Internet of Vulnerabilities: How Society Shapes Internet of Things Security

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science
University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Oscar Laurence Lauth
Spring 2025

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

Advisor

Rider W. Foley, Department of Engineering and Society

Introduction to Internet of Things

An 8-year-old girl hears an eerie song, *Tiptoe Through the Tulips*, playing in her bedroom. When she goes to investigate, a man's voice emanates from the newly installed Ring security camera, claiming to be Santa Claus while hurling racial slurs at her (Vigdor, 2019). A chilling scene that underscores an unsettling reality: the very devices designed to make our lives safer, more convenient, and more efficient can also be exploited in ways that are disruptive and harmful.

The Internet of Things (IoT) refers to a vast and rapidly expanding network of interconnected devices, ranging from smart fridges and fitness trackers to industrial automation systems. These devices, embedded with sensors and software, are built for specific tasks and are typically constrained in hardware capabilities, processing power, and energy consumption (Radouan Ait Mouha, 2021). Despite these constraints, IoT infrastructure forms the backbone of an increasingly connected world, automating daily life and optimizing processes across industries. The scale of this network is staggering. By the end of 2024, the number of IoT devices worldwide is estimated to be nearly 19 billion (Sinha, 2024). However, IoT infrastructure extends beyond the convenience of telling Alexa to turn off the lights or a mailman shouting at a Ring doorbell. It plays a crucial role in critical infrastructure and essential services.

In healthcare, for example, wireless glucose monitors, patient fall detectors, and real-time medical equipment tracking improve patient outcomes and streamline hospital operations (Schwartz, 2025). The transportation sector relies on IoT for vehicle-to-infrastructure communication, helping to reduce traffic congestion and enhance road safety (Kanthavel et al., 2021). In industrial settings, predictive maintenance systems use IoT sensors to monitor machinery, preventing costly failures and optimizing productivity (Moffa, 2023). These

applications illustrate IoT's deep integration into modern society, making its security more vital than ever. A single vulnerability in a connected device can have catastrophic consequences—a hacked pacemaker could endanger a patient's life, a compromised car system could lead to fatal accidents, or an industrial sabotage attack could disrupt supply chains and economies.

Security flaws in the design, maintenance, or use of these devices create opportunities for cyberattacks that can have widespread and devastating consequences. This research paper argues that society's engagement with IoT—how we design, deploy, maintain, use, and rely on these devices—directly contributes to security vulnerabilities. By examining the societal factors shaping IoT infrastructure and the risks they introduce, this paper aims to highlight critical weaknesses in current IoT practices and advocate for better engagements to ensure a safer and more secure future in an increasingly connected world.

A Deeper Dive into IoT and Security

Early IoT systems lacked robust security measures, as manufacturers prioritized time to market over safeguarding devices (Pepper Developments, 2024). This made them prime targets for cyberattacks. One of the earliest large-scale IoT security incidents was the Mirai botnet attack in 2016. In this attack, cybercriminals exploited weak default credentials in IoT devices, creating a botnet of hundreds of thousands of compromised devices. This botnet then launched a Distributed Denial-of-Service (DDoS) attack, temporarily bringing down major sites such as Amazon, Twitter, Netflix, Reddit, PayPal, and GitHub (Antonakakis et al., 2017). Since then, IoT security has become an increasing concern as the number of connected devices continues to grow. Despite growing efforts to secure IoT infrastructure, attacks are still on the rise. According to a 2023 report, cyberattacks targeting IoT increased by 400% in 2022 (Sinha, 2024).

To better understand security vulnerabilities in IoT, it is crucial to examine how these devices communicate and exchange information. A key feature of IoT systems is their reliance on communication standards, which define the rules and parameters for data transmission between devices. These standards ensure interoperability across different hardware and enable seamless wireless communication. They specify transmission and reception frequencies, modulation schemes, power levels, network protocols, and more. Some common wireless standards used in IoT are summarized and compared in the table below (see Table 1).

