Securing the Connected World: Analyzing IoT Device Vulnerabilities and Privacy Breaches

Ryan Blocker
Department of Computer Science
December 6th, 2023
rblocker@colostate.edu
Fort Collins, Colorado

***Abstract*—The rise of Internet of Things (IoT) devices, such as smart thermostats and fridges, brings along the need to understand their technical workings, especially regarding personal data privacy. In this paper I am going to go into the technical mechanisms of these devices, exploring data encryption methods, regulatory compliance, and raising consumer awareness about their ethical issues. I will examine how Internet Service Providers (ISPs) could potentially access and misuse our data, and how data collected from our interactions with these devices is used to create personalized online experiences.**

***Index Terms*—Internet of Things, Data Privacy, ISP, Personalized Algorithms, User Data, Data Encryption, Regulation Compliance, Consumer Awareness**

I. Introduction

The Internet of Things (IoT) has evolved significantly since its birth, transforming from a simple idea into a pivotal element of how modern devices communicate with one another. Advancements in wireless networking, sensor technology, and cloud computing have driven this evolution. Today, IoT encompasses various devices, from simple household gadgets like smart thermostats and refrigerators to sophisticated industrial tools and healthcare equipment.

As IoT continues integrating into various sectors, its impact on daily life has become more profound. In homes, IoT devices offer exceptional convenience for the user and efficiency, automating tasks and providing real-time monitoring. In industries, they enable more intelligent operations, and enhanced data analytics. In healthcare, IoT devices play a critical role in patient monitoring, improving the quality of care and patient outcomes.

All of these benefits that IoT offers seem almost too good to be true. However, alongside these benefits, IoT also introduces challenges, particularly concerning data privacy and security. The integrated nature of IoT devices, coupled with their ability to collect vast amounts of personal data, has raised significant privacy concerns. These concerns are not just speculation; incidents of data breaches and unauthorized surveillance have underscored the need for strong security measures in IoT ecosystems.

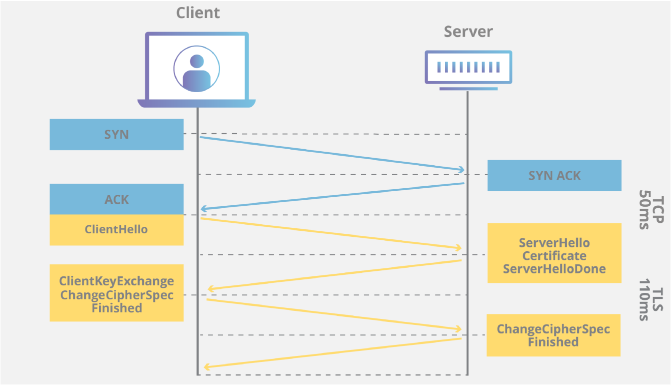
Additionally in this paper, I will touch on the nature of IoT devices and explain their technical mechanisms, the privacy implications they bring forth, and the ethical considerations they entail. Through a comprehensive examination of these aspects, the paper provides a deeper understanding of IoT's role in society and the user steps needed to safeguard themselves to ensure privacy and security.

II. Technical Mechanisms of IoT Devices

Current IoT devices operate on a complex network of interconnected technologies, each playing a crucial role in the system's functionality. At the heart of these devices are sensors which are tasked with collecting data from the environment and performing actions, based on their data. The variety of sensors in IoT devices is massive, ranging from simple temperature sensors in smart thermostats to complicated motion sensors in security systems. Data encryption in IoT is crucial for securing communication. Protocols such as SSL/TLS are commonly used to encrypt data transmitted over the network, safeguarding it from interception and tampering. Additionally, AES is also utilized and widely employed in IoT devices for data encryption, ensuring a high level of security when dealing with IoT data.

