July 2001

Inside Oversight

Office of Independent Oversight and Performance Assurance
U.S. Department of Energy

Inside this Edition

Front Page

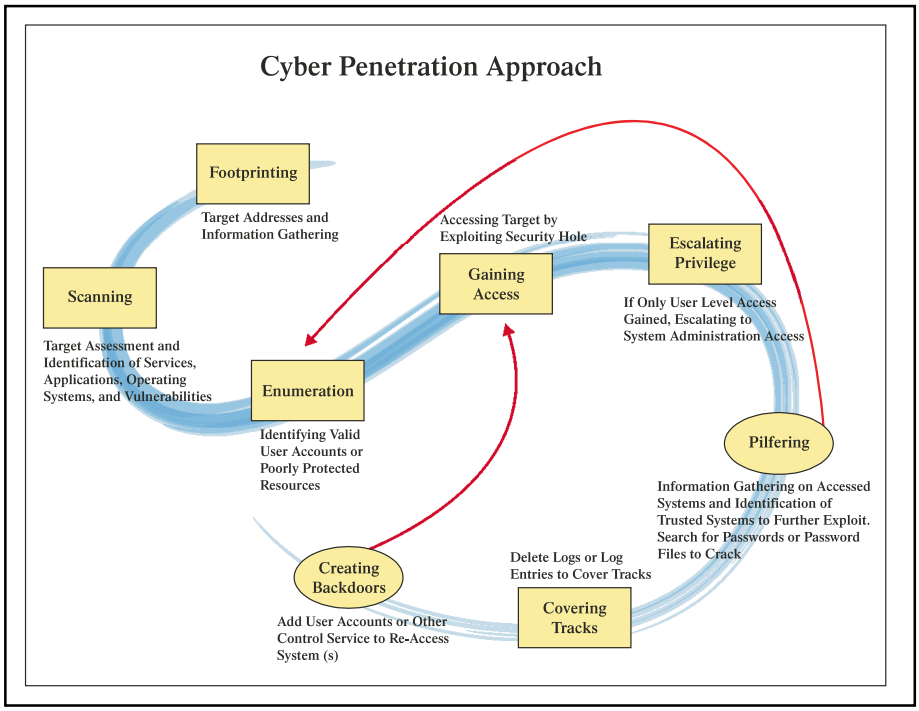
For More Information: Visit Our Website at: http://tis.eh.doe.gov/iopa

OA Demonstrates Cyber Network Penetration to Congress

At a hearing of the House Energy and Commerce Committee, Subcommittee on Oversight and Investigations, members of Congress watched a demonstration by OA network penetration specialists on how hackers could exploit vulnerabilities of government computer systems to gain access through the Internet to unclassified but sensitive information. The subject of this hearing was "Protecting America's Critical Infrastructure," focusing on the security of government information systems. The purpose of the demonstration was to provide members with a perspective on how adversaries can gather information on computer systems, exploit vulnerabilities, and compromise information technology resources over the Internet. Such techniques as footprinting, scanning, enumeration, gaining access, escalating privileges, pilfering, covering tracks, and creating backdoors (as illustrated below) were demonstrated.

Rep. W. J. "Billy" Tauzin (R-La.) states that agencies must get serious about computer security, while holding a report citing numerous security weaknesses in Federal computer systems.

During the hearing, OA was pleased to report that there have been significant improvements in DOE's cyber security over the past two years. However, much work remains to be done. Some sites still have not adequately protected their networks, and those systems could still be exploited via the Internet. Even the sites with a stronger cyber security posture must remain diligent to mitigate new vulnerabilities discovered daily and to counter the increasing sophistication of cyber attacks. Nevertheless, the concerted efforts of DOE management and the cyber security community are paying off.



OA uses many of the same steps during its penetration testing process that attackers use to gain unauthorized access to computer systems.

OA Drives Improvements in Vulnerability Assessment Methods

Vulnerability assessments are complex analyses conducted to determine the adequacy of security systems in protecting DOE assets against specific plausible threat scenarios. Within DOE, vulnerability assessments usually evaluate two types of probabilities:

- Probability of Interruption: the probability that an adversary will be interrupted by a response element, such as the site protective force, before accomplishing his or her objectives

- Probability of Neutralization: the probability that the interruption will be effective in neutralizing the adversary—that is, preventing the adversary from completing his or her intended actions.