Table 1. Comparison of Common IoT Wireless Standards (A. Al-Shareeda et al., 2023)

Wireless Standard	Properties	Use Cases
Wi-Fi (IEEE 802.11)	High throughput, long range, high power	Smart doorbells, home automation
Bluetooth Low Energy (BLE)	Medium throughput, medium range, low power	Fitness trackers, occupancy tracking
Near-Field Communication (NFC)	Low throughput, low range, low/no power	Tap to pay, smart clothing tags
Long Range Wide Area Network (LoRaWAN)	Low throughput, extremely long range, low power	Environmental monitoring, smart cities

These standards are typically established by organizations such as the Institute of Electrical and Electronics Engineers (IEEE) and the Bluetooth Special Interest Group (SIG). Within these organizations, working groups composed of industry representatives, researchers, and engineers are responsible for defining and updating the standards. These efforts are further overseen by committees and boards that ensure proper review and approval processes (IEEE Standards Association, 2025).

Beyond just understanding IoT communication, analyzing its security landscape requires familiarity with key cybersecurity principles. Malware refers to malicious software designed to compromise an IoT device, such as ransomware, worms, or spyware. A threat is a potential danger that could exploit a weakness in an IoT system—for example, the presence of a virus on a device constitutes a threat, but it remains inactive until it executes an attack. A vulnerability is a flaw in an IoT system's design, implementation, or usage that exposes it to potential threats. When an actual attempt is made to compromise an IoT system—such as data theft or service disruption—it is classified as an attack (Schiller et al., 2022). Some common attacks in the context of IoT include man-in-the-middle attacks, social engineering, buffer overflows, password attacks, and malware (Sasi et al., 2024). These are further detailed in Table 2 below.

Table 2. Common IoT Attack Methods

Attack	Description
Man-in-the-middle	Attacker sits between the communication of two IoT nodes, intercepting data
Social engineering	Attacker deceives users into leaking sensitive information
Buffer overflow	Attacker exploits unsafe functions to overwrite unauthorized portions of memory
Password attacks	Attacker guesses passwords through brute force, dictionaries, default credentials, or leaked passwords
Malware	Attacker injects malicious code such as spyware or ransomware to impact a system

With billions of IoT devices deployed across various industries, understanding how these systems communicate and transfer potentially sensitive data, along with the current security landscape, is essential for analyzing IoT security.

Understanding IoT as Social Infrastructure

The Internet of Things is more than just a collection of smart devices, it functions as an expansive and deeply embedded infrastructure that has become increasingly interwoven into society. However, like any infrastructure, IoT systems are not purely technical systems. They are actively shaped by social group practices, specifications, and broader societal influences. To better understand IoT as a societal infrastructure and analyze its security implications, Susan Leigh Star's infrastructure framework will be applied.

In *The Ethnography of Infrastructure,* Susan Leigh Star describes infrastructure not as a single entity, but as a relational concept that varies depending on context (Star, 1999). For example, a cook sees water infrastructure as invisible and taken for granted. The expectation is that clean water will simply flow from the tap. A plumber, however, views water infrastructure as an intricate and highly visible system, requiring maintenance and troubleshooting. This shift in visibility highlights how infrastructure operates differently depending on one's role in relation to it. Star further defines infrastructure through nine key properties. Of these, three are particularly relevant to IoT and will be used for analysis in this research: embodiment of standards, links to conventions of practice, and visibility when broken (Star, 1999).

The first key aspect, embodiment of standards, refers to how infrastructure adheres to standardized rules, protocols, and specifications that ensure interoperability and consistency across systems (Star, 1999). In IoT, wireless communication standards play a central role in enabling devices to connect and communicate. Beyond communication, IoT devices also adhere to hardware and software standards, such as IPC standards for electronic components and security frameworks for encryption and authentication. Standards are crucial to IoT security because they establish baseline protections across devices. However, their openness can also

create vulnerabilities. Attackers can study widely used standards to identify and exploit weaknesses. For example, researchers discovered a flaw in the Wi-Fi standard that allows attackers to trick users into connecting to a malicious network by imitating a trusted network's SSID (Service Set Identifier) (Gollier & Vanhoef, 2024). This demonstrates how standardized systems, while necessary for interoperability, can also introduce widespread security risks.