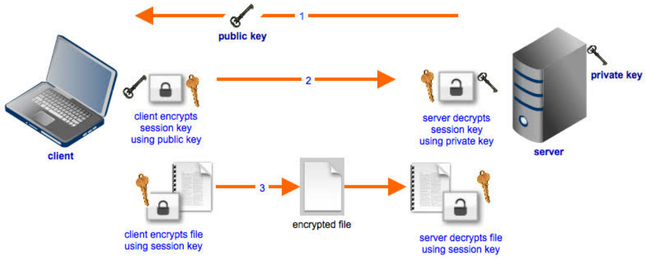
A. *Secure Socket Layer (SSL/TLS)*

Secure Socket Layer or SSL is a technology that was developed for securing an internet connection by encrypting data sent between a website and a browser (or between two servers). In terms of IoT devices, they utilize SSL/TLS which uses asymmetric encryption to authenticate whether or not the server the device is talking to is authentic and is not an attacker posing as the desired server. For example, if we had a "smart" lock that used a phone app to control whether a door on a home is locked or unlocked. That specific device would need to connect to a router (preferably one owned by the user) and then the device would use that router to connect to the client and then the client would send that information back to the user's app. So in this case SSL/TLS would be used to authenticate that the lock is connecting to the desired server and not some server posing as the client. Below is a great diagram that outlines the main phases that SSL/TLS goes through to authenticate the connection point



B. Advanced Encryption Standard Algorithm (AES)

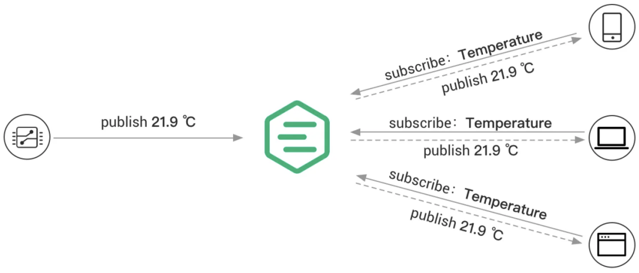
The Advanced Encryption Standard is an algorithm widely used for securing loads of devices. At its core, this algorithm is the best and most secure because it's implemented both at the hardware and software levels. Essentially AES works by taking plain text in blocks of 128 bits and then using keys of varying bit sizes (up to 256 bits) it converts that plain text into cipher text. Then it puts that data through several rounds of substitution and mixing to make it way harder for an attacker to decrypt. Then the recipient does the same steps in reverse then uses the affiliated secret key to decrypt the cipher text.



Beyond encryption, IoT devices rely on various communication protocols to interact with each other and with central servers or cloud platforms. MQTT and CoAP are specifically designed for IoT, providing efficient and reliable data transfer even in environments with limited bandwidth or high latency.

C. Message Queuing Telemetry Transport (MQTT)

MQTT or Message Queuing Telemetry Transport is a protocol designed for low-bandwidth and high-latency networks and is generally used with IoT devices since the networks are generally unreliable. This way this protocol allows for effective communication between IoT sensors/devices with the network and other IoT devices. It works on a publish/subscribe system which means unlike the standard client-server pattern which has a client that sends and receives messages MQTT splits the client into one that sends (publisher) and one that receives messages (subscriber). Then the MQTT Broker routes and distributes all of those messages. Here is a great example from [10] EMQX that uses a temperature sensor to show this system in use with the MQTT server.



D. Constrained Application Protocol (CoAP)

The Constrained Application Protocol is a web-based protocol that allows for the linking of IoT devices to the internet. However, the constrained portion of the protocol works with restricted device nodes to allow for IoT devices to be segmented and split away from other network devices in case there are a ton of devices on that network and you don't want them to interfere with them. The CoAP protocol works similarly to HTTP because it deals with GET/POST/PUT/DELETE requests. CoAP uses a request/response model to send and receive messages from IoT devices and observe network resources. CoAP also uses the UDP (User Datagram Protocol) as its transport layer to make it more usable on non-reliable or high-latency networks. This makes it incredibly useful for enterprises that have thousands of connected devices on a myriad of networks [11].

The architectural design of IoT devices often involves a layered approach, where each layer serves a distinct purpose, from physical devices and connectivity to data processing and application layers. This also adds a layer of security so that attackers have to go through multiple layers to access the IoT device data. This stratified architecture allows for enhanced adaptability in IoT systems, catering to various applications and devices.

In an ever-growing industry, standardization is so important. In IoT, this is an ongoing effort, aimed at ensuring interoperability among all devices and technologies. Standards bodies like the IEEE, IETF, and ISO are actively working on developing universal standards for IoT, which are crucial for seamless communication and integration of devices from different manufacturers.