DOE has developed a computer-based method for evaluating the Probability of Interruption called Analytic Software System for Evaluating Safeguards and Security (ASSESS). When properly used, ASSESS identifies the pathways that an adversary might use to reach a particular target and then calculates the Probability of Interruption for each one, thereby showing which pathways the adversary might be most likely to use. However, because ASSESS uses a simplistic method for calculating the Probability of Neutralization, the recent availability of enhanced computer simulations, such as Joint Tactical Simulation (JTS), has greatly improved the ability to simulate particular engagements and to evaluate large numbers of engagement scenarios through computer modeling.

The increased use of JTS, however, has introduced new difficulties. During FY 2000, OA examined the data used at several sites and determined that the JTS weapons characterizations and weapons effectiveness data were not consistent among the sites. In particular, some common weapons—such as the M-16 rifle—were not properly characterized. The accuracy of the results of engagement simulations conducted using improperly characterized weapons was placed in doubt. When these concerns were identified, DOE acted promptly by declaring a brief moratorium on the use of JTS while solutions were identified. Since that time, DOE has addressed these issues by distributing a revised JTS weapons effects database that is supported by classified Department of Defense data; establishing a methodology to ensure that approved databases are used in JTS simulations; and establishing a program of periodic updates of the JTS databases.

Recently, OA urged DOE to examine the general methodology used to determine the Probability of Neutralization, since the current methodology does not address a number of key issues. DOE does not have an approved method to combine force-on-force results with computer simulation results in computing the Probability of Neutralization. Also, the current method of simply using the ASSESS Probability of Interruption with JTS and force-on-force test results often does not provide the appropriate value. In addition, a method for combining ASSESS-derived Probability of Neutralization values with JTS and force-on-force results is needed if all three continue to be regarded as valid methodologies.

Accurate vulnerability assessments are key to developing and maintaining effective security systems. A thorough review of site vulnerability assessments has been an important element in OA inspections for many years. DOE is now considering the OA-identified issues described above. Other related issues, such as minimum standards for conducting force-on-force performance tests, JTS simulations, and ASSESS neutralization analyses when they are to be used for determining Probability of Neutralization, also need to be addressed.

Emergency Management Oversight Refocuses on Safeguards and Security Events

DOE implements emergency management and emergency response programs in order to deal effectively with emergencies of all kinds at its facilities—particularly serious emergencies that threaten life, property, or the environment. DOE sites routinely respond to minor emergencies, such as small fires, injuries, and other minor accidents, but these do not usually involve the full activation of emergency management resources that would exercise both response resources and emergency management skills. In the absence of actual major emergency operations that would demonstrate competence under worst-case conditions, oversight becomes a key way to assure that facilities and organizations develop and maintain adequate emergency operations capabilities.

From the beginning of the 1980s until the mid-1990s, the predecessors of today's Office of Safeguards and Security Evaluations conducted major emergency management performance tests as part of their safeguards and security program oversight. However, their charters were limited to evaluating DOE's safeguards and security programs, which do not include emergency management. Thus, their oversight in this area was limited to performance testing for security-related emergencies—such as terrorist attacks—and did not review overall programs or response elements other than site protective forces.

In the mid-1990s, when safeguards and security and environment, safety and health oversight were consolidated under the Deputy Assistant Secretary for Oversight (within the Office of Environment, Safety and Health), emergency management oversight emphasized the evaluation of programs and capabilities for managing emergencies related to industrial and environmental hazards. The 1997 chemical explosion at the Hanford Plutonium Reclamation Facility accentuated the need for effective response to hazardous material releases, and DOE conducted emergency management reviews at major sites. In mid-

(Continued on Page 4)

OA Moves To Protect Its E-Mail

The Federal wiretap statutes that make it a violation for anyone to disclose the contents of illegally intercepted communications were somewhat weakened in a recent U.S. Supreme Court decision. The Court ruled that the press may not be held liable for publishing such illegal intercepts. The Court, in a 6-3 vote, held that the public's interest in hearing information outweighed the privacy interests of the parties to the intercepted conversation, as long as the media themselves did nothing illegal. Justice John Paul Stevens writing for the Court said that the case, *Bartnicki v. Vopper*, was "a conflict between interests of the highest order...the interest in full and free dissemination of information concerning public issues…and the interest in individual privacy and, more specifically, in fostering private speech."

