PHYS.ORG

What can we learn about cybersecurity from the Russian hacks?

January 24 2017, by Thea Singer

Intelligence reports about Russian-sponsored hacking to influence the 2016 presidential election have dominated headlines. Northeastern professors Alina Oprea and Cristina Nita-Rotaru, both cybersecurity experts, explain what these break-ins tell us about the state of U.S. cybersecurity, whether an impenetrable system is even possible, and how such attacks might be prevented in the future. Image by iStock

On Inauguration Day, NBC News reported that the FBI—aided by the CIA, the National Security Agency, and the Treasury Department—was carrying out a counter-intelligence investigation to learn how, as NBC's

Ken Dilanian put it, "Russia's efforts to manipulate public opinion in the U.S. presidential election…was paid for and whether any Americans were involved." The month before, myriad news outlets reported Russia's hacking of the Democratic National Committee and other political organizations to influence the election, with both the CIA and FBI agreeing about the source and aim of the hacks.

We asked two Northeastern faculty and cybersecurity experts—associate professor Alina Oprea and professor Cristina Nita-Rotaru—to explain what these break-ins tell us about the state of U.S. cybersecurity, whether an impenetrable system is even possible, and how such attacks might be prevented in the future.

What do these break-ins tell us about the state of cybersecurity in the U.S.?

Oprea: Rather than informing us about the state of cybersecurity in the U.S. only, these attacks provide a picture on the state of cybersecurity on the global scale. They demonstrate that attackers are becoming increasingly sophisticated in developing new ways to gain remote access to critical systems. For instance, using various sources of reconnaissance, such as social networks and news reports, attackers are able to craft so-called spear-phishing emails that impersonate legitimate senders and look credible to human users. In the recent Russian campaigns, the attackers sent emails that were very similar to emails automatically sent by Google when suspicious activity in users' Gmail accounts is detected. Users were asked to change their Gmail passwords and redirected to a site controlled by attackers.

The "watering-hole attack" is another infection vector hackers are increasingly adopting. Here they silently inject lists of malicious commands, called "scripts," or pieces of software called "exploits" that take advantage of a vulnerability in legitimate websites. Similar to how predators in the natural world wait for their desired prey near watering holes, these attackers wait for their victims at "water-holed" websites.

Why is it so difficult to protect against computer hacks and other cybercrimes?

Nita-Rotaru: One of the principles of computer and network security is that a system is as secure as the weakest link. Most of the time humans are the weakest link. This is not to say that computers do not have vulnerabilities, but even if all the technical problems are addressed, the human in the loop remains a crucial element. A simple example is the fact that we require identifying secrets and passwords that a person must remember and change properly; many systems are broken because default passwords are not changed on accounts or devices.

Another comment you often hear about security is "Security is an add-on." The beauty of computing systems and software is that the pace of innovation keeps up with the services we as customers like. Security is not one of the services; it is an add-on and often perceived as a cost. Without legislation to enforce it and without customers' refusing to use services that are not secure, there is little incentive to provide it. It's also not clear that users are necessarily ready to pay for security.

The American Enterprise Institute's report, "An American Strategy for Cyberspace," notes that cyberspace "permeates every element of modern societies." How would you describe that all-encompassing network?

Nita-Rotaru: A joke in computer security is "If you want a secure system, lock it in a safe." Today everything is connected: Even devices that you might not consider part of a system, such as appliances (refrigerators, coffee machines, etc.), are connected to the internet. We want them to be connected because then we can control them remotely, but that also makes them vulnerable.

Given the ubiquity of cyberspace, what can we do to prevent cyberattacks in the future?

Oprea: I believe that the challenges of securing cyberspace can only be addressed by collaborative efforts, including data sharing and joint research, among the government, states, public and private institutions, and academic researchers. The American Enterprise Institute's report mentions the Cybersecurity Information Sharing Act, which creates a framework for organizations to share threat intelligence data. For instance, an organization that has been breached can share the details of the attack with other organizations, helping them to increase their resilience against the same attack. I believe that more investment is needed in the near future to enable threat-sharing platforms to effectively disseminate breach information in a timely manner.

There is also huge potential for security researchers to explore new advances in machine learning and data analytics to create more intelligent defenses and predicting adversaries' next steps. As a longer-term goal, the U.S. should create additional infrastructure for cybersecurity research, in which academics get access to realistic datasets and testbeds provided by industry and governments, as well as realistic attack scenarios, transforming cybersecurity research into a more rigorous discipline.

Is it possible to design a truly impenetrable system? If not, why?

Oprea: Given all these factors—human elements and the existence of technical vulnerabilities in software—it is indeed impossible to design a truly impenetrable system. However, my view is that we should think about system security holistically, that is, as including multiple levels of defense. Each level can be defeated with certain resources by attackers and protected at some cost by defenders. In such a view, a password simply provides one level of defense, but the security of the whole system should not completely break if the password is compromised. I believe that machine-learning based techniques applied to various security data, such as network traffic and system logs, have great potential to provide additional defenses.

In the context of the Russian attacks, for example, it might have been impossible to prevent users from clicking on the spear-phishing emails they received. However, machine-learning techniques could have readily detected when a user's machine established a connection to an external internet protocol located in Russia and sent gigabytes of data (the DNC's exfiltrated emails). The key challenges are to reduce false positives (legitimate activities that result in anomalies), detect the attacks early in their development, and enable rapid response to remediate the breach.

Provided by Northeastern University

Citation: What can we learn about cybersecurity from the Russian hacks? (2017, January 24) retrieved 18 April 2024 from https://phys.org/news/2017-01-cybersecurity-russian-hacks.html