September 2002

Inside Oversight

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

Inside this Edition

For More Information:
Visit Our
Website at:
http://www.oa.doe.gov

CYBER SECURITY

Know What You're Defending

If you've recently assumed duties as Information Systems Security Manager, or if you're a new line manager being briefed by your cyber security team, one of the first things you should ask is, "What is our defensive perimeter?" In the world of physical security this is a fairly easy question to answer—all you have to do is find the fence. But the situation is quite a bit more challenging in the virtual world of the Internet.

In this issue of *Inside Oversight*, we're spotlighting four efforts under way by the Office of Independent Oversight and Performance Assurance (OA) Office of Cyber Security and Special Reviews (OA-20). First, OA-20 has added a new weapon against vulnerabilities to the arsenal of tests it uses while conducting onsite cyber security reviews—the discovery and testing of wireless networks. Wireless network technology is inexpensive and extremely easy to use, but it represents an elevated risk to Department networks if not implemented securely.

Second, OA recently performed a cyber security assessment of a commercial petroleum pipeline company, a component of the nation's critical infrastructure. The results of that review were briefed to Mr. Richard Clarke, President Bush's Special Advisor for Cyberspace Security and Chair of the President's Critical Infrastructure Protection Board. As a result of that briefing, OA was asked to create guidelines to help various organizations improve the security of networks that make up our critical infrastructure.

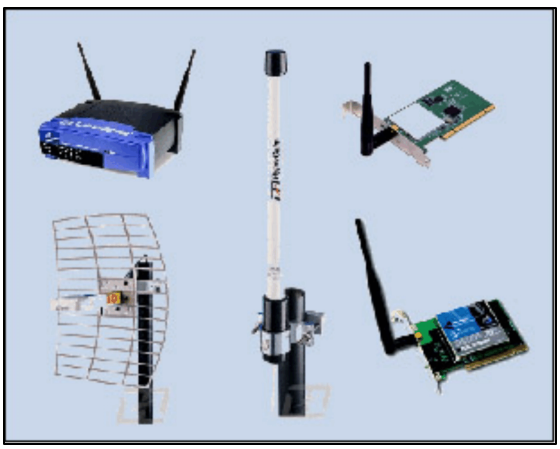
Third, in partnership with the Office of the Chief Information Officer, OA has begun an assessment of the Department's external network perimeter. This project is the first of its kind in the Department. The network topology of the DOE complex is just that—complex. Upon completion of this project, the Department will have an invaluable resource for further improving the security of critical and sensitive data.

Finally, OA is planning to initiate unannounced penetration testing within the DOE complex to provide a more realistic approach to network vulnerability analysis. In conducting these tests, OA will work closely with trusted agents from DOE Headquarters and the Computer Incident Advisory Capability (CIAC). This effort will allow OA to better meet its obligations in conducting performance testing, while at the same time promoting effective, real-world security within the Department. ■

Cyber Team Focuses on Wireless Networking

Based on information from the Systems Administration Networking and Security (SANS) Institute, wireless networks are abundant, and the vast majority does not use any security protection measures. The Office of Cyber Security and Special Reviews (OA-20) is now evaluating the security of wireless network technology—commonly called "WiFi"—within DOE.

Because of its low cost and ease of deployment, many organizations have implemented WiFi quickly and with insufficient planning, resulting in weak security that is not commensurate with the data passing over the wireless network. Wireless signals propagate beyond the physical boundaries of buildings or controlled areas, and anyone with a laptop computer and inexpensive hardware can capture those signals. Therefore, securing these networks is a vital concern. ***(Continued on Page 4)***



Wireless network detection equipment.

Improving the Security of Critical Networks

Many essential services—such as electricity, natural gas, water, waste treatment, and transportation—are controlled by supervisory control and data acquisition (SCADA) networks that are part of the nation's critical infrastructure. In the aftermath of September 11, 2001, President Bush created the President's Critical Infrastructure Protection Board to coordinate all Federal activities related to the protection of key information systems and networks, including SCADA systems.

