Beyond firewalls: The future of cybersecurity research

Sina Ahmadi

Computer Science and Engineering Research 2 (1): 1-2

Content available at Genesis Publishing Consortium Limited

Computer Science and Engineering Research

Journal homepage: www.genesispcl.com/journals/cser

Editorial

Beyond firewalls: The future of cybersecurity research

Sina Ahmadi*

The National Coalition of Independent Scholars (NCIS), Canada

Article info

Article history
Received: 03 January 2025
Revised: 07 January 2025
Accepted: 08 January 2025
Published: 10 January 2025

Keywords
Cybersecurity
Machine learning
Artificial intelligence
Social engineering
Threat intelligence

Abstract

The digital revolution has changed our world forever and it brought technology into our lives in every way. Be it for cross-border commerce, critical infrastructures, communications, or the very bonding of us as societies, all part of the paradigm today seem to take a more "inter-connected" flavor. While this brought ubiquitous connectivity into our lives, it also opened Pandora's Box, unleashing relentless waves of cyber threats that endanger individuals, organizations and even national security. But as with everything, cybersecurity practitioners must understand the advanced threats as they increase in their level of sophistication and scale, making high-quality and innovative cybersecurity research imperative. The intention of this article is to be forward looking in discussing the major threats facing the industry and presenting fruitful lines of inquiry to navigate this complex and dynamic landscape.

The digital revolution has changed our world forever and it brought technology into our lives in every way. Be it for cross-border commerce, critical infrastructures, communications, or the very bonding of us as societies, all part of the paradigm today seem to take a more "inter-connected" flavor. While this brought ubiquitous connectivity into our lives, it also opened Pandora's Box, unleashing relentless waves of cyber threats that endanger individuals, organizations and even national security (Kettani and Wainwright, 2019). But as with everything, cybersecurity practitioners must understand the advanced threats as they increase in their level of sophistication and scale, making high-quality and innovative cybersecurity research imperative. The intention of this article is to be forward looking in discussing the major threats facing the industry and presenting fruitful lines of inquiry to navigate this complex and dynamic landscape (Xu, 2020).

One of greatest cybersecurity concerns is the increasing sophistication of targeted attacks. Advanced Persistent Threats (APTs), which are typically carried out by well-funded entities, such as nation-state-sponsored groups and organized cybercrime networks, utilize a variety of stealthy and advanced techniques, ranging from zero-day exploits and polymorphic malware to complex social engineering operations and supply chain compromises, to penetrate systems and steal valuable data, intellectual property, and sensitive data (Alshamrani *et al.*, 2019). These attacks are targeted, persistent, and can be hidden for many months. A reactive response to known threats using signature-based detection is no longer sufficient. Further research needs to be conducted that addresses proactive defense mechanisms, including advanced anomaly, detection through behavioral analysis of user activity on the network enhanced threat intelligence that enable near real-time inter-organization communication, and robust attribution techniques to identify culprits and maintain accountability (Sen and Mehtab, 2020).

Another potential area for additional study as they relate to deception technologies, is honeypot-like deception and decoy systems, which can provide substantial intelligence during and after an APT attack, through detection and analysis of the attack. Other subtopics in this space likely to be of interest are researching and building AI-based threat hunting solutions to search proactively to identify indicators of compromise and what it is happening across the landscape (Campbell *et al.*, 2015). The uncontrolled growth of IoT devices has exponentially increased attack surfaces and provided an ecosystem full of different network-connected devices with poor inbuilt security capabilities. A large number of these, including smart home appliances, wearable devices, industrial control systems, and connected vehicles, often rely on weak security mechanisms and come with default passwords that never change, making them easy prey for attacks (Vhaduri and Poellabauer, 2018). Security research on IoT devices is extremely demanding due to the high heterogeneity and resource constraints of IoT devices. Key research directions in this area can involve lightweight cryptographic solutions which work seamlessly on resource-constrained devices, secure firmware update mechanisms that enable fast mitigation of vulnerabilities, and strong authentication mechanisms to disallow unauthorized access and device hijacking. Furthermore, large-scale IoT deployments could benefit from exploring decentralized security architectures, such as using blockchain for device identity management and operational data sharing. Ensuring the trustworthiness of IoT devices is crucial, and device attestation and integrity checking are key research areas in achieving this goal.

