IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 25, Issue 5, Ser. 2 (Sept. – October. 2023), PP 25-28
www.iosrjournals.org

Spectrum Of Cybersecurity And Ethics In The Contemporary World

Pulkit Gupta

Date of Submission: 27-09-2023 Date of Acceptance: 07-10-2023

I. Introduction -

Cybersecurity and ethics are two seemingly different fields, but have found themselves interwoven due to the daily increase in reliance on digital technology. This paper aims to delve into the complexity of these interrelations and discuss their implications in the modern world.

Cybersecurity protects internet-connected systems, such as hardware, software, data etc., from cyber threats. It involves implementing measures to prevent unauthorized access, use, modification, disruption, disclosure, or destruction of information. Meanwhile, ethics is a branch of philosophy that talks about questions regarding morality, virtue, and concepts like good and evil and right and wrong. When combined with cybersecurity, ethics refers to the moral principles and behaviours concerning the use and impact of cybersecurity technologies. These principles guide how one should protect information systems, respect privacy, and respond to cyber threats. However, as we explore the depth of this research paper, the relationship between cybersecurity and ethics is full of conflicts, ambiguity, and challenges. These challenges arise from the need to balance the protection of information systems with the preservation of individual privacy using certain ethical guidelines that fail to fully capture the complexity of the digital landscape. This gets even more complicated due to the emergence of new technologies, which are yet to be covered by these guidelines.

Through this paper, we aim to bring these challenges to light, discuss potential ways to address them and highlight the urgent need for evolved thinking in cybersecurity ethics. As we navigate through a digital world defined by its innovative advancements and the novel threats that accompany them, this research is not just well-timed but a vital disclosure in shaping a safer and fairer cyber world.

II. The Bug in the Matrix

One of the earliest instances of a cyberattack, the Morris worm, became a precursor to modern distributed denial of service (DDoS) attacks. Created by Robert Tappan Morris in 1988, the worm was initially intended to measure the size of the internet but inadvertently caused widespread disruption due to its rapid and uncontrollable spread.

The Morris worm, a self-propagating programme, significantly impacted the early internet, infecting around 10% of all computers at that time. Despite the creator, Morris, not intending to damage the internet, the worm's effects led to their prosecution under the Computer Fraud and Abuse Act. The aftermath of the Morris worm paved the way for ongoing vulnerabilities, particularly with the advent of the "Internet of Things," involving an increased number of connected devices.

This marked the beginning of the rising frequency and severity of DDoS attacks, emphasizing the proliferation of internet-connected devices and the subsequent surge in security vulnerabilities.

A multifaceted approach encompassing technological solutions, legislation, and proactive cybersecurity measures are some of the measures that are generally taken to fight cyber threats. However, the global and complex nature of cyber threats poses challenges for effective regulation and law enforcement. One of the solutions, among others, was to allow attack victims to engage in active defense measures and mandate enhanced security for internet-connected devices.

It also became really important to adopt cybersecurity as a core aspect of corporate social responsibility. Hence, the establishment of cybersecurity response teams and the potential creation of a national cybersecurity safety board became positive steps towards addressing cyber threats. Various guidelines and recommendations came up that highlighted the importance of digital signatures and end-to-end encryption (more about this later).

Eventually, there began an era to establish critical governments, organizations, and individuals to prioritise and implement robust cybersecurity measures to protect against future cyber threats.

III. Moral Values and Technology

Ethics in technology encompass the integration of moral considerations at every stage, from the design and development of systems with fairness and inclusivity to safeguarding privacy and data, ensuring robust security measures, minimizing environmental impact, promoting equitable access, governing autonomous systems responsibly, understanding social and behavioral implications, establishing legal frameworks, and fostering awareness and education for responsible technology use. It's a comprehensive approach to ensuring that technological advancements are aligned with societal values, respect for human rights, and a positive contribution to the collective well-being of humanity.

Due to the tension between privacy and security, the ethics of cybersecurity have garnered significant attention in the swiftly evolving digital landscape. Each approach to cybersecurity ethics is filled with hurdles and potential conflict points, presenting several ethical problems. In the constant struggle against cyber threats, security measures frequently have unintended consequences, the most common being the violation of the privacy rights of individuals.

Security protocols, such as extensive surveillance, data mining, and monitoring mechanisms, are two-sided. They may strengthen the fortress against cyber adversaries, but they may also violate privacy norms, which raises serious ethical concerns.

