

Government Computer News

DHS, industry use LOGIIC to combat cyberthreats

Joint exercise focuses on protecting systems
at oil and gas facilities

BY KERRI HOSTETLER | GCN STAFF

THE HOMELAND Security Department has teamed with 13 organizations on a 12-month project to secure the process control systems of the nation's oil and gas industries against cybersecurity threats.

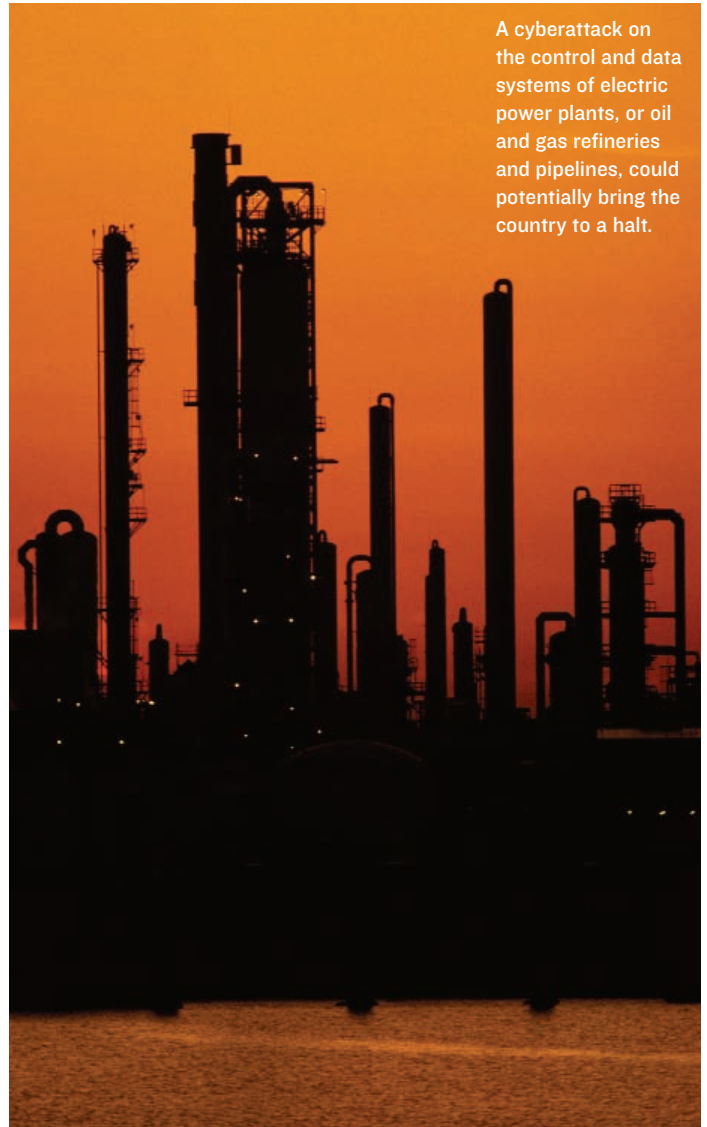
A cyberattack on the control and data systems of electric power plants, or oil and gas refineries and pipelines—two of 17 pieces of the nation's critical infrastructure—could potentially bring the country to a halt. The problem is compounded because private companies control 85 percent to 90 percent of the country's critical infrastructure—leaving the government few avenues to ensure that IT systems are secure.

Real-life process

Linking the Oil and Gas Industry to Improve Cybersecurity (LOGIIC) was born out of the

Cyber Security Research and Development Center, which is supported by DHS and run by SRI International of Menlo Park, Calif.

LOGIIC, for the first time, brought government, industry, research labs, security vendors and process control technology vendors together to recreate a real-life process control system test bed. They then attacked the test bed, at Sandia National Laboratories in Albuquerque, N.M., with viruses, worms and cyberterrorism techniques to see if they could fix system vulnerabilities.



A cyberattack on the control and data systems of electric power plants, or oil and gas refineries and pipelines, could potentially bring the country to a halt.

