Attacks on Power Systems:
Data Leakage, Espionage, Insider Threats, Sabotage

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

In this third in a series of articles about the need for information assurance in the electric power industry, the following sections present information dating back over the last decade that bear on electric power industry and related systems and involving

- Data leakage
- Industrial espionage
- Insider threats
- Sabotage

Data Leakage, Industrial Espionage, and Insider Threats

Data leakage is one of the intractable problems of information assurance because of the possibility of covert channels for extraction and exploitation of unrecognized copies of confidential data.[1] The situation is worsened by malicious software such as spyware that broadcasts confidential data.[2] Industrial espionage often involves insiders.[3]

2006 Japan’s Power Plant Security Info Leaked Onto Internet

In May 2006, security data about thermal power plants in Owase, Mie Prefecture which are run by Chubu Electric Power Co. (based in Nagoya) in Japan were leaked to the public Internet through a personal computer infected with a virus. Leaked information included plant locations and information about “the control room, instrument panel room and boilers….” as well as copies of “manuals on how to deal with unconfirmed reports of intruders in the plant… [and] a list of the names and home addresses of the security firm’s employees and other personal data on guards….”[4]

2007 Egypt Accuses Nuclear Employee of Spying

The Egyptian government announced on April 17, 2007 that Mohammed Sayed Saber Ali, an engineer from Egypt’s Atomic Energy Agency was being charged with espionage on behalf of Mossad, the Israeli intelligence service. Two foreigners, Brian Peter of Ireland and Shiro Izo of Japan, were also wanted in the case. Saber was accused of stealing and selling confidential documents to Mossad operatives for the equivalent of $17,000.[5] On June 25, 2007, Ali was convicted and sentenced to life in prison. He maintained his innocence: “He admitted taking documents from his workplace but he said they had been published and were not secret.”[6] Israel denied all involvement in the case.

2007 Former Nuclear Plant Engineer Allegedly Took Data to Iran

Mohammad Alavi, 51, who had worked at the Palo Verde power plant west of Phoenix, was
arrested on April 9, 2007 at Los Angeles International Airport and later charged with espionage. He was accused of providing Iran government officials with computer access codes and training software “to download details of plant control rooms and reactors,” according to police.

An early report indicated that some of the information described as confidential may have been available on the Web and shared by many of Alavi’s colleagues.[7]

The Office of the United States Attorney District of Arizona official press release included the following details:

Alavi admitted that he unlawfully transported the 3 KeyMaster software to Iran to use in future employment in the nuclear industry. The 3KeyMaster software was custom designed for the Palo Verde Nuclear Generating Station and is used as a simulator system to train employees on the operation of its nuclear reactors. The software contains detailed information on the reactor control rooms as well as maps, drawings, schematics and designs of the facility. 3 KeyMaster is owned and licensed by Western Services Corporation located in Frederick, Md. The customized software has a fair market value between $200,000 and $400,000….

[He] was found guilty by a federal jury on May 27, 2008 for Unauthorized Access to a Protected Computer. On June 24, 2008, Alavi pleaded guilty to Interstate Transportation of Stolen Goods. Alavi was directed by the District Court to self report to the Bureau of Prisons on March 2, 2009 with the added release condition that he be subject to electronic monitoring.

SCADA and other Power Industry Information Systems Sabotage

Employees who feel badly treated by their employers and who suffer from an exaggerated sense of entitlement are particularly prone to harming their current or former employers.[8]

2007 Saboteur of California Power Grid Gained Access Despite Warning

Lonnie Charles Denison, 32, was taken off his job at the California Independent System Operator (Cal-ISO) plant in Folsom (a suburb of Sacramento) by his employer, Science Applications International Corporation (SAIC) because of concerns over his mental health. SAIC warned Cal-ISO that Denison was a security threat due to a history of mental illness, alcoholism and a decade of methamphetamine addiction. Despite the warning, Denison managed to enter the Folsom plant using a card-swipe access control system and a biometric handprint reader. Once into the secured areas of the plant, prosecutors charge that he “broke a glass seal and pushed an emergency electricity shut-off button, plunging the … building … into darkness and crashing computers used to communicate with the power market.” Luckily, the damage did not cause a blackout. Recovery took seven hours of intense work and included the start of a detailed investigation and analysis of the incident. Denison was also accused of sending a false bomb threat to a former co-worker at the plant.[9]

In December 2007, “Denison pleaded guilty to attempted damage of an energy facility, a felony offence punishable with up to five years’ imprisonment and a $250,000 fine….” The incident cost the utility $14,000.[10]

Denison was sentenced to six months home confinement and five years probation; he was ordered to pay $34,163 in restitution to Cal-ISO. Conditions of the sentence included that “the defendant [was] required to participate in drug treatment and mental-health counseling, be
subject to random drug testing, and have no contact with CAL-ISO facilities or its employees.”[11]

2009  Fired Nuclear-Power-Plant Employee Arrested for Hacking Systems

Energy Future Holdings of Texas fired Dong Chul Shin without notice in March 2009; in June, he was arrested, accused of hacking into the Comanche Peak nuclear reactor to tamper with its energy forecasting system. According to John Leyden, writing in The Register, FBI agents accused him of using his “VPN access account (which was left active) … to log into the corporate intranet before modifying and deleting files. Proprietary company information was also transferred to a personal webmail account linked to Dong….“[12]

2009  (Former) IT Consultant Confesses to SCADA Tampering

Dan Goodin, writing in The Register, reports on a case involving a consultant whose contract with Pacific Energy Resources of Long Beach, CA ended in May 2008. In a federal court in Los Angeles in 2009, Mario Azar pled guilty to having hacked into the system controlling marine oil platforms to cause damage.[13]

In the next article in this series, we’ll look at incidents involving the electric power industry and

- Criminal hackers
- Malware.

* * *


Copyright © 2010 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.

Endnotes
[1] Cobb, Cobb and Kabay 2009, pp 15.7-8
[8] Post 2009, pp 13.3-4
[10] Leyden 2007
Bibliography