Encryption at the edge

New and enhanced technologies beef up military-strength encryption

BY JOHN EDWARDS

Military and industry are developing a variety of software- and hardware-based encryption systems, including new software encryption tools, self-encrypting drives and biometrics.

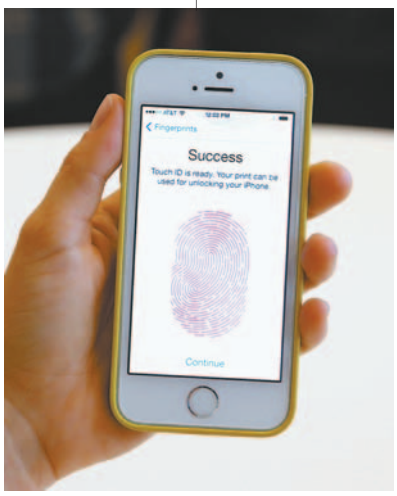
"Military encryption is constantly evolving, but in the last few years there has been a stronger focus on this matter due to a shift toward software encryption at the tactical edge and the Cryptographic Modernization [CM] program," said Tom Kirkland, senior director of Department of Defense programs for Thales Defense & Securities. A joint DoD/National Security Agency project, CM aims to boost the speed and security of both tactical and strategic networks.

"The program will also help [DoD] address and adapt to modern, sophisticated threats across the globe and increase interoperability between echelons and military forces," he said.

Software encryption allows the development and deployment of very small, power-efficient secure communication systems, such as the AN/PRC-154A Rifleman Radio, MBITR2 radios and commercial off-the-shelf mobile devices. "At the edge, the AN/PRC-154A provides soldiers with the ability to plan and execute missions and share position location information over secure networks encrypted by a Suite B algorithm," Kirkland said.

The U.S. has long lead encryption technology development, according to Mats Nahlinder, director of the IronKey encrypted flash drive product line for Imation. "Most of the encryption deployed today globally is based on U.S. research and technology algorithms in the Suite B cryptographic algorithms specified by the National Institute of Standards and Technology," he said.

Suite B is well on its way to becoming the standard encryption technology for federal agencies. "There's a U.S. government mandate to adopt Suite B by Oct. 1, 2015, for all National Security Strategy systems," said retired Col Cedric Leighton, a former deputy director of training for the NSA and currently the chairman of Cedric Leighton International Strategies. "The use of elliptic curve key exchanges and digital signatures modernizes authentication protocols and will also help secure all types of NSS," he said.



JUSTIN SULLIVAN/GETTY IMAGES

Many agencies show interest in biometric authentication, such as using fingerprints to unlock mobile phones.

"One of the many benefits of Suite B," said Kirkland, "is it allows for a product to be classified as non-CCI [non-Controlled Cryptographic Item], allowing for easier deployment of radios and networks to our service members and collation partners."

HARDWARE THAT ENCRYPTS ITSELF

Traditional electro-mechanical and more recent high-speed solid-state models of self-encrypting devices, or SEDs, can conveniently protect stored data. "Some consider SEDs a best-kept secret in the IT world," Leighton said. "We really do need to get to a point in which security in the form of SEDs and encryption in general is at the forefront of decisions to purchase hardware and software."

While SEDs are generally easy to use, they come with a catch. "The weakness of this technology is that usually a single encryption key is used to protect the data," said Todd Moore, vice president of encryption product management for SafeNet. "Once the disk is active, all of the data is unencrypted, creating a vulnerability."

BIOMETRICS: TOO IMPRACTICAL?

Moore detects a growing interest in biometric authentication technology. "The use of biometrics to provide a unique variable input into the encryption process is not widely used today, but is gaining popularity," he said.

MORE ONLINE

Cyber training tops agency priorities. Read more at **C4ISRNET.com/cyber**

Many agencies continue to be reluctant to adopt biometric authentication systems, often for practical reasons, said Leighton. "In many respects we are still in the password era," he said. "Biometric authentication technologies may also be difficult to incorporate in an environment, like a tactical military one, in which there are multiple human users of a piece of cryptographic equipment."

Today's leading encryption technologies are good enough to protect any kind of information from any type of adversary, according to Nahlinder. "As long as it is implemented correctly, it is just about impossible to hack," he said. ☐