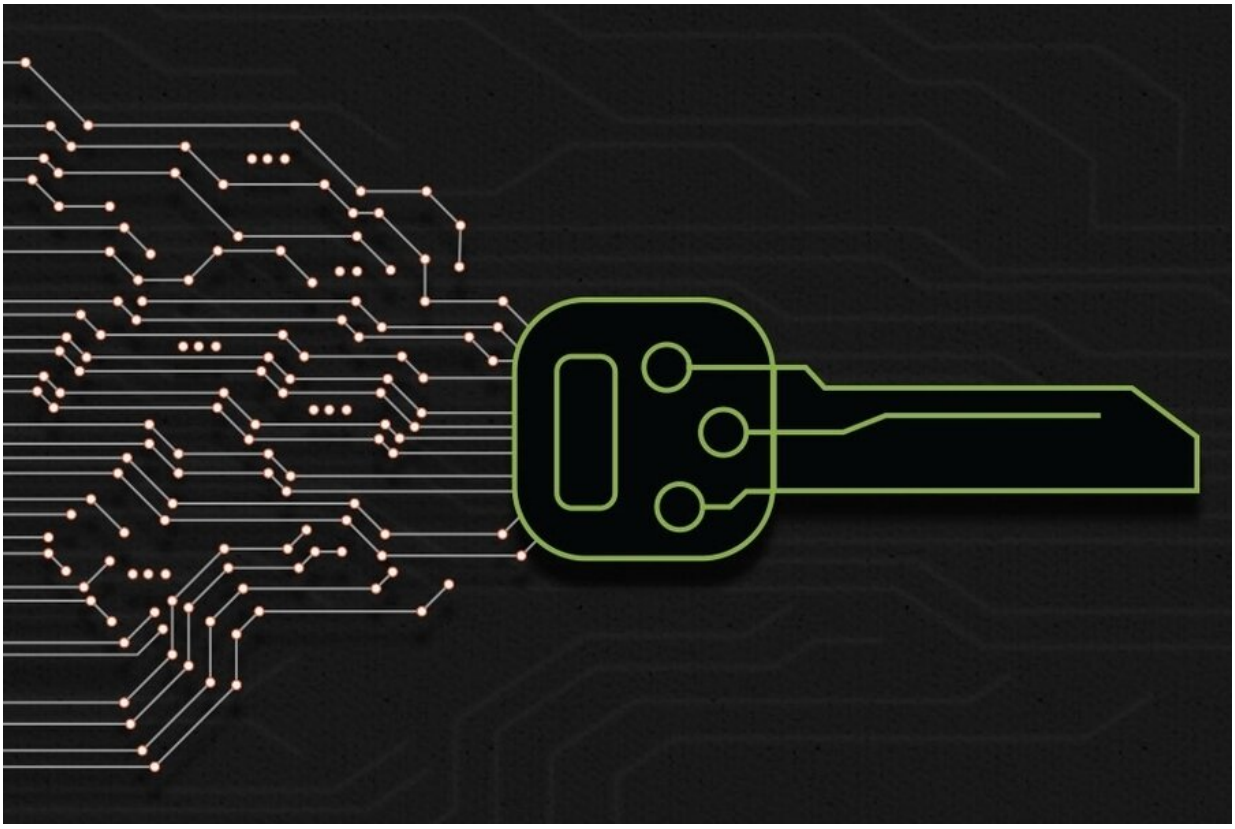
Helping companies prioritize their cybersecurity investments

September 4 2020, by Adam Conner-Simons



By securely aggregating sensitive data from cyber-attacks, CSAIL's SCRAM platform can quantify an organization's level of risk and suggest how to prioritize security investments. Credit: Chelsea Turner

One reason that cyberattacks have continued to grow in recent years is

that we never actually learn all that much about how they happen. Companies fear that reporting attacks will tarnish their public image, and even those who do report them don't share many details because they worry that their competitors will gain insight into their security practices.

