

## **DOD tackles security challenges of mobile computing**

*With lives on the line, defense organizations struggle to secure mainstream portable devices and technologies*

*By John Edwards / Jun 13, 2011*

Security concerns come with the territory for owners of a smart phone, tablet or other mobile device. Yet few people are more focused on mobile security than defense community personnel, who fully understand that missing or compromised data could lead to lost lives, not just lost money.

“Cybersecurity and data protection is one of the current ‘space races,’” said David Machuga, director of identity management and business solutions at Northrop Grumman, which supplies the Defense Department with secure mobile biometric data collection technology. “There are several challenges, but the three largest are how to certify the security, how to protect the information transmitted in a wireless mode and how to protect data at rest,” he said. “For DOD, this is a constant problem, whether dealing with cell phones, handheld bar code scanners used in a warehouse or mobile computers used to validate biometrics.”

Steve Lucas, chief engineer at the Space and Terrestrial Communications Directorate (S&TCD) at the Army’s Communications-Electronic Research, Development and Engineering Center, said the directorate’s rule of thumb is to view all commercially produced mobile devices with deep suspicion. “From our perspective, you’re taking an untrusted device because you can’t ensure where it was manufactured [or] what someone might have implanted on the device,” he said. “If we had more trust in the supply chain — who manufactured the hardware or where the software came from — I think we would feel a lot more comfortable in actually deploying these devices.”

Although many defense communications technology and security experts view commercial mobile devices and wireless networks with a sense of unease, if not outright distrust, many also understand that DOD and service branch decision-makers are facing increasing pressure to adopt commercial mobile technologies. DOD is awash with various types of highly secure terrestrial- and satellite-based mobile computer and communications platforms. But commercial alternatives tend to be more versatile in terms of real-world compatibility and application support, and they’re usually cheaper and easier and faster to deploy.

Yet none of those attributes helps tech experts such as Lucas, who are responsible for ensuring that commercial mobile devices will function securely and reliably in situations that approach the tactical extreme and beyond. When faced with systems that have little

or no real-world security track record, are built by global companies that are reluctant to divulge technology details, and are under constant attack by highly skilled and dedicated hacker adversaries, the only logical action plan is to create a well-stocked tool chest of security technologies. These tools, ranging from encryption to access controls, can then be applied to individual mobile devices in an appropriate manner with the goal of providing the highest practical level of data security. “You have an untrusted platform to begin with, and you're just trying to layer on traditional security mechanisms,” Lucas said.

### **Starting with hardware**

Hardware security is the first line of defense in the battle to protect mobile device data. DOD strives to ensure that any mobile technology it acquires is both highly reliable and secure. “The department has a challenging mission in a difficult environment that often cannot be met by [commercial off-the-shelf] systems,” Machuga said.

All of the major smart-phone and tablet makers have taken steps during the past few years to improve device security, such as by providing longer device unlock codes — in the case of Apple iOS devices — and extending encryption support to SD cards, as Research in Motion did for its BlackBerry units. Yet many defense technology experts, including Lucas and Dave Mihelcic, chief technology officer of the Defense Information Systems Agency, feel that protection measures remain insufficient for defense needs and therefore must be bolstered with additional safeguards. Ensuring that a specific mobile device is secure enough for defense community use is a responsibility that’s shared by DOD and the various military service branches.

For security guidance, mobile device administrators at any defense organization can consult a Security Technical Implementation Guide (STIG). Specific STIG versions are available for various mobile platforms and applications. “The STIGs basically specify how to configure mobile devices to achieve an appropriate level of security,” Mihelcic said. “The STIGs are collaboratively developed by DISA, national security agencies, as well as representatives of the military services.”

Decisions on which security technologies and practices are necessary for a particular device depend on how, where and by whom the unit will be used. “A lot of it is based on risk, like a risk assessment of the impact if that information should get divulged,” Lucas said. “So if the information itself is deemed very critical, that's going to elevate all the security requirements that you need to layer onto the particular device.”

