Seek

Volume 12
Issue 1 *Sring 2022*

Article 7

April 2022

Behind the Code: Researchers Tackle the New World Of Cybersecurity

Jennifer Tidball
Kansas State University


BEHIND THE
CODE

RESEARCHERS TACKLE THE NEW WORLD OF CYBERSECURITY

By Jennifer Tidball

Kansas State University cybersecurity researchers want you to know the difference between the stereotype of cybersecurity and the reality of it.

The stereotype: Cyberattacks are committed by hooded hackers cracking code to infiltrate our security systems.

The reality: Cyberattacks certainly can happen that way, but it's much more likely to come in the form of vulnerable and outdated hardware and software, social engineering, phishing scams and ransomware.

That reality can be a pretty scary place. An outdated piece of software can make an autonomous vehicle susceptible to cyberattacks. Clever social engineering can cause an unknowing employee to provide access to sensitive documents. Terrorists can take advantage of weaknesses in our infrastructure, such as power grids and water treatment plants. The things that make our life easier, such as smart doorbells or home security systems, also have the potential to be misused.

As the world becomes more computerized, we also become more vulnerable.

"A great example of the risks we face can be seen in Ukraine where several types of destructive malware aimed at government and financial organizations were deployed in the hours leading up to the invasion," said Scott DeLoach, head of the computer science department in the Carl R. Ice College of Engineering.

That's why K-State researchers are working behind the code to navigate the new world of cybersecurity and to keep our data, our infrastructure and our world safe.

Eugene Vasserman

A cybersecurity center of excellence

K-State has long been a research leader in the cybersecurity realm, thanks to the nationally recognized Center for Information and Systems Assurance. Since 2010, the center has held the designation of a National Center of Academic Excellence in Cyber Defense Research from the National Security Agency and Department of Homeland Security.

The center's multipronged mission is to conduct fundamental and applied research in information assurance and computer security; to advance student knowledge; and to engage the professional community.

"Our nation is at risk for cyberattacks," said Eugene Vasserman, center director. "Our critical infrastructure is vulnerable at all scales, from individual water treatment plants to large sections of the power grid."

The looming threat of cyberattacks is what motivates Vasserman and other affiliated researchers to study all areas related to cybersecurity. The center involves more than 16 researchers across multiple disciplines, including computer science; psychological sciences; sociology, anthropology and social work; electrical and computer engineering; physics; and communication studies.

The researchers study important topics such as digital literacy, security and safety online, social media, privacy, machine learning and artificial intelligence.

"We have a very diverse group of members to work with cybersecurity from a holistic perspective," said Vasserman, also an associate professor of computer science and a Michelle Munson-Serban Simu Keystone research scholar. "Cybersecurity is all-encompassing. It's not just technological solutions; it's a sociotechnical field that needs to also consider how groups and individuals interact with technology on a daily basis."

Arslan Munir

Safety and security

Arslan Munir, associate professor of computer science, takes a novel research approach by involving both safety and security — two key pieces to addressing cybersecurity.

While security involves stopping an intentional adversary, such as a hacker, safety involves addressing something unintentional, such as autonomous vehicle electronics failing.

"My research targets both safety and security because the end effect is similar," said Munir, also a Michelle Munson-Serban Simu Keystone research scholar and director of the Intelligent Systems, Computer Architecture, Analytics and Security Laboratory. "That's why we have to prepare for both."

Munir's team focuses on four areas of cybersecurity research:

- Autonomous vehicles. Munir works to help autonomous vehicles operate safely and securely while adhering to real-time constraints — such as braking at a red light or responding to changing road conditions.
- Hardware-based security for lightweight applications. The team is designing circuits that communicate securely and efficiently with other circuits, which is key for devices — such as smart doorbells, home security cameras or building access control — connected through the Internet of Things.
- Artificial intelligence. Munir is helping make devices that use artificial intelligence — such as autonomous vehicles — more resilient and less susceptible to cyberattacks on the artificial intelligence of the devices.
- Situational awareness. Munir's research has applications for the U.S. military, which uses sensors and devices for situational awareness to understand an environment and take action. For example, if a video camera sensor is providing data on an area, it is important that the sensor provides accurate data and cannot be hacked by an adversarial player.

