www.pipelinepub.com
Volume 19, Issue 1

Closing the Cyber Attack Gap with AI

By: Jacob Ukelson

The gap between the ability of cyber attackers to breach IT networks and the effectiveness of cyber defenses is widening. The elements contributing to this include automation and sophistication. Automation enables attackers to go after many more targets at very low cost to them. The increased sophistication of the attacks makes it more difficult to detect and defend against them.

The state of cyber defense today is that there is still a heavy reliance on manual processes. Security operations center (SOC) personnel need to respond to alerts and make decisions as to which alerts to investigate. With attackers highly automated and the defenders highly manual, it is easy to understand why we see ever-increasing losses to cybercrime.

Artificial intelligence would seem to be an obvious answer to closing the gap. After all, across industries, such technology is replacing or augmenting human expertise with an automated expert system. The promised benefits of AI in cyber defense, however, have been largely unfulfilled. This article reviews how AI technologies have been applied to cyber defense and examines emerging AI approaches that could make big progress in closing the cyber attack gap.

AI in cybersecurity

To begin, we should clarify some of the terms used when discussing AI. Cybersecurity vendors often claim their products use AI, or machine learning, or machine reasoning—sometimes interchangeably. Think of AI as an umbrella term encompassing different computer-based technologies that replicate human problem-solving or decision-making. Machine learning and machine reasoning are two types of AI technology that are used to solve different problems.

Machine learning applies statistical analysis and pattern recognition to large data sets to uncover patterns of behavior. Some common applications are speech and image recognition, traffic predictions, and fraud detection. Machine learning is also the more widely used AI technology in cybersecurity. It is primarily used for threat detection (real-time or post-event). For example, machine learning is the technology behind behavioral-based endpoint security systems. It is also used for anomaly-based threat detection in large networks, integrating and processing very large and disparate event log files.

Two issues have impeded progress in machine-learning based threat detection. The systems tend to have too many false positives while, at the same time, attackers are often able to modify their techniques to avoid detection. While AI has helped SOC teams manage workloads, it has not reversed the tide of breaches.

Organizations have concluded that they cannot stop all breaches. They are now pursuing a strategy of prevention combined with resilience. This approach seeks to minimize the chances of being breached while also minimizing the potential loss in the event of a breach. New developments in applying machine reasoning to this challenge are showing promise.

Machine reasoning-based risk and resilience management

Machine reasoning is a well-developed AI technology that many of us use in our daily lives. Personal assistants such as Siri and Alexa use machine reasoning to generate answers to the questions we ask—including questions they have never encountered before. So how can machine reasoning be applied to the challenge of prevention and resilience?

While machine learning is based on the statistical identification of hidden patterns within a large amount of data, machine reasoning is based on using facts and relationships, and drawing conclusions from them. Machine reasoning uses concepts and ideas coded as symbols. Reasoning systems represent data by semantic knowledge graphs that allow the machine to understand the meaning of the data through the semantics encoded in the graph, and to draw conclusions about that data by analyzing the graph of concepts and projecting them onto the new data.

The standard method for representing a semantic graph is Resource Description Framework or RDF—a directed graph described as triplets. A triplet in an RDF graph has three components: a node for the subject, a node for the object, and an arc with the predicate linking the subject to the object. (Figure 1 on next page) provides an example of a semantic graph that describes the IT concepts relevant to attackers and defenders. This simple and flexible data model has a lot of expressive power. It can represent complex situations and relationships, while also being abstract. RDF is considered one of the fundamental technologies of the Semantic Web. Reasoning systems excel in the ability to explain the "thought" process that led to the conclusion (explainability)—an ability that is lacking in most machine learning systems. Semantic graph technologies also make it possible to combine different types, formats, and sources of information into a common language that enables semantic and logical action capability on the integrated information.

This has great value in the cyber world. A semantic graph for cyber threats can be produced by using information and concepts found in standard information sources, such as MITRE ATT&CK and NVD CVE. Attack techniques can be analyzed to define the “requirements” of the attackers. By combining a semantic graph of cyber threats with a graph describing features of an organization’s IT systems, the reasoning system can deduce what information is needed to enable the technique and build a “virtual attacker” that can explain how, in principle, to attack an organization. This tells the organization how and where they are open to attack—without the need for other, often manual means of uncovering cyber exposures, such as penetration testing.

Once there is an accurate description of the IT systems of an organization, the connectivity between the systems and the description of the system’s identity and access information, the reasoning system can build specific attack scenarios for that organization—just as a real attacker would. If we then add to the system semantic information about defenses (mitigations) as they are defined by MITRE D3f3nd, the system can suggest ways to reduce the risks from those attacks.