Chief Justice William Rehnquist, in dissent, warned of future high-tech invasions of privacy, in an era where forms of communication such as e-mails are heavily used and relatively easy to intercept.

Well before *Bartnicki v. Vopper* was handed down, the Office of Information Management and Tracking (OA-40) had begun to work toward the deployment of a capability to protect OA documents and e-mails from hackers and snoopers using "public key infrastructure" (PKI) encryption technology, described in the figure below. While the *Bartnicki* decision focused on balancing individual privacy against freedom of the press, privacy of governmental communication (as in the Vietnam-era leaks of the "Pentagon Papers" to the *New York Times*) remains a closely related issue. For this reason, the software program *Entrust* will be installed at each OA desktop to provide security against unauthorized intercept of OA e-mails. The private sector is well advanced in the use of encryption tools for business security, particularly in the banking and finance sector. Outside of law enforcement, intelligence, and the military, the domestic agencies of the Federal government are just now beginning to push ahead with encryption of communications. For example, the Social Security Administration will be making a priority of automatic submission of W-2 PKI encrypted forms that would not only protect the intercept of social security numbers of its customers, but also allow for authenticated "digital signatures" on important documents to protect against Medicare fraud.

In the past, encrypted material relied on a same/symmetric (or private-secret) key held both by the sender and receiver. The logistics of supporting a symmetric/secret key system for private individuals and for the unclassified work of government agencies was impractical and cost prohibitive, until mathematics professors Whitfield Diffie and Martin Hellman introduced the concept of asymmetric (or public) key systems in 1976. Public key cryptography systems use complementary pairs of keys to separate the functions of encryption and decryption. In other words, one key, the private one, is kept secret while the other key, the public one, is open to everyone. Public key cryptosystems (e.g., the *Entrust* software for OA and DOE) can be used for the functions of encryption and/or "authentication," often called digital signing or digital signature. In the encryption mode, a sender uses the receiver's public key to encrypt a message to be sent. The receiver uses his private key to decrypt the message. Thus, only the recipient who has the private key can see the message in the clear.

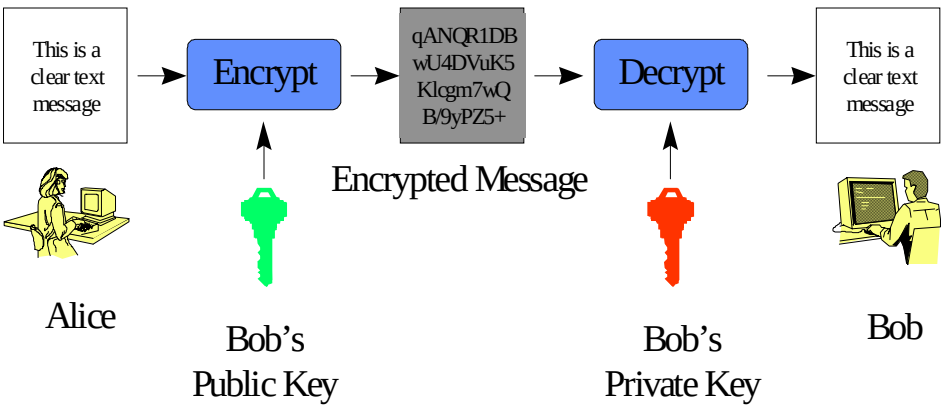
In the authentication mode, the public key is used as a decryption key. In this case, the sender uses her private key to encrypt the message and the recipient uses the sender's public key to decrypt the message.

Beyond the protection from snoopers intercepting and hackers manipulating e-mails, the powerful authentication capability of PKI technology will dramatically change the way many sorts of important documents are processed and handled. In our personal lives, processes for signing powers of attorney, wills and codicils, filing of taxes, mortgage documents, etc., will change. In the future, we may not have to be present to provide authentic signatures on legal documents; the PKI software may perform the current function of the Notary Public. Further in the future, the very notion of what constitutes a legal document or record, or, for example, representation of one person by another through power of attorney, will accordingly change.