Conventions of practice, another key property of infrastructure, refers to the habitual ways people interact with and maintain infrastructure (Star, 1999). In IoT, this can include both how engineers develop devices and how end users engage with them. Many security issues arise not just from technical flaws, but from predictable user behavior. For example, the Wi-Fi SSID confusion attack from above (Gollier & Vanhoef, 2024) exploits users' learned habit of trusting a network name that matches their expectations without further verification. Because people have been conditioned to assume that a familiar SSID means a network is safe, attackers can easily spoof legitimate network names and deceive users into connecting to malicious hotspots. This convention of assuming network legitimacy illustrates how ingrained habits can create security risks within IoT infrastructure.

The final aspect that informs this analysis is visibility when broken which describes how infrastructure is often invisible during normal operation, but becomes highly noticeable when it fails (Star, 1999). In the context of IoT, this aspect underscores the dangers of deploying insecure systems that, when compromised, can have severe real-world consequences. For example, in 2020, over 420 million IoT devices were deployed in the healthcare industry alone (Puat & Rahman, 2020). Many of these devices transmit sensitive personal health data, making them prime targets for attackers (Koppel & Kuziemsky, 2019). If such data were stolen, the consequences would be highly visible, manifesting as identity theft, blackmail, and fraud. These

breaches expose the hidden dependencies within IoT infrastructure, revealing its vulnerabilities only after significant harm has occurred. This aspect will primarily be used to illustrate the importance of secure IoT systems and the harsh impacts of insecure systems.

By applying Star's framework to IoT security, we can better understand how technical vulnerabilities are shaped by social forces. Each of the three aspects, embodiment of standards, conventions of practice, and visibility when broken, offers a lens for analyzing the societal interplay in IoT security. This framework will serve as a useful tool in analyzing evidence for how security risks emerge, their severity if exploited, and how they might be mitigated in the future.

Researching Security in IoT

From enabling smart manufacturing (Yang et al., 2019) and controlling smart home devices (Rock et al., 2022) to supporting medical technology (Sadek et al., 2019), IoT infrastructure is deeply integrated into societal behaviors and practices. As these systems are trusted to handle sensitive data and perform critical tasks, the nature of human interaction with IoT infrastructure becomes crucial to its design and security. This raises an important question: How do the current norms and practices associated with building IoT infrastructure contribute to security vulnerabilities?

To explore this question, two methods of evidence collection are used. The primary source is interviews with IoT security experts. The interview questions focus on topics such as the development process of IoT devices, engineering practices related to security, and the role and effect of standards. The specific interview questions used are detailed in Appendix A. Transcripts from each interview are recorded and qualitatively analyzed with Star's framework

to characterize the behaviors and practices of developers who maintain and build IoT systems. Interviewees were chosen based primarily based on their accessibility at the University of Virginia and their availability. The list of interviewees is shown in the table below (see Table 3).

Table 3. IoT Professionals Interview List

Name	Expertise	Affiliation
Angela Orebaugh, PhD	Cybersecurity in IoT	University of Virginia
Brad Campbell, PhD	Wireless IoT	University of Virginia
Sean Richardson, PhD	Cybersecurity in IoT	Morgan State University
Amanda Watson, PhD	Medical Embedded Devices	University of Virginia

To supplement interview responses, the second data source consists of various studies investigating flaws in IoT systems or applications of IoT in different fields like healthcare. These studies are mostly used to support interviewee's statements and provide additional evidence related to the real-world implications IoT security breaches. All collected data will be analyzed using Star's infrastructure framework, focusing on the three analytical sub-components: embodiment of standards, conventions of practice, and visibility when broken (Star, 1999).

Results

The security of IoT systems is deeply influenced by the practices and norms of their creators. The widespread use of standards, particularly in wireless communication, generally enhances security by providing well-vetted protocols for development. However, several common industry practices introduce vulnerabilities, including reliance on familiar but insecure

libraries, the use of unverified code from online forums, and pressures to prioritize speed-to-market over security. Strengthening IoT security is vital, as failures in these systems can have severe consequences, especially when they are embedded in critical infrastructure and sensitive applications. The results from this research will be organized by stepping through each of Star's three key properties of infrastructure: standards, conventions of practice, and visibility when broken. An overview and summary of findings is shown below in Table 4.