The Department of Energy plays a key role in protecting the nation's critical energy infrastructure. The Office of Energy Assurance has worked with Federal, state, and private partners to protect the national energy infrastructure, improve energy reliability, and assist in energy emergency response efforts. In cooperation with the President's Critical Infrastructure Protection Board, OA has also supported this effort by assessing several organizations with SCADA networks and, recently, by developing a set of guidelines for improving the cyber security of SCADA and other networks.

The Board recently released the guidelines developed in cooperation with the Department, specifically for SCADA systems, as part of homeland security initiatives. The focus on SCADA systems results from the fact that they are critical to the nation; if a cyber attacker were to disrupt service, redirect processes, or manipulate the data in a SCADA system, there could be serious consequences, in terms of public safety and the availability of indispensable public services.

But even in organizations that are not part of the nation's critical infrastructure, some computer systems or networks are more critical than others to organizational functioning. Here, OA describes actions that more broadly emphasize the need to identify which functions are most critical, and to provide security and manage risk commensurate with the relative importance of the service or process and the sensitivity of the data. These activities are conceptually simple—knowing what devices and connections are on the network, getting rid of unnecessary items, staying aware of threats and how to counter them, and promoting vigilance and accountability. Although these actions will not directly address every possible concern for every network, they can help any organization improve its overall cyber security posture.

☑ **Identify.** The first step—often, surprisingly, overlooked—is simply to identify all network connections: not only Internet connections, but also internal local area and wide area networks, including business networks; modem and dialup connections; and connections to business partners, vendors, and regulatory agencies. Also, as noted in a related article in this issue, wireless networks have recently proliferated, often without adequate recognition. The protective measures that are implemented for each connection must be identified, as well as the sensitivity of the data passing through the connection. This basic information underlies all well considered risk management decisions.

☑ **Disconnect.** Although networks can pass information efficiently and conveniently, unsecured connections are simply not worth the risk. After identifying all connections, disconnect or disable any unnecessary connections and network services. Any remaining connections should be thoroughly justifiable. For the most sensitive systems, consider whether complete isolation is desirable; in such cases, it might be appropriate to transfer data via physical media rather than via a network connection. If interconnection is essential, apply filtering and other technical and administrative controls to assure an appropriate level of security. Note that any such measures must be properly designed and implemented to avoid introducing additional risk.

☑ **Harden.** Many organizations and users do not implement even the relatively weak security features resident on their systems. While using these features is a good preliminary step, relying on proprietary protocols or default settings alone can be a mistake, and vendor "patches" to correct known weaknesses must be implemented promptly and properly to maintain security. Removing or disabling unused or inappropriate services and network daemons also reduces the risk of direct attack. Remote maintenance, for example, should be disabled unless a risk assessment shows that the benefit of the service far outweighs the potential for exploitable vulnerabilities. Similarly, any "backdoor" or vendor connection must be protected with strong authentication methods.

In short, any network is only as secure as its weakest connecting point. Most organizations need to at least consider implementing firewalls, internal and external intrusion detection systems, and other security measures at each point of entry into the network. Monitoring real-time activity at each entry point is often desirable, and most sensitive systems should have protective measures configured to identify suspicious activity and notify system administrators 24 hours a day, 7 days a week.

☑ **Evaluate.** Technical cyber security audits that include penetration testing and vulnerability analysis provide indispensable information for developing a robust protection strategy. Many cyber security tools can be used to identify active services, patch level, and common vulnerabilities. Although they cannot solve systemic problems, these tools can help eliminate many paths that an attacker could exploit. To be fully effective, technical audits must be part of an ongoing process that also involves tracking corrective actions, identifying trends, and retesting systems after corrective actions have been implemented.

An important, and often overlooked, aspect of systems security is physical security. Any unmanned or unguarded site that has a "live" network connection or access point is a potentially vulnerable target. Access controls should be adequate to prevent unauthorized physical access to hardware and any other possible source of information—including remote telephone, computer network, and/or fiber optic cables; exploitable radio or microwave links; and wireless local area network access points.