E. What is IEEE, IETF, and ISO?

As I said above we need to set a standard for what IoT looks like in our world. That's where IEEE, IETF, and ISO come in. These are all organizations that define standard requirements and parameters for what IoT devices can look like in all of their facets. For example, IEEE (Institute of Electrical and Electronics Engineers) in their P2413 project outlined that IoT is a three-tier framework of applications, networking and data communication, and sensing. They have set that LAN should be the default communication method for IoT devices when possible however for low-power mechanisms IEEE has come up with a system called LowPAN for low-transmission IoT devices. IEEE has also worked with IETF (Internet Engineering Task Force) to make IP compatible throughout IoT devices [12].

In summary, the technical mechanisms of IoT devices are a tapestry of complex and interwoven technologies, each essential to the overall functionality and security of the IoT ecosystem. Understanding these mechanisms is key to appreciating the capabilities and addressing the vulnerabilities of IoT devices.

III. Privacy Implications and Ethical Concerns

The general adoption of IoT devices in recent years has greatly amplified privacy concerns, [13] primarily due to the extensive data collection capabilities these devices possess. IoT devices often collect sensitive personal data, including location, personal habits, and even biometric data, which can be exploited if not adequately protected. This raises considerable privacy issues, particularly regarding user consent, data ownership, and the potential for malicious user surveillance.

Ethical concerns also arise from the potential misuse of this data. For instance, without stringent privacy controls, information gathered from smart home devices could be used for targeted advertising, potentially infringing on personal privacy. The possibility of IoT devices being used for unauthorized surveillance (Mostly surrounding IoT sensors like cameras and other smart home sensors) is another pressing concern, especially given the lack of transparency in data handling and processing by some manufacturers and service providers.

Moreover, the data collected by IoT devices can be vulnerable to breaches, exposing users to risks such as identity theft and fraud. Recent incidents which I will go into in the next section have highlighted these vulnerabilities, underscoring the need for strong security measures and ethical awareness in IoT deployment.

Regulatory frameworks like the EU's General Data Protection Regulation (GDPR) have begun to address these concerns by imposing strict rules on data collection, processing, and storage. [What is GDPR? + Source] However, the global nature of IoT complicates the ability to regulate compliance, especially when data crosses international borders.

In this complex landscape, balancing technological innovation with privacy rights and ethical considerations is crucial. It involves not only following the legal requirements but also creating a culture of privacy and security within the IoT industry. This entails implementing transparent practices, and user-centric privacy approaches, and fostering an ongoing dialogue between technology developers, policymakers, and the public.

IV. Specific Case Studies and Incidents

A. Ring Home – Security Camera Breach

The Amazon-owned company Ring experienced a security breach where cyber-criminals hacked into several families' connected doorbells and home monitoring systems. The attackers used a variety of weak, recycled, and default credentials, allowing them to access live feeds and even communicate remotely using the devices' integrated microphones and speakers. To be specific an investigation done by the Electronic Frontier Foundation (EEF) discovered that Ring's ecosystem was heavily integrated with third-party systems which resulted in users' data being distributed to external companies without explicit consent. Some of the disclosed recipients of this data included Facebook, Branch, a Google-owned Panel that received the most amount of user info including user names, addresses, app settings, and emails. Ring officially stated that it uses third-party software to help improve its own and that it limits the amount of data that it receives. This breach underscores the importance of strong, unique passwords and two-factor authentication in IoT device security [5] [14].

Another source at NordVPN wrote that the Ring Cameras were being accessed through the user's poor password choices. On rare occasions, hackers access the IoT device through the home's central network and eavesdrop on the traffic coming from their IoT devices. NordVPN also reported that criminals could even trick users into letting a stranger in their home by giving the user a fake video of someone they already know [15].

B. Stuxnet Attack on Iranian Nuclear Facility

This one we have studied previously, in a class write-up. To reiterate the Stuxnet worm targeted a uranium enrichment plant in Iran. It compromised the Siemens Step 7 software, allowing the attackers to control industrial program logic controllers. To be more specific the worm that was launched into the plant exploited the use of a USB drive with the worm on it and then it exploited vulnerabilities in the Windows OS to install itself and begin searching for its target which in this case was computers running the Siemens Step7 software which the workers used to program the industrial equipment. The worm attached itself to those computers and then the worm would make sure it was in the right environment to deploy by seeing what frequency at which the centrifuges operated, to determine if it was in the right time to execute the payload. Once the worm was executed it would disrupt the centrifuges by changing the speed of the centrifuges, speeding them up, and slowing them down to cause physical damage all the while showing everything was okay to the monitors. Additionally, there was a protocol in the worm that would remove itself from the system after a specific date leaving no trace of itself to make the damage look like it occurred naturally. This attack caused significant damage to the facility's infrastructure, underscoring the potential national security implications of IoT vulnerabilities [6] [25] [26] [27] [28].

