Emerging encryption tech

Mobile devices, big data drive the push for cutting-edge security

Oct. 7, 2013 | 0 Comments

Written by
JOHN EDWARDS

FILED UNDER

C4ISR & Networks
IT & Networks

Information security is becoming stronger, cheaper and available on more devices thanks to an emerging generation of encryption technologies. Military and industry engineers are developing a variety of hardware- and software-based encryption systems, ranging from self-encrypting drives to biometrics.

The new technologies are arriving just in time to help the military keep pace with new financial and security concerns.

“Big data and the pervasiveness of mobile devices in and around the battlespace have resulted in huge challenges for those trying to encrypt military communications,” said Cedric Leighton, a retired Air Force colonel who, until 2010, was deputy director for training at the National Security Agency.

Brad Curran, an aerospace and defense analyst with the research firm Frost & Sullivan, said that the military is increasingly turning to commercial sources for its encryption needs.

“Traditionally, you just go from comm center to comm center, or covered radio net to covered radio net,” he said. “Now there’s this ubiquitous use of mobile devices and cloud computing, and it drives the military more toward using commercial technology.”

Shrinking military budgets are leading to the pursuit of commercial off-the-shelf encryption systems, Curran said.

“The [Defense Department] is finding that it’s going to be a lot cheaper to go to a commercial technology than to develop it on their own,” he said. “Plus, they’re always going to be behind the power curve on technology changes and efficiency, so they want to

More Headlines


Automated intelligence
11:27 AM


Special Report: Special Ops Requirements
11:12 AM


House Defense Hawks Urge Tea Party to Drop Obamacare War
1:30 PM


UK MoD: Independence Could Harm Scotland's Security
1:56 PM

work with commercial companies to leverage the heavy lifting that they're doing."

Legacy systems

The NSA-developed KG and KIV families of devices, with their roots firmly planted in 1990s-era technologies, continue to be the military's mainstay encryption systems. Yet to keep pace with evolving needs, even these venerable devices are gradually being updated and improved.

"KIVs and KGs continue to evolve, so I wouldn't say they're going away," said Felipe Fernandez, a systems engineer at Fortinet Federal, a DoD security technology provider.

Digital data, once the province of the KG-84 family, is now encrypted primarily by the KIV-7, Leighton said.

"As we move to systems that rely less on microwave shots and more on fiber-optics, you will see systems like the KIV-7 morph or disappear," he said.

The KIV-7 is a compact, embeddable version of the KG-84 encryption device, which was developed in the mid-1990s by AlliedSignal to meet the military's need for secure data communication links. The KIV-7 was manufactured by Mykotronx I (currently SafeNet), as a COTS technology.

The types of encryption used by the military vary, to some extent, by mission and service.

"For example, over the past decade or so, U.S. strategic forces ... have been working on upgrading the encryption of their communications," Leighton said. "In the Navy's case, the KG-38 is being replaced by KIV-17 circuit modules, based on the commercially available VMEbus."

Self-encrypting drives

While KIV and KG devices continue to be widely used, DoD is also looking toward making encryption technology readily available in a wider number of locations. Self-encrypting drives (SEDs), an emerging generation of hard disk and solid-state drives featuring built-in cryptographic engines, are increasingly seen as a fast, cost-effective and practical solution for an increasingly mobile military. The units are designed for easy installation inside various types of mobile devices, as well as desktop computers and servers.

"While SEDs have become more prevalent, and most manufacturers today offer drives with the capability, the first attempts at a management standard did not work well enough to get widespread enterprise adoption," said Bob Stevens, senior director of federal operations for security software developer Symantec. "Until a clear standard that works consistently across all drive manufacturers [becomes available], SEDs will not see widespread adoption as more than a point solution, even with the

Slideshow

Military UAVs: State of the Art

speed advantages offered by these devices."

SEDs also lack the Type 1 security compliance offered by KIV and KG devices.

"SEDs are becoming more widely used within the military, but so far only for what's known as 'sensitive but unclassified' data," Leighton said. "SEDs are not yet permitted to handle truly classified information."

Fernandez, however, expects SEDs to become more secure.

"SEDs are definitely gaining ground," he said. "It may only be a short time until SEDs are mandated in most systems."

Biometric encryption

While showing significant promise, biometric encryption, which merges biometric data such as a fingerprint or iris scan with encryption algorithms to create a two-factor authentication platform, has yet to be widely adopted by the military.

"Biometric encryption is certainly increasing from a physical security standpoint," Fernandez said. "However, it has not found the diversity that some would have hoped."

Leighton believes that biometric encryption deployment may be driven by a growing need to restrict access to highly sensitive information.

"Although biometric data is being collected at an accelerated rate, there is no en masse adoption of biometric encryption yet," he said. "It will be interesting to see if the revelations by [accused NSA leaker] Edward Snowden, and the recent announcement by the director of NSA to drastically curtail the number of system administrators, will result in more of an effort to adopt biometric authentication and encryption mechanisms."

Quantum leap

On the cutting edge of military encryption is quantum cryptography, which uses the principles of quantum mechanics to help secure communications.

"Quantum encryption definitely has real-world potential," Leighton said. "There are some vulnerabilities to a system that relies on detecting a single photon in order to make it work, but efforts are being made to create single photon detectors and, if they work, that could mean that some data could be encrypted two orders of magnitude faster than is the case using conventional techniques."

Fernandez, however, is skeptical about quantum encryption's suitability for field-oriented applications.

"The need for quantum repeaters still limits implementation on a large scale," he said.

Curran wonders whether quantum encryption isn't already graining traction in areas that are hidden from the general public.

"We as citizens can't see it, but perhaps in the classified realm, in the black world, they may be using some of that," he said.

View Comments (0) | **Share your thoughts »**

RECENTLY ON DEFENSENEWS

1. House Defense Hawks Urge Tea Party to Drop Obamacare War
2. UK MoD: Independence Could Harm Scotland's Security
3. S. Korea Confirms North's Yongbyon Plutonium Reactor Restart
4. First Video Shows Inspectors at Syria Chemical Arms Sites
5. North Korea Warns US of 'Disaster' Over Joint Naval Drill
6. Sofradir, Onera To Seek New Thermal-Imaging Tech

ARCHIVES

View the last seven days

Yesterday, Oct 07
Sunday, Oct 06
Saturday, Oct 05
Friday, Oct 04
Thursday, Oct 03
Wednesday, Oct 02
Tuesday, Oct 01