A final aspect of evaluation is identifying potential attack scenarios and system vulnerabilities. Many organizations have established "Red Teams" to provide insight into weaknesses of the overall network, physical systems, and security controls. Since the threat from a malicious insider is one of the greatest threats for any organization, this risk, too, must be fully evaluated. Information from "Red Team" evaluations should be fed into risk management processes to assess the information and establish appropriate protection strategies.

☑ **Strengthen the Program.** A strong, ongoing cyber security program builds on the information and processes established by the previously described actions and uses them to promote effective threat identification and risk-based decision making. As a continuing effort, network architecture must be documented as it evolves, and new systems that serve critical functions or contain sensitive information must be identified and brought under control. Finally, the program should be administered through effective policies and procedures and clear definition of roles, responsibilities, and authorities for managers, system administrators, and users.

Checking the Fence Line: The Perimeter Scanning Project

In partnership with the Office of the Chief Information Officer, OA has initiated a review of the Department's external network perimeter—its "fence line" in cyberspace. This effort will identify the Department's vulnerabilities in cyberspace and collect technical data to help the Department develop better protection strategies.

During the past month, OA has completed extensive discussions with the Office of the Chief Information Officer to finalize plans and methods for conducting this perimeter scanning project. The primary activity in this project is external scanning—identifying, from a remote location, what services and ports on DOE systems are accessible from the Internet. The OA cyber team will first identify the scope of the Department's network perimeter by using both external and internal information sources. Public information sources, such as Network Solutions Registrar Database (InterNIC) and the American Registry for Internet Numbers (ARIN), will be consulted initially to identify the ranges of Internet Protocol (IP) addresses controlled by DOE. The team will confirm these IP addresses with Headquarters, program office, and field organizations and conduct pilot testing before proceeding to the meat of the project.

All project activities will be governed by performance test agreements negotiated between OA and the sites and organizations to be assessed. A draft agreement, similar to the agreements commonly used during regular cyber security inspections, is being prepared and will be included in the project.

The activities described below will be conducted remotely from OA's cyber security laboratories located in Germantown, Maryland and Columbus, Ohio. The software tools will be configured to identify Systems Administration Networking and Security (SANS) Institute/Federal Bureau of Investigation (FBI) "Top 20" vulnerabilities, as well as other common and important vulnerabilities. (The SANS/FBI Top 20 represent the security industry experts' consensus of the 20 most critical Internet security vulnerabilities.)

Network Discovery and Host Scanning

After initially defining and confirming the ownership of IP address space, the OA team will begin active "network discovery"—identifying all DOE-owned host systems that are accessible via the Internet. In this phase, the team will use nmap, which is one of the software tools a malicious hacker would use. The team will attempt to bypass and subvert firewalls and take advantage of any poorly implemented firewall rules, but will not attempt to evade intrusion detection systems.

Checking out the virtual fence line.

Nmap will also be used to scan the identified hosts to show which Internet-accessible services are running on each one and the effectiveness of the site's firewall policy.

Vulnerability Assessment

As the next step, the OA team will use the vulnerability identification tool Nessus to scan for the SANS/FBI Top 20 vulnerabilities, plus other potential vulnerabilities judged to be particularly relevant to DOE's network perimeter. These tests will be set up to avoid denial of service on the targeted systems and networks. Based on the results of these tests, the vulnerability assessment will yield detailed descriptions of specific vulnerabilities, as well as information on approaches to mitigating those vulnerabilities.

If the OA team discovers a potentially serious vulnerability that presents an immediate risk of compromise, the team will act expeditiously to inform the site of the vulnerability and will work with the site to address the situation.

Data Aggregation and Reporting

The tools used during this project will generate a large volume of scanning data. The OA team intends to import this data into a relational database in order to generate statistics applicable to the overall security of DOE's Internet-accessible assets. This information will be of use to the Office of the Chief Information Officer, DOE line management, and the Computer Incident Advisory Capability (CIAC) in improving the Department's cyber security posture. The database will be designed to provide full and adequate protection for this sensitive information.

