Tech Talk | Telecom | Security

26 Mar 2020 | 15:20 GMT

New Approach Could Protect Control Systems From Hackers

This algorithm creates “background noise” during data transmission to alert officials to hacking

By **Michelle Hampson**

Photo: George Frey/Getty Images

IEEE Journal Watch

Some of the most important industrial control systems (ICSs), such as those that support power generation and traffic control, must accurately transmit data at the milli- or even mirco-second range. This means that hackers need interfere with the transmission of real-time data only for the briefest of moments to succeed in disrupting these systems. The seriousness of this type of threat is illustrated by the Stuxnet incursion in 2010, when attackers succeeded in hacking the system supporting Iran’s uranium enrichment factory, damaging more than 1000 centrifuges.

Now a trio of researchers has disclosed a novel technique that could more easily identify when these types of attacks occur, triggering an automatic shutdown that would prevent further damage.

The problem was first brought up in a conversation over coffee two years ago. “While describing the security measures in current industrial control systems, we realized we did not know any protection method on the real-time channels,” explains Zhen Song, a researcher at Siemens Corporation. The group began to dig deeper into the research, but couldn’t find any existing security measures.

Part of the reason is that traditional encryption techniques do not account for time. “As well, traditional encryption algorithms are not fast enough for industry hard real-time communications, where the acceptable delay is much less than 1 millisecond, even close to 10 microsecond level,” explains Song. “It will often take more than 100 milliseconds for traditional encryption algorithms to process a small chunk of data.”

However, some research has emerged in recent years about the concept of “watermarking” data during transmission, a technique that can indicate when data has been tampered with. Song and his colleagues sought to apply this concept to ICSs, in a way that would be broadly applicable and not require details of the specific ICS. They describe their approach in a study published February 5 in *IEEE Transactions on Automation Science and Engineering*. Some of the source code is available here.

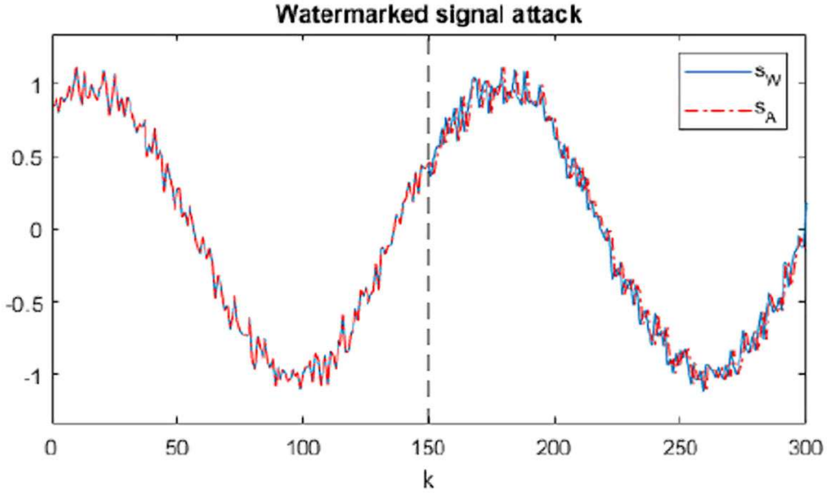

Image: Zhen Song

If hackers attempt to disrupt data transmission, the recursive watermark (RWM) signal is altered. This indicates that an attack is taking place.

The approach involves the transmission of real-time data over an unencrypted channel, as conventionally done. In the experiment, a specialized algorithm in the form of a recursive watermark (RWM) signal is transmitted at the same time. The algorithm encodes a signal that is similar to “background noise,” but with a distinct pattern. On the receiving end of the data transmission, the RWM signal is monitored for any disruptions, which, if present, indicate an attack is taking place. “If attackers change or delay the real-time channel signal a little bit, the algorithm can detect the suspicious event and raise alarms immediately,” Song says.

Critically, a special “key” for deciphering the RWM algorithm is transmitted through an encrypted channel from the sender to the receiver before the data transmission takes place.

Tests show that this approach works fast to detect attacks. “We found the watermark-based approach, such as the RWM algorithm we proposed, can be 32 to 1375 times faster than traditional encryption algorithms in mainstream industrial controllers. Therefore, it is feasible to protect critical real-time control systems with new algorithms,” says Song.

Moving forward, he says this approach could have broader implications for the Internet of Things, which the researchers plan to explore more.

About the Tech Talk blog

IEEE Spectrum's general technology blog, featuring news, analysis, and opinions about engineering, consumer electronics, and technology and society, from the editorial staff and freelance contributors.

Follow @IEEESpectrum

Subscribe to RSS Feed