DEFENSESYSTEMS
KNOWLEDGE TECHNOLOGIES AND NET-ENABLED WARFARE

Protection of moving data requires multipronged strategy

Moving data securely across a wide array of data transmission technologies remains difficult

- **By John Edwards**
- **Jul 27, 2011**

Defense security experts have traditionally differentiated data protection strategies based on whether the information is at rest or in motion. But in today's highly mobile world, many people have trouble distinguishing between the two modes.

For example, is the data really at rest when it's sitting inside a mobile device such as a laptop computer, smart phone or USB memory stick that is itself likely to be in motion much of the time?

Cmdr. Greg Czerwonka, chief of the Coast Guard's information assurance policy division, said any confusion about resting vs. moving data can be easily solved by understanding that the term "in motion" only applies to data traveling through a network. "The data could be an e-mail in transit, information being downloaded from a website, the process of remotely logging in [to a website or database] through a cellular phone or other mobile device, and so on," he said. "Data stored or being used on a mobile device is considered data at rest."

Definitions aside, the big task Defense Department and military service network administrators and users face is moving data securely across a mind-boggling array of data transmission technologies that include 3G/4G wireless networks, long-distance wired networks, Wi-Fi local-area networks and microwave links. The challenge is awesome, though the burden has now been somewhat eased by data-in-motion security practices that are now uniform across all DOD organizations. "The security rules are the same for all DOD personnel, regardless of location," Czerwonka said.

Wireless networks

For reasons related to cost, deployment speed and convenience, defense organizations are deploying larger numbers of commercial laptops, smart phones and tablets that send data across commercial 3G and 4G wireless networks, largely relying on the security protections commercial carriers build into their systems. "Increasingly, the U.S. military market has turned to [commercial] technologies for cost-effective solutions to enhance their mission," said Greg Akers, senior vice president in charge of security initiatives at Cisco Systems' Global Governments Solutions Group.

Ray Letteer, cybersecurity chief at the Marine Corps' Command, Control, Communications and Computers Department, said wireless carriers build a good deal of protection into their mobile networks. "3G provided significant security improvements from the older 2G systems," he said. "We do not, at this time, see any issues in pre-4G LTE implementations that show either an improvement or decrement to security" above 3G safeguards.

For extra protection, DOD organizations that use commercial wireless networks can add a military-level encryption layer to their transmissions. "We do use encryption to secure the data as it transits those cellular networks, and then we have gateways to allow those [networks] to connect into DOD networks," said Dave Mihelcic, chief technology officer at the Defense Information Systems Agency.

Although heavy-duty encryption is a cornerstone of DOD telecommunications security, it also carries a heavy price. "The largest challenge to encryption in the DOD is the heavy reliance on NSA Type 1 encryption devices," said Kathleen Fishman, an information assurance expert at the Army Program Executive Office for Command, Control and Communications-Tactical's Technical Management Division. "This increases the cost of the device and time to procure encryption devices dramatically."

Challenging hot spots

Although commercial wireless networks can be made highly secure, public Wi-Fi hot spots present an ongoing headache for DOD organizations. "Public Wi-Fi networks generally pose a higher risk to users than government or privately owned ones," Czerwonka

said. “It is not the preferred means to connect back into our network, but there are secure methods to use public Wi-Fi networks to reach back into government or corporate networks.” Device-based encryption, though expensive and cumbersome, can be used to move sensitive data across public hot spots.

DOD organizations also can use military-grade security software, such as Layer 2-mandated security overlays, to secure their Wi-Fi networks to the tightest possible degree, Letteer said. These overlays can be added to the required WPA-PSK authentication mechanism for 802.11 a/b/g/n wireless networks. Meanwhile, the Marine Corps, like many other DOD organizations, takes the extra step of actively probing the security of its own hot spots. “Our regional blue teams conduct periodic wireless ‘war-driving’ [missions] to identify and manage Wi-Fi network use on Marine Corps bases, camps and stations,” Letteer said.

Other wireless technologies

Although 3G/4G and Wi-Fi are the wireless modes receiving the most attention from DOD security experts, other over-the-air services also require protective measures. Near-field communications technologies, such as radio frequency identification systems, ZigBee sensor networks and the Bluetooth technology that’s built into an array of mobile gadgets also need to be locked down to prevent data leakage and device exploitation threats.

“Bluetooth is an avenue that sometimes can be exploited to take control of a device, whether it be a cell phone or a portable electronic device,” Mihelcic said. “We would normally look at ways to restrict Bluetooth to prevent something like somebody remotely turning on a [smart-phone] microphone, things like that.” Most often, users are simply instructed to switch off their device's Bluetooth technology.

Point-to-point terrestrial data paths and satellite uplink/downlink connections also require encryption and access controls to prevent unauthorized interception. “Microwave channels can be secured to the same standards as copper- or fiber-based channels,” Czerwonka said.

Wired networks

Wired LANs are easily secured with firewalls and other conventional enterprise security technologies. But wide-area networks, which can span cities, countries, continents or even the entire world, are far more difficult to safeguard.

“Network perimeters have changed and blurred, with new devices and services extending the network and creating new vulnerabilities,” Cisco’s Akers said. “There is an increasing need for deeper identity and policy controls for who, what, when and where users access the network.” Such controls often come as hardware appliances that are configured to manage and authorize accredited users while recognizing and repelling intruders. DOD also has other techniques at its disposal to safeguard wide-area wired networks. “We have NSA-developed encryptors that we use to secure communications on our terrestrial backbone as well,” Mihelcic said.

Balancing act

In-motion data security and user functionality are almost inversely proportional, Czerwonka said. “In the Coast Guard, we say the same thing about our port facilities: the most secure port is the one that doesn't let any commerce flow through it.” Yet turning off the spigot isn’t a suitable solution for either networks or ports. “We expend a lot of time and energy finding the best balance of security and functionality with our given resources,” Czerwonka said.

Letteer said users can add an extra layer of headaches. “The biggest challenge is the ‘shiny object syndrome,’ where end-users are enamored by the latest technical device but don’t understand the security ramifications as they rush to acquire and implement them in a government environment.”

Czerwonka concurred. “When the next generation of a mobile device hits the market, we receive lots of requests to instantly get it out into the hands of users,” he said. Yet it can take many months for a new mobile gadget to receive a full security evaluation and clearance. “This gets increasingly difficult when new generations of devices come out every year,” Czerwonka said. “If we can't adopt a device within 12 months of when it's introduced, it may not be available for purchase.”

Is protecting data in motion worth all the energy and resources DOD organizations pour into it? Akers said there's no other choice. “Security is a daunting task,” he said. “It is a matter of both the national and economic security of the United States; we cannot afford the alternative.”

About the Author

John Edwards is a contributing writer for Defense Systems.