“The goal was to come up with technology, then demonstrate the technologies that could reduce vulnerabilities in infrastructure. Oil and gas should be commended for doing just that,” said Doug Maughan, DHS’ program manager for cybersecurity research and development.

The potential costs of an infrastructure attack are significant. The Northeast Blackout on April 14, 2003, left 50 million customers and parts of eight states and Canada without power. The outage cost an estimated \$7 billion to \$10 billion in financial losses, and shut down parts of a 2 million barrel-per-day pipeline and airports in 13 cities, according to a report by an electricity consumers research council. Terrorism played no role in the power outages.

But DHS and the private sector created LOGIIC to safeguard against an attack that could create the same result, as well as other scenarios, such as disruptions of oil refineries or distribution operations.

The process control system simulated the two components of the oil and gas industry: the distributed control system (DCS), which manages the refining process (also known as the process control system, or PCS), and the supervisory control and data acquisition systems (SCADA), which manage oil and gas pipelines.

Control networks used to be run on proprietary networks with proprietary protocols. But the industry has converted to standard operating systems and protocols, which leaves them more vulnerable to attacks, said Paul Granier of ArcSight of Cupertino, Calif., a security vendor for the project, in a video released by DHS.

System vulnerabilities

The consortium identified five vulnerabilities of the process control system, but focused on two: securing the system against outside attackers using the Internet, and securing the system from hackers using

remote sites to breach physical security, said Ben Cook, principal member of research at Sandia.

“We asked ourselves, ‘How can this be exploited? What are cyberpaths attackers can take to compromise critical components?’” Cook said.

According to the video, the consortium aimed the first attack at the demilitarized

“We asked ourselves, ‘How can this be exploited? What are the cyberpaths attackers can take to compromise critical components?’” BEN COOK, SANDIA NATIONAL LABORATORY

zone that serves as a buffer between the business and process control network systems. The second attack targeted flow meters at physical sites.

Wiring the system

After the first pilot, industry members asked security and process control vendors who supply critical technologies to the oil and gas industry to be part of the second phase of the project. Then the lab connected the technology to the test bed and ran the attacks again.

“We wired the system together like real life. It was a simplified representation of what you would see in the field,” Cook said.

The new software created a correlation engine that let process control operators look at one screen and determine which alerts were critical to the security of the system, Cook said.

This was not possible before LOGIIC, said Raymond Parks, Sandia’s lab technology staff member, on the video.

A team member connected an embedded firewall to a network interface card in the test bed to determine the security system’s

ability to protect the SCADA system, said Charlie Payne, a researcher for Adventium Labs of Minnesota.

“The goal was to show you could detect and correlate suspicious events and report it on a host-based network,” said Payne.

The software from security and technology vendors proved its ability to address the vulnerabilities the oil and gas industry were concerned about, officials said.

“It [the new system] provided high-level insight into which breaches were critical. The system aggregates and correlates sensor feeds for high-level awareness,” Cook said.

Chevron contacted DHS in April 2004 to start an initiative to address oil and gas vulnerabilities, which led to a workshop for industry members in July. In February 2005, members of the LOGIIC team met to decide what problems the group could address.

DHS and industry both spent about \$600,000 on the project. Both hosted a workshop in Houston on Sept. 11, 2006, to present the LOGIIC project to industry members.

Maughan stressed the importance of the partnership model used in LOGIIC because he believes it is a model that can be used in other sectors. The Energy Department has contacted DHS to learn about the LOGIIC model.

DHS is not planning on regulating any of the technologies used in LOGIIC, which proved to protect process control networks from attacks.

“It’s up to oil and gas to bring in this technology and implement it. Our mission is to do research, development, testing, integration, evaluation and transition,” Maughan said. ■



About ArcSight

ArcSight, a leader in Network and Security Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action. ArcSight solutions address today’s complex enterprise networks that span multiple organizations and corporate business initiatives. By comprehensively collecting, analyzing, managing and responding to security and network data, ArcSight solutions mitigate information risk for real-time threat management, compliance reporting and automated network response. ArcSight’s customer base includes leading global enterprises, government agencies and MSSPs.