Protecting Your Robots: How to Design Security into Your Machines

Authors

Satish Thiagarajan
Vice President and Global Head, Cyber Security, Tata Consultancy Services

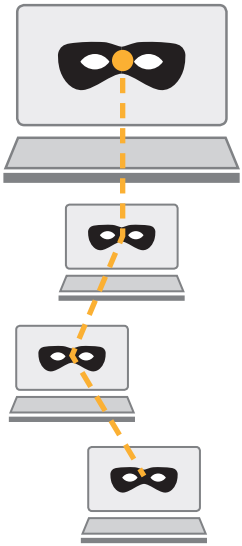
Sundeep Oberoi
Global Head, Enterprise Security & Risk Management,
Tata Consultancy Services

For many organizations, automating hundreds or thousands of manual tasks has become a competitive necessity. However the same attributes that make automation so effective also open up organizations to new risks.

The reason: Because AI enables a company to remotely manage machines and make them interact with other machines, bad actors could take control of the technology and wreak havoc.

Consider the common threats to a computer network: malignant software such as viruses and phishing emails for tricking people into revealing valuable information. If a worker clicks on a malware link and damages his computer on the network, the virus can spread to others. As a result, other workers on the network must then decide whether

to click on the malicious link. In contrast, when you take people out of a business process, a virus that finds its way on an automated machine-to-machine network spreads much faster, worsening the impact.



Now consider a bad actor who uses AI to do his nefarious deeds. That person could break into a network and scoop up information about a company's employees. Then, using AI to personalize text and images (i.e., showing pictures of familiar people), the hacker could convince employees to share customer data, or blackmail the company through a ransomware attack. ("Pay me $500,000 or I'll leak the data," the threat might be.)

Enterprise leaders are aware of this need. In 2016, General Motors CEO, Mary Berry, said the auto industry had to protect self-driving cars from cyberattacks "as a matter of public safety."[46] Among the risks highlighted in the Information Security Forum's 2019 and 2020 "threat horizon" alerts were bad actors using AI for malicious intent. For example, AI systems can automatically spread convincing misinformation.[47] Bad actors are expected to use AI "to develop malware that can learn from its surrounding environment and adapt to discover new vulnerabilities."[48] Notes a chief data protection officer at a major pharmaceutical firm: "Once AI technologies are widely available, cybercriminals will be able to launch a new wave of sophisticated attacks that may evade most traditional security-detection and monitoring tools."[49]

[46] Simson, Garfinkel, "Hackers Are the Real Obstacle for Self-Driving Vehicles," MIT Technology Review, August 22, 2017, accessed at: https://www.technologyreview.com/s/608618/hackers-are-the-real-obstacle-for-self-driving-vehicles/

[47] Information Security Forum, "Threat Horizon 2019," March 2017, accessed at: https://www.securityforum.org/uploads/2017/03/ISF_Threat-Horizon-2019_Report_PWS.pdf.

[48] Information Security Forum, "Threat Horizon 2020: Executive Summary," March 2018, accessed at: https://www.securityforum.org/uploads/2018/03/ISF_Threat-Horizon-2020_Executive-Summary-1.pdf.

[49] Scot Finnie, "Cyber threats fueled by AI: Security's next big challenge," CSO, October 30, 2018, accessed at: https://www.csoonline.com/article/3315740/cyber-threats-fueled-by-ai-securitys-next-big-challenge.html.

While machine-to-machine communications may obviate the need for human intervention, IT managers must rethink how they provide security clearance to access their growing number of automated systems. Even when a machine gets an automated request from another machine (rather than a person) to retrieve some data, the first machine must be able to rigorously authenticate the request. This is a new challenge for firms whose information systems are largely accessed by people and not by other computers. If a primary goal of AI-driven automation is to eliminate unnecessary manual work within and across departments, many of these companies are less likely to have enough security built into their machines.

This article will explain why many conventional computer security approaches are now inadequate in this Business 4.0 era of rampant automation and AI. We will discuss how to tighten security, a key tactic of which requires using AI. ***AI and machine learning algorithms can be used to thwart such attacks by detecting code patterns used in previous attacks, and using those insights to identify new threats.***

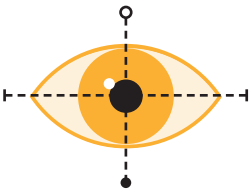
The Vulnerabilities of Existing Approaches

While CIOs have great interest in AI, IT security is of greater interest, according to a 2018 Gartner survey. Some 88% of 3,000 CIOs said cybersecurity was a top focus, more than double the number who said AI (37%).[50]

It's taken years—and many highly publicized data breaches, government regulations, and penalties—for companies to build effective IT security defenses. However, they have largely designed their approaches to thwart human attacks on machines—i.e., to stop the evil but skillful hacker. Guarding such systems begins with the people who manage them (such as system administrators) and people who use them (employees, business partners, customers). Passwords have served as a foundational human-computer gate-check. If you know the password, you have the authority to use this system.

[50] "Gartner Survey of More Than 3,000 CIOs Reveals That Enterprises Are Entering the Third Era of IT," October 16, 2018, Gartner press release accessed at: https://www.gartner.com/en/newsroom/press-releases/2018-10-16-gartner-survey-of-more-than-3000-cios-reveals-that-enterprises-are-entering-the-third-era-of-it.

