SPECIAL REPORT

CYBERSECURITY: SHIELDING AGAINST THE DARK SIDE

By Mike Hockett, Editor-in-Chief

iStock.com/MF3d

As long as humans keep advancing technology to make our lives and job functions easier, sadly, there will always be those who mean to do harm with it. That's been especially true ever since the rise of the internet, and amplified with the age of Industry 4.0 and connected devices. Cybersecurity is something all technology suppliers know they need, and most know they should improve upon.

But it's one thing to secure business operations from cyberattacks. That facet of the topic has been well-documented. It's a whole other animal to secure electronic test instruments and testing procedures.

Cybersecurity is certainly a priority for vendors of electronic test and measurement instruments. But it's a tricky topic for them to discuss, as most instrumentation vendors don't market solutions in cybersecurity. Nevertheless, we were able to gather commentary from a couple of such instrumentation providers to get their thoughts on trends in cybersecurity, the challenges it presents, and what solutions are on the market.

What's trending?

Yazma

Ron Yazma, vice president of software engineering at Marvin Test Solutions (MTS): "For stand-alone "box" instrumentation, one of the primary concerns for end users is a cybersecurity breach via an infected instrument. This could happen when an instrument is calibrated or sent to a repair facility—virtually any instrument that contains software that can be accessed or modified via a remote or internet connection could be susceptible to a security breach. Consequently, instrument vendors and calibration/repair facilities have put in place processes to protect against cybersecurity breaches/infections. One can expect these cyber deterrent methods and processes such as encryption and authentication to evolve over the next couple of years in order to maintain and protect the integrity of the supplied instrumentation.

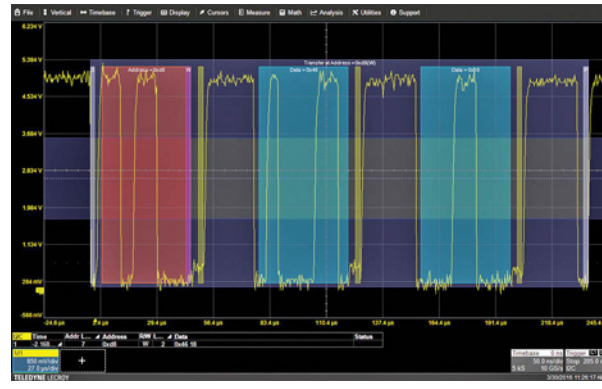
"For ATE systems which, in many cases, are connected to a network, the need to protect against cyberattacks and malware is more complex. And in particular, for ATE systems employed in military/aerospace applications, the need for cybersecurity is acute since not only can the test system be subjected to a cyberattack but a mission critical UUT being tested on the ATE could become infected. Consequently, over the next couple of years, one can expect to see suppliers of mil/aero test systems moving to adopt the methods / procedures detailed in the Department of Defense's (DoD) Application Security Technical Implementation Guide, which is based on National Institute of Standards and Technology (NIST) documents and details how to manage and maintain a secure software-based system such as an ATE system."

Bob Mart, product line manager at Teledyne LeCroy: "In terms of trends, we are seeing customers wanting to perform traditional testing on embedded system designs in the same ways as they always have, but now they also want to account for designs having cybersecurity requirements. They need to ensure that whatever cybersecurity features their designs incorporate are working as designed. A few years ago, no one was talking about cybersecurity; now it adds a layer of complexity to the test regimen over and above the standard functional test.

Mart

"Customers want to perform protocol analysis through mechanisms such as serial triggers and decodes so they can monitor control buses for suspicious or unwanted activity. Then, abnormalities can be correlated between the protocol and physical levels to determine whether some control signal or other event can provide insight into potential vulnerabilities. In the automotive market, we often encounter customers wanting to monitor protocols such as CANbus to ensure that there are no bad actors or unwanted traffic on the bus.

"Using our oscilloscopes' serial data decode table, users can filter out IDs or messages known to be sent by your own devices, which allows you to quickly capture any abnormal activity. From there, you use the tools in the oscilloscope to debug what might have happened to let that occur.



Teledyne LeCroy's TDME (trigger, decode, measure/graph, and eye diagram) packages can be leveraged for both protocol testing and cybersecurity verification.

Teledyne LeCroy

"Teledyne LeCroy offers TDME (trigger, decode, measure/graph, and eye diagram) packages for many serial protocols. These suites of tools can be leveraged for both protocol testing and cybersecurity verification. For the topic at hand (cybersecurity in embedded systems), an example would be the Embedded Bundle TDME, which covers the I2C, SPI, and UART/RS-232 protocols.