Munir's work has been supported by organizations such as NASA, the National Science Foundation, the Air Force Office of Scientific Research, the Air Force Research Laboratory and Semiconductor Research Corporation. His hardware security research has generated two patents through K-State Innovation Partners.

The privacy of social networks

How much information we do and don't share online through social media and social networks plays a key role in privacy and cybersecurity.

"How people reason about digital security is very different from how they think about their physical safety and security," Vasserman said. "We have millennia of experience in instinctive, subconscious reasoning about the physical world, but these 'mental shortcuts' can mislead us online. By drawing clear parallels between the physical and the digital, we can encourage people to use existing mental processes to more accurately evaluate digital risk."

"How people reason about digital security is very different from how they think about their physical safety and security."

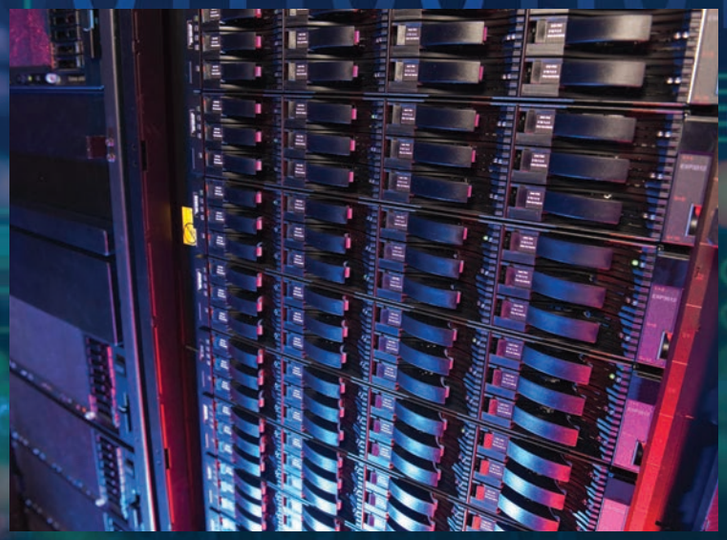
— Eugene Vasserman, associate professor of computer science

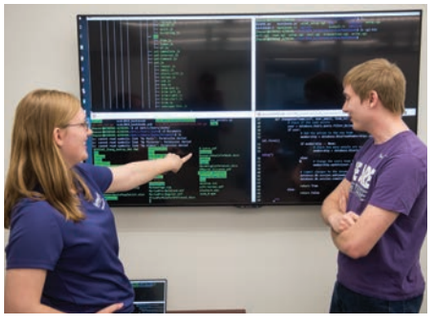
Vasserman is collaborating with George Amariucai, associate professor of computer science, on several projects related to digital literacy. The work involves social media, misinformation and disinformation and the privacy of social networks.

"We are investigating how targeted manipulation efforts can be more successful by collecting information from the targets' social media profiles and behaviors," said Amariucai, also a Michelle Munson-Serban Simu Keystone research scholar. "Privacy mechanisms can then be employed to thwart such attempts, thus lowering users' susceptibility to being manipulated."

Amariucai leads the Probabilistic and Information Theoretic Security, or PITS, Laboratory and is involved in multiple cybersecurity projects that have been supported by the National Science Foundation.

His work focuses on several areas related to privacy: privacy metrics under incomplete statistical information; privacy-utility solutions for dynamic environments with future uncertainty and constraints; privacy-utility strategies in human interactions on social media; and privacy as a defense strategy against stealthy attacks on cyber-physical systems, such as the power grid.





Computer science students collaborate on a project.

Opportunities for students

K-State's work in cybersecurity includes educational and research programs for undergraduate and graduate students. Through university initiatives and nationally funded programs, K-State is helping produce high-quality graduates to meet national, state, local and tribal government demand for skilled cybersecurity personnel.

The K-State Center for Information and Systems Assurance has offered the CyberCorps®: Scholarship for Service program for more than 10 years. The scholarship program, recently funded by a more than $3 million renewal from the National Science Foundation, supports undergraduate and graduate students who are interested in cybersecurity research and practice.

