. Provide for firmware updates/patches

Inevitably vulnerabilities will be discovered after devices have been deployed. Devices must be patchable or upgradable. Naturally, device firmware should only be modifiable with the proper digital signature. As it stands, device vendors and manufacturers have little financial incentive in ensuring ongoing IoT patch upgrades since revenue comes from the sale of the device, not the maintenance. Upkeep of IoT devices may detract from revenue. In addition, vendors are not legally held accountable to ongoing maintenance of devices beyond initial sales and competition drives vendors to cut corners, negating on quality for efficiency and speed of release into the market. While these factors may not have been critical previous to IoT, the interconnected nature

of IoT devices raises the bar to a new level in terms of functionality and accountability.

Detrimental also is the tendency of vendors towards planned obsolescence of devices in order to maximize profit through continued sales rather than through upkeep of existing devices. Furthermore, IoT devices are not efficiently designed or configured to respond to OTA (over the air) updates, resulting in, at best costly, and at worst, unmanageable procedures. As it stands, many IoT devices are un-patchable, and as such, cannot be made secure.

Researchers have observed that the ubiquitous advancement of IoT and the placement of unsecured and unattended IoT devices throughout homes and businesses will increase exponentially, opening up opportunities for hackers to exploit critical vulnerabilities [9].

Further to planned obsolescence, many IoT devices simply have limited life cycles. Vendors need to remain transparent and forthcoming about the life cycle of devices, especially in terms of service and upkeep, including the length of time they plan to support their devices. They need to take an active role in providing details on patches and upgrades as well as security risks and privacy concerns, ensuring that the consumer and/or user is informed about changes in vendor policy, functionality and security. The full lifecycle of the IoT device must be considered, beginning at manufacturing where security credentials must be “generated, allocated, and provisioned into the devices in a secure manner” [8]. Deliberations must also integrate the lifecycle of the original manufacturer. When the original vendor no longer exists, it becomes impossible to trace credentials in order to patch vulnerabilities and security breaches, and vendors are inevitably replaced and/or go defunct or bankrupt.

3. Perform dynamic testing

It is crucial that IoT devices undergo thorough testing,and establish minimum baseline for security. Static testing is not intended or designed to find vulnerabilities that exist in the off-the-shelf components such as processors and memory into which may be a component of the overall application.

Dynamic testing, on the other hand, is capable of exposing both code weaknesses and any underlying defects or vulnerabilities introduced by hardware and which may not be visible to static analysis. Dynamic testing may discover vulnerabilities that are created when new code is used on old

processors. We recommend manufacturers who purchase hardware and software from others do dynamic testing to ensure the items are secure.

4. Specify procedures to protect data on device disposal

Eventually devices become obsolete and users may decide to throw them away. Devices should be discarded without exposing private data. This is a security issue because improperly discarded devices may be converted to serve malicious purposes. This is a privacy issue because, if left in operation or if disposed of improperly, obsolete hardware could be used to reveal personal information about the user or other stakeholders in the IoT ecosystem. The same will be true for IoT devices that are sold to second owners or that become standard equipment in homes and are conveyed upon sale of the house.

The preparation of a formal plan by manufacturers for users to sanitize and dispose of obsolete IoT devices would address both security and privacy issues. Industry practice in other fields prescribes a "discard, recycle or destroy" (DRD) policy with periodic review of the plan to determine which devices require disposal and how to dispose of them. Some manufacturers encourage users to dispose of products directly through the manufacturer. This may be sensible for laptops and servers, but for IoT devices that may be small and cheap, or that are part of a much larger device (like a refrigerator) special accommodations may be required.

Individual users, when purchasing a used IoT product, might attempt to identify what personally identifiable information (PII) or authentication information such as username and password (UNPW) remains stored on the device, or is accessible by the device, or is required to be stored elsewhere in order to use the device. For example, the Amazon Echo Dot requires users to store their Wi-Fi network router passwords on an Amazon server. The question could be posed as to whether users should be expected to determine an individual DRD policy or not, which may include deleting information from an Internet-accessible location other than the device itself.