Data analysis and reporting activities are expected to begin this fall. Initially, each site or organization that is evaluated will receive a management-level summary, along with a compact disk containing all the technical data gathered during testing (including full scan results for the IP addresses for which the site or organization is responsible). Site technical personnel will be able to use this data immediately to initiate corrective actions.

At the conclusion of the project, OA and the Office of the Chief Information Officer will analyze the data for individual sites and organizations, and for the DOE complex as a whole. Analysis results will be validated, and a summary report will be prepared. The final report will be provided to lead program secretarial offices and other organizations that are in a position to foster technical and programmatic improvements.

Upcoming Oversight Activities

ES&H and Emergency Management

Pantex

Sandia National Laboratories - New Mexico

Y-12

Emergency Management

Office of Transportation Safeguards

Safeguards and Security Follow-up

Argonne National Laboratory - West

Security and Cyber Security

Los Alamos National Laboratory

Savannah River Site

Nevada Test Site

Chicago Operations Office - Cyber Security only

Cyber Team Focuses on Wireless Networking (continued)

The OA-20 technical team has recently completed research and developed performance testing methodologies that can be used at DOE sites to identify WiFi signals that could be intercepted and exploited. The results of this effort are now being applied during onsite inspections to improve the comprehensiveness of OA-20 cyber security technical performance testing.

The Process

A first step in locating and assessing wireless networks is "war driving": OA-20's cyber penetration testing team drives around the site or city with a wireless-capable laptop computer, "sniffing" for wireless network access points. (The term "war driving" is adapted from the term "war dialing," popularized in the 1983 film *War Games*.) The team also uses a free software application called NetStumbler to characterize the access points that are identified. NetStumbler collects a great deal of information about each wireless network in a fraction of a second—for example, the network name, the brand and model of the device, and whether or not the integral security protocol, Wired Equivalent Privacy (WEP), is turned on.

By using different types of antennas, OA can not only identify that a signal is present, but also pinpoint where, in a specific building, the signal originated. This information can then be used to attempt to record network broadcast information and "hijack" the network connection. OA performance testing is designed to check for unauthorized WiFi access points as well as security weaknesses in any authorized access points.

Over the Horizon

Many companies, and DOE sites, have implemented wireless networking technology to create massive distributed networks with many public and private access points. As often happens, security has been an afterthought. It is virtually certain that attackers will try to exploit WiFi vulnerabilities at DOE sites, and OA-20 has taken the first steps toward identifying what an attacker could accomplish.

In upcoming cyber security inspections, OA-20 will include wireless networks in its program of technical testing, with the goal of identifying vulnerabilities and noting opportunities for improvement. As the technology develops, OA-20 will continue to expand its testing protocols to help DOE remain ahead of would-be attackers.

Making Your Improvements Count

The ultimate test of any security program is whether it can respond well to an actual attack. OA has a longstanding commitment—and a Federal mandate—to conduct performance testing that simulates, as closely as possible, the parameters of a real-world attack. OA's realistic performance testing has led to significant gains in many areas of safeguards and security, such as physical security systems, protective force operations, and nuclear material control and accountability. Now, in cooperation with DOE Headquarters and CIAC, OA is planning to bring these benefits to the DOE cyber security community.

The cornerstone of this effort is unannounced penetration testing from a remote location. Protocols to guide this testing are under development. With the assistance of trusted agents from Headquarters and CIAC, the OA penetration testing team will conduct tests that more closely simulate the conditions of a real attack. To better represent the resources that would be available to a real attacker, the OA team will employ some "social engineering" techniques to help gain access to protected systems. However, OA will continue to observe its self-imposed restriction on using denial-of-service in its testing methodology.

As the safeguards and security community has learned, challenging performance tests represent an unparalleled opportunity to show that their programs work well. Now, DOE cyber security programs can have the same opportunity to demonstrate their ability to detect and repel remote attackers.

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
OA-1/Germantown Building
U.S. Department of Energy
1000 Independence Avenue, SW
Washington, DC 20585-1290
301-903-3777

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

This newsletter can be found on the OA web site at **http://www.oa.doe.gov**