Table 4. Summary of Findings

Analytical Sub-component	Contribution to IoT Security	Key Examples
Embodiment of Standards	Overall positive	Open standards can be studied by attackers for flaws
		Security experts can specialize in making the best possible standards that everyone can use
		Open standards have thousands of eyes on them, looking for and patching security flaws
Conventions of Practice	Troubling norms	Security traded for better user experience
		Build products with base functions and no security to get to market first
		Use of familiar and comfortable software libraries, instead of what's secure
		Reliance on online coding forums and generative AI
Visibility when Broken	Severe consequences	Fatal consequences with medical devices and cars
		Leak of private and valuable medical data
		Financial punishments for negligent companies

The Good and Bad of Standards

Standards are a fundamental part of nearly all infrastructure, and IoT systems are no exception. They ensure reliable communication between devices and interoperability across different companies' products. However, despite their ubiquity in IoT, it's not immediately clear

whether they enhance security or create new vulnerabilities. By design, standards are open and well-defined, making them easy to adopt across various products, but also giving malicious actors the opportunity to study their specifications, identify weaknesses, and exploit the countless devices that rely on them. As Orebaugh notes, this "is a catch 22, probably with any standard." (Orebaugh, 2025). For example, two researchers from KU Leuven university discovered a design flaw in the current Wi-Fi specification (IEEE 802.11 standard) that can be exploited to trick end-users into connecting to a different network than the one they intend to join (Gollier & Vanhoef, 2024). They demonstrated this with a successful attack against both a standard network setup and enterprise network setup that a university or company might use. The researchers were able to find this flaw by examining the Wi-Fi standard's process where the SSID is not always authenticated. With hundreds of billions of Wi-Fi enabled devices (Pahlavan & Krishnamurthy, 2021), this example shows a danger standards in IoT can present.

However, despite the potential drawbacks stemming from the openness of standards in IoT, the expert interviewees unanimously agreed that standards are overwhelmingly beneficial for security. One positive of standards in relation to security is that of specialization. Campbell states that when creating a standard there's a "very small group that's actually writing the standard and then another small group that actually understands what security approaches exist or cryptographic approaches exist that are appropriate and how to apply them correctly." (Campbell, 2025). Following this, Campbell says how this specialization is "really good, because now it means that majority [of IoT developers] are not sort of having to try to come up with this [wireless protocols] on their own." (Campbell, 2025). To reiterate, one of the key advantages of standards in IoT is that a small group of security experts can focus on developing robust, well-

designed standards, while the larger pool of developers, who may not be security specialists, can simply implement these standards rather than designing their own, potentially weaker, protocols.

On top of specialization, standards also promote security in IoT infrastructure due to their openness. Orebaugh states that "because it [a standard] is open, lots of eyes have been on it, and lots of eyes who think security minded of all around the globe, too, who are vetting these [standards]." (Orebaugh, 2025). In further support of this, Campbell posits how when standards are open and can be viewed by everyone, he thinks "that the increased eyeballs wins out, because it's fewer people trying to find that vulnerability to hack and exploit them versus fix them." (Campbell, 2025). Additionally, Richardson says how with open standards "It's easier to find vulnerabilities as well and easier to get it fixed…because you have pretty much the best minds around the world. You have, like maybe thousands, thousands of eyes on this [standard]." (Richardson, 2025). These responses clearly demonstrate that another strength of standards is their open nature which allows thousands of domain experts to identify and address potential vulnerabilities, outpacing the smaller number of malicious attackers looking for exploits. These findings connect to Star's view of standards as a property of infrastructure that promotes seamlessness and transparency (Star, 1999). The embodiment of standards within IoT devices enables developers to smoothly implement trusted, secure, and interoperable systems without needing to reinvent or deeply understand the underlying security mechanisms.

Troubling Conventions of Practice

Many different social groups engage with IoT infrastructure, from end-users talking to Alexa to assembly line workers soldering circuit boards for smart doorbells. When considering the security of IoT systems, the examination of the conventions of practice linked to the

