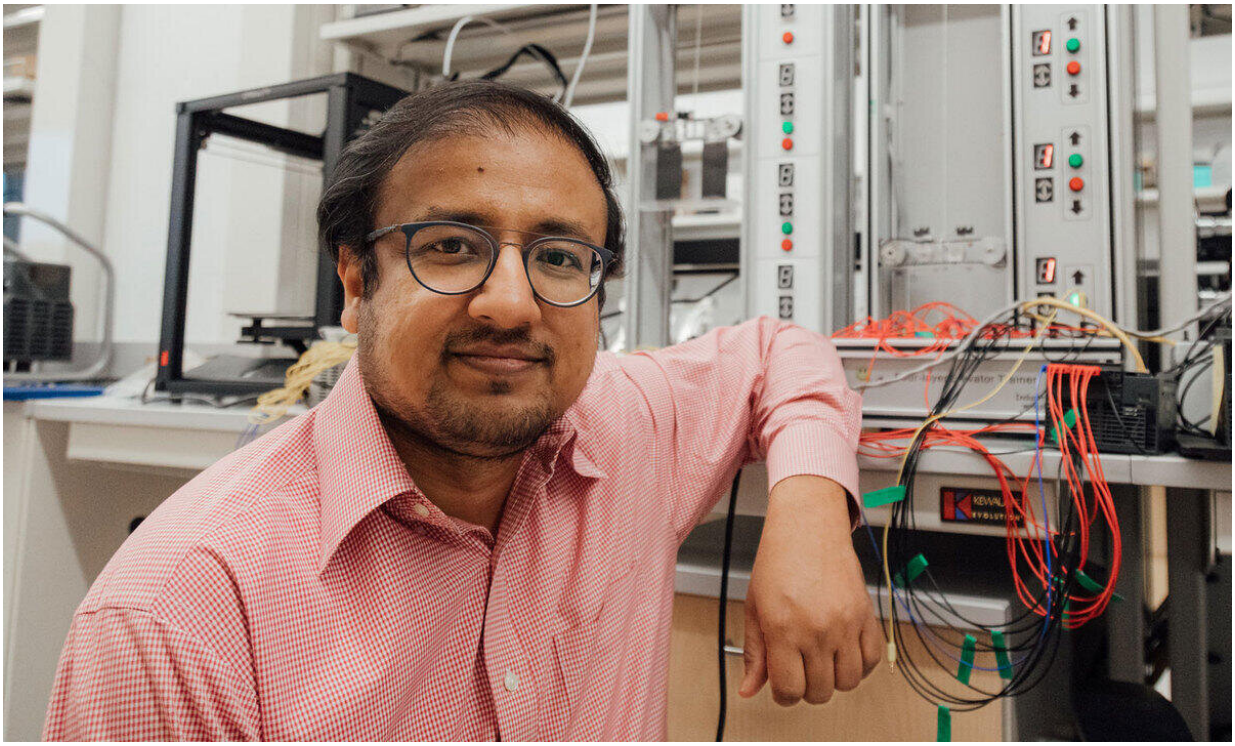
Researchers fight cybercrime with new digital tools and techniques

April 21 2023, by Joseph McClain



Irfan Ahmed, Ph.D., associate professor of computer science, next to a scale elevator model used to test physical systems. Credit: VCU Engineering

In the never-ending cybersecurity war, Irfan Ahmed, Ph.D., provides the good guys with digital forensic tools—and the knowledge to use them.

Ahmed is an associate professor of computer science and director of the

Security and Forensics Engineering Lab within VCU Engineering's Department of Computer Science. In the SAFE Lab, he leads a pair of projects aimed at keeping industrial systems safe from the bad guys, and showing how the same tools crafted for investigating cyberattacks can be used to probe other crimes.

Cyberattacks on physical infrastructure may be initiated to cause chaos by disrupting systems and/or to hold systems for ransom. Ahmed's SAFE Lab focuses on protecting industrial control systems used in the operation of nuclear plants, dams, electricity delivery systems and a wide range of other critical infrastructure in the U.S. The problem isn't new: In 2010, the Stuxnet computer worm targeted centrifuges at Iranian nuclear facilities before getting loose and infecting "innocent" computers around the world.

Cyberattacks often target a portion of software architecture known as the control logic, which receives instructions from the user and hands them off to be executed by a programmable logic controller. For instance, the control logic monitoring a natural gas pipeline might be programmed to open a valve if the system detects pressure getting too high. Programmers can modify the control logic—but so can attackers.

One of Ahmed's projects, called "Digital Forensic Tools and Techniques for Investigating Control Logic Attacks in Industrial Control Systems," allows him to craft devices and techniques that cyberdetectives can use in their investigations. He noted that investigation capabilities are an under-researched area, as most emphasis has been on prevention and detection of cyberattacks.

"The best scenario is to prevent the attacks on industrial systems," Ahmed said. "But if an attack does happen, then what? This is where we try to fill the gap at VCU. And the knowledge that we gain in a cyberattack investigation can further help us to detect or even prevent

similar attacks."

In the cat-and-mouse world of cybersecurity, the way criminals work is in constant evolution, and Ahmed's SAFE Lab pays close attention to the latest developments by malefactors. For instance, an attacker may go for a more subtle approach than modifying the original control logic. An attack method called return-oriented programming sees the malefactor using the existing control logic code but artfully switching its execution sequence. Other attackers might insert malware into another area of the controller, programmed to run undetected until it can replace the function of the original control logic.

Attackers are always coming up with new methods, but each attack leaves a trail of evidence. The SAFE Lab examines attack scenarios through simulations. Scale models of physical systems, including an elevator and a belt conveyor system, are housed at the lab to facilitate the work. The elevator is a four-floor model with inside and outside buttons feeding into a programmable logic controller. The conveyor belt is more advanced, equipped with inductive, capacitive and photoelectric sensors and able to sort objects.

The tools and methods applied in fighting cybercrime can be useful in tracking down other malefactors. That's where Ahmed's second project comes in. It's called "Data Science-integrated Experiential Digital Forensics Training based-on Real-world Case Studies of Cybercrime Artifacts." Ahmed is principal investigator, working with co-PI Kostadin Damevski, Ph.D., associate professor of computer science.

The goal is to keep law enforcement personnel abreast of the latest trends in cybercrime investigation and to equip them with the latest tools and techniques, including those developed in the SAFE Lab.

"For example, investigators often have to go through thousands of

images or emails or chats, looking for something very specific," Ahmed said. "We believe the right data science tools can help them to narrow down that search."

The FBI and other law enforcement agencies already have dedicated cybersleuthing units; the Virginia State Police has a computer evidence recovery section in Richmond. Ahmed and Damevski are arranging sessions showing investigators how techniques from data science and machine learning can make investigations more efficient by sorting through the mounds of digital evidence that increasingly are a feature of modern crime.

Provided by Virginia Commonwealth University

Citation: Researchers fight cybercrime with new digital tools and techniques (2023, April 21) retrieved 2 May 2024 from https://techxplore.com/news/2023-04-cybercrime-digital-tools-techniques.html