

Symantec ICCP Signatures

Real-time vulnerability detection and intrusion prevention for power generation and transmission companies

Overview

The ICCP protocol has brought tremendous efficiency and cost benefits to utility companies by enabling them to control electricity resources remotely. But like any network protocol, it can contain vulnerabilities. Due to interconnections with other utilities, ICCP connections open up SCADA networks to hackers, worms, and other threats. Symantec ICCP Signatures for Symantec™ Network Security 7100 Series appliances detect attempts to exploit these vulnerabilities, providing real-time protection for SCADA networks and helping utilities comply with NERC CIP standards.

Features and benefits

- Safeguard the entire ICCP protocol, not just the features most commonly implemented in SCADA networks.
- Prevent attacks, including ICCP-based denial-of-service (DoS) attacks.
- Detect vulnerabilities with high accuracy while minimizing false positives.
- Protect against “zero-day” threats and attacks.
- Keep monitoring and system control functions up and running.
- Help prevent SCADA network instability and asset damage that can lead to customer outages.

- Assist utilities in meeting regulatory control requirements by ensuring that timely actions are taken to manage SCADA network security risks.
 - Have been tested and validated by leading ICCP and SCADA/EMS/DCS vendors.
-

What is ICCP?

The Inter-Control Center Communications Protocol (ICCP) is the primary protocol used to communicate information between energy control centers that operate SCADA/EMS/DCS systems, and between control centers and power generators. In recent years, ICCP has also been used for communications between control centers and remote terminal units (RTUs) or substations. Also known as the Telecontrol Application Service Element (TASE.2), ICCP is an application layer protocol specifically tailored to the data communications needs of electric utilities.

In addition to utility companies and non-utility power generators, other entities that use ICCP include power pools, regional control centers, regional transmission organizations, and independent system operators. The data exchanged typically consists of real-time power system monitoring and control data, including measured values, scheduling data, energy accounting data, and operator messages.

ICCP was developed under the Manufacturing Message Specifications to ensure its compatibility with U.S. and international (ISO) standards.



ICCP vulnerabilities: A growing risk

The efforts of utility companies to make efficient, enterprise-wide use of SCADA information have led to the development of “open standard” SCADA systems. That means SCADA system security may be only as strong as the security of the organization’s underlying corporate network. As utilities send more and more types of data over their networks, the dangers of lax network security increase. Securing the ICCP protocol itself is a vital part of a utility’s overall security posture.

Vulnerabilities in ICCP can lead to the following security threats:

- Intruders gaining unauthorized access to components of the control center network (such as the ICCP server) via overlooked key access points. Vulnerable access points could include dial-ups, connections to partner networks that are not secured, or unsecured networks (in the relatively rare instances in which they are used for ICCP).
- Disgruntled employees posing a wide range of threats, especially authorization violations. For example, an authorized user might gain access to the control center and SCADA networks via the corporate network for an unauthorized purpose.
- An intruder initiating a DoS attack by sending repeated information requests that “lock up” an ICCP server, preventing the server from performing its legitimate operations and serving legitimate users.

- Viruses or worms infecting the ICCP server or other devices, performing malicious activities such as emailing critical information to another host for retrieval by a hacker.
- Hackers initiating packet sniffing at an ISP or carrier and then modifying packets with malicious intent.

Symantec ICCP Signatures: Proactive protection

Up to now, exploits that take advantage of vulnerabilities in ICCP have usually not been dealt with due to a lack of tested and validated ICCP-specific vulnerability signatures. Attacks have therefore gone undetected, potentially causing disruptions mistakenly attributed to other SCADA-related issues.

Recognizing the critical need for increased security of SCADA networks and systems, Symantec has worked with electric power industry leaders to identify known and potential vulnerabilities in SCADA networks in general, and the ICCP protocol in particular. This research has allowed Symantec to develop proactive vulnerability signatures that detect malicious exploits, blocking attacks before they begin.

For example, Symantec ICCP Signatures enable a utility to detect and block a buffer overflow exploit that otherwise would permit a DoS attack against the company’s SCADA network. Such an interruption of SCADA communications could prevent a generating plant from receiving an order to increase its output, resulting in insufficient power reaching another part of the system, or even disrupting customer power supplies.

Fact Sheet: Intrusion Protection Symantec ICCP Signatures

Symantec ICCP Signatures are now available to Symantec Network Security 7100 Series appliance customers, providing real-time vulnerability detection and intrusion protection for power generation and transmission companies.

The signatures are also available to customers of Symantec™ Managed Security Services. When used in conjunction with Symantec Managed Security Services, Symantec ICCP Signatures can help power generation and transmission companies manage outbreaks of malicious activity, mitigate the risks associated with emerging threats, improve the resiliency of their information infrastructures, and demonstrate regulatory compliance.

Symantec Managed Security Services offer a higher level of vigilance that improves an organization's overall security posture. The Symantec Managed Security Services team provides 24x7 real-time monitoring and management of intrusion detection and intrusion prevention systems across the globe. By offloading the burden of real-time network monitoring, advanced security analysis, and integration of global intelligence to Symantec, IT groups can focus their attention on gaining insight into critical business risks and improving internal control of security processes.

Product availability

Symantec ICCP Signatures are available immediately and offered at no additional cost with Symantec Network Security 7100 Series appliances, and with Symantec Managed Security Services. Please see the Symantec Network Security appliances data sheets for system requirements.

More information

Visit our Web site

<http://enterprisesecurity.symantec.com/industry/power/default.cfm>

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our Web site.

About Symantec

Symantec is the world leader in providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

20330 Stevens Creek Boulevard

Cupertino, CA 95014 USA

1 (408) 517 8000

1 (800) 721 3934

www.symantec.com

