Impact of Proactive Cyber Threat Intelligence on Exploits from the Dark Web

Lawrence J. Awuah

Abstract: The desire to defend against the ever-growing cyber threat landscape necessitates the need to link exploits from the Dark Web to known vulnerabilities with the sole aim of proactively utilizing Cyber Threat Intelligence (CTI) solutions, with Deep Learning (DL) model and Exploit Vulnerability Attention Deep Structured Semantic Model (EVA-DSSM), to maximize data protection, privacy, and security.

A review of "Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-based Deep Structured Semantic Model". By Samtani, S., Chai, Y., & Chen, H. (2022). *MIS Quarterly, 46*(2), 911-946. DOI: 10.25300/MISQ/2022/15392

Summary: "Black hat hackers use malicious exploits to circumvent security controls and take advantage of system vulnerabilities worldwide, costing the global economy over $450 billion annually. While many organizations are increasingly turning to cyber threat intelligence (CTI) to help prioritize their vulnerabilities, extant CTI processes are often criticized as being reactive to known exploits. One promising data source that can help develop proactive CTI is the vast and ever-evolving Dark Web. In this study, we adopted the computational design science paradigm to design a novel Deep Learning (DL)-based Exploit Vulnerability Attention Deep Structured Semantic Model (EVA-DSSM) that includes bidirectional processing and attention mechanisms to automatically link exploits from the Dark Web to vulnerabilities. We also devised a novel Device Vulnerability Severity Metric (DVSM) that incorporates exploit postdate and vulnerability severity to help cybersecurity professionals with their device prioritization and risk management efforts. We rigorously evaluated the EVA-DSSM against state-of-the-art non-DL and DL-based methods for short text matching on 52,590 exploit-vulnerability linkages across four testbeds: web application, remote, local, and Denial of Service. Results of these evaluations indicate that the proposed EVA-DSSM achieves Precision at 1 scores 20% - 41% higher than non-DL approaches and 4% – 10% higher than DL-based approaches. We demonstrated the EVA-DSSM's and DVSM's practical utility with two CTI case studies: openly accessible systems in the top eight US hospitals and over 20,000 Supervisory Control and Data Acquisition (SCADA) systems worldwide. A complementary user evaluation of the case study results indicated that 45 cybersecurity professionals found the EVA-DSSM and DVSM results more useful for exploit-vulnerability linking and risk prioritization activities than those produced by prevailing approaches. Given the rising cost of cyber-attacks, the EVA-DSSM and DVSM have important implications for analysts in security operations centers, incident response teams, and cybersecurity vendors."

Keywords*: cyber threat intelligence, deep learning, deep structured semantic models, vulnerability assessment, hacker forums, dark web, security operations, cybersecurity analytics*

The desire for researchers and subject matter experts to help organizations understand the complexity of attack vectors and support their cyber defense with automated incident response capabilities, driven by machine intelligence, has become so critical in today's world. We have reached a point where cybersecurity trainees, researchers, and professionals need to continuously

gain insights into innovative cybersecurity solutions in the field. The fact that malicious actors consistently use hacking techniques to circumvent security controls and exploit system vulnerabilities in the wake of the current threat landscape motivated Samtani et al. [1] to develop proactive Cyber Threat Intelligence (CTI) model from the perspective of the Dark Web. More to the point, pattern recognition, anomaly detection, and predictive analytics remain to offer threat intelligence and cybersecurity analytics capabilities that are key ingredients in automated incident response and threats mitigation efforts in the ever-evolving threat landscape.

Additionally, machine intelligence has become so ubiquitous and an indispensable tool, in defensive and offensive operations, that it remains to be a useful resource to cybersecurity leaders and device vendors. As part of their study, the authors adopted a novel Deep Learning (DL)-based model, an Exploit Vulnerability Attention Deep Structured Semantic Model (EVA-DSSM), which comprises bidirectional processing and attention mechanisms with the capability to automatically link exploits from the Dark Web to known vulnerabilities [1]. Additionally, a Device Vulnerability Severity Metric (DVSM) model was developed to be employed by cybersecurity professionals when engaging in device prioritization and risk management activities. A high-Level CTI Framework that captures EVA-DSSM and DVSM models is depicted in figure 1.