However, in a world of rampant automation, passwords have glaring weaknesses. They are vulnerable to sharing, and thus being hijacked to access multiple systems. People write them down and share them. Moves to strengthen passwords have focused on securing people's access to machines. Two-factor authentication, such as when a user receives a text message, is a second checkpoint for someone with a password. Hardware such as USB fobs act as a digital key to unlock computer access. Other techniques, like a fingerprint reader or facial recognition



system, use a person's fingerprint or facial appearance, to authenticate an authorized user's identity. But all of these approaches are limited to protecting computers against unwarranted entry by people.

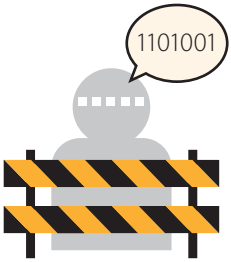
These techniques were designed to let one person access a machine and do many tasks. The same theme applies to a system administrator who uses a script, or program, that enables her to manage many computers. With one script, an administrator can update software security patches on 1,000 servers. The problem, again, is that one script provides a green light to many machines. Like a password or a fingerprint reader, it does not account for the prospect of machine-to-machine connections.

The security model must be upgraded when machines interact with other machines. We can tell workers not to put Post-it Notes passwords on their computer screen. We can tell them not to leave their computers running and unattended, and not to click on untrustworthy email links. We can institute network security protocols to detect and block network intrusions. All of these moves can reduce the chances of unwanted access to valuable systems.

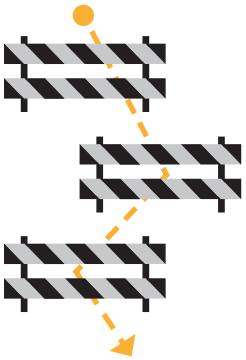
The trouble comes when an automated process lets machines communicate with other machines. Passwords and other conventional checks won't be nearly enough. We need better ways for machines to detect and deny access from the illegitimate machines.

Three Keys to Protecting Your Robots

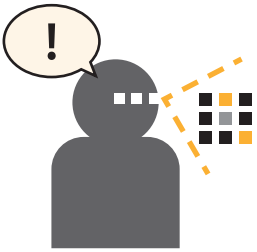
Three moves will go a long way toward securing your robots, both of the hardware and software types:



Managing credentials for machines. Building new gates that require the machines to present the right credential, like a form of password or a digital identifier, so that a machine can verify that another machine has access rights. Using specialized hardware to store and safeguard passwords is one technique. Cryptography, in which automated parties exchange digital signatures to authenticate their interactions, is another.



Tighten systems' ports of entry through 'fine-grained' access. A traditional system administration approach is having one remote administration account to access multiple devices on a network. From a risk perspective, it would be better to create separate accounts for each asset, down to individual items like a shared printer. Why so granular? Attackers seek out often-overlooked access points (such as remote management of a printer) to gain access to a corporate network. Requiring authentication to access every asset reduces this risk.



Use AI for defense. As noted, bad actors can use AI to personalize phishing emails and otherwise accelerate their efforts. But AI can also be used against them. Security experts can develop systems using AI and machine learning to analyze various threats—network intrusions, distributed denial-of-service attacks, viruses in emails, phishing scams—and identify patterns of behavior. AI and deep learning approaches have detected and prevented malware by analyzing its software code.

AI can strengthen existing anti-virus software, which use more reactive approaches. These conventional tools check for patterns too, but they are vulnerable when bad actors change course and create new methods. It can take time for conventional anti-virus systems to catch up.

The use of AI in IT security is an emerging field. Yet it's also one of great interest. A SANS Institute survey found that 57% of firms from a range of industries were implementing, or planning to implement, security solutions that use AI.[51] In the United States, financial services firms, encouraged by government regulators to explore new ways to fight corruption, are exploring the use of AI to detect money laundering and disrupt terrorists' financing.[52] IDC projects banks globally will spend $5.6 billion this year on AI-enabled automated threat identification and prevention, fraud analysis, and investigation systems.[53]

As they secure their systems, enterprise leaders should monitor the legal and regulatory landscapes in the geographies in which their companies operate. A number of countries are likely to develop laws that penalize perpetrators for their involvement in damaging cyberattacks. They are also likely to establish regulations that require corporations to show they have made every effort to secure their systems—and to account for their actions. That means that as the regulatory landscape takes shape, leaders must also ensure that their AI systems are trained in a way that prevents their robots from turning rogue.

[51] G.W. Ray Davidson and Barbara Filkins, "Security Gets Smart with AI," SANS Institute, March 2019. Press release accessed at: https://www.sans.org/press/announcement/2019/03/14/1.

[52] Dean DeChiaro, "Hunting money launderers? There's AI for that," Roll Call, March 26, 2019, accessed at: https://www.rollcall.com/news/policy/artificial-intelligence-fintech-money-laundering.

[53] IDC, "Worldwide Spending on Artificial Intelligence Systems Will Grow to Nearly $35.8 Billion in 2019," press release, March 11, 2019, accessed at: https://www.idc.com/getdoc.jsp?containerId=prUS44911419.

Raising Awareness of Security Benefits

Tightening IT security in the ways we've mentioned takes time and money. As a result, some leaders may balk and hope present security procedures and processes are adequate. That's why it's crucial to make leaders aware of the threats of a security breach or virus outbreak.

Another challenge is keeping up with the pace of emerging threats. That's why technology companies are making huge investments in AI-based security solutions.

Converting manual work into automated work is making companies more competitive. But the machines that are doing the work that people once did are subject to cyberattacks too. Protecting them from the new wave of human and robotic hackers has become paramount.

As they secure their systems, enterprise leaders should monitor the legal and regulatory landscapes in the geographies in which their companies operate.