As it stands, users are inadequately prepared, not possessing the digital skills needed to navigate this kind of level of security, and being ill-equipped to understand the complexities of password storage in connected devices.

Exposure of such complexities often comes too late, as was the case in the recent revelation that modern copiers and fax machines have hard drives that retain copies of documents. Even corporate users with IT departments trained in security where unaware of this fact. The implications for security in the above example are numerous and highlight how easy it is for major security risks to be left unaccounted for.

Securing Networks

5. Use strong authentication

IoT devices should not use easy-to-guess username/password credentials, such as admin/admin. Devices should not use default credentials that are invariant across multiple devices and should not include back doors and debug-mode settings (secret credentials established by the device's programmer) because, once guessed, they can be used to hack many devices.

Each device should have a unique default username/password, perhaps printed on its casing, and preferably resettable by the user. Passwords should be sophisticated enough to resist educated guessing and so-called brute force methods.

Where possible we recommend two-factor authentication (2FA), which requires a user to employ both a password and another authentication form that does not rely on user knowledge, such as a random code generated via SMS text messaging. For IoT applications, we especially encourage the use of context-aware authentication (CAA), also known as adaptive authentication, which use contextual information and machine-learning algorithms to continuously evaluate risk of malice without bother to the user by demanding authentication. If risk is high, then the subscriber (or hacker) would be asked for a multi-factor token to continue having access.

6. Use strong encryption and secure protocols

Even if device passwords are secure, communications between devices may be hackable. In the IoT there are many protocols, including Bluetooth, Zigbee, Z-Wave, 6LoWPAN, Thread, Wi-Fi, cellular, NFC, Sigfox, Neul, and LoRaWAN. Depending on the protocol and on available computing resources, a device may be more or less able to use strong encryption. Manufacturers should examine their situation on a case-by-case basis and use the strongest encryption possible, preferably IPsec and/or TLS/SSL.

There may be cases where encryption is not desirable, such as in SAE J2735 Basic Safety Messages (BSMs), the wireless communications cars can use to avoid collisions. In those cases, messages can be sent in the open and verified using digital signatures. However, consideration should be given to the implications of omitting encryption. In the SAE J2735 case, BSMs could be used to alert collision-management systems falsely and immobilize an automobile. There is no stock answer that avoids the need for careful thought about the threat models anticipated and the vulnerabilities that will be tolerated. If data are transmitted unencrypted and unsigned, precautions should be made to ensure that false data have little or no chance of causing harm.

7. Minimize device bandwidth

Recently DDoS attacks have been conducted in large measure by armies of poorly protected IoT devices that have become zombie systems in massive global campaigns. Most IoT devices are made of commodity components that have vastly overpowered network capabilities for the function they are supposed to perform causing congestion on home networks and potentially contributing to huge costs for the targets of IoT-borne DDoS attacks.

If in the future there were 50 billion devices connected to the Internet, and if we assume (based on current conditions) that 1.1% of them are compromised and under coordinated remote control, that is 55 million rogue IoT devices. Suppose each device is capable of generating line-rate attack traffic equivalent to gigabit Ethernet (81,274 - 1,488,096 frames per second), for example the ARM9 system-on-a-chip (SoC) has two such connections built-in, and it costs less than $5 to make per chip. Using this 55-million-device zombie army to generate DDoS events, attackers could generate between 4.47 to 81.8 trillion frames per second or 55 petabits per second. This is well beyond the defensive capabilities of any single service provider. An attack of this magnitude would overwhelm the fastest network interface built to date (300Gbps) by a margin of 183,333 to 1.