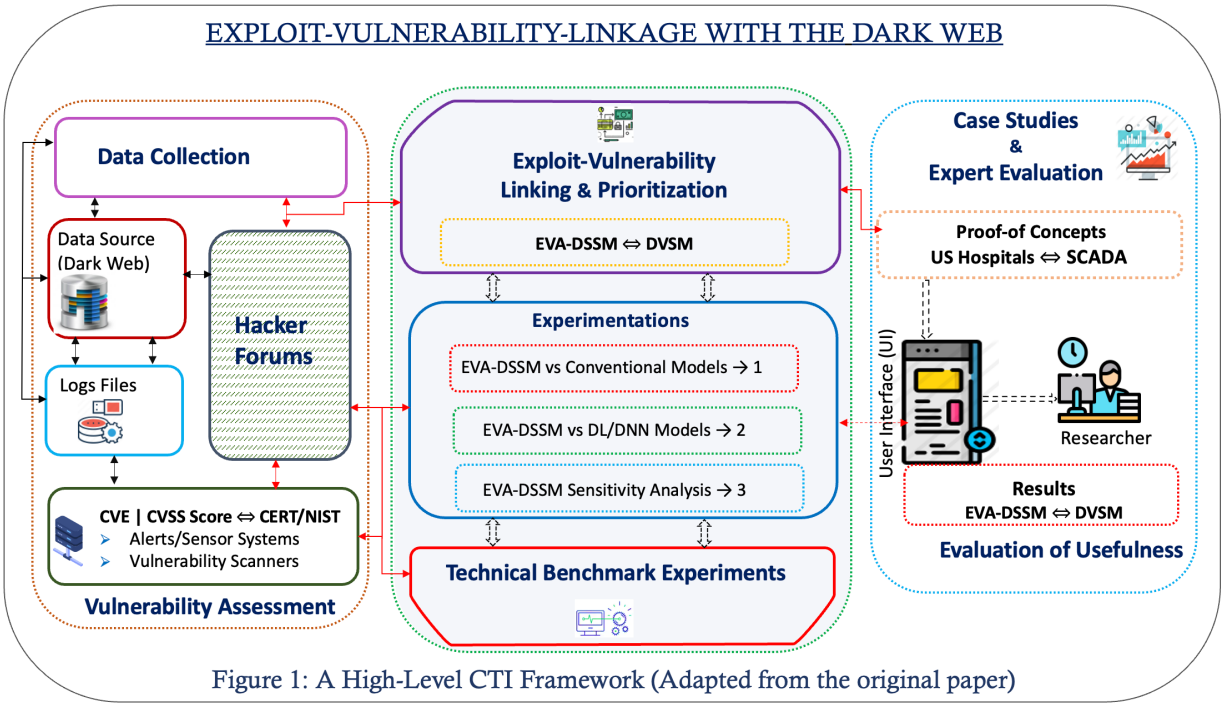

Figure 1: A High-Level CTI Framework (Adapted from the original paper)

In another study, Zhu et al. [4] adopted a computational design science solution to develop a DL-based, hierarchical, multi-phase Activity of Daily Living (ADL) framework to address similar concerns. Yet, others deployed Tor-use Motivation Model (TMM) and found a network impacted by illicit commerce and money laundering and concluded that criminality on this dark web is based more upon greed and desire, rather than any particular political motivations [3]. These models and frameworks play key roles in emerging cybersecurity mitigation strategies.

Moreover, the vulnerability assessment as part of the automated CTI process, coupled with analytics, facilitate intelligence required by CTI professionals to conduct initial triage of security

incidents for anticipated mitigation strategies. Motivated by the dynamic threat landscape, the authors develop a CTI framework and compared the operational differences between the conventional DSSM and their proposed EVA-DSSM [1]. When the proposed EVA-DSSM model was evaluated against both non-DL and DL-based methods for exploit-vulnerability linkages across selected testbeds (figure 1), the DL-based technique was determined to have achieved a much higher precision than the non-DL counterpart.

Furthermore, when a user evaluation of the CTI case study was conducted, the results indicated that a number of cybersecurity professionals found the EVA-DSSM and DVSM to be more efficient in exploitation-vulnerability linking and risk prioritization activities than those produced by conventional solutions. On the other hand, the user evaluation indicated that these professionals serving in the Security Operations Center (SOC), Incident Response (IR), Vulnerability Management (VM), and Operational Cybersecurity (OS) domains of practice found the EVA-DSSM and DVSM results more useful than those generated without these two models (figure 1). Given the rising cost of cyber-attacks, the EVA-DSSM and DVSM have perceived practical significance and important implications for analysts, for example, in the areas of security operations centers, incident response teams, and cybersecurity vendors.

In summary, there is a strong desire to support the fact that the practical and theoretical significance of the proposed EVA-DSSM and DVSM models evidently benefits analysts in SOC and IR teams, as well as security operations vendors. From the preceding analysis, there is also evidence to suggest that DL-based machine intelligence, as noted by the authors, plays a key role in SOC-related engagements. To that end, in mitigating evolving threats, organizations should empower the security operations teams and vendors with automated AI-based mitigation solutions. To efficiently mitigate these threats, organizations should endeavor to empower the security operations team and leadership with appropriate strategies needed to offer security orchestration and response processes to fully automate and manage the complexity of the SOC ecosystems [1-2]. In other words, the ability to seamlessly automate and manage the complexity of security operations to address the dynamic threat landscape remains an important challenge for security researchers, cybersecurity professionals, and cybersecurity vendors. Finally, from the preceding analysis, the EVA-DSSM and DVSM models certainly have crucial implications for those analysts in the SOC-based environment and cybersecurity vendors. Researchers and professionals alike have a major role to play in search of broader cybersecurity solutions for the interest of society.

References:

[1] Samtani, S., Chai, Y., & Chen, H. (2022). Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-based Deep Structured Semantic Model. *MIS Quarterly, 46*(2), 911-946. DOI: 10.25300/MISQ/2022/15392
[2] Kinyua, J. & Awuah, L. (2021). AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *Intelligent Automation & Soft Computing, 28*(2), 527–545. DOI:10.32604/iasc.2021.016240
[3] Dalins, J., Wilson, C., & Carman, M. (2018). Criminal motivation on the dark web: A categorisation model for law enforcement. *Digital Investigation, 24* (1), pp. 62-71. https://doi.org/10.1016/j.diin.2017.12.003

[4] Zhu, H., Samtani, S., Brown, R., & Chen, H. (2021). A Deep Learning Approach for Recognizing Activity of Daily Living (ADL) for Senior Care: Exploiting Interaction Dependency and Temporal Patterns. *MIS Quarterly 45*(2), pp. 859-896.