DEFENSESYSTEMS
KNOWLEDGE TECHNOLOGIES AND NET-ENABLED WARFARE

iPhones, Android devices held back by encryption limitations

Defense organizations explore whether commercial devices can provide enough encryption to meet security requirements

- **By John Edwards**
- **May 04, 2011**

With more defense organizations thinking about using iPhones, BlackBerrys, Droids and other commercial handheld devices for field activities, there's growing interest in whether such devices can be secure enough to safeguard sensitive information.

Recent advancements in device performance, functionality and encryption support are making handheld devices more appealing to an array of defense organizations that previously might have turned to custom-developed systems, said William Marlow, CEO and chief technology officer of Protected Mobility, a mobile security software developer based in Reston, Va., that's active in the government sector. "There's finally a realization that commercially available products can and will serve as the basis of secure communications," he said.

Marlow said the technology's attraction is clear as the latest commercial devices tend to be compact, powerful, convenient, infinitely useful and universally available. "Yet the best part of using commercial products is that they are more human-oriented rather than being designed for a specific task," Marlow said. "This reduces training and, when done right, the device costs are significantly lower."

Despite their growing appeal, commercial devices have limitations when deployed in defense applications. Although most handheld devices fit comfortably into routine enterprise-level operations, security concerns proliferate when the technology moves into defense settings, said Stephen Lucas, chief engineer of the Space and Terrestrial Communications Directorate at the Army's Communications-Electronics Research, Development and Engineering Center. That is particularly true when users operate in field environments that are close to the tactical edge.

"There's a different mindset between the commercial side versus the military side when it comes to layering on security," Lucas said. "Ultimately, lives can be in jeopardy when information falls into the wrong hands." And that makes high-level encryption a top priority for defense adopters across all sectors, especially those in tactical environments.

Which is most secure?

Apple, BlackBerry and Android-based products dominate the commercial market, and those devices also tend to attract the most interest from defense users. However, encryption support varies among the three product families.

With Apple iPhones and iPads that operate on iOS 4, adopters can take advantage of hardware device encryption. Apple's e-mail application also supports app-level encryption. However, it's a minimal amount of encryption support and is insufficient for defense organizations. A proprietary platform is a further detriment.

Marlow said Apple's hermitic policy limits the ability of third-party encryption providers to design compatible products. "They refuse to allow access to the iOS, which would allow better designed products," he said. "Currently, there are workarounds, and of course, there are solutions for jail-broken devices."

Lucas said BlackBerry devices are perhaps the most intruder-resistant commercial handheld products. "When it comes to encryption, the BlackBerry appears to be the most inherently secure," he said. "It supports full-device encryption, including media cards, keeping your data secure when your phone becomes lost or stolen." BlackBerrys rely on a two-key Triple Data Encryption Algorithm for creating message keys and master encryption keys.

Lucas said he also likes the fact that all BlackBerrys, unlike Apple or Android-based products, feed data through a central point: the BlackBerry Enterprise Server. "All security controls are enforced from that centralized server," he said.

Android-based phones and tablets are at the opposite end of the handheld encryption spectrum because they have no native

encryption capabilities, though rumors are circulating that the upcoming Android 3.0 operating system, code-named Honeycomb, will incorporate some level of encryption. “The overall security architecture for the Android is immature compared to iPhone and BlackBerry,” Lucas said.

Despite the lack of any built-in encryption, Lucas said most Defense Department organizations are focusing on the Android platform. “This is largely because the Android OS is hardware agnostic, meaning applications developed to run on the Android OS can run on most current and planned hardware platforms,” he said.

With Android popularity steadily rising in the defense community, Lucas said the Army is working to build a security foundation for those and other handheld devices. The Army's Space and Terrestrial Communications Directorate "has invested a lot of resources into understanding third-party security tools, as well as beginning the research and development of a SIM card/lightweight security toolset that would provide all cryptographic features,” he said.

The toolset is being designed to protect a variety of data types. Other attributes include a personal firewall, input/output controls, security policy management, antivirus capabilities, multifactor authentication, tactical DOD public-key infrastructure and Secure/Multipurpose Internet Mail Extensions support, Lucas said.