C. Nortek Security Control – eMerge E3 Unauthorized Access

With the recent shift to businesses incorporating "smart" sensors into their security apparatus. One of the companies that supplies these devices is Nortek. They market to businesses with a wide variety of IoT devices ranging from cameras to fingerprint readers. In a study by a cyber-security firm Applied Risk, they discovered several vulnerabilities in Nortek's eMerge E3 products that would allow hackers to take full control of the IoT device network in the building. For example, after gaining access the criminal would then be allowed to open/lock doors, install malware, and launch DoS attacks all while not being detected by the security measure Nortek had set in place. In the report by Applied Risk, they outlined several breach points for attackers in the Nortek hardware and software. There were quite a few security holes but here are the major few that were exploited by Applied Risk in their testing:

1) **Unauthorized Access** - Default passwords could be obtained easily from product documentation allowing access to devices that were just being set up
2) **Command Injection** - Another issue arose in the software where Nortek's application failed to terminate special elements in externally influenced input, which not eradicated could modify the intended OS command, leading to the execution of dangerous commands on the operating system.
3) **Privilege Escalation** - The application had a flaw where a low-privileged user could change a parameter in the code (Ex. like 'UserRole') in a POST request to a value that represents higher privileges and set it to '1' to escalate to Super User privileges.

I believe this incident highlights the critical need for rigorous security testing and vulnerability patching in IoT devices especially because it came from such a respected security firm [5] [16].

D. St Jude Medical – Pacemaker IoT Vulnerabilities

Now not all devices are smart lights and security cameras. Even devices that go inside our very bodies are getting the IoT treatment. For example, we have developed pacemakers for the elderly alongside their life-saving function of keeping the patient alive. Also, provide their doctor with useful data in real-time to act like an early warning system to see if there is anything wrong. In a study done by the FDA, they confirmed that they have discovered vulnerabilities in pacemakers and that they have the potential to be breached. To be more specific the FDA conducted their study using the St Jude Medical's implantable cardiac devices and found them to have holes in their security that could allow hackers to manipulate the devices remotely.

This poses a severe risk to patients' health! Based on the information that was disclosed to the public I found that the major vulnerability hackers could use to gain access to the pacemaker through the transmitter (uses RF wireless telemetry). The hacker after gaining access to the transmitter could then deplete the battery of the pacemaker, eavesdrop on real-time heart data, and collect it for their use. These vulnerabilities in IoT demonstrate the critical importance of encrypting data and conducting regular vulnerability assessments, especially when someone's life depends on it [5] [17].

E. The Mirai Botnet

The Mirai Botnet was a piece of software that was discovered in 2016. It was created by three men Paras Jha, Josiah White, and Dalton Norman for financial gain to take down rival Minecraft Servers to drive up their own Minecraft server traffic. The botnet was designed to infiltrate IoT devices through their default usernames and passwords and then once it gained access it would use the IoT devices to launch large-scale DDoS attacks. After the release of this botnet, it grew so large and powerful that it ended up taking down some major websites such as Netflix, CNN, and Twitter before the men were eventually caught. All three men pleaded guilty and were sentenced to prison however as part of their plea agreement the FBI recruited them to leverage their expertise to help stop future cyber attacks on the US. [6] [18] [19].

Another IoT-related attack that was attributed to the Mirai botnet that occurred in October of 2016 disabled the "smart" enabled heating systems in two buildings in Lappeenranta, Finland. The severe DDoS attack that Mirai inflicted on their system caused their network to go into a constant state of reboot so the heating was never active. This occurred over and over for about a week at a time when the temperature outside was well below freezing! From a design perspective, I would have never thought of including any security against DDoS attacks for something as simple as a heating/cooling system. This is but one example of how IoT devices on their own are so vulnerable to attack. [20] [21]

F. The Jeep Hack

In 2015, a security test on a Jeep SUV brought significant attention to the dangers of IoT inside vehicles. Researchers Charlie Miller and Chris Valasek were able to remotely take control of a Jeep SUV by exploiting vulnerabilities in the vehicle's connectivity systems. They achieved this connection by using the Sprint cellular network, which the Jeep's head units were connected to, even without active wireless service subscriptions from the vehicle owners!

