Essay submission

IIC future leaders competition | July 2023

Online technologies represent the best of human ingenuity and interconnectedness.

The capabilities of the information technologies have expanded since the 70's into the early 2000's and now the 2020's. In each iteration of information technologies, we have encountered enormous possibilities as well as a range of challenges. The nature of device-to-device communication over networks as an evolution means that vulnerabilities in traditional IT systems are augmented. With IoT, where devices are connected to devices and not just users, the risk of unauthorized access to private data, manipulation of data, and consequent harm presents difficulties similar to those of the past but also new challenges.

I intend to address this topic in the following way:

- Outline the definitions of and main security risks in IoT and Edge devices
- Explain how these have changed as technology has transformed
- Outline the current mitigation mechanisms and whether mitigation is the only viable solution given many technological tools are dual purpose
- Outline where I think responsibility is and where it should be, based on an ethical framework in our understanding of cybersecurity
- Outline a suitable angle for policy intervention where possible

The Internet of Things (IoT)

The Internet of Things (IoT), according to Oracle, describes a network of physical objects[1] that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data and other devices and systems over the internet. Several technologies have made the concept of IoT possible over the years, including innovations in AI, Machine learning, Cloud computing, low-cost low-power sensors, and connectivity protocols. The internet of things allows for the collection of huge amounts of data for endless use cases, driving new business models and increasing business value.

Privacy in Technology

Privacy, as a metaphysical concept, is intrinsic to the liberal democratic societies we live and participate in. According to the CSRC, privacy in technology is the 'assurance that the confidentiality of, and access to, certain information about an entity is protected.' A suitable working definition I will use in this essay, by Toby Hayes[2], is that privacy is the understanding that individuals have about how their personal data is used and their ability to influence the outcomes of that use. Data privacy, then, is about having some choice in the decision-making process when data is created, shared, and stored within a given system[3]. Cybersecurity neatly fits into data privacy. We can define cybersecurity for our purposes as a set of strategies, techniques, and controls used to reduce risk and to ensure that one's data is protected. A very useful corollary is GDPR, as an example of privacy by design, given there is a mandated obligation to get users' consent. This was not something thought of when the internet was starting to take off and represents an evolution in our understanding of privacy and security.

Technology and the associated risks have changed over time, this has presented challenges and opportunities and where policy can step in for security by design, specific to IoT and Edge cases.

Cybersecurity is not uniquely concerned with data, it is more concerned with the protection of assets in general such as critical infrastructure, preventing disruption, and malware. Cybersecurity functions as part of the larger body of tools that assist in the enforcement of the protection of such data after it has been consented to being managed by an enterprise.

Definitions aside, important risk considerations in IoT include but are not limited to the following:

- DDoS – Distributed denial of service attacks
- Malware
- Misuse and misrepresentation of data
- Replay attacks
- Compromised stakeholders.

[1] https://www.oracle.com/uk/internet-of-things/what-is-iot/

[2] https://www.linkedin.com/pulse/what-we-talk-when-privacy-toby-hayes/

[3] https://iotac.eu/9-important-security-requirements-to-consider-for-iot-systems/

The universe of IoT devices is vast. Industrial automation, provision of networks at concerts or sporting events, and the data collection that entails, baby monitors all fit this definition. The security of each aspect should be recognized as quite distinct. It would be important to recognize this heterogeneity in crafting solutions and policy implementation. The history of society has never been fully secure. Likewise, the internet has never been a fully secure place. We accept a certain degree of risk for our participation. As such, the internet has been sometimes characterized by many security incidents.

The most cited information security requirements are confidentiality, integrity, and availability [Christen, Gordin, Loi 2020]. That order has also represented the importance of those concepts in traditional IT systems. I think that a suitable position would be such that these requirements are important, and a few additional ones can be adopted for the securing of data across networks and privacy specifically. These are Authenticity, Nonrepudiation and DDoS protection.

