NATIONAL INFRASTRUCTURE PROTECTION CENTER

HIGHLIGHTS

A publication providing information on infrastructure protection issues, with emphasis on computer and network security matters.

Issue 3-02
June 15, 2002

Editors: Linda Garrison
Martin Grand

- **Information Sharing and Analysis Center – Oil & Gas**
- **Pipeline Security: Economic Reliance Underscores New Threat Reality**
- **New Storage Technologies: Challenges for Data Security**
- **Wastewater Control Systems: Australian Case Illustrates Threat and Risks**

We welcome your comments and suggestions for improving this product. For more information, or to be added to the distribution list, please contact the NIPC Watch at nipc.watch@fbi.gov or call (202) 323-3204.

Information Sharing and Analysis Center – Oil & Gas

This article continues the series of overviews of critical infrastructure industry initiatives established in response to Presidential Decision Directive 63 (PDD-63).

An important security asset was introduced for the oil and natural gas sectors on November 1, 2001, as the Energy Information Sharing and Analysis Center (ENERGY-ISAC) began operations. This ISAC, taking its place beside the Electric Power ISAC established about a year earlier, was created to help mitigate the oil & gas sector's collective issues, and resulted in part from the recommendations contained in a study by the National Petroleum Council titled "Securing Oil and Natural Gas Infrastructures in the New Economy" (http://www.npc.org).

Some of the services provided by the Energy ISAC include:

- A one-stop clearinghouse for security information (including Warnings and other information shared with the sector by the National Infrastructure Protection Center).
- Near-real-time warnings of potential threats on a 24/7 basis.
- Identification of infrastructure vulnerabilities from both cyber and physical threats.
- Analysis by professionals providing strategies for dealing with those threats.
- Information technology solutions, patches and access to Best Practices information.
- The ability for members to communicate securely.

A key aspect of the ENERGY-ISAC consists of its two-way information sharing capability. While data will be acquired from a broad range of global sources, perhaps the most important source of information will come from the ISAC members themselves. For example, if a member experiences an attempted exploit against one of its systems, it can notify the ISAC, which, in turn, can disseminate this information in near real time to other members, and the NIPC. Notably, items may be submitted anonymously, thus avoiding unwarranted exposure.

The membership policy of the ENERGY-ISAC ensures that information stays within the ENERGY-ISAC. For example, while government agencies can submit data to the ISAC, they cannot access ENERGY-ISAC information. In fact, a Board of Managers must approve any information provided by the ISAC to other entities. The importance of having a security entity dedicated to the needs of the oil & gas sectors has become increasingly clear in the post-September 11th threat environment. Furthermore, since applications of related technologies-such as Supervisory Control And Data Acquisition (SCADA) systems can be industry specific; having an ENERGY-ISAC in place to provide tailored vulnerability information is an invaluable resource.

For more information on the Energy ISAC, please visit their web site at http://www.energyisac.com. For information on membership eligibility, please see http://www.energyisac.com/join.cfm.

Pipeline Security: Economic Reliance Underscores New Threat Reality

On October 4, 2001, a man armed with a .338 caliber rifle fired several shots at the Trans-Alaska pipeline, causing a puncture that released an estimated 285,000 gallons of oil. Although this was an isolated incident not related to a known terrorist organization, it did occur shortly after Sept. 11th despite increased pipeline protections to thwart terrorist threats.

The Trans-Alaska pipeline carries approximately one million barrels of oil a day. A well-coordinated attack against multiple transmission and distribution locations would have severe ramifications on our nation's economy. Compounding this vulnerability is the current political climate of oil producing nations that could leave the U.S. increasingly susceptible to supply interruptions.

Pipeline industry representatives have requested help from the federal government in addressing terrorist threats. The following needs have been identified:

- Government/industry partnerships in order to address security needs,
- A more coordinated federal approach to pipeline security,
- Closer local level ties to law enforcement and emergency management agencies,
- Specific information on threats, and
- Assistance in providing armed protection at key facilities.

The Office of Pipeline Safety (OPS), administered by The Department of Transportation's Research and Special Programs Administration, has traditionally dealt with safety issues, but subsequent to the Sept. 11th attacks has been primarily focusing on pipeline security. OPS will support the Transportation Security Administration, also tasked with pipeline security.

In response to these challenges, legislation has been introduced which addresses security issues, including:

- December 20, 2001, "The Pipeline Infrastructure Protection To Enhance Security and Safety Act" (H.R. 3609) was introduced in the House of Representatives and has been referred to House Committee on Energy and Commerce.

- March 7, 2002, Senator John McCain proposed a pipeline safety amendment to the Energy Bill (S. 517). Congress, led by Billy Tauzin (R-La.), is currently attempting to reconcile this Senate bill with the House bill (HR 4).

- March 12, 2002, "Energy Pipeline Research, Development, and Demonstration Act" (H. R. 3929) currently in House Committee on Energy and Commerce.

Pipelines, and their related facilities are among our country's most critical infrastructure components. Due to our nation's recent heightened threat environment, pipeline security is receiving renewed attention. It is important to capitalize on this awareness to ensure we are prepared for future threats.

