Developing an Effective Universal IoT Standard

A Sociotechnical Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Ryan Lenfant

April 6, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

Ryan Lenfant

Sociotechnical advisor: Peter Norton, Department of Engineering and Society

Developing an Effective Universal IoT Standard

Internet of Things (IoT) devices are popular: "there were an estimated 12.5 billion IoT devices, almost twice as much as the world's population of 6.8 billion" (Sirvaraman et al. 2018). IoT can expose users to data theft. Consumers do not understand the security risks of owning IoT devices and expect manufacturers to put the proper protections in place to ensure their devices are safe (Zheng et al. 2018). According to Zubiaga et al. (2018), "the challenges posed by the limited security of today's IoT devices are a major concern for the public." Connected devices must be secure. New technology is susceptible to exploits and must therefore be designed for security (Oka et al. 2014). An ethical standard could ensure sufficient security in all purchasable IoT devices. Tech companies, app developers, investors, the Consumer Technology Association (CTA), data brokers, and consumer advocacies are competing to determine the standards that will govern IoT. Tech companies, app developers and investors tend to be risk tolerant and may therefor develop or invest in vulnerable IoT devices. CTA, data brokers, and consumer advocacies generally favor stricter device security standards. Because these groups' interests vary, the security standards they favor vary too. Existing systems for classifying vulnerabilities and scoring risk do not apply to IoT devices (Mell et al. 2006). A universal IoT device standard could protect consumers and keep manufacturers accountable for their devices.

Review of Research

IoT security has not kept pace with IoT proliferation (Mendez et al. 2018). Mendez et al. (2018) propose incorporating security early in device design and introducing security standards in production. Meneghello et al. (2019) concur that security is integral to IoT device design. A new security standard is needed.

Tech companies are seeking to develop an IoT security standard. Complicating the security problem, however, are the 12.5 billion IoT devices that are already in service (Sirvaraman et al. 2018). Models can characterize and assess threats IoT systems and test their security (Martin et al 2020). Many device owners exacerbate device vulnerabilities, for example by using the same logins and passwords for all of their devices (Oravec, 2017). Many device owners neglect security, leaving it to the developers (Zheng et al. 2018). IoT developers can bolster security by identifying and securing the most vulnerable elements, where attacks are concentrated.

Researchers have used blockchain to improve device security. Derhab et al. (2019) used a blockchain-based integrity checking system (BICS) to enable a network of IoT devices to detect tampering to any of the devices in the network. With IoT sentinels, the network can thereby manage all security threats (Botello et al. 2020). Because a blockchain system would alert users to attacks, they could counteract them. Botello et al. (2020) favor building a generation of blockchain-capable devices that can report threats.

Consumers have the most at stake. Researchers have implemented security labeling on devices to inform consumers. When consumers demanded more label information, manufacturers agreed to mandatory labeling (Johnson et al. 2020). They felt mandatory labeling would work (Johnson et al. 2020). To enlist owners' support in security efforts (Zheng et al. 2018), some recommend education efforts addressed to consumers.

Trust is necessary to IoT communication. According to Ferraris et al. (2020), however, "Due to the uncertainty, interoperability and the heterogeneity of IoT, achieving trust between is still a challenge." IoT products should only communicate with each other if they trust each other. Yet trust is difficult to establish, because "isolated research communities" preclude uniform

standards (Ferraris 2020). IoT companies control requirements in device development, at a cost to "trust, and related domains such as security, identity, usability and privacy" (Ferraris et al. 2020).

Some IoT consumers are alert to the security deficiencies in IoT. According to Zubiaga et al. (2018), "the challenges posed by the limited security of today's IoT devices are a major concern for the public." IoT security vulnerabilities can attract media attention. Nevertheless, public perceptions of IoT remain generally favorable (Bian et al. 2016).

Addressing Security Objectives

Clear security objectives in device development can improve IoT security. Manufacturers' interest in their own reputations has not been sufficient to prevent security deficiencies (Ramalingam et al. 2020). More secure IoT will protect consumers and improve consumer trust.