OA-40 plans to have all of OA equipped and trained in the use of *Entrust* by year's end.

****

The case Bartnicki v. Vopper *involved a labor dispute in Pennsylvania and the repeated airing on radio of an illegally intercepted and taped 1993 cell telephone conversation between teacher's union negotiator Gloria Bartnicki and teacher's union president Anthony Kane. In the cell phone conversation, union president Kane says that if the union's demand for a pay raise is not met "we're gonna have to go to their homes…to blow off their front porches." The illegally taped copy of the call was provided to radio talk show host Frederick Vopper, who repeatedly played the tape on his local radio program.*



Public Key Encryption Process

Upcoming Oversight Activities

Hanford/Pacific Northwest National Laboratory Comprehensive Inspection
Purpose: Evaluate topics in safeguards and security, cyber security, and emergency management.
Date: July 23 - August 2, 2001
Contact: Barbara Stone, 301-903-5895

Office of Transportation Safeguards Exercise Evaluation
Purpose: Observe and evaluate full-participation exercise.
Date: July 23 - August 2, 2001
Contact: Chuck Lewis, 301-903-1554

Lawrence Livermore National Laboratory Limited-Scope Review
Purpose: Review selected areas of safeguards and security.
Date: August 13-21, 2001
Contact: Barbara Stone, 301-903-5895

Lawrence Livermore National Laboratory Emergency Management Review
Purpose: Evaluate status of emergency management program.
Date: August 13-21, 2001
Contact: Chuck Lewis, 301-903-1554

Better Self-Assessments Mean Better Programs

Feedback and continuous improvement are key elements to managing DOE safeguards and security programs. In agreement with leading management experts, DOE's integrated safeguards and security management approach emphasizes self-directed efforts in promoting feedback and continuous improvement and in maximizing overall program effectiveness. Although the self-assessment process is one of the DOE manager's most vital tools, recent inspections show that some self-assessment programs are not as successful as others in serving management needs. Two specific practices characterize the most successful programs.

☑ A self-assessment should be more than a set of completed checksheets. The best self-assessments are based on a balance of activities that assess both compliance with specified requirements and the fulfillment of appropriate performance standards to determine the overall effectiveness of program elements. This approach requires a mix of compliance-based and performance-based assessment activities.

☑ The best self-assessments focus on finding the real causes of problems, not just the symptoms. This focus helps managers determine how best to assign responsibility for corrective actions—including line management, as well as security managers—and assures that the corrective actions will prevent the recurrence of similar problems. Managers must also encourage candor in the self-assessment process, since the self-identification and self-correction of problems is integral to DOE's integrated safeguards and security management approach.

By building on these successful practices, managers can improve their self-assessment programs to provide more meaningful feedback. ■

Emergency Management Oversight Refocuses on Safeguards and Security Events (continued)

1999, responsibility for emergency management oversight was included in the mission of the newly created Office of Independent Oversight and Performance Assurance (OA). Since then, OA has continued the previous emphasis on emergencies involving industrial and environmental hazards, with special focus on hazardous material releases.

Now, in response to current DOE needs and priorities, OA is broadening emergency management reviews to emphasize operational emergencies initiated by safeguards and security events and conditions. Although response to hazardous material releases will also be reviewed, OA will assess capabilities for managing security-related emergencies (such as terrorist attacks and bombings) and their consequences. OA will conduct performance tests, including large-scale exercises and tabletop exercises, to determine whether all emergency response and management elements perform effectively. By broadening the scope of oversight, OA will provide the Secretary of Energy, the National Nuclear Security Administrator, and other senior DOE managers better information on the status of DOE's emergency management capabilities. ■

Solicitation of Comments, Questions, and Suggestions

OA welcomes your thoughts about our newsletter. Please send or phone comments, questions, or suggestions to:

Glenn S. Podonsky, Director
Office of Independent Oversight and Performance Assurance
U.S. Department of Energy
19901 Germantown Road
Germantown, MD 20874
301-903-3777

e-mail: Glenn.Podonsky@eh.doe.gov

This newsletter can be found on the OA web site at **http://tis.eh.doe.gov/iopa**.