development and creation of these devices is crucial. One troubling norm in IoT development is that security is often treated as an afterthought rather than being built in from the start. Orebaugh, reflecting on her experience with cybersecurity in IoT over the last decade, states “Product developers are usually not thinking cyber security. Cyber security is not usually built in from the ground up. It's usually an afterthought.” (Orebaugh, 2025). Supplementing this, Campbell discusses the priority of security in the development lifecycle of IoT systems, stating, “Then you try to build the thing [IoT device] and I think you kind of forget about security…And then when the thing [IoT device] is ostensibly working, it's sort of time to kind of add those [security features] back in.” (Campbell, 2025). From the expert interviewee responses, it’s clear security is not something interwoven into the design and creation of IoT infrastructure, but why is this the case? One explanation is the difficulty in creating a product with a desirable and seamless user experience, that is also secure. Campbell speaks to this point stating, “and that's where this tension of something that's secure, but is maybe difficult to use is always at play. And if your goal is to make something people like, people can't really see security.” (Campbell, 2025). Beyond providing consumers with a seamless user experience, market forces also contribute to security being treated as an afterthought. For example, Orebaugh shared her experience with IoT devices being rushed into the market, saying “companies were just putting products to market. They really only cared about being first to market with whatever their product was a wearable, some sort of smart home device, something like that. They didn't think about security one bit.” (Orebaugh, 2025). Supporting this further, Richardson spoke to this market pressure, particularly from cheaper and knockoff IoT products from overseas, “the business model of time to market where you have to try to get that product out there as quickly as possible… But security is kind of the last thing on your mind.” (Richardson, 2025). The market incentives and interests of IoT

companies clearly drive fast-paced development, resulting in products with base functionality, but little to no security.

Another potentially harmful practice among IoT developers is relying on familiar, proven tools and libraries without properly evaluating them for security. Orebaugh referenced a vulnerability discovered in 2020 known as Ripple20 which she states “showed there were millions of IoT devices out there using a TCP/IP stack from the 90s…Known to be vulnerable to many attacks.” (Orebaugh, 2025). When answering why exactly so many developers were using such an outdated network communication library, Orebaugh pointed out an alarming norm, she said “But why?... That's what the other products are using, we'll use that… That's my go to that I've always gone to, this particular library…So they're not thinking security minded.” (Orebaugh, 2025).

This concept of prioritizing functionality over security mirrors a newer emerging practice among IoT system designers and builders: the use of online code forums like Stack Overflow and code generation tools like ChatGPT. While these tools can certainly aid in software development, they also have the potential to introduce security risks. Orebaugh speaks to how the IoT industry, particularly smaller companies, rely on online code forums, “they're going to be looking at Stack Overflow. They're going to be putting it together. They're just going to want to make it work so they can get their product out there.” (Orebaugh, 2025). Furthering the point, Campbell raises a potential issue with using online code forums and generative AI, stating that the “one size fits all that I think can happen with sort of copying from a forum or asking ChatGPT sort of encourages people [developers] to even more not think about what they should be doing for their use case”. (Campbell, 2025). Here, Campbell is illustrating that when using forums and generative AI tools, the developer loses some understanding of what exactly they’re

programming and what requirements their program might need. He posits this could lead to security issues, “I think to do a lot of the security things correctly require some investment in time thinking through what's actually needed and what kind of guarantees you are intending to provide.” (Campbell, 2025). Concerns over the use of coding forums in IoT are not unfounded. A 2023, large-scale empirical study analyzed over 11,000 IoT-related code snippets shared on online coding platforms like Stack Overflow. The study showed the snippets had 29 distinct Common Weakness Enumeration (CWE) types, revealing that nearly 40% of the vulnerable code contains weakness that could be mapped to real-world threats, such as Denial of Service (DoS) attacks and buffer overflows (Selvaraj & Uddin, 2023). While these tools can aid in more efficient development, the interviewee responses and studies show that there are risks associated with relying on them without thoroughly vetting the code for security vulnerabilities, potentially exposing IoT systems to real-world threats. These practices among developers reflect what Star describes as “conventions of practice” embedded in infrastructure which are routine and normalized behaviors that shape how systems are built (Star, 1999). These results show that in IoT development, the prioritization of speed to market and user experience, reliance on familiar but insecure libraries, and the use of generative AI and coding forums have become normalized conventions that often result in less secure IoT infrastructure.

The Visibility of Failures

IoT infrastructure is embedded within our daily lives, operating almost invisibly and seamlessly. However, when these systems fail or are breached, this illusion of transparency disappears and the consequences become tangible. On the extreme, in critical fields such as the medical or automative industry, failures can be fatal. For example, Richardson highlights the

danger of insecure IoT systems, stating, “let's say a patient's blood pressure monitor or pacemaker…If that stuff is hacked…It could be a senator with a peacemaker…or even a car that has an embedded system in it…you could take control of a car and affect the braking.” (Richardson, 2025). This underscores the severe risks of IoT security vulnerabilities and how opaque infrastructure breakages can be, endangering lives, including those of high-profile individuals.

Beyond life or death, IoT security issues can have softer, but still visible impacts on data privacy and financial costs. For example, Watson speaks to the importance of data privacy in healthcare wearables, “HIPPA compliance is a huge thing in medicine…trying to make sure we are not letting any data out through a data leak, trying to make sure that we keep people's identities safe” (Watson, 2025). Furthermore, medical data is particularly enticing for attackers due to its sensitive nature and potential for exploitation in blackmail or fraud (Koppel & Kuziemsky, 2019). This highlights the need for IoT systems to appropriately secure sensitive and valuable medical data.

Beyond just exposing people’s personal medical records, failures in IoT medical systems can also have consequences for companies. Watson, for example, explains that for a medical device company, “every piece of HIPPA data that gets out that they can prove got out because of your negligence from either not dealing with your security issues, not doing whatever, is a [very large] fine.” (Watson, 2025). Supporting this, a data breach cost analysis in healthcare showed that in 2020, the cost per single record breached was $429 and the average total data breach cost nearly $4 million (Seh et al., 2020). This evidence demonstrates how IoT infrastructure can become very visible when exposure of medical data can violate patient privacy and cost companies millions of dollars. Together, these results reinforce Star’s view that infrastructure

becomes highly visible when it breaks down (Star, 1999). The very invisibility that makes IoT devices feel seamless can quickly give way to stark visibility, manifested in casualties, privacy breaches, and financial harm, highlighting the severe consequences of system breakdowns.

The results show a positive norm in adopting and using standards in IoT, but also many troubling conventions of practices among system builders. Additionally, the ramifications of failures in IoT infrastructure emphasize the need in ensuring a secure connected world.

Discussion

There is often a tendency to view engineering as a purely objective field, insulated from the complex social factors that shape other aspects of life. Yet, through Star's infrastructure framework, this research demonstrates how deeply intertwined technology is with human influence. IoT infrastructure is not developed in a vacuum, humans design, build, and interact with these systems, embedding their own habits, desires, and constraints into the technology. Three of Star's key properties of infrastructure, embodiment of standards, links to conventions of practice, and visibility upon breakdown, make this socio-technical entanglement clear. The embodiment of standards in IoT infrastructure is beneficial for security. Developers are able to inherit rigorously tested and vetted standardized protocols, without needing to reinvent their own less secure versions. On another note, this research reveals concerning habits among developers in the IoT development space. Normalized developer practices like rushing products to market, the adoption of familiar but unvetted software libraries, and relying on online coding forums such as StackOverflow for quick solutions all result in less secure IoT infrastructure. Finally, Star's concept of infrastructure becoming visible when it breaks highlights the serious consequences of these troubling norms and practices. When IoT infrastructure fails, it becomes

apparent to those who use it, leading to financial liabilities for companies, weakened privacy for individuals, and potentially even loss of life. From this, it is clear that security in IoT is not just a technical challenge, but a socio-technical one.

This research has several limitations. First, the IoT space spans many sub-fields such as healthcare, industrial automation, home security, and more. The practices present in the medical sector, where patient privacy and strict data regulations are paramount, may differ significantly from those in consumer IoT, such as smart doorbell development. This research covers IoT infrastructure as a whole, rather than focusing on a specific sub-field or industry. While this simplifies the analysis and data collection, this may limit the applicability of the findings across different sectors. Another limitation is that three out of four interviewees, the primary data source, were University of Virginia (UVA) professors. This UVA-heavy sample may introduce bias, as perspectives on IoT security could differ significantly among professionals more involved in industry or individuals from different regions and global contexts.

There are several different directions to take this research in the future. Firstly, future research could investigate the actual quality and security of AI-generated code. Evaluating how AI-assisted development compares to traditional coding practices in terms of vulnerabilities and robustness would provide valuable insights. Another important direction for future research is exploring other social groups involved in IoT infrastructure beyond developers. Focusing research on how user, and not developer, behaviors, norms, and habits contribute to security risks could offer new perspectives on improving IoT safety. Additionally, it would be valuable to examine the intersection between an engineer's intended design and how consumers actually interact with the product. This could involve conducting an experiment with participants interacting with a mock IoT product to really understand how users approach this technology.

