Fresh AI on Security: Digital Fingerprinting Deters Identity Attacks

Deep learning software bolsters defenses against one of the toughest challenges corporate networks face.

Author: Nicola Sessions

Add AI to the list of defenses against identity attacks, one of the most common and hardest breach to prevent.

More than 40% of all data compromises involved stolen credentials, according to the 2022 Verizon Data Breach Investigations Report . And a whopping 80% of all web application breaches involved credential abuse.

“Credentials are the favorite data type of criminal actors because they are so useful for masquerading as legitimate users on the system,” the report said.

In today’s age of zero trust , security experts say it’s not a matter of if but when they’ll experience an identity attack.

The director of cybersecurity engineering and R&D; at NVIDIA, Bartley Richardson, articulates the challenge simply.

“We need to look for when Bartley is not acting like Bartley,” he said.

Last year, his team described a concept called digital fingerprinting . In the wake of highly publicized attacks in February, he came up with a simple but ambitious idea for implementing it.

He called a quick meeting with his two tech leads to share the idea. Richardson told them he wanted to create a deep learning model for every account, server, application and device on the network.

The models would learn individual behavior patterns and alert security staff when an account was acting in an uncharacteristic way. That’s how they would deter attacks.

The tech leads thought it was a crazy idea. It was computationally impossible, they told him, and no one was even using GPUs for security yet.

Richardson listened to their concerns and slowly convinced them it was worth a try. They would start with just a model for every account.

Security managers know it’s a big-data problem.

Companies collect terabytes of data on network events every day. That’s just a fraction of the petabytes of events a day companies could log if they had the resources, according to Daniel Rohrer, NVIDIA’s vice president of software product security.

The fact that it’s a big-data problem is also good news, Rohrer said in a talk at GTC in September (watch free with registration). “We’re already well on the way to combining our cybersecurity and AI efforts,” he said.

By mid-March, Richardson’s team was focused on ways to run thousands of AI models in tandem. They used NVIDIA Morpheus , an AI security software library announced a year earlier, to build a proof of concept in two months.

Once an entire, albeit crude, product was done, they spent another two months optimizing each portion.

Then they reached out to about 50 NVIDIANs to review their work — security operations and product security teams, and IT folks who would be alpha users.

Three months later, in early October, they had a solution NVIDIA could deploy on its global networks — security software for AI-powered digital fingerprinting.

The software is a kind of LEGO kit, an AI framework anyone can use to create a custom cybersecurity solution.

Version 2.0 is running across NVIDIA's networks today on just four NVIDIA A100 Tensor Core GPUs . IT staff can create their own models, changing aspects of them to create specific alerts.

NVIDIA is making these capabilities available in a digital fingerprinting AI workflow included with NVIDIA AI Enterprise 3.0 announced in December.

For identity attackers, "the models Bartley's team built have anomaly scores that are off the charts, and we're able to visualize events so we can see things in new ways," said Jason Recla, NVIDIA's senior director of information security.

As a result, instead of facing a tsunami of 100 million network events a week, an IT team may have just 8-10 incidents to investigate daily. That cuts the time to detect certain attack patterns from weeks to minutes.

The team already has big ideas for future versions.

"Our software works well on major identity attacks, but it's not every day you have an incident like that," Richardson said. "So, now we're tuning it with other models to make it more applicable to everyday vanilla security incidents."

Meanwhile, Richardson's team used the software to create a proof of concept for a large consulting firm.

"They wanted it to handle a million records in a tenth of a second. We did it in a millionth of a second, so they're fully on board," Richardson said.

Looking ahead, the team has ideas for applying AI and accelerated computing to secure digital identities and generate hard-to-find training data.

Richardson imagines passwords and multi-factor authentication will be replaced by models that know how fast a person types, with how many typos, what services they use and when they use them. Such detailed digital identities will prevent attackers from hijacking accounts and pretending they are legitimate users.

Data on network events is gold for building AI models that harden networks, but no one wants to share details of real users and break-ins. Synthetic data , generated by a variant of digital fingerprinting, could fill the gap, letting users create what they need to fit their use case.

In the meantime, Recla has advice security managers can act on now.

"Get up to speed on AI," he said. "Start investing in AI engineering and data science skills — that's the biggest thing."

Digital fingerprinting is not a panacea. It's one more brick in an ever-evolving digital wall that a community of security specialists is building against the next big attack.

You can try this AI-powered security workflow live on NVIDIA LaunchPad starting Jan. 23. And you can watch the video below to learn more about digital fingerprinting.

Original URL: https://blogs.nvidia.com/blog/2023/01/23/ai-security-digital-fingerprinting/