Encryption is essential for privacy protection because it prevents unauthorized access to sensitive information. They turn sensitive data into indecipherable, meaningless text that can be converted into something meaningful using the correct decryption key. It is the very same concept that WhatsApp uses. Encryption keeps our private conversations, financial transactions, and sensitive data safe from hackers.

But this very encryption, the assurance of privacy, simultaneously becomes a blockade for law enforcement and security agencies. When the data is encrypted, cybercriminals can use this encryption to shield their activities, making it harder for authorities to track down illicit activities, investigate cyber crimes, or prevent potential threats. Even with legitimate reasons, these agencies cannot access the information they need.

This conflict generates a plethora of moral dilemmas. Respect for individual privacy, an extension of personal autonomy and confidentiality, is a crucial ethical consideration. In terms of privacy ethics, unauthorized access to confidential information, whether by malicious hackers or by well-meaning security agencies, raises red flags. The possibility of misusing or mishandling personal information exacerbates these concerns. But on the opposite side of the argument, security advocates contend that, for the greater good, it may necessitate certain invasions of personal privacy. When we consider factors such as informed consent, the sensitivity of the data in question, and the specific contexts in which privacy-security conflicts arise, the ethical tug-of-war between these opposing views intensifies.

Building on the consequent ethical tug of war, it becomes evident that grey areas, conflicts, and the ambiguity of the ethical guidelines significantly complicate cybersecurity's ethical landscape. Conflicting ethical principles, vague definitions, and incomplete guidelines lead to these challenges. For example, let us consider the ethical principle of non-maleficence, which specifies ‘do not harm’. It gets murky when counter-hacking measures come into play. Is it ethical for a breached organization to hack back the attacker, to recover stolen information to prevent damage? On one side, such actions may seem necessary as an immediate response to protect one’s assets. However, on the other side, the counter argument asserts that two wrongs do not make one right. Hence, such actions might inadvertently inflict harm on innocent third parties if the attacker was using a compromised system.

IV. Case Study: Apple vs. FBI

A terrorist attack occurred in San Bernardino, California, in December 2015, which killed almost 22 people and injured several more. An iPhone 5C was recovered from one of those deceased attackers by the FBI. That phone belonged to Syed Rizwan Farook, and the phone was expected to contain crucial information about the attack and any potential co-conspirators.

The FBI asked for Apple’s technical help in unlocking the iPhone, specifically asking for help in bypassing the device’s security features. The iPhone was protected by a passcode, and after multiple incorrect attempts to unlock it, the device had a factory data reset feature that would wipe all its data. The FBI wanted Apple to create a custom version of its operating system that would allow them to overpower the auto-erase feature and enable them to perform a brute-force attack to guess the passcode.

Apple publicly refused to comply with the FBI's request. The company argued that creating a "backdoor" or a custom operating system with weakened security measures would set a dangerous example in the market, lowering their company’s security promises. They believed that such a tool could be misused in the future and would compromise the privacy and security of all iPhone users. Apple maintained that it was committed to protecting user data and that helping the FBI in this case would undermine the principles of encryption and user privacy.

The case escalated into a legal battle. The FBI obtained a court order under the All-Writs Act, compelling Apple to assist in unlocking the iPhone. Apple challenged the court order, arguing that it exceeded the government's authority, posed a significant threat to user privacy and digital security, and would be against its ethics. This was the time when Apple widely marketed the security features of the iPhone. The case received support from various tech companies, civil liberty organizations, and privacy advocates who were concerned about the broader implications of the government's request and the threat to user information and loss of customer trust.

Before the court could issue a final ruling, the FBI announced in March 2016 that they had successfully unlocked the iPhone without Apple's assistance. They had allegedly received help from a third-party contractor who had developed a method to bypass the security features.

The FBI vs. Apple case highlighted the tension between law enforcement's need for access to digital evidence in criminal investigations and the importance of preserving strong encryption and individual privacy rights. It raised critical questions about the government's authority to compel tech companies to create backdoors and weaken security measures. The case also reignited discussions about the balance between security and privacy in the digital age.

While the case was resolved without a definitive legal ruling, it underscored the ongoing debates surrounding encryption, government access to digital data, and the role of tech companies in protecting user privacy. It remains a pivotal moment in the ongoing conversation about digital security and individual rights.

Therefore, while indispensable, the ethical guidelines in cybersecurity are often riddled with conflicts, gray areas, and a degree of incompleteness. This inherent ambiguity underscores the necessity of continual dialogue, regular updating of guidelines, and the cultivation of ethical sensitivity among cybersecurity professionals.

