

BILL
SWEETMAN

H4XOR3D! MEANS HACKED

The Joint Strike Fighter and other major defense programs are targets of cyber-espionage by criminal groups working on behalf of state intelligence agencies, according to cyber-security experts. In some cases defense programs operate with protection that would not be considered state-of-the-art by many businesses. The problem came to light in May when *The Wall Street Journal* reported a major breach in the JSF program, in which “terabytes” of data were believed compromised.

There is a global effort underway to improve security in development programs and other areas to prevent them from being hacked, or in the shorthand of IT experts, “HAXOR3D.” But it’s not

networks—for protecting data on the Internet. Encryption and traditional secure means of communication—e.g., documents or CD-ROMs carried by couriers—can be used for the most sensitive information, but not for all of it.

Two factors make VPN vulnerable. The first is that it has a large “attack surface.” VPN involves a great many people and has many portals for traffic to enter. Once compromised by malware, the entire network is vulnerable.

The second is the result of what Nigriny describes as an “advanced, persistent threat.” Steve Hawkins, Raytheon’s vice president of integrated security solutions, is clear about the source of the threat: “There is interaction between

evolved in parallel. The threat today is not the threat of five years ago, “amateur hackers, doing it to show they can do it,” but using software tools that evolve in response to defensive measures.

Nigriny and Hawkins agree that the principal weapon against protected networks is an e-mail missile with a malware warhead. Hackers, Nigriny says, use “social engineering” to identify system administrators and others with high-level access, and create messages that look genuine. They may comb conference-attendee lists for names familiar to a target individual, then create an e-mail address in one of those names. Once activated, the malware copies user names and passwords and allows the hacker network access.

There are ways to improve protection. Since 2007, CertiPath has managed the Transglobal Security Collaboration Program (TSCP), launched in 2002 by the U.S. Defense Dept. and U.K. Defense Ministry, “to define an all-encompassing specification for secure data collaboration,” Nigriny says.

Secure hangars and sealed buildings cannot protect major programs like JSF from cyber-spies.

The vision for TSCP is that “data travels on the net in an MRAP”—tightly encrypted packages—“because we don’t trust any aspect of the network.” The other element is “a very high assurance of who the sender and recipient are.” This is a function where CertiPath has helped with a recent advance, says Nigriny—a Personal Identity Verification-Industry (PIV-I) standard to work alongside U.S. government PIV systems.

PIV-I will guide the design and maintenance of smart cards that control access to information systems and physical facilities, with self-contained encryption systems, biometric data and access rules. With a common data system, too, any PIV-I user will know if a cardholder is current.

Nigriny believes smart cards and encryption can solve a lot of problems, with one drawback: “TSCP was formed in response to JSF, but unfortunately started too late.” ■



JSF PROGRAM OFFICE

easy. The challenge with a program like JSF is that it includes tens of thousands of people who need access to nonpublic data (ranging from confidential to special access), in thousands of locations worldwide. The program’s scope and schedule mandate that large amounts of data are transmitted electronically, but providing a separate secret network is impossible, so data flows over public networks.

Jeff Nigriny is president of CertiPath, which provides security tools for aerospace and defense, and chief security officer of Exostar, which provides supply chain management tools for aerospace and defense companies. He believes the JSF program is probably vulnerable. “It was started before 2004,” he points out, “and I’m aware of nothing more than passwords and VPN”—virtual private

nation-states and organized crime groups, with nations hiring the groups to do their work. It can’t be labeled. The threat may appear to come from one area, but it could be somewhere else.”

Nigriny says cyber-espionage is different from non-electronic spying. In the latter, secrets can be confined to secure rooms and vaults, and held on physical documents. If the spaces are broken into or documents stolen, security managers know what is compromised. Today, “you are not stealing data, you are copying it. The loss is difficult to detect. And when you find it, you don’t know whom to blame or prosecute.”

Hawkins believes criminal groups work with nation-states because the methods of attack used for financial gain and to access military secrets have

To read weblog posts on JSF, go to DTI’s homepage, AviationWeek.com/dti, and click on ‘Extras for this issue’ under ‘DTI Interactive.’