There is no good way to reduce the malicious traffic produced by these systems apart from squelching it at the source. We recommend that device manufacturers should limit the amount of network traffic IoT devices can generate to levels reasonably needed to perform their functions. There is very little need for an Internet-connected refrigerator to spew Internet Control and Management Protocol (ICMP) messages at gigabit-per-second speeds. While some refrigerators are outfitted with video screens, they more than likely do not need to have high-speed upload capabilities.

Vendors should use hardware and kernel-level bandwidth limitations to throttle network transmission rates to levels reasonable for the tasks of each device. Such limitations make it much harder for an attacker to use a device in a DDoS attack, even if he has completely compromised it. Additionally, devices should be programmed to self-monitor for unusual behaviors and restore themselves to factory settings when alarming behavior is detected. If resetting devices to factory settings is not feasible, devices should at least reboot to potentially clear code the attacker has running in memory.

Now, supposing the aforementioned 55 million malicious IoT devices had hardware/kernel-enforced attenuated bandwidth, say 10 Ethernet frames per

second, then their aggregate potential attack profile drops to 550 million frames per second, and not more than 6.6 terabits per second. This nearly 150,000 times smaller, and while it is still too big for a single defender, that size attack is feasible for a distributed set of defenders to stop.

Additional kernel-level controls within devices that notice and attenuate large amounts of uploaded traffic or stop other unexpected behavior could further reduce the destructive capabilities of compromised devices without requiring heroic efforts by network defenders. Thus, we recommend serious consideration of the performance requirements of each device and that modest limitations be emplaced that are difficult to circumvent. This will greatly increase the safety of IoT devices and make it possible to safely field many more of them in the future.

8. Divide networks into segments

Separate the network into smaller local networks using VLANs, IP address ranges, or a combination thereof. Network segmentations are utilized in next-generation firewall security policies to clearly identify one or more source and destination interfaces on the platform. Each interface on the firewall must be assigned to a security zone before it can process traffic. This allows organizations to create security zones to represent different segments being connected to, and controlled by, the firewall. For example, security administrators can allocate all cardholder or patient data repositories in one network segment identified by a security zone (e.g., Customer Data). Then the administrator can craft security policies that only permit certain users, groups of users, specific applications, or other security zones to access the Customer Data zone – thereby preventing unauthorized internal or external access to the data stored in that segment.

This type of solution is more common in industrial applications but may be useful in broader circumstances. A separate, detached private network for a security system, perhaps with a dedicated channel to a "home base" in the case of a home security system, might suffice. If the system must use the Internet, a virtual private network (VPN) might be implemented.

Secure the overall IoT system

9. Protect sensitive information

The basic idea of IoT is to connect everyday objects via Internet or ad-hoc network. IoT devices provide services that are discoverable by other IoT devices. Most of the protocols leak sensitive personally identifiable

information (PII,) like owner's name or information that may be linkable to an individual, like a device's host name. This information can be linked to other information sources to target attacks. Service mechanisms and authentication protocols are required so that only authorized clients can discover the device.

10. Encourage ethical hacking and vulnerability disclosure

In order to fix security vulnerabilities, manufacturers and software developers must first know that these vulnerabilities exist. Researchers who discover serious vulnerabilities and report them responsibly provide a service to the industry similar to people who discover safety flaws in automobiles and other safety-critical machinery. One way to differentiate between research and unethical hacking is to encourage responsible disclosure of discovered vulnerabilities. Responsible disclosure requires the researcher to first notify the manufacturer or governing authorities and allow reasonable time for the vulnerability to be independently verified and fixed before going public with a system hack.

Manufacturers do not benefit financially from exposing flaws in their products but these flaws must be identified to improve functionality and security. Manufacturer-paid bug bounty systems can enable manufacturers to mitigate bad press while improving product quality at a cost lower than the cost of hiring paid penetration testers.