"In the future, cybersecurity will be an area of growing concern, and we'll continue to adapt our tools to cover emerging needs."

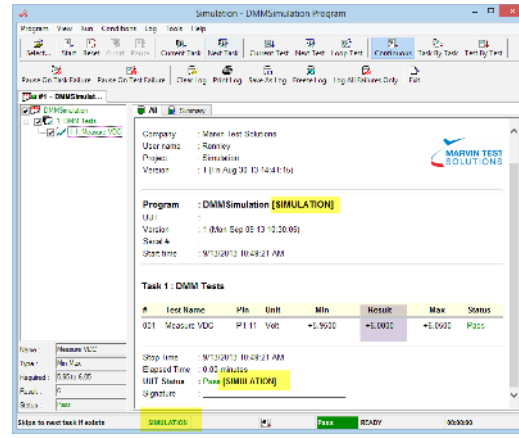
David Holt, director of new product introduction at B&K Precision: "Based on our customer's feedback, embedded cybersecurity is not a high priority for B&K Precision. When remote connectivity is used with our products, both the computer and test instruments are behind a firewall on a private network. For remote connections using the worldwide web, the end user must consider many issues that go well beyond the test instrument."

Vulnerabilities

Yazma, MTS: "Cybersecurity cannot be overlooked and in fact, the cost of not proactively managing cybersecurity is far greater than the cost of actively managing the implementation of safeguards to protect against security breaches/infections. As noted above, ATE systems that are networked can be the most prone to cybersecurity threats which, consequently, requires additional methods and procedures to ensure that systems are protected from cyberattacks. Additionally, to ensure the integrity and protection of test programs, ATE software tools can include the option to encrypt both source code and executables—ensuring the integrity of the test program and preventing unauthorized tampering of code."

Simulation Software

Simulation software has seen great adoption over the past decade, allowing users to run tests through a virtual platform that mitigates the cyber risk their computer could otherwise be exposed to with direct testing.



A screenshot of instrument simulation being performed with Marvin Test Solutions ATEasy software.

Marvin Test Solutions

One of these simulation tools is application virtualization—a process that packages computer programs and their dependencies from the underlying operating system into a single executable bundle, which is then transportable across systems. This can be an especially effective tool for legacy software that has more vulnerabilities than a modern counterpart.

The December 2018 issue of *EE* featured an article titled, "Mitigate software obsolescence and cyber risk using application virtualization," by Dr. Christopher P. Heagney and Lance J. Walker, who work with the U.S. Navy as science advisor and electrical engineer, respectively. Their article detailed, in-depth, how application virtualization serves as an advanced technology solution for all Department of Defense programs to reduce their overall cost, improve fielded systems, and mitigate cyber risk. It does this by blocking user access, restricted executables, requires no installation, and reduces cyberattack surface through isolation of the "just enough" operating system. The duo presented a paper at AutoTestCon in September 2018 that explained how application virtualization is an 80% solution that they called "good enough" to maneuver within the cost and performance trade space.[1]

Yazma, MTS: "Marvin Test Solutions' ATEasy software suite has offered simulation capability for several years and supports simulation of the complete ATE system—not just simulation of the test instrumentation. We have not seen it being used as a method for boosting or verifying cybersecurity although it could be used for this purpose by constructing an "infected" system component to show cause and effect. Rather, we see simulation offering users the means to develop and test their test programs without having to rely upon the test system for verification of the program, which improves overall productivity and shortens test program development/verification time."

MTS markets ATE software in the form of ATEeasy, a 10th generation product. It includes both a test executive and test development environment, and offers a handful of cybersecurity features:

- Encryption of both executables and DLLs, which maintains executable integrity and prevents hacking, reverse engineering, text viewing, or modifying of the executable (non-repudiation)
- Encrypted binary source code for drivers, system, and program files ensures file integrity and protects files from malicious changes
- Password or hardware key license serial number offers access protection for drivers, system, and program files, which prevents the use, viewing, reverse engineering, or changing of code
- Management of multiple users and privileges via a unique password/user ID mechanism
- Run-time protection from buffer overruns, call stack mismatch when calling external components

MTS is working toward complying with DoD application security and development requirements (ASD 47), of which there are more than 300. EE

REFERENCE

1. Dr. Christopher P. Heagney and Lance J. Walker, "Mitigate software obsolescence and cyber risk using application virtualization," Evaluation Engineering, December 2018.