Cybersecurity and encryption for the masses

Aerospace and defense systems designers investigate fast and affordable ways to safeguard computers and communications from cyber attack by plugging vulnerabilities and layering COTS cybersecurity.

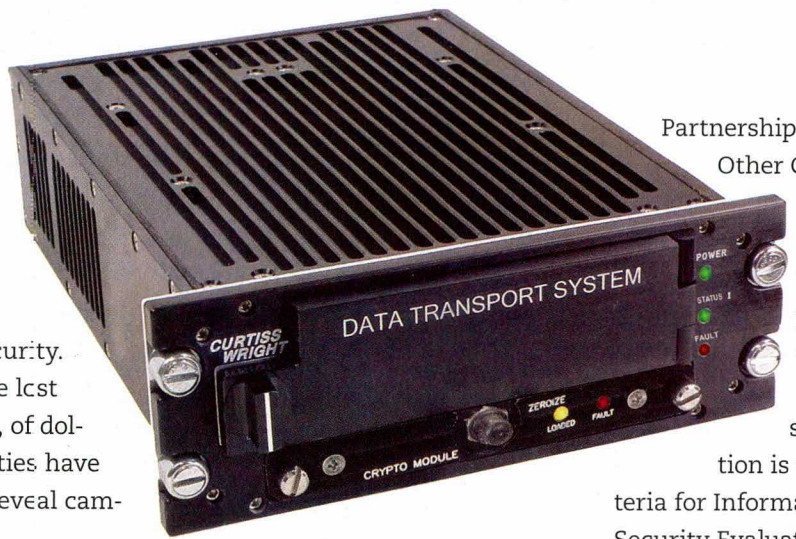
BY **John Keller**

No one has to be told these days about the importance of data encryption and cybersecurity. Retail chains have had their computer hacked to compromise customer security. Financial institutions have lost thousands, if not millions, of dollars, and U.S. political parties have suffered e-mail hacks to reveal campaign secrets.

Consensus among experts says the problem will just get worse over time. One of the primary keys to cybersecurity for government and private industry is encryption. The problem, however, is that encryption historically has been expensive to obtain, and time-consuming to certify.

Some of that might be changing, as encryption approaches are emerging that are more affordable than traditional methods, and that can be tied into new systems and upgrades far more quickly than could be done in the past.

One of the more influential aspects of a new generation of timely and affordable encryption is the Common Criteria Recognition Arrangement (CCRA), an international agreement among 26 member countries that makes available different encryption approaches for business, military, and civil uses.



The Data Transport System (DTS1) from Curtiss-Wright is a rugged network attached storage (NAS) file server for use in unmanned aerial vehicles (UAV), unmanned underwater vehicles (UUV), and intelligence surveillance reconnaissance (ISR) aircraft.

The U.S. arm of the CCRA is the U.S. Department of Defense (DOD) National Information Assurance Partnership at Fort Meade, Md. Other CCRA members include the United Kingdom, France, Germany, India, Japan, Israel, and Canada.

The technical basis of the organization is the Common Criteria for Information Technology Security Evaluation, which typically is known simply as the Common Criteria, or just CC. It offers products that licensed independent laboratories can evaluate for different security applications.

The Common Criteria represents a wide variety of mutually recognized encryption products for secure IT products. More on the Common Criteria and the CCRA is online at https://www.commoncriteriaportal.org/.

What's good enough?

Wide availability of cybersecurity and encryption products begs the question: if these encryption

schemes are so available and well-known, how secure can they really be?

For some applications these encryption products taken individually may be perfectly adequate. For others — especially for military, aerospace, homeland security, and other life- and mission-critical applications — just one might not be enough for reasonable assurance of security against malicious hackers or eavesdroppers.

Until recently the only other viable alternative for reliable and certifiable encryption and cybersecurity was the long-established Type I security available through sources approved by the U.S. National Security Agency (NSA) at Fort Meade, Md.

For a fair number of applications, however, NSA Type I encryption is just too expensive to consider — even such that some systems designers had to go without encryption and hope for the best. Sometimes taking such a risk has met with dire consequences.

One of these involved the so-called RQ-170 Incident in December 2011 when Iranian military forces commandeered a U.S. Lockheed Martin RQ-170 Sentinel stealth unmanned aerial vehicle (UAV) near Kashmar in northeastern Iran. An Iranian cyber warfare group took control of the U.S. UAV, landed it, and took it apart to discover its technical secrets.

From the lack of a reliably secure control data link, the U.S. may have lost technological secrets that would take years to overcome. This pivotal event caused a rethinking of encryption and cybersecurity in the Pentagon, defense industry, and other enclaves where security is essential.