11. Institute an IoT Security and Privacy Certification Board

Because of prevalent problems with security already caused by IoT devices, engineers must accept responsibility for their creations. IEEE or some international organization should provide a professional certification program for designers, builders, and providers of new IoT technologies who pledge to hold to established best practices for creation of new devices outlined in this paper and other sources in their creation of IoT products. The program board should be empowered to verify whether the provider abides by responsible engineering practices (especially practices that enable security and privacy of the IoT), and would provide endorsement of providers who are bound by them. Negative action would be another dimension of this certification program and should be limited to loss of certification status and potentially reporting to the FTC or other government body for further action.

The certification body should verify at least the following elements of a provider's products, protocols, and documents:

a) Data are handled, used, protected, and shared responsibly.
b) Protocols used or recommended do not leak information about users beyond the explicit intent of those users.
c) When privacy issues arise, the certified provider responds promptly to concerns.
d) Authentication is suitably strong and follows proven protocols.
e) Devices are not over-powered or under-protected.
f) Devices should have an identifying label that cannot be easily forged and that contains a web link where customers can go to find the certification status of the device along with a device

description (model and serial number, etc.). This can be done in cooperation with the FTC or other national bodies.

Certification programs such as these decrease uncertainty and provide device makers, engineers, and authors with best practices to follow. Courts can consider certification as evidence that acceptable practices that are generally followed. In the event of litigation, a provider can point to the certification and say that it followed good engineering practice.

Conclusion

This report presents a list of best practices for manufacturers who would produce IoT devices, for engineers who would design IoT solutions, and for researchers who would evaluate IoT systems. The list is not intended to be comprehensive nor to offer government policy recommendations, rather it represents the kinds of activities that we believe will result in better IoT security.

The list can be viewed by policy makers as just one example of an engineering perspective on the kinds of procedures that constitute effective IoT security.

Individuals, companies and countries have suffered great harm resulting from unnecessarily weak computer and Internet security. The sheer number of potential IoT devices implies that, if not defended effectively, the IoT has the potential to permit even greater harm. Much of this potential harm is preventable by enforcing a few simple rules. We hope the list of best practices presented here represents a possible starting point for the formulation of future laws and technical standards.

Acknowledgements

The authors would like to thank Mr. S. Cullen Tollbaum of Pacific Northwest National Laboratory, Richland, Washington, USA, for his security recommendations and insight particularly in the section on minimizing device bandwidth. The authors would also like to thank Dena Hoffman, Society Products and Member Engagement Manager at IEEE for her invaluable assistance providing and hosting the necessary collaborative tools that made this project possible.

References

[1] Kan, Michael. "Chinese Firm Recalls Camera Products Linked To Massive DDOS Attack". PCWorld. N.p., 2017. Web. 19 Feb. 2017.

[2] Stankovic, J. A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), 3-9.

[3] Minerva, R., Biru, A., & Rotondi, D. (2015). Towards a definition of the Internet of Things (IoT). IEEE Internet Initiative, Torino, Italy.

[4] Broadband Internet Technical Advisory Group. (2016). Internet of Things (IoT) Security and Privacy Recommendations. Retrieved from BITAG website: https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf

[5] US Department of Homeland Security. (2016). Strategic Principles for Securing the Internet of Things (IoT). Retrieved from DHS website: https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL.pdf

[6] Federal Trade Commission. (2015). Internet of Things: Privacy and Security in a Connected World. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things- privacy/150127iotrpt.pdf

[7] Automotive Information Sharing and Analysis Center. (2016). Automotive Cybersecurity Best Practices. Retrieved from Auto-ISAC website: https://www.automotiveisac.com/best-practices/

[8] Federal Trade Commission. (2016). Connected Cars USA 2016: Keynote Remarks of Commissioner Terrell McSweeny. Retrieved from FTC website: https://www.ftc.gov/system/files/documents/public_statements/913813/mcs weeny_-_connected_cars_usa_2016_2-4-16.pdf

[9] Ensink, Bob. (2016). Patching the Internet of Things: IoT Software Update Workshop 2016. Retrieved from IETF website: https://www.ietf.org/blog/2016/07/patching-the-internet-of-things-iot- software-update-workshop-2016/