"It's really a nice gift that we've given to cyber-criminals," says Taylor Reynolds, technology policy director at MIT's Internet Policy Research Initiative (IPRI). "In an ideal world, these attacks wouldn't happen over and over again, because companies would be able to use data from attacks to develop quantitative measurements of the security risk so that we could prevent such incidents in the future."

In an economy where most industries are tightening their belts, many organizations don't know which types of attacks lead to the largest financial losses, and therefore how to best deploy scarce security resources.

But a new platform from MIT's Computer Science and Artificial Intelligence Laboratory (CSAIL) aims to change that, quantifying companies' security risk without requiring them to disclose sensitive data about their systems to the research team, much less their competitors.

Developed by Reynolds alongside economist Andrew Lo and cryptographer Vinod Vaikuntanathan, the platform helps companies do multiple things:

- quantify how secure they are;
- understand how their security compares to peers; and
- evaluate whether they're spending the right amount of money on security, and if and how they should change their particular security priorities.

The team received internal data from seven large companies that

averaged 50,000 employees and annual revenues of $24 billion. By securely aggregating 50 different security incidents that took place at the companies, the researchers were able to analyze which specific steps were not taken that could have prevented them. (Their analysis used a well-established set of nearly 200 security actions referred to as the Center for Internet Security Sub-Controls.)

"We were able to paint a really thorough picture in terms of which security failures were costing companies the most money," says Reynolds, who co-authored a related paper with professors Lo and Vaikuntanathan, MIT graduate student Leo de Castro, Principal Research Scientist Daniel J. Weitzner, Ph.D. student Fransisca Susan, and graduate student Nicolas Zhang. "If you're a chief information security officer at one of these organizations, it can be an overwhelming task to try to defend absolutely everything. They need to know where they should direct their attention."

The team calls their platform "SCRAM," for "Secure Cyber Risk Aggregation and Measurement." Among other findings, they determined that the three following security vulnerabilities had the largest total losses, each in excess of $1 million:

Failures in preventing malware attacks

Malware attacks, like the one last month that reportedly forced the wearables company Garmin to pay a $10 million ransom, are still a tried-and-true method of gaining control of valuable consumer data. Reynolds says that companies continue to struggle to prevent such attacks, relying on regularly backing up their data and reminding their employees not to click on suspicious emails.

Communication over unauthorized ports

Curiously, the team found that every firm in their study said they had, in fact, implemented the security measure of blocking access to unauthorized ports—the digital equivalent of companies locking all their doors. Even still, attacks that involved gaining access to these ports accounted for a large number of high-cost losses.

"Losses can arise even when there are defenses that are well-developed and understood," says Weitzner, who also serves as director of MIT IPRI. "It's important to recognize that improving common existing defenses should not be neglected in favor of expanding into new areas of defense."

Failures in log management for security incidents

Every day companies amass detailed "logs" denoting activity within their systems. Senior security officers often turn to these logs after an attack to audit the incident and see what happened. Reynolds says that there are many ways that companies could be using machine learning and artificial intelligence more efficiently to help understand what's happening—including, crucially, during or even before a security attack.

Two other key areas that warrant further analysis include taking inventory of hardware so that only authorized devices are given access, as well as boundary defenses like firewalls and proxies that aim to control the flow of traffic through network borders.

The team developed their data aggregation platform in conjunction with MIT cryptography experts, using an existing method called multi-party computation (MPC) that allows them to perform calculations on data without themselves being able to read or unlock it. After computing its anonymized findings, the SCRAM system then asks each contributing company to help it unlock only the answer using their own secret cryptographic key.

"The power of this platform is that it allows firms to contribute locked data that would otherwise be too sensitive or risky to share with a third party," says Reynolds.

As a next step, the researchers plan to expand the pool of participating companies, with representation from a range of different sectors that include electricity, finance, and biotech. Reynolds says that if the team can gather data from upwards of 70 or 80 companies, they'll be able to do something unprecedented: put an actual dollar figure on the risk of particular defenses failing.

More information: Secure Cyber Risk Aggregation and Measurement: scram.mit.edu

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology