Summary Report on Perseus Mirrored Shield - Enhancing System Robustness and Privacy Through Insights from Cyber Threat Intelligence

Advait Hirlekar

***Abstract*—This report explores strategies to enhance system robustness and privacy using Cyber Threat Intelligence (CTI). Drawing from the Perseus myth, it emphasizes proactive defenses against evolving cyber threats, such as malware and LLM-based attacks. Key contributions include automating vulnerability assessments, strengthening software supply chains, and raising cybersecurity awareness. By integrating tools like DiffCVSS and privacy wrappers, the study presents innovative solutions for mitigating risks. This report was inspired by Professor Xiaojing Lao's talk, whose passion for cybersecurity research deeply influenced this exploration of critical issues.**

I. Introduction

CYBERCRIME has emerged as a significant challenge in the digital age, jeopardizing the security of individuals and organizations alike. Over the past five years, an estimated 3.79 million complaints have been reported, with a staggering 33.7 billion dollars spent to mitigate its impacts. These crimes exploit vulnerabilities in systems and platforms, manifesting in various forms, including promotional infection attacks, which have targeted over 11,000 high-profile domains. As the attack surface continues to expand to mobile computing systems, approximately 90,000 Google Play apps have been infected, compromising personal information on a massive scale.

The advent of Large Language Models (LLMs) has further exacerbated the problem, with cybercriminals leveraging these advanced tools to develop sophisticated malware. This underscores the pressing need for robust cybersecurity measures to detect and mitigate threats proactively. This report draws inspiration from the mythological Perseus, who used a mirrored shield to deflect Medusa's deadly gaze. Similarly, modern cyber defense systems must adopt innovative techniques to turn an attacker's tools against them, safeguarding critical systems and data.

II. Comprehensive Insights into Cyber Threat Intelligence and System Protection

Cyber Threat Intelligence (CTI) serves as a cornerstone of modern cybersecurity strategies. Defined as the collection, analysis, and dissemination of information about potential threats, CTI enables organizations to anticipate and neutralize cyber risks. According to Gartner, CTI has two primary applications:

Advisors: Nicholas LaRacuente, Dongruo Zhou, Assistant Professors, Computer Science Department

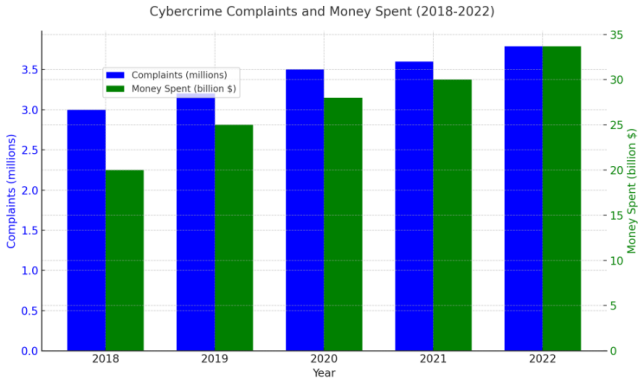

Fig. 1. Cybercrime complaints (in millions) and money spent (in billions of dollars) from 2018 to 2022.

1) Intuition Detection Tools: Using malware signatures to detect and prevent attacks.
2) Vulnerability Analysis: Identifying weaknesses in systems to prioritize protective measures.

The lifecyle of CTI involves:

- Identifying sources, such as VirusTotal.
- Aggregating and sharing threat intelligence with security vendors.
- Applying insights to downstream applications for proactive defense.

Despite its potential, CTI faces credibility challenges. For instance, inconsistencies in the Common Vulnerability Scoring System (CVSS) can hinder the accurate assessment of vulnerabilities. A study revealed that nearly 50 percent of security professionals misjudge vulnerability severity due to these inconsistencies.

