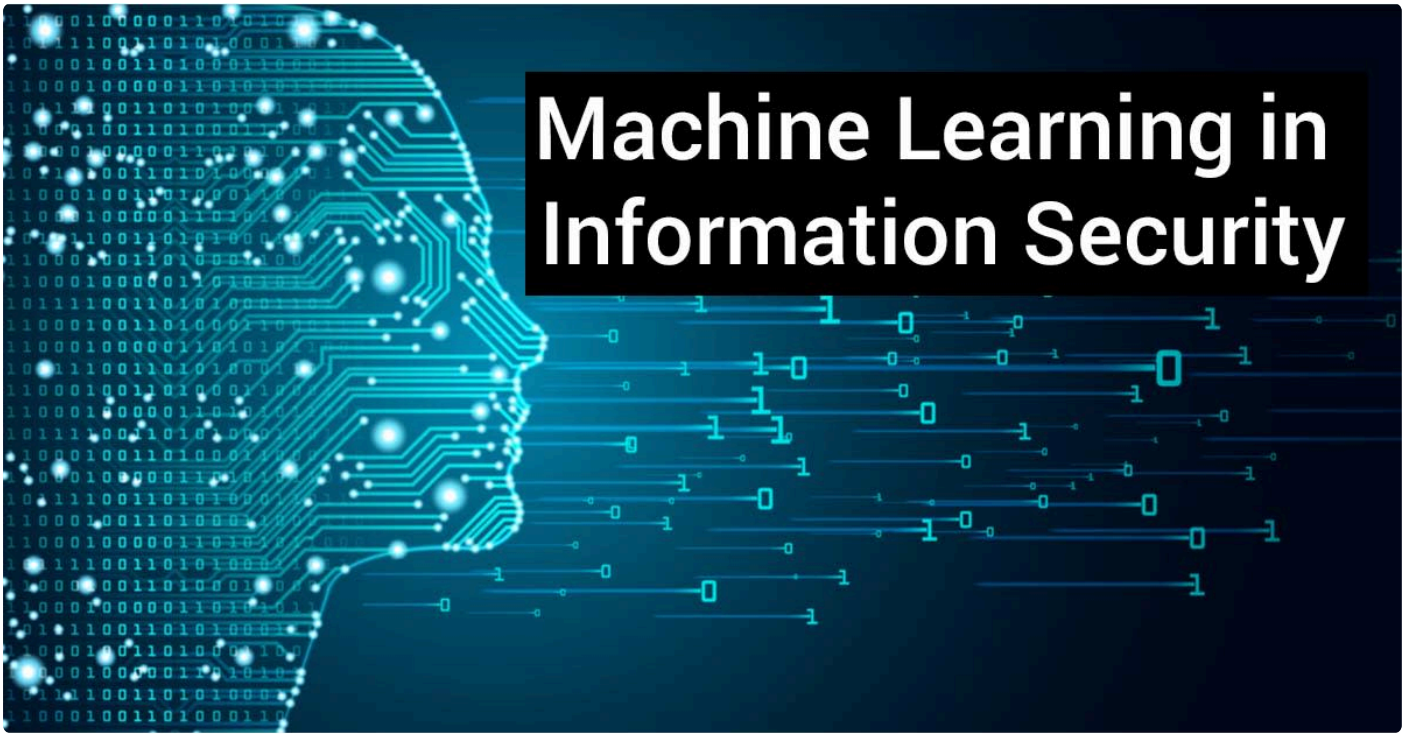
Machine Learning in Information Security

Ewa Anna Szyszka · 2020-09-07



Data is the new oil and the fundament of our digital economy. On a mass scale, we give away personal information carelessly for free, while scrolling, sharing, and liking. Machine learning is a tool that can act as a double-edged sword. On one hand, it is used by marketers to predict our consumer habits and nudge our behaviors by targeted campaigns into desired directions. On the other hand, it can protect individuals and institutions by enabling fast cyber-attack recognition. How can we use AI to create a more secure tomorrow?