The human element continues to be one of the most crucial vulnerabilities in the cybersecurity chain. Even with significant advancements in human and technical security controls, social engineering attacks, which leverage the psychology of people to manipulate them into revealing sensitive information or even taking high-risk decisions (Luo *et al.*, 2023), remain one of the most

Corresponding authors
Email address: sina0@acm.org (Sina Ahmadi)

doi: https://doi.org/10.69517/cser.2025.02.01.0001

powerful types of attacks. This has also laid bare the dire need for research into the intersection between Human-Computer Interaction (HCI) and cybersecurity; to know exactly how users interact with technology, to know which cognitive biases and heuristics attackers utilize, and to design effective security awareness training and intuitive security tools that let users help themselves. Research should also be carried out on the use of behavioral biometric, and other authentication methods that are less susceptible to social engineering attacks, including continuous authentication and implicit authentication based on user behavior.

When it comes to cybersecurity, the rapid growth of Artificial Intelligence (AI) and Machine Learning (ML) is a double-edged sword. These technologies employ powerful threat detection techniques that use intricate patterns for anomaly detection while enabling task automation such as vulnerability scanning, incident response and enhancing overall security operations efficiency (Kumar *et al.*, 2017). Conversely, these developments present new opportunities for attackers as well. For instance, adversaries leverage AI/ML to develop more sophisticated malwares with the ability to effectively bypass conventional detection systems, come up with personally tailored phishing campaigns, and even simulate instances that can deceive AI based security systems. Future research still needs to focus on developing robust explainable AI/ML-based security solutions that are resilient against adversarial attacks and can adapt to ever-changing risk environment while providing insights into their decision-making mechanisms to human operators.

Moreover, the research of ethical issues associated with AI adoption in cybersecurity, for example bias, fairness, potential harm and accountability is necessary. Safeguarding users' privacy is extremely important in the information age. In the current inter-connected world where personal information is constantly gathered and disseminated across numerous platforms and services, the possibility of privacy infringements, data abuse threats as well as surveillance keep rising geometrically. Research should be carried out on Privacy Enhancing Technologies (PETs) which include differential privacy, homomorphic encryption and secure multi-party computation because they can safeguard private information while allowing data to be analyzed and shared (Schneider, 2020). It is also important to study data governance frameworks, privacy regulations and user-centered privacy controls to create a strong sustainable privacy ecosystem.

Lastly, another important area of research is machine learning algorithms that respect privacy. To solve these complications, the way must be paved through inter-disciplinary collaboration. The involvement of different experts from various fields such as computer science, engineering, psychology, law, social sciences and economics is critical for cybersecurity researchers. These groups should have open communication so that they are able to share data and best practices and work together on research projects in a bid to foster creative solutions at a faster rate than would otherwise be the case. This will enable us achieve increased security in our connected world and help maintain consumer rights and freedoms in this digital age.

Acknowledgments

Not applicable.

Ethical approval statement

None to declare.

Data availability

Not applicable.

Informed consent statement

Not applicable.

Conflict of interest

The author declare no competing interests.

Authors' contribution

Sina Ahmadi: Conceptualization, formal analysis, writing-original draft preparation, review and editing. The author has read and approved the final version of the published editorial.

References

Alshamrani A, Myneni S, Chowdhary A and Huang D, 2019. A survey on advanced persistent threats: Techniques, solutions, challenges, and research opportunities. IEEE Communications Surveys & Tutorials, 21(2): 1851. https://doi.org/10.1109/comst.2019.2891891

Campbell RM, Padayachee K and Masombuka T, 2015. A survey of honeypot research: Trends and opportunities. Proceedings of the ICITST, 208. https://doi.org/10.1109/icitst.2015.7412090

Kettani H and Wainwright P, 2019. On the top threats to cyber systems. INFOCT Proceedings, 175. https://doi.org/10.1109/infoct.2019.8711324

Kumar RSS, Wicker A and Swann M, 2017. Practical machine learning for cloud intrusion detection: Challenges and the way forward. arXiv (Cornell University). https://doi.org/10.48550/arxiv.1709.07095

Luo X, Brody R, Seazzu A and Burd S, 2023. Social engineering: The neglected human factor for information security management. IGI Global. https://www.igi-global.com/gateway/article/55064

Schneider T, 2020. Engineering privacy-preserving machine learning protocols. Proceedings of ACM CCS, 3. https://doi.org/10.1145/3411501.3418607

Sen J and Mehtab S, 2020. Machine learning applications in misuse and anomaly detection. IntechOpen eBooks. https://doi.org/10.5772/intechopen.92653

Vhaduri S and Poellabauer C, 2018. Biometric-based wearable user authentication during sedentary and non-sedentary periods. arXiv (Cornell University). https://doi.org/10.48550/arXiv.1811

Xu S, 2020. The cybersecurity dynamics way of thinking and landscape. Proceedings of ACM CCS, 69-80. https://doi.org/10.1145/3411496.3421225