New Storage Technologies: Challenges for Data Security

Electronic data storage technologies are evolving at a rapid pace. Key salient developments in storage technology include:

- **Solid State Storage Devices -** Small memory cards and other types of flash media, popular for use with consumer electronics, some of which store hundreds of megabytes of electronic data, can function as plug and play computer data storage.
- **Data Transfer Interfaces -** Most new computers are equipped with Universal Serial Bus (USB) ports, allowing storage media to be simply plugged in to an operating computer. The IEEE-1394 standard, also called FireWire or i.LINK, offers similar hot-pluggable convenience with data transfer rates up to 50 megabytes per second.
- **Data Storage in Consumer Electronics -** Many non-computer electronic devices now feature impressive digital storage capacities such as one portable digital music player that has a 10-gigabyte hard disk accessible via a FireWire interface.

Developments in storage media have security implications in any environment where sensitive or proprietary information is digitally processed. The shrinking size of data storage devices results in the ability to conceal them easier than ever before. Additionally, the storage capacities of these devices often allow hundreds of megabytes of data to be transported in a very small package. USB and FireWire interfaces allow hot-pluggable, high-speed data transfer to removable storage by anyone with physical access to an unprotected computer. In the case of consumer electronics, their capacity to function as computer data storage devices may not be readily apparent allowing the bearer to avoid suspicion that would accompany the carrying of traditional storage media.

These factors suggest the potential for information security breaches. For example, a visitor may be able to copy the owner's entire e-mail database or hundreds of megabytes of files containing research data or business plans. Additionally, network attack tools or other malware could be introduced onto a computer network, evading the protective measures implemented at the network boundary. In either case, it may not be readily apparent to staff that the malicious actor is carrying any computer storage media, and the local (i.e., non-network) data transfer may not be recorded in any log.

In order to protect against the risk of industrial espionage or an insider attack, infrastructure owners and operators need to implement a comprehensive plan encompassing both technological and operational measures that address both the physical and cyber perspectives. Security practices such as locking all unattended workstations, escorting visitors, physical security patrols, and internal network monitoring acquire much higher priority in today's environment than they have in the past.

Wastewater Control Systems: Australian Case Illustrates Threat and Risks

Wastewater utilities need to evaluate a wide range of elements from hazardous chemical storage to the physical and electronic security of treatment and monitoring processes to guard against criminal/terrorist actions. As computer networks and digital monitoring and control technologies continue to play an increasing role in the water industry, risks posed by breaches in electronic security become more widespread.

In the spring of 2000, Maroochy Shire, a community on Australia's Sunshine Coast, began having a series of problems with its wastewater system. In one particularly damaging incident in March 2000, a failure at a pumping station caused up to one million liters (264,000 gallons) of raw sewage to flow onto the grounds of a local tourist resort and eventually into a storm sewer. The problems were traced to disruptions in the community's new computerized sewage control system. Suspicion fell upon a former employee of the company that had installed the control system. On 23 April 2000, police intercepted Vitek Boden, less than an hour after another control system malfunction. A search of his vehicle found a two-way radio and antennae, a remote telemetry system, and a laptop computer.

Authorities subsequently charged Boden with perpetrating at least seven sabotage attempts against the community's sewer system, alleging he used his computer and telemetry units to manipulate the computerized control system via remote radio transmissions. Prosecutors stated that the deliberate sewage overflows cost the community approximately $95,000 in repairs, monitoring, clean-ups, and extra security resulting in significant damage to the environment and to the quality of life of local residents.

In October 2001, an Australian jury found Boden guilty of 30 charges in connection with the incidents. Sentenced to one year in prison for willfully causing serious environmental harm and two years for computer hacking and theft of equipment needed to effect access, he was also ordered to pay approximately $7,000 in compensation to the local council whose systems had been penetrated.

This incident has broad application to the wastewater industry and its related sectors.

- Although not directly connected to the Internet or other public networks, all remote telemetry and control systems are at risk from both external and insider attackers experienced in enterprise networks including intrusion, manipulation, malicious code, and denial of service. Malicious actors are able to purchase, steal, build, or otherwise obtain specialized electronic equipment needed to access even obscure and proprietary electronic systems.
- The threat posed by insiders should also include former employees and contractors who may have motive to exploit their insider access and/or knowledge of control systems and specialized equipment.
- Control and telemetry systems should be monitored for possible trends that may evolve into malicious activity.

Implementers need to consider access control and authentication issues for infrastructure control systems carefully, including access to default or system accounts or any other account that may have been active during system development and testing. Passwords should be changed regularly and **all** access should be reviewed if system irregularities are suspected. Depending on the architecture, various technologies such as call-back connections to known telephone numbers or filtering of incoming connections may help mitigate risks of unauthorized persons accessing control systems.

According to the U.S. Environmental Protection Agency, the United States' wastewater infrastructure includes approximately 16,000 publicly owned wastewater treatment plants and 100,000 major pumping stations. The securing of electronic systems used to control and monitor these facilities will be a significant task. However, the possible consequences of sabotage to our wastewater infrastructures such as: the public health impacts including immediate and long term illnesses, loss of life in worst case scenarios, contamination of drinking water, significant environmental damage, destruction of wildlife, closing of recreational areas, disruption of fishing and other commercial ventures, and deterioration of quality of life, are significant and should be considered.