At the moment, the best encryption support for Android devices comes from third-party add-on products. Whisper Systems‘ RedPhone voice-over-IP application uses an encryption protocol named ZRTP that was designed by Pretty Good Privacy inventor Phillip Zimmerman. The app uses encrypted Short Message Service messages to quickly establish calls across a VOIP connection, all behind the convenient mask of a normal dialing interface or contact list. However, RedPhone and most third-party handheld add-ons lack official validation, which prevents their use by any defense organization.

Getting validated

Tom Karygiannis, a senior researcher at the computer security division of the National Institute of Standards and Technology, said meeting government encryption standards can create a significant obstacle when acquiring commercial technology. “In the past…a government agency could issue a contract for someone to build, at a huge cost, custom hardware and software,” he said. “Now, the way the market is, very capable devices are available at your local retailer.”

However, Karygiannis said, acquiring handheld devices that are suitable for defense personnel isn’t as easy as walking into the nearest Best Buy. “A government agency that wants to send or store sensitive information has to use cryptographic algorithms that have been validated by an independent and accredited lab,” he said.

“The Defense Department mandates use of a NIST FIPS 140-2-validated encryption product to prevent compromise of data security,” said an Air Force Space Command electronics engineer who is familiar with mobile encryption technologies and DOD mandates. FIPS 140-2 is the government computer security standard used to accredit cryptographic modules. FIPS 140-2 requires two-factor authentication, which is based on something you know, such as a password, and something you have, such as a fingerprint.

Meanwhile, with new handheld devices hitting the market on a seemingly daily basis, it’s becoming increasingly difficult for the FIPS validation process to keep up with the constant flow of product introductions. “The rapid pace of introduction and short life cycle of commercial handheld products makes it impractical to obtain FIPS 140-2 certification for every device,” the engineer said. “This impacts the rate of adoption of new devices" by DOD.

Karygiannis agreed. “New [handheld models] come out every three to six months, maybe even more frequently,” he said. “They're introduced in the market quickly, so government agencies need to figure out how to get these devices tested and validated and procured quickly.”

That’s especially tough for organizations that have users on the tactical edge. “It is very difficult to take a commercially developed product and convince the NSA that the product is secure enough for a military environment,” Lucas said. “Currently, the NSA certification process can take 12 to 24 months to acquire certification, and the costs are immense.”

Some relief might eventually come from OpenSSL, an open-source initiative that promises to produce open-source validated encryption modules almost as quickly as new handset models arrive on the market. “If these could be used on the [handheld] devices, then that solves a pretty big problem for the government agencies,” said Karygiannis, who expects the first validated encryption modules to arrive sometime in fiscal 2012.

Performance drag

Validation issues aside, another challenge facing handheld device adopters is the tendency of advanced encryption algorithms and supporting software to create a noticeable performance drag. “In general, encryption does increase the amount of storage necessary for the data,” the Air Force engineer said. “Also, the process of encryption/decryption may cause the user to experience a slight lag

time to display the content.”

Karygiannis said rapidly advancing handheld technology is helping to minimize performance concerns. “The hardware capabilities of some of these devices today are much better than what you would have found on a desktop a few years ago,” he said. Karygiannis said displays and Global Positioning System subsystems can be a bigger drain on the battery than the extra computational cycles that encryption might add. “I’d be more worried about the battery life for these types of devices being used in the field than the extra load introduced by encryption,” he said.

Future trends

Like handheld devices, encryption technology is growing more efficient and capable. “Currently, you can get excellent data encryption using AES-256, SHA-256/384, ECC 521 and others,” Marlow said. “Within two years, you should see full Suite B encryption available on these devices,” he said, referring to a set of cryptographic algorithms promoted by the National Security Agency as part of its Cryptographic Modernization Program.

Lucas said progress is being made on multiple fronts. As NSA adopts commercial technologies and DOD further defines encryption requirements, "more and more organizations get involved ... [and] we can expect to see better protection in the years ahead,” he said.

About the Author

John Edwards is a contributing writer for Defense Systems.