III. Innovations in Vulnerability Assessment

To address the inherent limitations of the Common Vulnerability Scoring System (CVSS), the project team undertook the development of the DiffCVSS tool, a sophisticated solution designed to enhance vulnerability analysis through a more context-aware, operating system (OS)-centric approach. While CVSS has been a widely used framework for assessing the severity of vulnerabilities, it often lacks the granularity needed for accurate evaluation across diverse operating systems. The

DiffCVSS tool aims to bridge this gap by incorporating OS-specific considerations, ultimately providing a more nuanced understanding of vulnerabilities within a given system architecture.

The DiffCVSS tool incorporates three key components, each contributing to a more refined and actionable vulnerability assessment process:

- Function Mapping: Leveraging advanced natural language processing (NLP) techniques, DiffCVSS analyzes Linux kernel functions to generate accurate CVSS metrics. By understanding the context of these kernel functions, the tool can identify specific areas where vulnerabilities may arise, enhancing the overall precision of vulnerability scoring. This is particularly valuable as it accounts for the differences in how functions operate across various OS derivatives, offering a tailored, function-centric analysis that traditional CVSS methods overlook.
- Severity Differentiation: One of the main challenges of CVSS is its inability to distinguish the severity of vulnerabilities across different system derivatives, which can significantly vary in their impact. DiffCVSS addresses this issue by incorporating OS-specific factors to more accurately identify the severity of vulnerabilities. This enables a deeper understanding of how the vulnerability will manifest in different environments, ensuring that mitigation strategies are more targeted and effective based on the operating system in use.
- Efficiency Improvement: Traditional vulnerability analysis can be time-consuming, with some processes taking hours to complete. DiffCVSS addresses this inefficiency by reducing analysis time from several hours (typically around four hours) to just 20 minutes. This significant reduction in processing time enables cybersecurity teams to respond to threats more quickly, mitigating risks and preventing potential damage before they escalate. By speeding up the analysis process, the tool enhances overall cybersecurity response times, ensuring timely interventions.

In addition to DiffCVSS, the team introduced the CEAM (Contextual Entity Alignment Method) tool, which employs cutting-edge entity alignment techniques to detect and eliminate ”incredible” vulnerability artifacts—those that may be irrelevant, incorrect, or misleading within a vulnerability database. By refining vulnerability datasets in this way, CEAM ensures that only accurate and reliable information is used for decision-making, further enhancing the precision of vulnerability assessments.

These advancements not only improve the reliability and accuracy of vulnerability assessments but also contribute to a more streamlined cybersecurity response process. By providing more precise, OS-aware vulnerability scoring, reducing analysis time, and improving the quality of vulnerability data, these tools empower cybersecurity professionals to make more informed decisions and respond to threats with greater agility. This, in turn, strengthens the overall cybersecurity posture of organizations, minimizing the risk of exploitation and ensuring more effective protection against emerging threats.

IV. Privacy and Security in Software Supply Chains

Modern software systems increasingly depend on third-party software development kits (SDKs) to enhance functionality, streamline development, and reduce costs. However, the widespread use of these SDKs introduces significant vulnerabilities within software applications, creating potential risks for users and organizations alike. These vulnerabilities can range from poor integration practices to more severe issues, such as unintentional data leakage or malicious SDK behavior. One of the key challenges arising from the integration of SDKs is the difficulty in monitoring and controlling the data interactions between third-party libraries and the main software application. This problem is exacerbated by the lack of proper privacy safeguards in place for many SDKs.

A critical issue that has emerged with the integration of third-party SDKs is non-compliance with privacy regulations, which is a growing concern within the software development community. A comprehensive study conducted by the Lalaine tool, which analyzed over 2,000 mobile applications, uncovered a startling number of non-compliance issues, particularly around user privacy. Many of these apps falsely claimed not to collect user data, despite secretly harvesting sensitive information such as location data. This data was often shared across SDKs, creating additional privacy concerns. In some cases, apps were found to be cross-sharing user data with other third-party SDKs without the user's explicit consent, breaching privacy regulations such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

To address these pressing concerns, the development team worked closely with major SDK vendors, including industry giants like Google and Apple. The collaboration aimed to implement stricter privacy controls that would ensure transparency and compliance with global privacy standards. As a result of this partnership, significant steps were taken to improve the privacy landscape in the mobile application ecosystem. One notable achievement was the introduction of the Apple Privacy Manifest, a new privacy language designed to enhance transparency and provide developers with clearer guidelines for handling user data. This initiative was a key step forward in providing both developers and users with better visibility into how their data is being used by various SDKs integrated into applications.

In addition to the Privacy Manifest, the team also developed a groundbreaking solution known as the SDK Privacy Wrapper. This innovative tool helps isolate potentially malicious or non-compliant SDKs from legitimate ones, ensuring that data interaction between the app and its integrated third-party SDKs remains secure. The SDK Privacy Wrapper serves as a protective barrier, preventing malicious SDKs from accessing or sharing sensitive user information without proper authorization. By isolating these SDKs, developers can create more secure and privacy-compliant applications, reducing the risk of data breaches and enhancing user trust.

Overall, these efforts represent a significant step towards improving the privacy and security of modern software systems that rely on third-party SDKs. As privacy regulations continue to evolve and become more stringent, it is imperative that software developers and SDK vendors work together to ensure that user data is protected and that software systems remain secure. The initiatives undertaken by the team in collaboration with Google and Apple demonstrate the importance of proactive efforts to address privacy concerns, mitigate risks, and create a safer digital environment for users worldwide.

V. Proactive System Protection

Beyond merely addressing vulnerabilities, the research underscores the critical importance of proactively safeguarding systems before threats can exploit weaknesses. This proactive approach goes beyond simply patching up security gaps and emphasizes the need to anticipate and mitigate potential risks through a deeper understanding of real-world threat models. By thoroughly decoding these models, researchers can uncover gaps in security that may not be immediately visible and can identify areas where regulations may have overlooked emerging risks. This forward-thinking strategy aims to create a more robust and resilient system architecture, designed to withstand not only current threats but also those that could evolve in the future.

A vital part of this effort involves leveraging advanced compliance analysis tools, such as those used to assess iOS App Privacy Nutrition Labels, which have proven invaluable in evaluating how user data is managed and protected within mobile applications. These tools offer critical insights into data handling practices, helping developers and security experts understand how data is:

- Collected from users
- Shared with third parties
- Stored and processed within the app

This transparency is essential to ensure that privacy policies are being adhered to and that users' personal information remains secure. By conducting these detailed analyses, it becomes possible to detect discrepancies and non-compliance, providing an early warning system for potential privacy violations before they become widespread issues.

However, addressing vulnerabilities and ensuring compliance is not solely a technical challenge; it also requires a shift towards socio-technical solutions. These solutions bridge the gap between technological innovation and regulatory compliance, fostering an ecosystem where both technical advancements and social considerations are equally prioritized. The integration of legal and ethical standards into the development process is crucial, ensuring that privacy protection and data security are not merely add-ons but are embedded within the very fabric of the system. By combining technical innovation with rigorous adherence to evolving regulations, this holistic approach helps create secure, user-centric systems that can navigate the complexities of an increasingly digital and interconnected world.

In essence, this research advocates for a more integrated approach, where technology and regulation work hand-in-hand to prevent vulnerabilities and safeguard users' rights, ensuring that both innovation and security are sustained in tandem.

VI. Raising Awareness and Broader Impact

To combat the growing threat of cybercrime, it is crucial to raise awareness, particularly among vulnerable populations. With the rapid proliferation of mobile devices, children have become an increasingly significant at-risk group. Recent statistics show that 53

To address this pressing issue, the team took proactive measures by co-authoring the book Lorie in Cybersecurity Wonderland, an educational tool designed to teach children about online safety in an engaging and relatable way. The book uses storytelling to introduce complex cybersecurity concepts, making it accessible to young readers. The narrative follows Lorie, a young character, as she learns important lessons about protecting her digital identity, recognizing online threats, and practicing good cybersecurity hygiene. This approach not only educates but also empowers children to make safe and informed decisions while interacting online.

