Control network security lessons from Stuxnet

A UK expert describes how Stuxnet and other threats to industrial infrastructure cyber security are prompting national and international action. Knowledge is power.

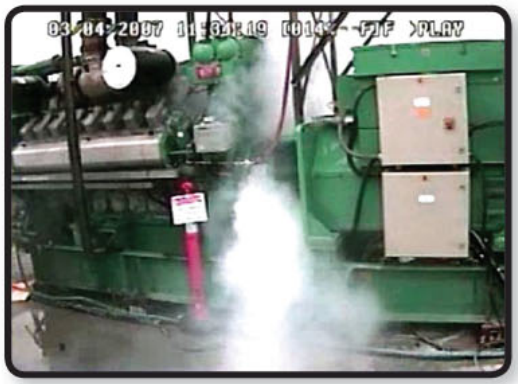
Dr. Richard Piggin, *network and security consultant*

Information on industrial protocols is widely available, and some systems have already been targeted. These include the Modbus protocol and the Stuxnet trojan/virus, which affected Siemens WinCC SCADA, Step 7 Programming Software, and Simatic PLCs. While fixes were quickly developed, Stuxnet was a game-changer for its complexity and reach. As security breaches are analyzed, governments are responding with general and sector-specific guidance to protect critical national infrastructures.

U.S. Department of Homeland Security and the UK's Centre for the Protection of National Infrastructure (CPNI) work with operators of key services and lead government departments to identify and protect critical national infrastructure. An often-cited example of risk is the Queensland sewage treatment plant, where 46 hacks into the system released millions of liters of waste into public waterways. The CIA has confirmed a cyber attack caused power outages in multiple cities (including New Orleans in 2008). The CIA also shared information on intrusions into and extortion demands on utilities. The U.S. government has been taking potential reconnaissance of the power grid by Russia and China seriously, and formed the U.S. Cyber Command, to direct the defense of U.S. Defense Department networks and conduct military cyberspace operations. In the UK, the Centre for the Protection of National Infrastructure (CPNI) is the government authority that provides protective security advice to the national infrastructure. CPNI advice includes a series of process control and SCADA security good practice guidelines. U.S. National Institute of Standards and Technology (NIST) and U.S. Homeland Security helped.

The Stuxnet trojan/virus is the first publicly known "worm" to target industrial control systems. The Stuxnet threat has been portrayed as beyond anything previously seen. Its goal was to sabotage a real-world industrial plant, not disrupt abstract IT systems. It was aimed at industrial control systems with intent to reprogram PLCs and sabotage the plant, hiding changes from programmers or users.

Stuxnet highlights the potential to directly attack industrial control systems used in critical national infrastructure, including energy, water, and transport sectors. Research by Symantec (September 2010) showed that nearly 60% of about 100,000 hosts infected by Stuxnet were in Iran, with relatively high infection rates also in India and Indonesia. This led to speculation that Stuxnet's goal was to disrupt Iran's delayed Bushehr nuclear power plant or the uranium enrichment plant at Natanz.



The Aurora Generator Test by Idaho National Laboratory simulated an attack on a power generator SCADA system. A YouTube video describes the test. www.youtube.com/watch?v=fJyWngDco3g

Symantec described Stuxnet as one of the most complex threats it has analyzed. "Features" include: Four zero-day exploits, which are exploits that are unknown, undisclosed to the software vendor, or for which no security fix is available. This is a rarity for any virus, and would be considered wasteful by most hackers. It also has a MS Windows rootkit, which is software that enables privileged access to a computer while hiding its presence and a first-ever "PLC rootkit," which infected PLC programs while remaining undetectable. It has antivirus evasion; two stolen Taiwanese digital signatures to authenticate Windows software; complex process injection and hooking code to prevent programmers from seeing the infected code; network infection routines; privilege escalation; peer-to-peer updates, and remote command and control.

Since PCs used for control system programming are not normally connected to the Internet, Stuxnet replicates via removable USB drives via auto-execution. It spreads across the local area network via a Microsoft Windows Print Spooler vulnerability, and via a Windows Server Remote Procedure Calls vulnerability. It copies and executes on remote computers through

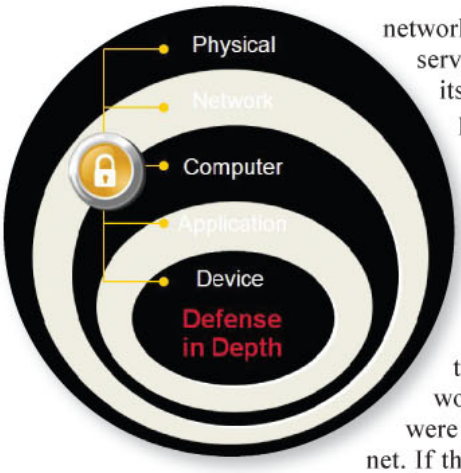
ONLINE

Best practices for industrial control network protection; What is a threat?

Stuxnet as a Precision Weapon http://bit.ly/hSHP91

Cybersecurity standard aims at critical infrastructure in process industries http://bit.ly/gd8nzo

Securing Legacy Control Systems http://bit.ly/hOhHQL



The goal of the Stuxnet virus was to reprogram PLCs in a manner that would sabotage the plant, hiding the changes from programmers or users.

network shares and Siemens WinCC database servers (SCADA software). It also copies itself into Siemens Step 7 PLC program projects and executes when a project is loaded, and updates versions via peer-to-peer communication across a LAN. Stuxnet communicates with two command and control servers originally in Denmark and Malaysia to enable code download and execution for updates.

Stuxnet fingerprints PLC configurations that use the Profibus industrial network for distributed I/O. Configurations were gleaned using earlier versions of Stuxnet. If the fingerprint does not match the target configuration, Stuxnet remains benign. If the fingerprint matches, PLC code is modified with the infected programming software and the changes are hidden. Modified code prevents the original code from running as intended by interrupting processing of code blocks, injecting network traffic, and modifying output bits of PLC I/O.

Stuxnet may be a blueprint for attacks on real-world infrastructure, providing generic methods to reprogram industrial control systems. Stuxnet's sophistication and complexity requires significant resources, making it unlikely similar threats would develop rapidly.

To address vulnerabilities, process control and SCADA security good practice guidelines from CPNI and NIST include a series of sector "road maps" for securing the water, electricity, and chemical sectors, emphasizing cost-effective security for legacy systems and new architecture designs and secure communications. Expanding standards include ISA99 Parts 1 and 2 on industrial automation and control systems security. IEC is working on ICS standards in light of ISA's work. In the first public speech given by Britain's secret intelligence agency GCHQ, Chief Ian Lobban demanded a swifter response to match the speed of cyber events. The challenge is to implement appropriate measures and continue assessment, adjustment, and review in light of emerging vulnerabilities, threats, and consequences. **ce**

Dr. Richard Piggin (rpiggin@iee.org) is a UK-based network and security consultant, works with IEC Network & System Security and Cyber Security working groups, and is developing IEC 62443 Security for Process Measurement and Control – Network and System Security.

PRODUCT & LITERATURE SHOWCASE