Routine checks and automation

With global internet traffic on the rise, cybersecurity became an issue concerning every industry. According to the *Reinventing Cybersecurity with Artificial Intelligence* report, 49% of executives participating in the study have experienced cyber attacks in their companies using cloud services. 21% reported breaches involving unauthorized access in 2018 only. The volume and ever-evolving nature of cyberattacks can be overwhelming for security officers and organizations relying on external software solutions. This is where deep learning comes in handy. Some of the available solutions on the market offer deep-learning based analysis of the Advanced Persistent Threat (APT), ransomware attacks, backdoor, virus, and spyware attacks. Security officers are valuable and expensive resources for companies. Machine learning technologies can be used to automatize mundane tasks and diversify the attention of Security Officers towards more essential and complex tasks. A reinforcement of the security team by machine learning solutions can also help Security Officers establish better response policies based on the type of malware identified.

In 2016 a Carnegie Mellon University team won a Cyber Grand Challenge organized by DARPA with their proposed *Mayhem* AI-based bug detector. Mayhem identifies bugs with the help of two techniques: fuzzing and symbolic execution. Fuzzing is a software exploration technique that inserts permutations of data such as strings, arrays, images etc. into the code. It explores potential bugs that are revealed as a result of the inference. Symbolic execution is a software debugging technique focusing on using mathematical models in which inputs crash the software. The development of Mayhem was a milestone for security automation. Those types of solutions are particularly relevant in addressing zero-day exploits. This is a type of breach in which the party managing the software is unaware of the vulnerability and leaves it open for exploitation. The automatic anomaly detection could shorten the response time of the security teams and prevent a lot of damage.

Security technologies for which developments in machine learning approaches are crucial are the Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Firewalls. The first kind is an alerting system that flags suspicious traffic and allows any traffic through. IPS is an alerting system equipped with a response toolkit, not allowing flagged content to pass through. Finally, a firewall is a kind of barrier that does not allow any traffic to pass through, apart from the content flagged as non-malicious. Machine learning helps IDS analyze patterns based on previously seen data and automatically detect different anomalies such as point, contextual and collective anomalies.

White hat hacking

Machine learning is a holy grail for black hat hackers as much as it is a nascent source of security for companies. We might be approaching the future where attacks will be performed primarily with AI, and response systems will also be AI-based.

In this "AI against AI" future, there will be a need for more machine learning implementation in white hat hacking. DeepLocker, developed at IBM Research, is an excellent example of the capabilities of AI-powered attacks. Scientists at IBM deliberately created AI-based malware to explore different ways in which machine learning can be weaponized in the security domain. The DeepLocker team exploited different ways in which attacked targets can be fulled by covering malicious software in benign-looking packets of data. In their research, they used publically available data of an individual to create facial recognition systems that would unlock devices and direct users to malicious links. These links, for example, included infected video conferences. More and more data is made publicly available and searchable through web scraping and searching using solutions. Companies like Clearview.ai, an American facial recognition startup, fed three billion publically available images into their systems. As a result of the availability of an immense amount of data, machine learning models can be trained in very sophisticated ways. Those new technological capabilities allow black hat hackers to weaponize AI to create new breeds of attacks that would be extremely difficult to counterattack using human resources only.

Deep fakes

The implications of poor security in the face of new breeds of malware will be particularly visible in the political arena. Deep fake is artificially created content, including voice and face swap of a person. It allows us to create authentic videos of people based on publicly available data. Researchers have already come up with frameworks for detecting deep fakes such as *FaceForensics++*. However, the detection

accuracy for compressed fake videos of lower quality is quite small. Manipulation of data using deep fakes or similar voice manipulation technologies opens a world of new possibilities for security breaches. In the uncertain times like the COVID-19 pandemic, more and more businesses move their work online. This trend is likely to persist as the job market becomes more digitized. Deep learning algorithms detecting deep fakes in video and voice message format would be essential for the well being of the digitized economies.

Sources

[1] https://www.oneconsult.com/wp-content/uploads/2017/05/computerworld-6-2017-ki-in-security.pdf

[2] https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity*Report*20190711_V06.pdf

[3] https://www.acatech.de/publikation/kuenstliche-intelligenz-und-it-sicherheit-bestandsaufnahme-und-loesungsansaetze/ (Germann)

[4] https://www.wired.com/story/bot-hunts-software-bugs-pentagon/

[5] https://www.normshield.com/machine-learning-in-cyber-security-domain-7-idsips-with-ml/

Image: shutterstock / Ryzhi

This article was published on the Search Guard blog: https://search-guard.com/blog/machine-learning-information-security/