In addition to the book, the team has organized a series of interactive initiatives aimed at further engaging children and raising awareness about cybersecurity. Among these initiatives is the mobile security summer camp, specifically tailored for young learners. These camps offer a fun and hands-on learning environment where children can develop their cybersecurity skills through games, simulations, and group discussions. By using interactive activities, the camps help children understand the importance of online privacy, safe browsing habits, and how to recognize common cyber threats such as phishing and malware.

Through these multifaceted efforts, the team seeks to elevate risk awareness among children and foster a culture of digital responsibility. By educating the younger generation, the hope is that they will be better equipped to protect themselves from cyber threats and grow into responsible digital citizens who can confidently navigate the online world.

VII. Conclusion and Future Work

This research underscores the need for a comprehensive approach to cybersecurity that combines innovative tools, proactive threat management, and awareness initiatives. Key takeaways include:

Highlighting the credibility challenges in CTI.

Automating vulnerability assessments to streamline security processes.

Enhancing privacy and security in software ecosystems through tools like the SDK Privacy Wrapper.

Educating broader populations, particularly children, about cybersecurity risks.

Future work will focus on refining these tools and strategies, exploring underutilized CTI sources, and fostering collaboration between academia, industry, and regulatory bodies to create a safer digital environment.

VIII. Inspiring Lectures: Insights from Leading Researchers

In addition to Professor Xiaojing Lao's insightful talk, I found two other lectures particularly engaging due to their relevance and innovative approaches to tackling complex challenges:

1) Aligning Foundation Models with the Open Multifaceted World (Prof. Junjie Hu): Professor Junjie Hu's lecture shed light on the challenges of aligning foundation models with real-world complexities. The talk emphasized the importance of adapting these models to reflect diverse, multifaceted perspectives, rather than relying on narrow or biased datasets. I found this particularly fascinating because it addressed critical gaps in model alignment, especially as foundation models are increasingly integrated into decision-making systems. The proposed techniques for improving adaptability and inclusivity inspired me to explore further possibilities in bridging the gap between artificial intelligence and real-world diversity.
2) Tensors Everywhere in Complexity (Prof. Joshua Grochow): Professor Joshua Grochow's lecture highlighted the pervasive role of tensors in understanding and solving problems in computational complexity. What captivated me most was his ability to draw connections between abstract tensor operations and their implications for real-world computational challenges, such as data compression and machine learning. His perspective on using tensors as a unifying framework across diverse applications deepened my appreciation for their potential to simplify complex systems and revolutionize computational approaches.

These lectures not only broadened my understanding of foundational concepts but also sparked curiosity about their practical applications in addressing pressing global challenges.

References

[1] Y. Qin, Y. Xiao, and X. Liao. Automated Expansion of Privacy Data Taxonomy for Compliant Data Breach Notification. *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, 2025.

[2] Y. Xiao, D. Kirat, D. L. Schales, J. Jang, L. Xing, and X. Liao. JBomAudit: Assessing the Landscape, Compliance, and Security Implications of Java SBOMs. *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, 2025.

[3] J. Cui, H. Kim, E. Jang, D. Yim, K. Kim, Y. Lee, J. W. Chung, S. Shin, and X. Liao. Tweezers: A Framework for Security Event Detection via Event Attribution-centric Tweet Embedding. *Proceedings of the ISOC Network and Distributed System Security Symposium (NDSS)*, 2025.

[4] E. Gumusel, Y. Xiao, Y. Qin, J. Qin, and X. Liao. Understanding Legal Professionals' Practices and Expectations in Data Breach Incident Reporting. *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2024. (Acceptance rate: 16.7%).