The researchers used a femtocell which is a compact cellular base station, to infiltrate the Sprint network and conduct a mass scan of IP addresses. This enabled them to identify Chrysler vehicles with vulnerable head units. Interestingly, they found it easier to hack all Jeeps than a specific one, but they did end up figuring out they could hack a specific Jeep by using its onboard GPS tracker

The most crucial part of the approach they took was getting access to the CAN (Controller Area Network) bus. That is the internal network of the Jeep that connects to critical parts of the car like the engine, transmission, and sensors. The hackers gained initial access through the multimedia system, which is not directly connected to the CAN system they were able to communicate to the V850 controller, which was connected to the CAN bus. By reprogramming the V850 controller with malicious firmware, they were able to bypass the security measures and send commands through the CAN bus. This allowed them to control crucial aspects of the vehicle, such as the steering wheel, engine, transmission, and braking system, all remotely.

The consequences of this hack were significant, leading to the recalling of 1.4 million vehicles to address this defect. This incident highlights the growing importance of cyber-security in the automotive industry, especially as vehicles become increasingly connected and reliant on the internet [6] [22] [23] [24].

V. Conclusion and Potential Solutions

In conclusion, integrating IoT devices into our daily lives brings both convenience and efficiency, opportunities, and significant challenges, particularly in terms of privacy and security. The discussed incidents discussed above highlight the urgent need for comprehensive security measures in the IoT landscape.

Potential solutions include robust encryption and security protocols, regular software updates and patch management, user education and awareness, company compliance, and device regulatory compliance and standardization, and exploring advanced security technologies like blockchain and AI.

As IoT continues to evolve, collaboration among manufacturers, policymakers, and users is crucial for addressing these challenges, ensuring the benefits of IoT are realized without compromising privacy and security.

References

[1] CPO Magazine, ”Smart Devices Leaking Data To Tech Giants Raises New IoT Privacy Issues,” 2020.

[2] R. Jain and M. Gyanchandani, ”Internet of Things (IoT) Frameworks: A Comparative Study,” *Journal of King Saud University - Computer and Information Sciences*, 2020.

[3] A. Soltani and S. Canty, ”ISP Privacy: An Analysis of Broadband Provider Privacy Practices,” *Privacy and Security Research Paper Series*, 2021.

[4] T. Robertson and R. Vatrapu, ”Harnessing Personal Data for Building Personalized Algorithms: A Privacy Calculus Perspective,” *International Journal of Information Management*, 2021.

[5] Conosco, ”IoT Security Breaches: 4 Real-World Examples,” https://conosco.com/industry-insights/blog/iot-security-breaches-4-real-world-examples, 2021.

[6] CM Alliance, ”IoT Security: 5 cyber-attacks caused by IoT security vulnerabilities,” https://www.cm-alliance.com/cybersecurity-blog/iot-security-5-cyber-attacks-caused-by-iot-security-vulnerabilities#:~:text=IoT%20devices%20are%20particularly%20vulnerable,and%20effort%20to%20recover%20from., Accessed 2023.

[7] Finite State, ”A Look Back at the Top 12 IoT Exploits of 2021 (Part 1),” https://finitestate.io/blog/top-12-iot-exploits-of-2021-p1, 2022.

[8] ”AES 256 Encryption,” *Kiteworks Risk Compliance Glossary*, [Online]. Available: https://www.kiteworks.com/risk-compliance-glossary/aes-256-encryption/. [Accessed Dec. 6, 2023].

[9] Cloudflare, ”What is SSL?,” *Cloudflare Learning SSL*, [Online]. Available: https://www.cloudflare.com/learning/ssl/what-is-ssl/. [Accessed Dec. 6, 2023].

[10] EMQX, ”The Easiest Guide to Getting Started with MQTT,” *EMQX Blog*, [Online]. Available: https://www.emqx.com/en/blog/the-easiest-guide-to-getting-started-with-mqtt. [Accessed Dec. 6, 2023].

[11] Coding Ninjas, ”CoAP Protocol,” *Coding Ninjas Studio Library*, [Online]. Available: https://www.codingninjas.com/studio/library/coap-protocol. [Accessed Dec. 6, 2023].

