

FEATURE

How to protect algorithms as intellectual property

Algorithms can now be considered trade secrets or even patent-worthy. Prevent them from being stolen by taking these security steps.

By Stacy Collett

Contributing Writer, CSO

JUL 13, 2020 3:00 AM PDT

Ogilvy is in the midst of a project that converges [robotic process automation](#) and Microsoft Vision AI to solve a unique business problem for the advertising, marketing and PR firm. Yuri Aguiar is already thinking about how he will protect the resulting algorithms and processes from theft.

[Keep up with 8 hot cyber security trends (and 4 going cold). Give your career a boost with top security certifications: Who they're for, what they cost, and which you need. | Sign up for CSO newsletters.]

“I doubt it is patent material, but it does give us a competitive edge and reduces our time-to-market significantly,” says Aguiar, chief innovation and transformation officer. “I look at algorithms as modern software modules. If they manage proprietary work, they should be protected as such.”

Intellectual property theft has become a top concern of global enterprises. As of February 2020, the FBI had about 1,000 investigations involving China alone for attempted theft of US-based technology spanning just about every industry. It's not just nation-states who look to steal IP; competitors, employees and partners are often culprits, too.

Security teams routinely take steps to protect intellectual property like software, engineering designs, and marketing plans. But how do you protect IP when it's an algorithm and not a document or database? Proprietary analytics are becoming an important differentiator as companies implement digital transformation projects. Luckily, laws are changing to include algorithms among the IP that can be legally protected.

Patent and classify algorithms as trade secrets

For years, in-house counsel rightly insisted that companies couldn't patent an algorithm. Traditional algorithms simply told a computer what to do, but AI and machine learning require a set of algorithms that enable software to update and "learn" from previous outcomes without the need for a programmer intervention, which can produce competitive advantage.

Tech Spotlight: Analytics


- How to choose a data analytics platform (InfoWorld)
- 6 best practices for business data visualization (Computerworld)
- Healthcare analytics: 4 success stories (CIO)
- SD-WAN and analytics: A marriage made for the new normal (Network World)
- How to protect algorithms as intellectual property (CSO)


"People are getting more savvy about what they want to protect," and guidelines have changed to accommodate them, says Mary Hildebrand, chair and founder of the privacy and cybersecurity practice at Lowenstein Sandler. "The US Patent Office issued some new guidelines and made it far more feasible to patent an algorithm and the steps that are reflected in the algorithm."


Patents have a few downsides and tradeoffs. "If you just protect an algorithm, it doesn't stop a competitor from figuring out another

algorithm that takes you through the same steps," Hildebrand says.

RECOMMENDED WHITEPAPERS

Cloud Volumes ONTAP


Cloud Volumes ONTAP for AWS: 10 Customer Success Stories


AWS use cases with NetApp Cloud Volumes ONTAP


What's more, when a company applies for a patent, it also must disclose and make public what is in the application. "You apply for a patent, spend money to do that, and there's no guarantee you're going to get it," says David Prange, co-head of the trade secrets sub-practice at Robins Kaplan LLP in Minneapolis.

Many companies opt to classify an algorithm as a trade secret as a first line of defense. Trade secrets don't require any federal applications or payments, "but you have to be particularly vigilant in protecting it," Prange adds.

To defend against a possible lawsuit over ownership of an algorithm, companies must take several actions to maintain secrecy beginning at conception.

Take a zero-trust approach

As soon as an algorithm is conceived, a company could consider it a trade secret and take reasonable steps to keep it a secret, Hildebrand says. "That would mean, for example, knowing about it would be limited to a certain number of people, or employees with access to it would sign a confidentiality agreement." Nobody would be permitted to take the algorithm home overnight, and it must be kept in a safe place. "Those are very common-sense steps but it's also very important if you're propelled to prove that something is trade secret."

On the IT front, best practices for protecting algorithms are rooted in the principles of a zero-trust approach, says Doug Cahill, vice president and group director of cybersecurity at Enterprise Strategy Group. Algorithms deemed trade secrets "should be stored in a virtual vault," he says. "The least amount of users should be granted access to the vault with the least amount of privileges required to do their job. Access to the vault should require a second factor of authentication and all access and use should be logged and monitored."

Confidentiality agreements for all

Companies should ensure that every employee with access to the project or algorithm signs a confidentiality agreement. Hildebrand recalls one inventor who met with three potential partners whom he believed were all representing the same company. He thought that he was covered by a confidentiality agreement signed by the company. It turned out that one of them was an independent consultant who hadn't signed anything and ran away with the IP. The inventor lost the trade secret status to his invention. Hildebrand always counsels clients going into those meetings to make sure everyone in the room has signed.

