MIT LINCOLN LABORATORY

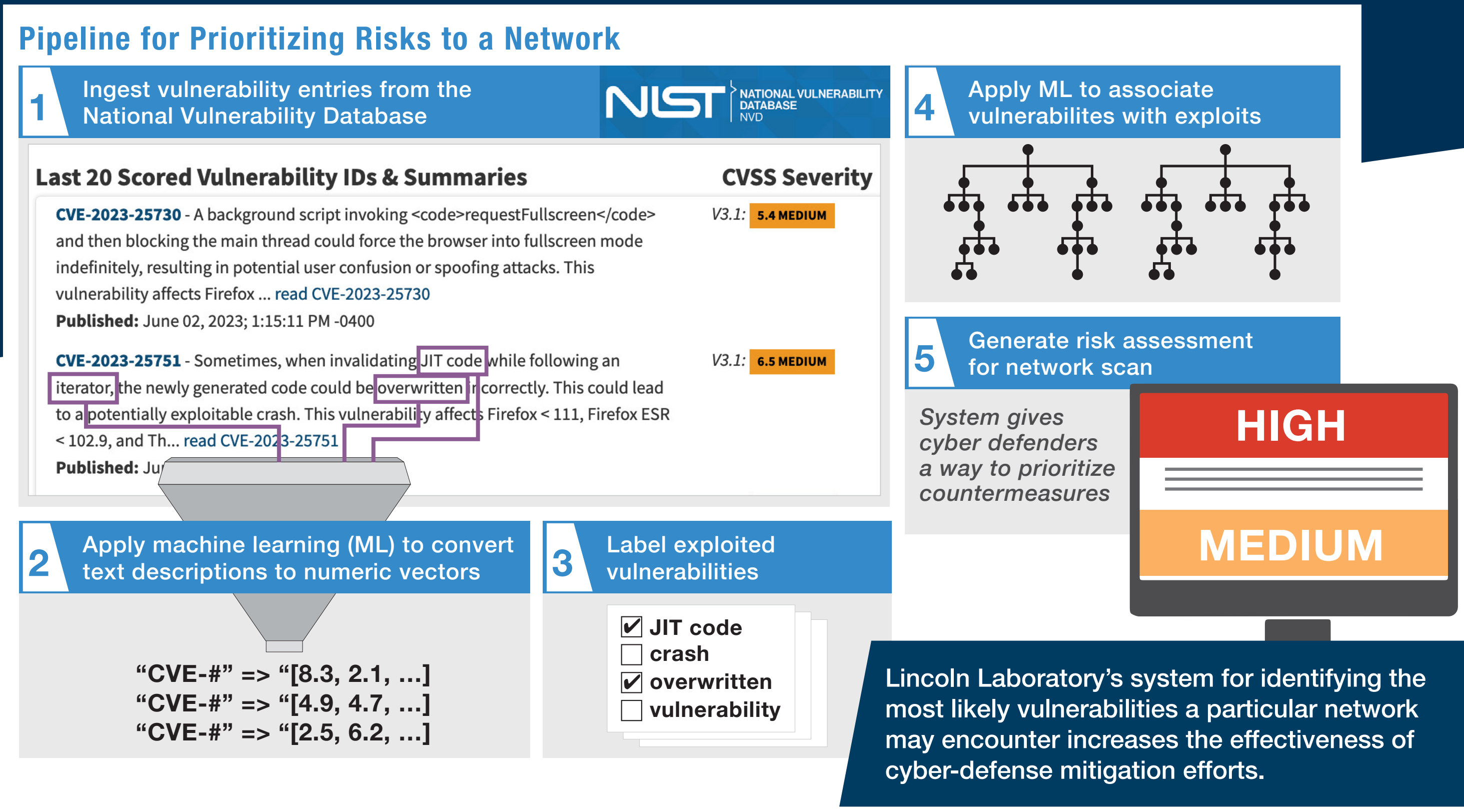
INNOVATION HIGHLIGHT

Technology in Support of National Security

WWW.LL.MIT.EDU

Targeted Risk Prioritization to Improve Network Cyber Defense

Pipeline for Prioritizing Risks to a Network



1 Ingest vulnerability entries from the National Vulnerability Database

Last 20 Scored Vulnerability IDs & Summaries **CVSS Severity**

CVE-2023-25730 - A background script invoking <code>requestFullscreen</code> and then blocking the main thread could force the browser into fullscreen mode indefinitely, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox ... read CVE-2023-25730 *V3.1:* 5.4 MEDIUM

Published: June 02, 2023; 1:15:11 PM -0400

CVE-2023-25751 - Sometimes, when invalidating JIT code while following an iterator, the newly generated code could be overwritten incorrectly. This could lead to a potentially exploitable crash. This vulnerability affects Firefox < 111, Firefox ESR < 102.9, and Th... read CVE-2023-25751 *V3.1:* 6.5 MEDIUM

Published: Ju

2 Apply machine learning (ML) to convert text descriptions to numeric vectors

"CVE-#" => "[8.3, 2.1, ...]
"CVE-#" => "[4.9, 4.7, ...]
"CVE-#" => "[2.5, 6.2, ...]