Source; Johnathan Charles

We have known that how connected a device is directly proportional to how effective a service is. Such an approach was crucial to the growth of the internet in the 1900s and 2000s. However, this seems to cause issues with IoT, and edge devices and services are concerned. In general, in telecommunications large amounts of data about networks is stored and collected so that artificial intelligence, for example, may be used to manage, configure, and adapt networks to changing requirements. This is largely necessary; however, it remains crucially important to secure such data. This means care must be taken in collection as the more connected devices are, the larger the footprint for a potential attack [McFadden, 2023].

The nuances of this are such that insider attacks will always be more problematic than that of outsiders. As such, differing levels of authorization of different personnel as best practice, among others, should be followed [Forsyth, 2023].

My position is that policy can be effective in the arena where mitigation is likely to be most effective such as rollout and design, and stakeholder management and in areas where this is not possible to provide a reasonable floor.

IoT and edge devices pose several unique risks in the domain of confidentiality, examples include the Mirai botnet [Jia et al,2020] a DDoS tool that is proficient in managing around 3 million IoT device bots, AWS DDoS assault in February 2020 with a volume of 2.3Tbps [Crane, 2020], another example is a six month campaign on the google foundation with an 'assimilated 2.5Tbps DDoS' in September 2017, [Kovacs,2020 ; Deviscourse, 2020] . Confidentiality means protection of information from illegitimate read access, however not all information in IoT use cases needs confidentiality. Addressing this heterogeneity issue is paramount first. Business data generated in traditional IT systems such as emails, employee salaries, technical specifications, and business plans should all be kept confidential. Similarly, account credentials such as passwords and cryptographic keys should also be kept confidential. Data from IoT systems tend not to have strict security requirements as they are sensor readings. These readings could theoretically be obtained by measuring the parameters by anyone who wanted the data themselves. This raises a few issues, specifically in areas such as healthcare, retail, and even home automation systems such as baby monitors due to the sensitive and personal nature of these domains.

The Integrity aspect of security relates to whether the data is accurate and fit for purpose. IoT devices interact with physical environments to collect data to keep track of or control physical processes. If the data is changed, then tracking can become inaccurate and a number of issues from the critical national infrastructure perspective as well as the industrial enterprise perspective are at risk. The results of such security incidents can range from mere system failures to fatal accidents. Similarly, security firmware updates sent to IoT devices should be made more secure, and these devices should not be viewed as mere sensors given the complex interdependencies, they are a part of. Updates to security measures can be modified leading to significant consequences.

Availability pertains to information always being available to those who may need it at the time of need. Availability is important for healthcare, industrial process and security, and surveillance applications. While availability may be desirable, it may not lead to as serious consequences depending on the domain (such as healthcare, where decisions can have fatal consequences) if information is not available in a timely manner.

Responsibility, and Risk. Most technologies being dual use and Cyber Security as cat and mouse game with constantly hanging rules.

It would be unrealistic and intellectually disingenuous to not state that in every instance of technology, most tools are dual purpose. Meaning that the potential exists to cause harm or do good depending on the user. Additionally, security in general is a cat and mouse game of keeping up with a changing landscape and changing rules. This forms a challenging background where using security tools to keep privacy and enact security by design will function. My personal position is that life has very few solutions. It is important to engage with the world as it is and not how you would like it to be. Most of what you have in front of you are actually trade-offs and not necessarily solutions. In this way, mitigation of attacks may not be the only thing we want to optimize for in considering whether security by design is possible.

This provides a useful segue to discuss the issues of risk and externalities, which cannot be ignored. The moral hazard presents itself in that it may not be in a manufacturer's best interest to disclose certain security risks because there is no economic incentive to doing so, and little consequence for not doing so. There are issues present on the levels of individuals, enterprises/organizations, and states. Security personnel need to often decide how they will deal with newly discovered vulnerabilities, which leads us to a further question on the merits of full disclosure versus responsible disclosure.

On the one hand, publishing too much or too early can cause significant harm. On the other hand, keeping a vulnerability a secret may keep users from taking action on their own and robs them of any agency for taking responsibility. This presents intriguing questions about how one can be responsible for things they do not understand or know about, assuming the responsibility is not symmetric between consumer and manufacturer. For organizations, finding the balance between investing in security, where the reward is something never happening, and accepting remaining risks is difficult as organizations have differing needs. Also at an architectural level, it remains challenging to predict how a new security system or mechanism will be used, and standardization falls behind in IoT environments where many products reach the market before standardization is considered [McFadden 2023].