The university also continues restructuring and improving interdisciplinary cybersecurity curriculum.

Robby

John Hatcliff

High-stakes cybersecurity

A high-stakes element of cybersecurity involves military- and defense-related systems. Two K-State researchers are up for the challenge.

John Hatcliff, university distinguished professor of computer science, and Robby, professor of computer science and Don and Linda Glaser — Carl and Mary Ice Keystone research scholar, work to make U.S. military operations more secure. Their research has received funding from the U.S. Army, the U.S. Air Force and the Defense Advanced Research Projects Agency, or DARPA. They also have collaborated with Collins Aerospace.

The technology that Hatcliff and Robby have developed has been successfully used in DARPA demonstrations to provide cyber assurance for the mission control software on CH-47 Chinook helicopters.

Through a partnership with Adventium Labs, they are using an Air Force Phase II Small Business Innovation Research award to make aircraft more secure. They are addressing information security vulnerabilities in complex cyber-physical systems.

Research from Hatcliff and Robby covers other important military-related topics, such as ways to better secure systems on fighter planes or ways to rapidly update the software on a tank with new capabilities without interfering with the vehicle's existing functionality.

But their work has applications beyond the military as well. While their U.S. Department of Defense-funded projects are improving important military technology — such as self-driving cars, tanks and unmanned aerial vehicles — the same computer architecture can apply to biosecurity, precision agriculture and automated farming.

"The same technologies we are working on for military control systems and information systems can be applied to the automation of experiments or agriculture," said Hatcliff, also the Lucas-Rathbone professor in engineering. "There is an opportunity to take a holistic view to automation controls where the platforms and architectures we are working on can be applied broadly to automated agriculture, advanced manufacturing and biosecurity."

Kevin Steinmetz

The social science of cybercrime

Many cybersecurity incidents start with a social engineering element. Think deceptive phishing emails with website links to steal personal information or a cybercriminal using a false identity to trick someone into giving up information.

Criminologist Kevin Steinmetz, professor of sociology, anthropology and social work in the College of Arts and Sciences, is studying how and why social engineering works and how to prevent it. He also is collaborating with law enforcement to better understand cybercrime.

For one project, Steinmetz is using a three-year, $350,000 National Science Foundation grant to study social engineering and online fraud. Through 54 interviews with information technology professionals and social engineers, Steinmetz created tips for developing and implementing policy recommendations to improve cybersecurity at organizations.

"Effective policies are those that are adequately communicated to organizational members," Steinmetz said.

On another three-year, nearly $500,000 NSF grant, Steinmetz is working with law enforcement to help with cybercrime investigations. The project is a collaboration with Indiana University Southeast.

The researchers are interviewing cybercrime law enforcement who investigate internet crimes against children, network intrusions or cyber fraud. While previous research has been more survey-focused, Steinmetz and his collaborators took a different approach and have conducted 47 in-depth interviews with people at six different policing units at the local, state and federal level. They are now finalizing the data for publication.

"We wanted to get more of a boots-on-the-ground perspective of what are the challenges that law enforcement deal with in grappling with cybercrime investigations," Steinmetz said. "We are also interested in how this type of work affects how they view themselves as police, because this is very different work than what we stereotypically associate with law enforcement."

Steinmetz also is working on updates to "Cybercrime and Society," a book he co-authored with Majid Yar. It is one of the leading textbooks on the social science of cybercrime. *k*

Seek more

Read more about cybersecurity research at K-State.
k-state.edu/seek

Tips to prevent social engineering

K-State criminologist Kevin Steinmetz has developed the following tips to help organizations develop policies that help prevent social engineering.

- Educational programs, such as security awareness training, are key to communicating effective policy to organizational members.
- Policies should be effectively written.
- Policies should be tested to measure their effectiveness.
- Technology security measures, such as automated email warnings from outside organizations, should be implemented to support policies.
- Organizations should invest sufficiently in human resources to support policies and good security.
- Leadership matters and organizational administration should champion security.
- Organizations should be structured to support security through a diffusion of responsibility.