The lessons learned from the RQ-170 Incident have given rise to several new initiatives to safeguard data flowing over networks, as well as data that resides on storage devices in unpowered computer systems.

Protecting UAV data links

On the UAV front, cybersecurity experts at Rockwell Collins in Cedar Rapids, Iowa, are working with specialists at other companies and government agencies to develop software that can repel hackers even over unsecured data links.

One effort, sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA) in Arlington, Va., is called High- Assurance Cyber Military Systems (HACMS). The Air Vehicle team in the HACMS project involves Rockwell Collins in Cedar Rapids, Iowa, as well as the Boeing Co. Defense & Security Segment in St. Louis; Data61 in Canberra, Australia; Galois Inc. in Arlington, Va.; and University of Minnesota in Minneapolis.

The Rockwell Collins team is developing embedded computing software that can enable a UAV to keep operating safely despite offboard and onboard cyber attacks, Rockwell Collins officials say. The team has demonstrated prototype secure software on quadcopter UAVs, as well as on the Boeing Unmanned Little Bird helicopter, which was able to resist several cyber attacks launched by a team of advanced hackers.

"Our world is becoming more connected every day, and that includes the aviation industry," says Darren Cofer, fellow at Rockwell Collins. "Cybersecurity used to be a concern only for traditional

computing systems and networks. Now anything with embedded software can be vulnerable to cyber attack. As a result, we have to be vigilant about protecting critical systems like avionics."

Coffer explains that hackers have three approaches to attacking embedded computing systems: external interfaces; software bugs; and communications and software interfaces.

First, hackers can exploit weak external interfaces that have weak or no encryption. Second, they can exploit software bugs to create

Warfighters deployed in the field need the ability to safeguard data on the move and at rest from attempts to intercept or tamper with mission-critical information.

vulnerabilities. Third, they can use communications and software component interfaces in a way that software developers never intended.

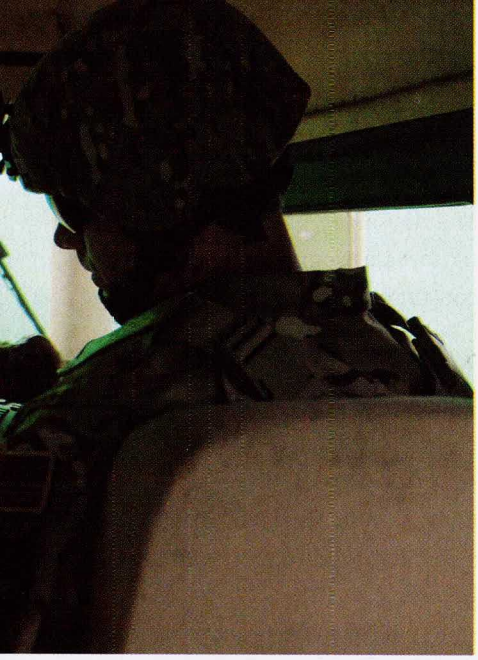
Researchers involved in the DARPA HACMS program are concentrating on those three vulnerabilities to safeguard systems that are unencrypted from potential cyber attacks.

Layered COTS security

The RQ-170 Incident also has given rise to the NSA's Commercial Solutions for Classified program (CSfC) — a new way of delivering encryption and cybersecurity solutions that capitalize on industry developments.

The idea behind the NSA's CSfC program is to provide encryption and information assurance both quickly and affordably — and provide a viable alternative to expensive NSA Type I encryption for systems that might not be able to afford it or have the time to implement it.

NSA experts founded the CSfC program on the principle that



properly configured, layered solutions can provide adequate protection for classified data in a variety of different applications. This can enable aerospace and defense systems based on commercial off-the-shelf (COTS) hardware and software to communicate securely based on commercial standards in a solution that can be fielded in months, not years, NSA officials say. More on the NSA's CSfC program is online at https://www.nsa.gov/resources/everyone/csfc/.

The core approach of the CSfC program is to layer two or more commercially developed encryption and cybersecurity approaches to provide information security solutions that might not be entirely impregnable, but that are good enough for the applications at hand.

Military communications and computer developers describe the redundant practice of using two or more security approaches as "belt and suspenders," or "using the parking brake after putting the transmission in park."

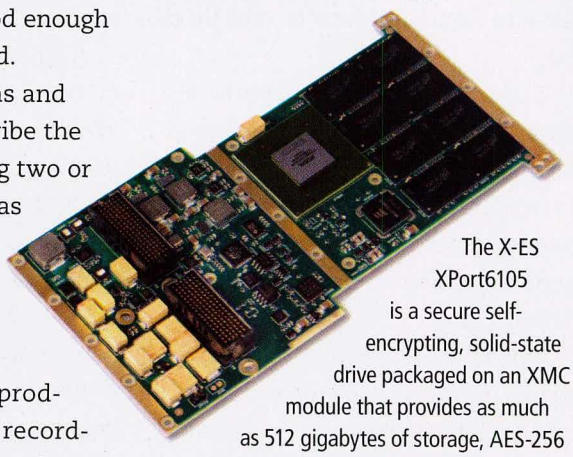
Paul Davis, director of product management for data recording and storage products at the Curtiss-Wright Corp. Defense Solutions segment in Ashburn, Va., describes the CSfC approach as overlaying two pieces of Swiss cheese.