- Many tools are implemented first [Think break things, ask questions later Mark Zuckerberg] where the installed base becomes very large without attention to the security considerations for those IoT devices and edge services.
- This is not a problem with an obvious solution.

Competing perspectives on in either a direction of a free for all or a fully constrained environment

Policy in my opinion will be limited, but this does not negate its importance, similar to how we do not suspend our moral enterprise because we sometimes do not live up to our ideals. Here it would be useful to introduce the other concepts such as authenticity, nonrepudiation, and DDoS protection[1] alongside availability, integrity, and confidentiality. Denial of service protection is a unique security vulnerability for IoT and edge devices (Gubbi et al., 2013), in addition to brute force assaults and botnet attacks, since IoT works on assorted networks embedded with large and small devices. The smaller devices have lower computational power (a benefit that allowed the IoT to be widely adopted) and less storage capacity, and as such, protection mechanisms and cryptographic algorithms used for security are difficult to implement over them (Kumari et al., 2023). As such, there are situations where these small IoT devices have no privacy-preserving algorithms. DDoS attacks stop the network by flooding the server or site with many requests simultaneously from different locations, which has the effect of reducing the genuine users' bandwidth (Lau et al., 2000). All of these issues make security by design a challenging paradigm, and as such, policy can only hope to create a suitable floor or minimal set of security best practices that would apply to all.

Devices and Services. Responsible regulation may make it so that devices and services which do not meet this threshold cannot be offered in such an environment, even where heterogeneity is a feature of the landscape.

The solutions include incorporating aspects such as authenticity into a security framework. Where authenticity is of importance for control commands, configuration parameters and software updates received by IoT devices. It is important that data authentication origination is taken seriously as attackers could spoof fake data into a system. The consequences of this are the same as modifying data illegitimately like an SQL attack.[1]

Similarly, non-repudiation means that the data's origin can not only be verified by the intended receiver but that this can also be verified by third parties, think of append only lists in a line of code or the blockchain. This sort of protocol may be incredibly helpful for high stakes industries such as transport and healthcare [because of fatalities and critical infrastructure] and information is held for longer so it can be audited when fatal incidents occur. This may not be the standard in even traditional IT environments but can be important in an IoT environment.

In the same vein, access control and authorization should also be a baseline in an IoT and edge scenarios [This is already the case in traditional IT spheres] . This limits the scope of inside attacks and is a good baseline for stakeholder management. While best practice protocols may be out of date by the time they are published, we should still strive towards a fundamental baseline of policy which customers can expect. These include:

- No default passwords
- Full public APIs
- Code audits within reason

Additionally, the novelty of the IoT ecosystem should be taken into account when considering solutions. [Chen et al 2018] offers a trust architecture solution based with a cross-layer authorization protocol. This can be applied to types of applications to solve the scalability issue in an IoT dynamic environment. A reputation evaluation scheme is proposed that could help modification attacks, replay attacks, and message dropping attacks while achieving higher detection accuracy of attack nodes. This does not address the detection of malicious and organizational behaviours but represents a good start.

Similarly, [Brumfitt et al 2015] highlighted some challenges in traditional network security models and proposes a new framework that takes into account the specifics of IoT. The framework includes a lightweight forensics application (LFA), a Central Security Manager (CSM), and a Collaborative component (Col network). The LFA is designed so it can be adaptable to any device it is integrated on, including devices with low processing power such as small sensors. It prioritizes collecting data that the CSM can use to enforce security. This happens by adhering to a predefined set of classifications. The CSM makes the decisions and collects data from the LFA and collaborative components. This part is designed to be processing power heavy and automated, making decisions for itself as opposed to waiting for an admin to make them. The collaborative component collects data in the distributed networks which can indicate possible vulnerabilities, threats, and attacks. The benefit of this is that it can work across domains such as business and home.

