NEWLY DEVELOPED SECURITY MECHANISM AIMS TO GUARD EXISTING REAL-TIME SYSTEMS AGAINST CYBERATTACKS

April 12th, 2017

Technology processes with strict timing and safety requirements—from the operating mechanisms on your car (say, engine control or even anti-lock braking mechanisms) to unmanned aerial vehicle (UAV) controls—are called real-time systems. Due to the physical isolation and stringent safety requirements of real-time systems, they were considered immune from cyberattacks, yet recent attacks have highlighted their vulnerabilities.

In response to these attacks, PhD student Monowar Hasan, advised by ITI research assistant professor Sibin Mohan, has developed novel methods to integrate safety algorithms within these systems without interrupting normal behavior.

Monowar Hasan, advised by ITI research assistant professor Sibin Mohan, won Best Paper Award for his work presented at the Real-Time Systems Symposium (RTSS).

Hasan won Best Paper Award for this work presented at the Real-Time Systems Symposium (RTSS), the top conference for this field. ITI research affiliate Rakesh Bobba from Oregon State University and Rodolfo Pellizzoni from University of Waterloo collaborated on this work.

“Real-time systems are increasingly connecting and syncing to the Internet, which makes it easier to communicate between devices, but because of that, there are more sources of vulnerability and more chances for cyberattackers to intrude,” said Hasan.

A well-known security attack on real-time systems—from a virus called Stuxnet—targeted automation like assembly factory lines or power plants. In 2010, it caused substantial damage to Iran’s nuclear program by targeting the real-time systems that controlled the automation of the centrifuges separating nuclear material. Left unchecked, the attack caused the fast-spinning centrifuges to tear themselves apart, destroying one fifth of the centrifuges. Researchers have also demonstrated attacks against other real-time systems, such as the hacking of cars while on a highway.

Real-time systems often operate under time and safety constraints and automate processes that happen at the millisecond scale, not to mention limited computing power and memory. Malware can infiltrate within those tiny spaces. To create safety measures, Hasan had to work within those same constraints.

“The biggest challenge was timing and resource constraints, while trying to maintain the safety of the system,” said Hasan. “So what we implement has to do be done efficiently and within the limited computational capabilities of the system.”

His solution can work seamlessly with existing systems and does not interfere with the expected behavior of the system.

The safety measures, detailed in the paper, “Exploring Opportunistic Execution for Integrating Security into Legacy Hard Real-Time Systems,” are being integrated now as prototypes. The team is conductingfurther testing, and they aim to make it more robust and adaptive to provide greater security based on varying cyberattack situations.

“This work has the potential to improve the security of a variety of domains, from cars and avionics to power plants and manufacturing systems. In particular, these solutions can improve the security oflegacy systems—

most real-time systems have a lifetime of a few decades," said Mohan, a research assistant professor in computer science and ITI. "Hence, uprooting the large base of existing systems to retrofit complex security mechanisms is infeasible. With the techniques presented in this paper, we can more easily improve the security posture of existing systems as well."

Information Trust Institute
University of Illinois at Urbana-Champaign :: Coordinated Science Laboratory
1308 West Main St, Urbana, IL 61801-2307
+1 (217) 333 3546 iti.illinois.edu