"If you have two pieces of Swiss cheese, there are several holes," he explains. "If you rotate one piece 90 degrees, most of the holes are covered up. Any one piece might not be adequate to protect a system, but if you use two layers and cover most of the holes, it can be good enough for that application."

The CSfC approach couldn't come at a more important time. Not only are experts in the DOD and private business increasingly concerned about cybersecurity and encryption, but the need to safeguard data also is expanding exponentially with an explosion in the use of sensors, digital signal processing, and the so-called Internet of Things (IoT).

"It is definitely gaining more momentum," says David Jedynak, chief technology officer at Curtiss Wright Defense Solutions. "We can start with things on the Common Criteria list, and instead of doing this big Type I thing, we can take this commercial solution with that commercial solution and bring them together."

Where time to market is a big concern, this layered approach can



The X-ES XPort6105 is a secure self-encrypting, solid-state drive packaged on an XMC module that provides as much as 512 gigabytes of storage, AES-256 XTS encryption, and fast clear.

The Harris Corp. RF Communications segment in Rochester, N.Y., designs and manufactures the KGV-72 encryption device, shown above, which provides the ability to process classified messaging traffic.

make the difference between winning and not winning a contract. "The rationale is cost and time," Jedynak says. "A Type I development can be five to six years long, while a CSfC development is two to three years — sometimes only 18 months."

Curtiss-Wright is using CSfC two-layer approach to encryption and cybersecurity with a product to be launched in September called the Data Transport System 1 (DTS1) for protecting stored data at rest at times when computer systems are unpowered. It's part of the company's Trusted COTS (T-COTS) initiative.

"People want to protect data at rest, but are also concerned about having it encrypted and how people can break through that encryption if they have it in their possession. We are working to address and enhance our offerings in both areas," says Steven Edwards, director of secure embedded solutions at Curtiss-Wright. Company officials say they expect NSA certification for the DTS1 by the end of 2017.

Digital defenses

Most encryption approaches to cybersecurity represent efforts to keep potential digital intruders out. These and other conventional approaches are part of a mindset of building walls and guard towers around important data and data pathways.

What happens, then, when the hackers get in? Mark Testoni, president and CEO of SAP National Security Services (SAP NS2), a cybersecurity specialist in Rockville, Md., says security experts are starting to think about how to contain and otherwise deal with hackers after they've broken in, rather than simply preventing them from access to sensitive data.

"On the protection side, historically we have done a really good job of building perimeters around our systems," Testoni says. "We continue to do that, but most recently encryption has taken on a more important role with data on the move and data at rest."

Security experts have to face the fact that few, if any, defenses can be 100-percent effective. "Beyond perimeters, how do we look at our own systems, assuming people are going to get in," Testoni says. "We have to make a mental presumption that they are going to get in, and we have to figure out how to root them out."

Perhaps the primary opportunity today for cybersecurity providers is how to help companies look at their systems and network architectures, and help assimilate data on various activities going on in the network, Testoni says.

One approach to this is bringing in lots of metadata-level information to help establish a baseline for normal activity of the network and the network's users, Testoni says. The downside of this, however, is it requires a tremendous amount of compute power to research these behaviors and detect anomalies.

"We're starting to work on the importance of the digital DVR," Testoni says. "We look at and capture the data inside your system, and when you see deviations it can identify anomalies for further investigation."

Security experts at SAP NS2 are working on what Testoni calls HANA, short for High-Performance Analytic Appliance, that relies on a traditional database architecture. "You have core compute power, data storage, and hundreds of thousands if I/Os going back and forth," he says.

HANA seeks to place all data and computing is one place, not in storage, with petabytes of information available for analysis. "This is a real possible breakthrough," Testoni says.

Another way to deal with digital break-ins involves user behavior analytics (UBA), which looks at individual behavior on the network, based on documented normal behavior, Testoni says. "This isn't THE answer, but it's a piece of the answer," he says.

A third approach is to effect a cultural change that increases the vigilance of computer and network users to potential cyber threats such as those contained in what look like routine e-mails, such as dangerous attachments. Cyber defenses, detecting anomalies, and increasing individual vigilance "is a three-headed approach that will enable us to be successful," Testoni explains.