Understanding where mismatches occur, such as users bypassing security features for convenience, could help inform better design practices that align security with real-world usage.

Ever since taking the Wireless Internet of Things class at UVA, I have had a growing interest in building IoT devices and working with wireless protocols. Writing embedded software for these different connected devices in the IoT infrastructure is something I want to do in industry after I graduate. Thus, I feel this research will help advance my own work as an engineer, ensuring I'm aware of current troubling practices, the gravity of my work, and how I can produce high quality, but also secure products. It will also equip me with a more informed and critical perspective when evaluating how other engineers build and implement IoT systems in my future workplace.

Conclusion

Our lives are becoming increasingly connected through the vast, often invisible infrastructure of IoT, with no signs of slowing down. These devices now permeate nearly every aspect of daily life: home security, fitness, transportation, smart cities, healthcare, and more. As IoT systems take on critical roles where lives, privacy, and finances are at stake, ensuring their security becomes ever more vital. This research highlights how industry practices shape security outcomes, providing engineers and developers with greater awareness of their agency in building secure systems. By understanding how their choices, whether in tool selection, coding habits, or adherence to standards, can either strengthen or weaken security, they can take more intentional action. Additionally, this research advocates for positive industry norms, such as the use of open standards and thorough manual code reviews, ensuring that even AI-generated code is carefully

vetted for security. Moving forward, continued efforts to refine best practices and foster a security-conscious engineering culture will be crucial in safeguarding the future of IoT.

References

A. Al-Shareeda, M., Abdullah Alsadhan, A., H. Qasim, H., & Manickam, S. (2023). Long range technology for internet of things: Review, challenges, and future directions. *Bulletin of Electrical Engineering and Informatics*, *12*(6), 3758–3767. https://doi.org/10.11591/eei.v12i6.5214

Antonakakis, M., April, T., Bailey, M., Bernhard, M., Bursztein, E., Cochran, J., Durumeric, Z., Halderman, J. A., Invernizzi, L., Kallitsis, M., Kumar, D., Lever, C., Ma, Z., Mason, J., Menscher, D., Seaman, C., Sullivan, N., Thomas, K., & Zhou, Y. (2017). Understanding the mirai botnet. *Proceedings of the 26th USENIX Conference on Security Symposium*, 1093–1110.

Campbell, B. (2025, February 4). *STS 4600 IoT Security Interview* [In-person].

Gollier, H., & Vanhoef, M. (2024). SSID Confusion: Making Wi-Fi Clients Connect to the Wrong Network. *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 156–161. https://doi.org/10.1145/3643833.3656126

IEEE Standards Association. (2025). Developing Standards. *Developing Standards*. Retrieved January 29, 2025, from https://standards.ieee.org/develop/

Kanthavel, D., Sangeetha, S. K. B., & Keerthana, K. P. (2021). An empirical study of vehicle to infrastructure communications—An intense learning of smart infrastructure for safety and mobility. *International Journal of Intelligent Networks*, *2*, 77–82. https://doi.org/10.1016/j.ijin.2021.06.003

Koppel, R., & Kuziemsky, C. (2019). Healthcare Data Are Remarkably Vulnerable to Hacking: Connected Healthcare Delivery Increases the Risks. *Studies in Health Technology and Informatics*, *257*, 218–222.

Moffa, A. (2023, July 19). *What Is IoT Predictive Maintenance?* https://www.ptc.com/en/blogs/iiot/what-is-iot-predictive-maintenance

Orebaugh, A. (2025, February 25). *STS 4600 IoT Security Interview* [Online Meeting].