Security features should be managed by developers with experience in cybersecurity. According to Rytel et al. (2020), "many manufacturers do not have experience with cyber security and often neglect it." Developers with poor security objectives create more vulnerable devices. Security in the design process is neglected as "only 10% out of 331 IoT companies sampled had any vulnerability disclosure policy in place" (Rytel et al. 2020). Companies that economize on device security or that fail to disclose vulnerabilities leave their customers exposed. Manufacturers depend on their customers to learn about vulnerabilities. Consumers tend to suppose that developers manage device security, and therefore neglect it themselves (Zheng et al. 2018). Developers must consider the consumer mindset in their design to ensure their devices are safe before production.

According to Sirvaraman et al. (2018), in 2010 there were "an estimated 12.5 billion IoT devices." Because "IoT devices are limited in computation and memory space due to their small physical sizes" (Hwang et al. 2020), they must work collaboratively. An effective IoT standard would compel companies to assume responsibility for device security.

Features of the Standard

Although IoT "is still in its infancy" (Nord et al. 2019), effective security techniques are available. For ease of access, such techniques should be assembled in a single document. Blockchain, enforced security measures, and proper labeling of devices can improve network security.

With a blockchain system, a network of IoT devices can detect when any of the devices has been tampered with (Derhab et al. 2019). A universal blockchain system adds a second layer of protection to a user's home network. A generation of blockchain-capable devices that can report vulnerabilities, bolstering security (Botello et al. 2020). Users could tell when any device in the network is exploited, including devices manufactured by a different company.

Manufacturers must update device security features after production. Anand et al. (2020) contend that devices are "flooded in the market with known vulnerabilities," with no "afterthought to their security considerations." Updates are necessary to keep devices secure. To protect IoT users, companies need incentives to update devices or to warn users of vulnerabilities. Mandatory security updates in development and production would compel companies to keep track of vulnerabilities. Consumers will pay more for secure IoT devices (Johnson et al., 2020).

Many device owners practice deficient cyber hygiene, thereby causing vulnerabilities (Oravec 2017). An informative universal labeling system could define security risks for consumers. Such a system would educate users security, thereby empowering them.

Combating Social Issues

Tech companies, app developers, investors, the Consumer Technology Association, data brokers, and consumer rights advocacies should be considered in an ethical standard. Such a standard would promote trust.

Consumers who distrust IoT security may choose not to buy IoT devices. Of consumers who planned on buy an IoT device in 2016, 66 percent doubted device security (Burt 2016). Universal systems can classify and score vulnerabilities (Mell et al. 2006). These standards simplify identification and repair of vulnerabilities across manufacturers. To work, universal security specifications for IoT devices must be agreed to by both manufacturers and consumers.

Media reports influence public perceptions of IoT. An effective IoT standard would earn favorable publicity for IoT security.

Conclusion

IoT security has been deficient. A mandatory IoT security standard is needed. To work, such a standard must be developed collaboratively by interest groups representing manufacturers, consumers, law enforcement, and privacy advocacies.

References

Anand, P., Singh, Y., Selwal, A., Singh, P. K., Felseghi, R. A., & Raboaca, M. S. (2020). IoVT: Internet of Vulnerable Things? Threat Architecture, Attack Surfaces, and Vulnerabilities in Internet of Things and Its Applications towards Smart Grids. *Energies (19961073)*, *13*(18), 4813. https://doi.org/10.3390/en13184813

Bian, J., Yoshigoe, K., Hicks, A., Yuan, J., He, Z., Xie, M., Guo, Y., Prosperi, M., Salloum, R., & Modave, F. (2016). Mining Twitter to Assess the Public Perception of the "Internet of Things." *PLoS ONE*, *11*(7), 1–14. https://doi.org/10.1371/journal.pone.0158450

Botello, J. V., Mesa, A. P., Rodríguez, F. A., Díaz-López, D., Nespoli, P., & Mármol, F. G. (2020). BlockSIEM: Protecting Smart City Services through a Blockchain-based and Distributed SIEM. *Sensors (14248220)*, *20*(16), 4636. https://doi.org/10.3390/s20164636

Burt, J. (2016). Consumers Worried About IoT Security, Survey Finds. *EWeek*, 1.