For example, a user may have a personal Col network at home with family devices connected to one CSM. As they arrive at work, their device automatically switches to the business Col network to ensure policies are followed. This will ensure devices are usable at home as normal, although at work restrictions may take hold in order to follow the corporate policies [Brumfitt et al 2015].

[Ding et al 2019] also note that traditional access control technologies are not suitable for IoT cases and propose a novel attribute-based control scheme for IoT systems which simplifies access management. Blockchain technology is used to record the distribution of attributes to avoid single point failures and data tampering. This enables devices to effectively secure themselves. The process is also optimized for security, lightweight calculation, and can be scaled across different devices of differing processing speeds and can effectively resist attacks.

All the above notwithstanding, security remains a non-zero-sum game that ratchets upward. It would be unrealistic to expect every manufacturer or every customer to be up to date with everything all the time. While all these solutions can form a unique baseline for security and privacy in IoT and edge devices, it is important to recognize that not all of them will be easily implemented across business models and domains. It remains incumbent upon all stakeholders to define acceptable standards and decide on acceptable risks. None of these solutions are fool proof and the burden remains on all of us as intelligent consumers and responsible producers to not simply transfer costs but embed secure protocols to protect the markets we service.

References.

[1] Abiodun Esther Omolara, Abdullah Alabdulatif, Oludare Isaac Abiodun, Moatsum Alawida, Abdulatif Alabdulatif, Wafa' Hamdan Alshoura, Humaira Arshad,The internet of things security: A survey encompassing unexplored areas and new insights,Computers & Security,Volume 112,2022,102494,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102494 https://www.sciencedirect.com/science/article/pii/S0167404821003187)

[2] Chen, J., Tian, Z., Cui, X. *et al.* Trust architecture and reputation evaluation for internet of things. *J Ambient Intell Human Comput* **10**, 3099–3107 (2019). https://doi.org/10.1007/s12652-018-0887-z

Christen, Gordij, Loi, 'The ethics of Cybersecurity, ISSN 1875-0044 ISSN 1875-0036 (electronic)

The International Library of Ethics, Law and Technology

ISBN 978-3-030-29052-8 ISBN 978-3-030-29053-5

[3] S. Ding, J. Cao, C. Li, K. Fan and H. Li, "A Novel Attribute-Based Access Control Scheme Using Blockchain for IoT," in *IEEE Access*, vol. 7, pp. 38431-38441, 2019, doi: 10.1109/ACCESS.2019.2905846.

[4] Mohamed Aly Bouke, Azizol Abdullah, Sameer Hamoud ALshatebi, Mohd Taufik Abdullah, Hayate El Atigh,

An intelligent DDoS attack detection tree-based model using Gini index feature selection method, Microprocessors and Microsystems, Volume 98,2023,104823,ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2023.104823 (https://www.sciencedirect.com/science/article/pii/S0141933123000698)

[5] E. R. Naru, H. Saini and M. Sharma, "A recent review on lightweight cryptography in IoT," *2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, 2017, pp. 887-890, doi: 10.1109/I-SMAC.2017.8058307.

[6] C. Landwehr, D. Boneh, J. C. Mitchell, S. M. Bellovin, S. Landau and M. E. Lesk, "Privacy and Cybersecurity: The Next 100 Years," in *Proceedings of the IEEE*, vol. 100, no. Special Centennial Issue, pp. 1659-1673, 13 May 2012, doi: 10.1109/JPROC.2012.2189794

[7] Pooja Kumari, Ankit Kumar Jain,A comprehensive study of DDoS attacks over IoT network and their countermeasures, Computers & Security, Volume 127,2023,103096, ISSN 0167-4048,

https://doi.org/10.1016/j.cose.2023.103096, https://www.sciencedirect.com/science/article/pii/S0167404823000068)

[8] R and K. S, "Deep Learning Approach for Intrusion Detection and Mitigation in IoT Environment: A Comprehensive Study," *2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI)*, Chennai, India, 2023, pp. 1-6, doi: 10.1109/RAEEUCCI57140.2023.10134161.