Another reason to take signed confidentiality agreements seriously: "Engineers and scientists in particular love to talk to their peers about what they're working on," which is fine when they're working in teams and learning from one another, Hildebrand says, but it's not OK when they go out to dinner with competitors or discuss their research at the neighborhood BBQ.

Small teams and need-to-know access

Consider who really needs to have first-hand knowledge of the project or algorithm, Prange says. In smaller companies, people wear more hats and may need to know more, but in larger, more diversified companies, fewer people need to know everything. Even with a small group having access, "maybe use two-factor authentication, limit whether you can work on things outside the company or the physical building. Or you lock down computers so you can't use thumb drives," he adds.

Educate lines of business on protecting algorithms

IT leaders must educate lines of business so they understand what it is they need to protect and investments the company is making, Prange says. For instance, "Salespeople like to know a lot about their products. Educate them on what aspects of the product are confidential."

Don't let departing employees take algorithms with them

Make sure employees know what they can't take with them when they leave for another job. "Whenever there's an employee working in a sensitive area or has access to sensitive information, they should be put through an exit interview to understand what they have and to emphasize that they have these signed obligations" that prohibit them from using the information in their next job, Prange says.

Partnerships should be treated the same way, Prange adds. "We see a lot of cases where a company is in a joint development relationship and it sours or fizzles out, and one or both of the companies may independently move on. Then suddenly there's a dispute when one hits the market with the information they were sharing."

Establish proof you own an algorithm

"Tried and true tactics will clearly be employed to gain access to algorithms, including socially engineered spear-phishing attacks to steal developer credentials via bogus login and password reset pages to gain access to the systems that store such intellectual property," Cahill says.

It's hard to protect against someone with the intention of taking an algorithm or process, Prange says. "You can have all kinds of restrictions, but if someone has the intent, they're going to do it — but that doesn't mean you don't do anything."

To help prove ownership of an algorithm and prevent theft or sabotage, IBM and others have been working on ways to embed digital watermarks into the deep neural networks in AI, similar to the multimedia concept of watermarking digital images. The IBM team's method, unveiled in 2018, allows applications to verify the ownership of neural networks services with API queries, which is essential to protect against attacks that might, for instance, fool an algorithm in an autonomous car to drive past a stop sign.

The two-step process involves an embedding stage, where the watermark is applied to the machine learning model, and a detection stage, where it's extracted to prove ownership.

The concept does have a few caveats. It doesn't work on offline models, and it can't protect against infringement through "prediction API" attacks that extract the parameters of machine learning models by sending queries and analyzing the responses.

Researchers at KDDI Research and the National Institute of Informatics have also introduced a method of watermarking deep learning models in 2017.

Another problem with many watermark solutions is that current designs have not been able to address piracy attacks, where third-parties falsely claim model ownership by embedding their own watermarks into already-watermarked models.

In February 2020, researchers at The University of Chicago unveiled “null embedding,” a way to build piracy-resistant watermarks into deep neural networks (DNNs) at a model’s initial training. It builds strong dependencies between the model’s normal classification accuracy and the watermark, and as a result, attackers can’t remove an embedded watermark or add a new pirate watermark to an already-watermarked model. These concepts are in the early stages of development.

Next read this

- [*Hacking 2FA: 5 basic attack methods explained*](#)
- [*8 things CISOs should be thinking about, but probably aren't*](#)
- [*The 10 most dangerous cyber threat actors*](#)
- [*6 minimum security practices to implement before working on best practices*](#)
- [*How to rob a bank: A social engineering walkthrough*](#)
- [*How API attacks work, and how to identify and prevent them*](#)
- [*17 cyber insurance application questions you'll need to answer*](#)
- [*6 most common types of software supply chain attacks explained*](#)
- [*DarkSide ransomware explained: How it works and who is behind it*](#)
- [*Booming dark web gig economy is a rising threat*](#)

Stacy Collett is a contributing writer for Computerworld, CSO, and Network World, covering a variety of security and risk issues.

Follow     

SPONSORED LINKS

Truly modern web app and API security thinking. It's a thing. See how.

dtSearch® instantly searches terabytes of files, emails, databases, web data. See site for hundreds of reviews; enterprise & developer evaluations

Cisco SecureX Simplify with the broadest, most integrated security platform

Reliable remote networks. Set up remote work quickly. Get secure remote network access.

See how the new Webex Suite powers the McLaren F1 Team.

NETSCOUT Visibility Without Borders helps you see it all from the data center to the cloud, and everywhere in between.

Reimagine remote work to catch the next wave in digital transformation. Read e-book

Bridge the clouds you have to the experience you want. Get started, today

Preparing Your Technology Foundation for a New Hybrid World

Getting a Grip on Basic Cyber Hygiene with the CIS Controls