Derhab, A., Guerroumi, M., Gumaei, A., Maglaras, L., Ferrag, M. A., Mukherjee, M., & Khan, F. A. (2019). Blockchain and Random Subspace Learning-Based IDS for SDN-Enabled Industrial IoT Security. *Sensors (14248220)*, *19*(14), 3119. https://doi.org/10.3390/s19143119

Ferraris, D., & Fernandez-Gago, C. (2020). TrUStAPIS: a trust requirements elicitation method for IoT. International Journal of Information Security, 19(1), 111–127. https://doi.org/10.1007/s10207-019-00438-x

Hwang, J., & Yoo, J. (2020). A Memory-Efficient Transmission Scheme for Multi-Homed Internet-of-Things (IoT) Devices. *Sensors (14248220)*, *20*(5), 1436. https://doi.org/10.3390/s20051436

Johnson, S. D., Blythe, J. M., Manning, M., & Wong, G. T. W. (2020). The impact of IoT security labelling on consumer product choice and willingness to pay. *PLoS ONE*, *15*(1), 1–21. https://doi.org/10.1371/journal.pone.0227800

Martin, T., Geneiatakis, D., Kounelis, I., Kerckhof, S., & Nai Fovino, I. (2020). Towards a Formal IoT Security Model. *Symmetry (20738994)*, *12*(8), 1305. https://doi.org/10.3390/sym12081305

Mell, P., Scarfone, K., & Romanosky, S. (2006). Common vulnerability scoring system. *IEEE Security & Privacy*, *4*(6), 85-89.

Mendez Mena, D., Papapanagiotou, I., & Yang, B. (2018). Internet of things: Survey on security. *Information Security Journal: A Global Perspective*, *27*(3), 162–182. https://doi.org/10.1080/19393555.2018.1458258

Meneghello, F., Calore, M., Zucchetto, D., Polese, M., & Zanella, A. (2019). IoT: Internet of Threats? A survey of practical security vulnerabilities in real IoT devices. *IEEE Internet of Things Journal*, *6*(5), 8182-8201.

Nord, J. H., Koohang, A., & Paliszkiewicz, J. (2019). The Internet of Things: Review and theoretical framework. *Expert Systems with Applications*, *133*, 97–108. https://doi.org/10.1016/j.eswa.2019.05.014

Oka, D. K., Furue, T., Langenhop, L., & Nishimura, T. (2014, November). Survey of vehicle IoT bluetooth devices. In *2014 IEEE 7th international conference on service-oriented computing and applications* (pp. 260-264). IEEE.

Oravec, J. A. (2017, July). Emerging "cyber hygiene" practices for the Internet of Things (IoT): professional issues in consulting clients and educating users on IoT privacy and security.

In *2017 IEEE International Professional Communication Conference (ProComm)* (pp. 1-5). IEEE.

Ramalingam, S., Gan, H., Epiphaniou, G., & Mistretta, E. (2020). A Holistic Systems Security Approach Featuring Thin Secure Elements for Resilient IoT Deployments. *Sensors (14248220)*, *20*(18), 5252. https://doi.org/10.3390/s20185252

Rytel, M., Felkner, A., & Janiszewski, M. (2020). Towards a Safer Internet of Things—A Survey of IoT Vulnerability Data Sources. *Sensors (14248220)*, *20*(21), 5969. https://doi.org/10.3390/s20215969

Sivaraman, V., Gharakheili, H. H., Fernandes, C., Clark, N., & Karliychuk, T. (2018). Smart IoT devices in the home: Security and privacy implications. *IEEE Technology and Society Magazine*, *37*(2), 71-79.

Zheng, S., Apthorpe, N., Chetty, M., & Feamster, N. (2018). User perceptions of smart home IoT privacy. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1-20.

Zubiaga, A., Procter, R., & Maple, C. (2018). A longitudinal analysis of the public perception of the opportunities and challenges of the Internet of Things. *PLoS ONE*, *13*(12), 1–18. https://doi.org/10.1371/journal.pone.0209472