New AI model aims to plug key gap in cybersecurity readiness

May 22 2023, by Tom Rickey

Scientists from several institutions worked together to harness artificial intelligence, linking computer vulnerabilities, weaknesses and attack patterns to increase cybersecurity. Credit: Timothy Holland | Pacific Northwest National Laboratory

Imagine you're the new manager of a large apartment building and someone has stolen one of your keys—but you're not sure which one. Was it to a first-floor apartment? The mail room? Maybe it's a master key to all the units.

All locks are vulnerable, as far as you know, and you'll need to change every lock to be completely secure.

But if you knew exactly which key went missing, you could target your efforts, changing just the relevant lock and eliminating the threat posthaste.

Multiply that problem thousands of times over and you'll understand what cyber defenders grapple with. There are more than 213,800 available known "keys"—unofficial entry points into computer systems, better known as vulnerabilities or bugs—and they're already in the hands of criminals. There are likely many more that are not known. How can all the threats and attacks be tracked, prioritized and prevented?

That's impossible for any one person or team. While computer analysts share leads by feeding information into multiple databases, they don't have a map of how adversaries might use most of those bugs to wreak havoc.

Now, a team of scientists at the Department of Energy's Pacific Northwest National Laboratory, Purdue University, Carnegie Mellon University and Boise State University have turned to artificial intelligence to help solve the problem. The researchers have knitted together three large databases of information about computer vulnerabilities, weaknesses and likely attack patterns. Their work was published as part of the *2022 IEEE International Symposium on Technologies for Homeland Security (HST)*.

The AI-based model automatically links vulnerabilities to specific lines of attack that adversaries could use to compromise computer systems. The work should help defenders spot and prevent attacks more often and more quickly. The work is open source with a portion now available on GitHub. The team will release the rest of the code soon.

"Cyber defenders are inundated with information and lines of code. What they need is interpretation and support for prioritization. Where are we vulnerable? What actions can we take?" said Mahantesh Halappanavar, a chief computer scientist at PNNL who led the overall effort.

"If you are a cyber defender, you may be dealing with hundreds of vulnerabilities a day. You need to know how those could be exploited and what you need to do to mitigate those threats. That's the crucial missing piece," added Halappanavar. "You want to know the implications of a bug, how that might be exploited, and how to stop that threat."

From CVE to CWE to CAPEC: A path to better cybersecurity

The new AI model uses natural language processing and supervised learning to bridge information in three separate cybersecurity databases:

- Vulnerabilities—the specific piece of computer code that could serve as an opening for an attack. These 200,000+ "common vulnerabilities and exposures" or CVEs, are listed in a National Vulnerability Database maintained by the Information Technology Laboratory.
- Weaknesses—a slimmer set of definitions that classify the vulnerabilities into categories based on what could happen if the

vulnerabilities were acted upon. There are about 1,000 "common weakness enumerations" or CWEs listed in the Common Weakness Enumeration database maintained by MITRE Corp.

- Attacks—what an actual attack exploiting vulnerabilities and weaknesses might look like. More than 500 potential attack routes or "vectors," known as "CAPECs," are included in the Common Attack Pattern Enumeration and Classification resource maintained by MITRE.

While all three databases have information crucial for cyber defenders, there have been few attempts to knit all three together so that a user can quickly detect and understand possible threats and their origins, and then weaken or prevent these threats and attacks.

"If we can classify the vulnerabilities into general categories, and we know exactly how an attack might proceed, we could neutralize threats much more efficiently," said Halappanavar. "The higher you go in classifying the bugs, the more threats you can stop with one action. An ideal goal is to prevent all possible exploitations."

The work received the best paper award at the IEEE International Symposium on Technologies for Homeland Security in November.

In previous work, the team used AI to link two of the resources, vulnerabilities and weaknesses. That work, resulting in the model V2W-BERT, earned the team—Das, Pothen, Halappanavar, Serra and Ehab Al-Shaer from Carnegie Mellon University—a best application paper award at the 2021 IEEE International Conference on Data Science and Advanced Analytics.

AI links computer bugs to potential cyberattacks automatically

The new model, VWC-MAP, extends the project to a third category, attack actions.

"There are thousands upon thousands of bugs or vulnerabilities out there, and new ones are created and discovered every day," said Das, a doctoral student at Purdue who has led development of the work since his internship at PNNL in 2019. "And more are coming. We need to develop ways to stay ahead of these vulnerabilities, not only the ones that are known but the ones that haven't been discovered yet."

The team's model automatically links vulnerabilities to the appropriate weaknesses with up to 87 percent accuracy, and links weaknesses to appropriate attack patterns with up to 80 percent accuracy. Those numbers are much better than today's tools provide, but the scientists caution that their new methods need to be tested more widely.

One hurdle is the dearth of labeled data for training. For example, currently very few vulnerabilities—less than 1%—are linked to specific attacks. That's not a lot of data available for training.

To overcome the lack of data and perform the work, the team fine-tuned pretrained natural language models, using both an auto-encoder (BERT) and a sequence-to-sequence model (T5). The first approach used a language model to associate CVEs to CWEs and then CWEs to CAPECs through a binary link prediction approach. The second approach used sequence-to-sequence techniques to translate CWEs to CAPECs with intuitive prompts for ranking the associations. The approaches generated very similar results, which were then validated by the cybersecurity expert on the team.

"We're putting this out there for others to test, to go through the vulnerabilities and make sure the model bins them appropriately," said Halappanavar. "We really hope that cybersecurity experts can put this open-source platform to the test."

More information: Siddhartha Shankar Das et al, Towards Automatic Mapping of Vulnerabilities to Attack Patterns using Large Language Models, *2022 IEEE International Symposium on Technologies for Homeland Security (HST)* (2023). DOI: 10.1109/HST56032.2022.10025459

Provided by Pacific Northwest National Laboratory

Citation: New AI model aims to plug key gap in cybersecurity readiness (2023, May 22) retrieved 25 April 2024 from https://techxplore.com/news/2023-05-ai-aims-key-gap-cybersecurity.html