3 Label exploited vulnerabilities

☑ JIT code
□ crash
☑ overwritten
□ vulnerability

4 Apply ML to associate vulnerabilites with exploits

5 Generate risk assessment for network scan

System gives cyber defenders a way to prioritize countermeasures

Lincoln Laboratory's system for identifying the most likely vulnerabilities a particular network may encounter increases the effectiveness of cyber-defense mitigation efforts.

Lincoln Laboratory developed an innovative technique enabling cyber analysts to prioritize efforts for mitigating software vulnerabilities that attackers may use to infiltrate a network. Applying natural language processing descriptions of vulnerabilities used in prior attacks, our method estimates the risk presented by specific vulnerabilities, helping alleviate the network defenders' burden of trying to counter any of thousands of potential vulnerabilities.

KEY FEATURES

- Algorithms can tailor the risk assessment to profiles of specific known attackers
- Machine learning models are trained on attack data specific to a defended network
- Algorithms can reprioritize vulnerabilities as new information on threat activity emerges

LINCOLN LABORATORY
Massachusetts Institute of Technology

Background

Reported software vulnerabilities threatening the security of computer systems number in the hundreds of thousands, and new vulnerabilities are discovered daily. Cybersecurity professionals tasked with defending enterprise networks run scans, looking for the presence of vulnerabilities documented in the National Vulnerability Database maintained by the National Institute of Standards and Technology. Each of these vulnerabilities is assigned a Common Vulnerability Scoring System (CVSS) value indicating the perceived severity of the vulnerability (lowest 0 to highest 10). Cyber defenders then typically prioritize vulnerability mitigations and/or patch deployments on the basis of high CVSS scores.

However, this approach, a time- and labor-intensive method, often results in ineffectual network defense. The vast number of known, potentially serious vulnerabilities discovered on a network makes it daunting to determine what resources to expend on which vulnerabilities. And, because CVSS scores quantify aggregated data from many and diverse sources, a score may not represent the risk to a particular network or from a specific type of attacker. For example, an attack on a commercial company most likely was perpetrated by actors and exploited vulnerabilities different from those involved in attacks on government networks.

Lincoln Laboratory Technique

We developed an approach that targets cyber-defense efforts to vulnerabilities most likely to be used against a network. Hypothesizing that attackers would employ strategies similar to those they used effectively in the past, we converted descriptive human assessments of vulnerabilities to numeric (vector) values and applied machine learning to classify vulnerabilities associated with different successful network infiltrations. These associations inform a risk-assessment scoring system that takes into account the particular networks attacked by specific actors. By improving the accuracy of tying vulnerabilities to likelihood of exploitation, this system gives cyber defenders a way to prioritize their countermeasures, leading to more secure networks while decreasing costs to their time and resources. Through several evaluations, our supervised-learning approach achieved better accuracy in predicting risks than approaches relying on CVSS scores.

APT 28 CVEs % Mitigated	Custom Attacker	CVSS	Exploit-DB
80%	6.5%	34.3%	39.4%
90%	8.0%	34.3%	40.8%
100%	8.3%	47.0%	98.7%

The table summarizes percentages of 12 vulnerabilities, identified as advanced persistent threat (APT) group 28, recommended for mitigation by three models (Lincoln Laboratory's Custom Attacker, CVSS, and Exploit-DB). To capture 80% of the APT 28 Common Vulnerabilities and Exposures (CVEs), the Attacker model recommends remediating the top 6.5% of vulnerabilities, whereas the Exploit-DB model recommends remediating the top 39.4%, and CVSS the top 34.3%. The results for capturing 90% and 100% are more dramatic. For all three scenarios, the attacker model significantly outperforms Exploit-DB and CVSS, focusing the cyber defenders' mitigations to a much more manageable set of CVEs.

INTERESTED IN ACCESSING THIS TECHNOLOGY?

Contact the MIT Technology Licensing Office
https://tlo.mit.edu/
tlo-inquiries@mit.edu 617-253-6966

INTERESTED IN WORKING WITH MIT LINCOLN LABORATORY?

https://www.ll.mit.edu/partner-us

Contact the Technology Ventures Office
tvo@ll.mit.edu

U.S. PATENT #11,036,865

More Information

K. Alperin et al., "Risk Prioritization by Leveraging Latent Vulnerability Features in a Contested Environment," *Proceedings of the 12th ACM Workshop on Artificial Intelligence and Security*, 11 November 2019.

Approved for public release; distribution is unlimited. This material is based upon work supported by the U.S. Department of the Air Force under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings and conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Air Force.