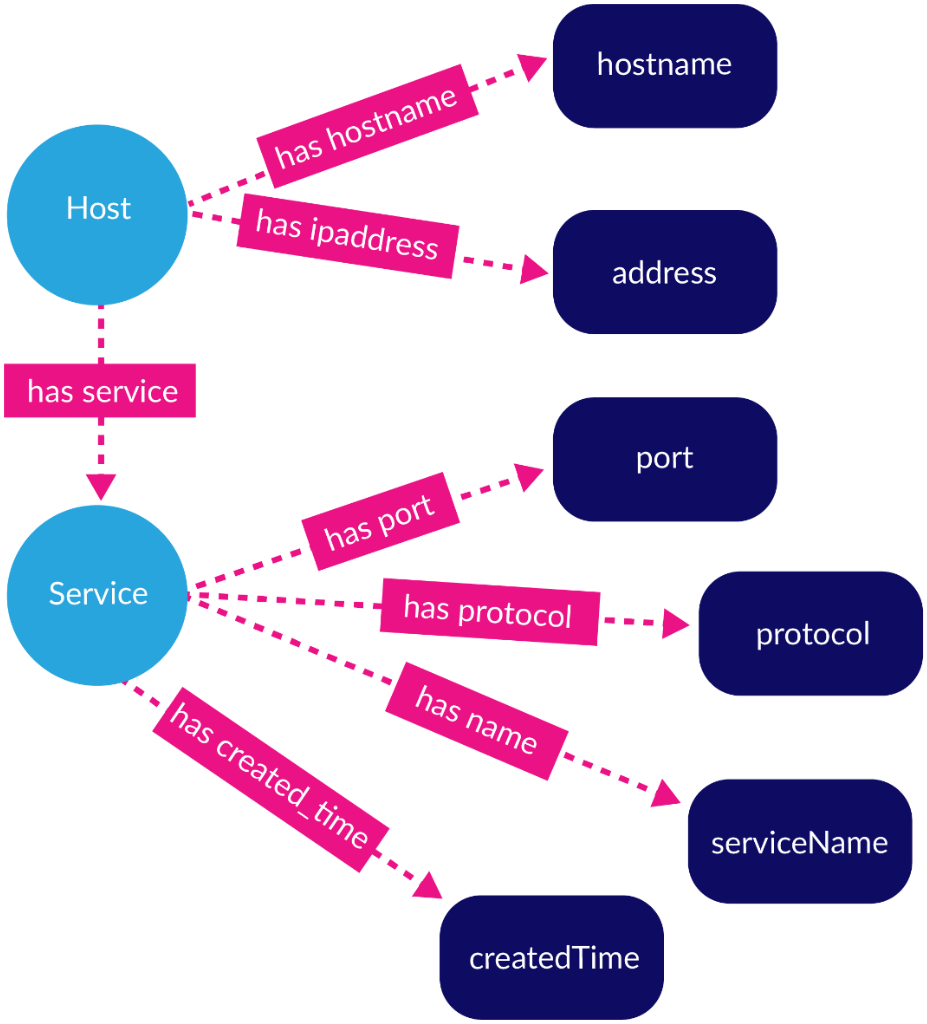

Figure 1: A simple semantic graph describing basic concepts from the IT relevant to attackers and defenders

For these reasons, machine reasoning is particularly suitable as a system for assessing an attacker’s ability to succeed in attacking the organization without conducting the attack. It also enables the assessment of organizational resilience to prevent or minimize the loss from cyber attacks.

Challenges in building a risk and resilience reasoning system

There are three major challenges in building a comprehensive reasoning-based system. The first is the precise semantic analysis of attack techniques, such as those described in MITRE ATT&CK. These are described for human understanding and are not suitable for reasoning systems. The solution is relatively simple to understand but difficult to implement: the techniques need to be rewritten with consistent and precise basic concepts (that is, an appropriate semantic model). Only then can a reasoning system be built.

Take for example MITRE ATT&CK technique T1210, "Exploitation of Remote Services." One of the accepted methods is to use a CVE that allows a remote service to be invoked. Therefore, it is necessary to enter into the reasoning system the ways to check the existence of the CVE on a system (Security Content Automation Protocol or SCAP can help) and to classify the vulnerabilities according to the ability to enable the activation of a remote service. For example, a prerequisite for finding a CVE is the ability to connect to that computer via the network—that is, having physical and logical connectivity that allows the vulnerability to be activated. These two facts are a start that enables reasoning regarding the use of the T1210 technique: "Find a system with the vulnerability that has connectivity that allows the exploitation of the CVE."

The second challenge is to create a language (ontology) that connects concepts from different attack domains—such as permissions, vulnerabilities, and configurations—and to create the semantic graph. There are some detailed ontologies that explain the relationship between various cyber concepts such as the UCO of the University of Maryland or MITRE D3F3ND.

The third challenge is collecting relevant information from the organization's systems. This can be done by interfacing with existing systems and translating the information into the common language or by a dedicated scanner.

With these challenges met, the system essentially becomes a digital cyber twin of the organization. It has all the information it needs to simulate millions of cyber attacks, thus identifying which specific attack scenarios represent exposures to the organization and calculating the risk from those exposures. Digital twinning technology is already being used in many industrial applications such as engineering design, building maintenance, and operations management. The time is right for it to be applied to cybersecurity, enabling teams to determine the courses of action that will mitigate attacks, reduce risk, and build cyber resilience.

The end game

Organizations are struggling to answer basic questions regarding their cyber risk exposure. These include organization-wide questions such as: What is our risk of being breached? What will the cost consequences be of a breach? What assets are most at risk? What steps do I need to take to lower my risk of being breached? How much should I spend on security? There are also operational questions regarding cyber exposure: What will be the risk impact to the business if we migrate a specific application to the cloud? If we implement two factor authentication? If we change our firewall controls?

Reasoning systems are showing great promise toward providing organizations with answers to both strategic and operational questions. Along with machine learning systems, reasoning systems will have an increasing use in cyber defense—especially in the world of risk analysis and management. They will provide IT and security teams with the tools and information they need to manage and control risks, better allocate security spending, and narrow the attack defense gap.