Meanwhile, a vendor that hopes to get DOD acceptance for its mobile offering needs to follow steps mandated by the DOD Information Assurance Certification and Accreditation Process (DIACAP). The program was created to assure that information systems, including mobile devices, comply with DOD security requirements. “It’s the DOD’s way of certifying that a product or a service has very good risk management in it and that there are no issues that will happen when you deploy and use the system,” said

Hussam Mahgoub, senior vice president of corporate research and development at Diversinet, a company that supplies secure mobile health care technology to the Army.

Diversinet, like many vendors seeking DOD acceptance, relies on an outside organization that specializes in DIACAP certification to ensure that its products aren't rejected for an overlooked fault or shortcoming. "As a mobile security company with a deep history in that [field], every year, we get third-party organizations that specialize in risk assessment and so on to test our products and ensure that we adhere to the highest security standards, and that the product will not fail in attacks, or threats and all of that," Mahgoub said.

### **Adding encryption**

Encryption is generally regarded as the strongest tool available to lock down data stored on a mobile device. "Even if the device was lost or stolen, an adversary still can't get access to that data because it's been encrypted on that device," Lucas said.

Yet not just any encryption scheme will suffice for mobile devices used by defense personnel. All mobile encryption tools must comply with FIPS 140-2, the government computer security standard used to accredit cryptographic modules. FIPS 140-2 demands a two-factor authentication, which is based on something a user has, such as a fingerprint, and something he or she knows, such as a password. Like DIACAP, FIPS 140-2 certification is a rigorous process that sometimes motivates applicants to seek outside help. Yet certification, though a nuisance, is inescapable. "FIPS 140-2 is an important standard that's necessary in working with the military," said Rick Engle, a mobile solutions architect at Microsoft.

Besides protecting data residing on at-rest mobile devices, encryption also plays an important role in securing information moving across wireless networks. Once data leaves a mobile device and heads onto a commercial 3G or 4G network, it's the network operator's job to ensure that the information is securely transported to its destination. All major domestic carriers have developed encryption measures designed to safeguard data flowing through their cellular networks, though the results are have often been something less than inspiring.

Overseas, the situation can be even worse. In many countries, carriers lack even a minimal commitment to network security. It's also been known for service providers to directly collaborate with governments and crime- or terrorism-focused organizations to monitor and intercept wireless data.

Given the known security risks and lack of direct oversight, DOD organizations continue to maintain a cautious stance toward commercial wireless networks, both at home and abroad. "When it comes to the cellular commercial 3G or 4G type of network, I guess guidance on that is still evolving," Lucas said. "The Army does not currently deploy [on] any of those types of networks." Yet Lucas held open the possibility that the current stance on 3G/4G networks may eventually change, at least on domestic networks. "We're currently working to do that, but there is no deployed capability currently," he said.

Wi-Fi networks also pose problems. Anyone can operate a wireless hot spot, ranging from commercial operators and DOD to hacker kids and organized crime syndicates and terrorist groups. Fortunately, security over wireless links can be enhanced by placing encryption technology directly onto the mobile devices. “In terms of securing the confidentiality of the data, we can always make use of NSA-grade encryption,” Mihelcic said. “Then we have gateways to allow those [devices] to connect into DOD networks.” He added that as “more devices are approved for classified data, those gateways will be in place at the various classification levels.”

Data encryption allows mobile devices to take advantage of virtual private network technology, which creates secure connections between two or more locations anywhere in the world via encrypted tunnels through the Internet. “Commercial networks are definitely a part of our architecture,” Lucas said. “We rely on them, but many times what we'll do is tunnel across those types of networks.” S&TCD also takes advantage of other approaches to safeguard networks. “In general, they're authentication and access control mechanisms.” These tools may include complex passwords, biometric recognition technologies, such as fingerprint and iris readers.

The term defense in depth is frequently used at S&TCD to describe its multifaceted security approach, Lucas said. “It's a layering of various security technologies,” he explained. “You don't just throw encryption at the problem all of the time.”