Pahlavan, K., & Krishnamurthy, P. (2021). Evolution and Impact of Wi-Fi Technology and Applications: A Historical Perspective. *International Journal of Wireless Information Networks*, *28*(1), 3–19. https://doi.org/10.1007/s10776-020-00501-8

Pepper Developments. (2024, February 22). *The Evolution of Cybersecurity in IoT*. DataGr8. https://datagr8.com/blogs/information/the-evolution-of-cybersecurity-in-iot-addressing-emerging-challenges

Puat, H. A. M., & Rahman, N. A. A. (2020). IoMT: A Review of Pacemaker Vulnerabilities and Security Strategy. *Journal of Physics: Conference Series*, *1712*(1), 012009. https://doi.org/10.1088/1742-6596/1712/1/012009

Radouan Ait Mouha, R. A. (2021). Internet of Things (IoT). *Journal of Data Analysis and Information Processing*, *09*(02), 77–101. https://doi.org/10.4236/jdaip.2021.92006

Richardson, S. (2025, February 5). *STS 4600 IoT Security Interview* [Online Meeting].

Rock, L. Y., Tajudeen, F. P., & Chung, Y. W. (2022). Usage and impact of the internet-of-things-based smart home technology: A quality-of-life perspective. *Universal Access in the Information Society*, 1–20. https://doi.org/10.1007/s10209-022-00937-0

Sadek, I., Rehman, S. U., Codjo, J., & Abdulrazak, B. (2019). Privacy and Security of IoT Based Healthcare Systems: Concerns, Solutions, and Recommendations. In J. Pagán, M. Mokhtari, H. Aloulou, B. Abdulrazak, & M. F. Cabrera (Eds.), *How AI Impacts Urban Living and Public Health* (pp. 3–17). Springer International Publishing. https://doi.org/10.1007/978-3-030-32785-9_1

Sasi, T., Lashkari, A. H., Lu, R., Xiong, P., & Iqbal, S. (2024). A comprehensive survey on IoT attacks: Taxonomy, detection mechanisms and challenges. *Journal of Information and Intelligence*, *2*(6), 455–513. https://doi.org/10.1016/j.jiixd.2023.12.001

Schiller, E., Aidoo, A., Fuhrer, J., Stahl, J., Ziörjen, M., & Stiller, B. (2022). Landscape of IoT security. *Computer Science Review*, *44*, 100467. https://doi.org/10.1016/j.cosrev.2022.100467

Schwartz, D. (2025). *IoT Applications in Healthcare*. Retrieved January 29, 2025, from https://www.wirelesswatchdogs.com/blog/iot-applications-in-healthcare

Seh, A. H., Zarour, M., Alenezi, M., Sarkar, A. K., Agrawal, A., Kumar, R., & Ahmad Khan, R. (2020). Healthcare Data Breaches: Insights and Implications. *Healthcare*, *8*(2), 133. https://doi.org/10.3390/healthcare8020133

Selvaraj, M., & Uddin, G. (2023). *A Large-Scale Study of IoT Security Weaknesses and Vulnerabilities in the Wild* (No. arXiv:2308.13141). arXiv. http://arxiv.org/abs/2308.13141

Sinha, S. (2024). *State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally*. https://iot-analytics.com/number-connected-iot-devices/

Star, S. L. (1999). The Ethnography of Infrastructure. *American Behavioral Scientist*, *43*(3), 377–391. https://doi.org/10.1177/00027649921955326

Vigdor, N. (2019, December 15). Somebody's Watching: Hackers Breach Ring Home Security Cameras. *The New York Times*. https://www.nytimes.com/2019/12/15/us/Hacked-ring-home-security-cameras.html

Watson, A. (2025, February 7). *STS 4600 IoT Security Interview* [In-person].

Yang, H., Kumara, S., Bukkapatnam, S. T. S., & Tsung, F. (2019). The Internet of Things for Smart Manufacturing: A Review. *IISE Transactions*, *51*(11), 1190–1216. https://doi.org/10.1080/24725854.2018.1555383

Appendices

Appendix A: Interview Questions

1. What is your background and experience with IoT systems?
2. How do developers verify and test the security of IoT systems?
3. At which level (hardware, software, user interaction) do you think IoT systems fail the most at?
4. Standards are ubiquitous in IoT, especially wireless communication standards. How do you feel these standards contribute positively and negatively to security? Why?
5. Is the use of online coding forums like StackOverflow present in the IoT space? If so, is it a security issue?
6. Are generative AI tools used in the development of IoT products? If so, what security implications do these tools have?
7. Does security feel like a priority in the IoT industry right now? How have consumer and business attitudes changed towards security in IoT over time?