[12] ”IoT Standardization: The Road Ahead,” *IntechOpen*, [Online]. Available: https://www.intechopen.com/chapters/60331. [Accessed Dec. 6, 2023].

[13] ”A Review of Security and Privacy Concerns in the Internet of Things (IoT),” *Hindawi Journal of Sensors*, 2022. [Online]. Available: https://www.hindawi.com/journals/js/2022/5724168/. [Accessed Dec. 6, 2023].

[14] ”Technology,” BBC News, 2020. [Online]. Available: https://www.bbc.com/news/technology-51281476. [Accessed Dec. 6, 2023].

[15] P. Ilevičius, ”Ring hacked: How to protect your Ring smart device,” NordVPN Blog, Mar. 2023. [Online]. Available: https://nordvpn.com/blog/ring-doorbell-hack/. [Accessed Dec. 8, 2023].

[16] G. Krstic, ”Nortek Linear eMerge E3-Series 1.00-06 Multiple Vulnerabilities,” Applied Risk, 2019. [Online]. Available: https://applied-risk.com/assets/uploads/whitepapers/Nortek-Linear-E3-Advisory-2019.pdf. [Accessed: Accessed Dec. 8, 2023].

[17] S. Larson, ”FDA confirms that St. Jude's cardiac devices can be hacked,” CNN Money, Jan. 9, 2017. [Online]. Available: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack/. [Accessed: Accessed Dec. 8, 2023].

[18] J. Cox, ”Feds Bust Designers of the Botnet That Crippled the Internet,” The Daily Beast, Dec. 13, 2017. [Online]. Available: https://www.thedailybeast.com/feds-bust-designers-of-the-botnet-that-crippled-the-internet. [Accessed: Accessed Dec. 8, 2023].

[19] ”Botnet: No jail time for Mirai-creators,” G DATA CyberDefense AG, Sep. 24, 2018. [Online]. Available: https://www.gdatasoftware.com/blog/2018/09/31124-botnet-no-jailtime-for-mirai-creators. [Accessed: Accessed Dec. 8, 2023].

[20] ”DDoS Attack Takes Down Central Heating System Amidst Winter In Finland,” The Hacker News, Nov. 6, 2016. [Online]. Available: https://thehackernews.com/2016/11/heating-system-hacked.html. [Accessed: Dec. 8, 2023].

[21] ”DDoS attack halts heating in Finland amidst winter,” Metropolitan.fi, Nov. 9, 2016. [Online]. Available: https://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter. [Accessed: Dec. 8, 2023].

[22] ”Black Hat USA 2015: The full story of how that Jeep was hacked,” Kaspersky official blog, 2015. [Online]. Available: https://www.kaspersky.com/blog/blackhat-jeep-cherokee-hack-explained/9493/. [Accessed: Dec. 8, 2023].

[23] ”The 2015 Jeep Hack: What Happened?,” Fractional CISO, 2015. [Online]. Available: https://fractionalciso.com/jeep-hack/. [Accessed: Dec. 8, 2023].

[24] ”Vehicle Cybersecurity: The Jeep Hack and Beyond,” Carnegie Mellon University Software Engineering Institute, 2015. [Online]. Available: https://insights.sei.cmu.edu/sei_blog/2015/10/vehicle-cybersecurity-the-jeep-hack-and-beyond.html. [Accessed: Dec. 8, 2023].

[25] ”Stuxnet: The world's first cyber weapon,” FSI, Stanford University. [Online]. Available: https://cisac.fsi.stanford.edu/content/stuxnet-worlds-first-cyber-weapon. [Accessed: Dec. 8, 2023].

[26] B. Vigliarolo, ”Stuxnet: The smart person's guide,” TechRepublic, Aug. 15, 2017. [Online]. Available: https://www.techrepublic.com/article/stuxnet-the-smart-persons-guide/. [Accessed: Dec. 8, 2023].

[27] ”Richard Clarke on Who Was Behind the Stuxnet Attack,” Smithsonian Magazine. [Online]. Available: https://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-125528/. [Accessed: Dec. 8, 2023].

[28] ”Stuxnet explained: What it is, who created it and how it works,” Kaspersky. [Online]. Available: https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet. [Accessed: Dec. 8, 2023].