Microsoft's Engle agreed on the need to secure mobile devices at the access level. “You can have a very good operating system and very strong security for applications, but if your devices are just sitting there wide open and not locked and somebody has access to it, then you're going to have a problem.”

### **Outrunning the avalanche**

Simply dealing with a rapidly growing onslaught of mobile devices, mobile operating systems and wireless network services is one of the biggest challenges facing administrators who work to maintain control over mobile device data. “One of the biggest problems is just the newness of the technology,” Mihelcic said. He noted that emerging products typically have only a minimal security knowledge base and are more likely to contain undiscovered security vulnerabilities than technologies that have been around for several years.

Even security technology vendors are struggling under the pressure of constantly arriving hardware, software and service platforms. “We have what I call a device and OS fragmentation,” Mahgoub said. “It makes it very difficult for companies like us to keep track of everything.”

Mahgoub observed that today's increasingly cluttered mobile landscape makes the desktop PC scene appear almost tranquil. “Essentially, in the desktop world, you have the Microsoft operating system, and it's being changed maybe only once every two or three years,” he said. In the mobile market, where Windows shares the stage with Apple's iOS,

Google's Android and other software platforms designed for use on a variety of mobile devices, significant changes can arrive as often as every few weeks.

New and innovative mobile device applications, which pop up even more frequently than hardware and software platforms, also create a constant headache for technology administrators. Because downloading and installing smart-phone and tablet software are as simple as pressing a button, it has become amazingly easy for mobile device users to inadvertently add unsecured apps to their devices. "The more third-party apps that are used on a mobile device, the more chances there are that one of them is going to be malicious or have security vulnerabilities due to its poor design," said Alexi Lesnykh, business development manager at DeviceLock, a company that develops data security technologies used by the Army Corps of Engineers and others.

Facing the security challenges posed by rapidly evolving operating systems, dodgy apps and other factors, the Army is hoping to gain an upper hand on security vulnerabilities by developing its own Android-based smart phone. The device, dubbed the Joint Battle Command-Platform, is the first unit developed through an Army effort to create an Android-based smart-phone framework and an accompanying suite of applications for tactical operations. The overall government-owned framework, known as Mobile/Handheld Computing Environment, aims to ensure that applications will be secure and interoperable with existing mission command systems, regardless of who developed them. The platform is also designed to allow information to flow seamlessly across all force echelons.

Originally prototyped by Mitre, a nonprofit technology research organization, the framework is being developed at the Army's Software Engineering Directorate. The Mobile/Handheld CE development kit is scheduled to be released to industry in July. Meanwhile, the Army is working on a set of mission command apps, including mapping, blue force tracking, Tactical Ground Reporting tactical graphics and critical messaging among all mission command systems. The basic app suite will also include an address book and OpenOffice for document viewing.

### **Policies and training**

Just as a gun never accidentally misfires, a data loss can always be traced back to one or more acts of neglect, omission or carelessness committed by the device manufacturer, software developer, network service provider, department administrator or user. In retrospect, many data loss incidents can be viewed as a concerted team effort.

Should a mobile device get lost or stolen or network security falter, DOD is prepared to exert damage control and investigate any security breach. "DOD has in place standard approaches to handle security incidents across the entire spectrum of devices and classification levels," Mihelcic said. "For every system that we have in the Department of Defense, we have assigned a Computer Network Defense Service Provider whose responsibility it is to handle those incidents."

Most security experts agree that users operating or transporting devices in an unsafe manner form the weakest link in the data security chain. Lucas said he believes that creating and enforcing a mobile device use policy is the best way to ensure the highest possible level of data security. He noted that there's no secret to effective user training other than making it comprehensive and providing it in the first place. "They just should be trained, by policy, for what they should and shouldn't do with a particular system when operating it," he said.

Meanwhile, DOD, DISA, the National Institute of Standards and Technology and various military service branch technology offices continue to work internally and with hardware and software vendors to make mobile devices safer and more reliable. Mihelcic noted that vendors are generally eager to assist the defense community "in terms of understanding and trying to work to address our requirements in their future designs, but the reality is that it is not going to happen overnight.