V. Guidelines and Recommendations:

Business ethics, and the associated conflicts that arise specifically because of competing interests in security and making money, do not fit easily within the Menlo framework. Security should not be ignored in the interests of channeling funds into profit-making activities, and a minor degree of prescience will suggest that good security will strengthen a company’s reputation and client trust in that organization. Hence, some privacy-preserving technologies come into play. The new General Data Protection Regulation (GDPR) states that “the collection and processing of personal data for cybersecurity reasons is legitimate; however, it is still subject to the rest of the requirements of the regulation.”

VI. Digital Signatures:

Digital signatures were created to guarantee the authenticity and integrity of electronic communications and to avoid their repudiation. It is used to provide authentication for individuals.

An alternative to digital signatures, when both the sender and receiver possess shared information, is the use of message authentication codes (MACs). These codes rely on cryptographic hash functions with a shared secret key to validate and ensure the integrity of the transmitted message. Typically employed in symmetric encryption-based communications, MACs offer a method to verify that the message has not been altered during transmission, reinforcing data security and trust between the communicating parties.

VII. End-to-End Encryption

If you have ever used ‘WhatsApp’, a popular messaging feature, you have sometimes seen ‘End-to-End Encrypted’ written there. What does that mean, though?

End-to-end encryption represents a secure communication method in which messages shared between two or more parties are shielded from prying eyes, all without relying on a centralized server's intervention. Unlike traditional message exchange protocols, where encryption occurs mainly during transit to or from a central server, in end-to-end encryption, the central server merely serves as a conduit for encrypted content, unable to decipher the message's contents.

This security mechanism is typically facilitated by equipping all participants with a key pair generated from a public-key encryption system. The central server, apart from facilitating message exchange, operates as a repository of public keys, allowing users to access the public keys of intended recipients. Once a user acquires another user's public key, it can be employed to encrypt messages, rendering them decipherable solely by the owner of the corresponding private key.

For increased efficiency, users can opt for an alternative approach—exchanging random session keys designed for symmetric encryption. These session keys are secured by encrypting them with public-private key pairs and then used to encrypt messages employing a symmetric encryption scheme, ensuring confidentiality during communication sessions.

Cybersecurity is one of the most complimentary things that comes with the ‘Internet of Things’. Its threats are rapidly evolving and difficult to get completely rid of. It is a $6 trillion industry that is growing by over 15% each year. Hence, it is critical to learn to guard against them. Ethical cybersecurity strategies should be implemented to prevent cyberattacks from inflicting harm against quicker and more sophisticated attacks.

Works Cited –

[1]. Christen, Markus, Et Al. “The Ethics Of Cybersecurity.” Springer Ebooks, 2020, Https://Doi.Org/10.1007/978-3-030-29053-5.

[2]. Aliyev, Samir. “A Holistic Approach To Ethical Issues In Cyber Security.” Swiss Cyber Institute, Feb. 2023, Swisscyberinstitute.Com/Blog/A-Holistic-Approach-To-Ethical-Issues-In-Cyber-Security/#Transparency_And_Disclosure.

[3]. Townsend, Alicia. “Cybersecurity Lessons Learned From The Matrix.” Onelogin Identity Management Blog, Feb. 2022, Www.Onelogin.Com/Blog/Cybersecurity-Lessons-From-Matrix.

[4]. Shackelford, Scott. “30 Years Ago, The World’s First Cyberattack Set The Stage For Modern Cybersecurity Challenges.” The Conversation, Theconversation.Com/30-Years-Ago-The-Worlds-First-Cyberattack-Set-The-Stage-For-Modern-Cybersecurity-Challenges-105449.

[5]. “Ethical Issues In Cybersecurity: Comptia’s Future Of Tech.” Comptia’s Future Of Tech, Www.Futureoftech.Org/Cybersecurity/4-Ethical-Issues-In-Cybersecurity.

[6]. Tedx Talks. “The Five Laws Of Cybersecurity | Nick Espinosa | Tedxfonddulac.” Youtube, 7 Sept. 2018, Www.Youtube.Com/Watch?V=_Nvq7f26-Uo.

[7]. ---. “Why Cybersecurity Is Important! | Romeo Farinacci | Tedxgrandcanyonuniversity.” Youtube, 10 Apr. 2017, Www.Youtube.Com/Watch?V=Jijslca8q5g.