iSign International

Protecting America’s Power Grid from Data Breaches and Cyberattacks–iSign International & Southwest Electric Cooperative Team Up to Thwart Hackers

The Challenge

Reports on the potential of cyberattacks on the United States power grid have made the news in recent months. Lloyd’s of London has developed a scenario for this kind of attack estimating the impact on the United States economy to be as much as $1 trillion.

To understand its own exposure to cyberattack threats, particular those that live dormant under the radar like Dragonfly, Southwest Electric Cooperative (SWEC) decided to participate in a pilot program with digital security experts iSign International. Going into the pilot program, the team at SWEC had taken all known precautions to protect its computer network from hackers. Their security setup included industry best practices hardware, software, and business processes.

About Southwest Electric Cooperative

80 Employees | 40,000 Services

Founded in 1939, Southwest Electric Cooperative (SWEC) is a not-for-profit, private electric cooperative owned by its members.

Headquartered in Bolivar, Missouri, SWEC provides electricity throughout eleven counties in southwest Missouri covering 5,470 miles of power lines and more than 40,000 services.

The Solution

The SWEC IT team installed iSign’s iSecure Protector on the email server to analyze network packets. This analysis found that the network had been hacked not once but dozens of times. Suspicious access was detected from unauthorized IP addresses from around the world. SWEC’s current IT setup including firewall did not detect any of this activity. iSecure Protector was then used to automatically block traffic from these IP addresses protecting the email server from further unauthorized access.

Because of these impressive results, the pilot was expanded to address SWEC’s series of Internet-connected devices out in the field. By connecting iSign’s iSmart Guard to the network, all incoming traffic was blocked and all outgoing traffic was monitored and blocked if deemed destined for an unauthorized destination.

The Pilot Project: Uncovering and Preventing Malicious Activity

Southwest Electric Coop (SWEC) is entrusted to bring uninterrupted power to thousands of customers in Missouri. To safeguard its IT infrastructure, SWEC has in place what is commonly thought to be industry best practices in terms of hardware, software, and business processes.

To confirm that they were safe from hackers, SWEC enlisted the help of iSign's team of digital security experts. To kick off the project iSign’s iSecure Protector–Server Edition was installed on the email server to analyze the network packets. This analysis found that, despite the precautions in place, the network was being accessed from suspicious IP addresses of Internet Services Providers (ISPs) from around the world. To protect the network from further unauthorized access, iSecure Protector was set up to automatically block traffic from these IP addresses. No further intrusions were found.

The impressive results in Phase 1 led SWEC to expand the pilot to include its series of Internet-connected devices out in the field. Internet of Things, or IoT, devices can easily be exploited by hackers. iSecure Protector was installed on the SCADA control system and the programmable logic controllers (PLCs) in the field were safeguarded by iSign's iSmart Guard. By connecting iSmart Guard to the network, all incoming traffic was blocked and all outgoing traffic was monitored. Any data found leaving a device headed for a rogue destination was blocked automatically by iSmart Guard keeping SWEC safe from any dormant malware (such as Dragonfly) and/or hacking group.

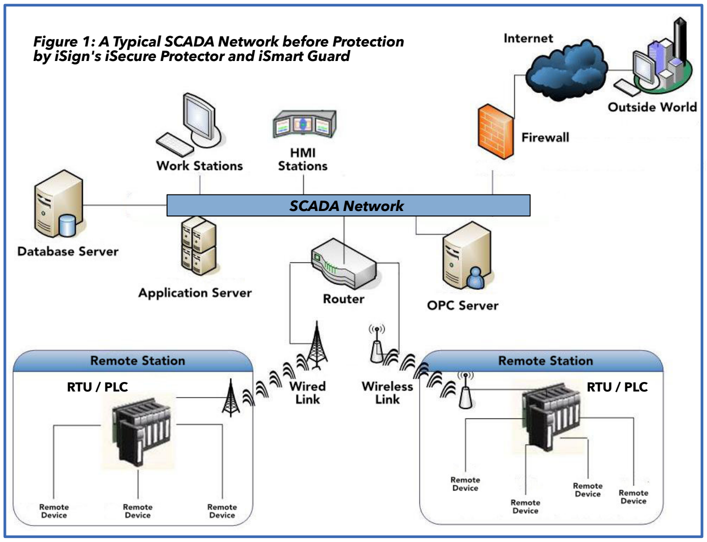


Figure 1: A Typical SCADA Network before Protection by iSign's iSecure Protector and iSmart Guard

The final piece of the puzzle was to completely secure authentication. Typical 2-factor authentication has been proven to be vulnerable to hacking. iSign's system is protected by its proprietary AI Security Protocol (see Figure 2). Faster, easier, and more secure than 2-factor, the AI Security Protocol utilizes 5-Factor Authentication – Application & Server Authentication, Device Learning, Biometric Signature, GEO Recognition, and Dynamic PKI Encryption.

The result for SWEC was a completely impenetrable system.

The Kaspersky Danger

As a part of the implementation, the team checked to see if anti-virus software from Kaspersky Labs had been previously installed anywhere on the network. The team located a laptop that had Kaspersky. During the software removal process, the computer froze and would not let the team multi-task or run any other applications suggesting that some unauthorized activity was taking place in the background.

iSecure Protector–PC Edition was installed and suspicions were confirmed. iSecure Protector detected information being sent from the laptop to Kaspersky IP addresses in Russia via third countries. Even after the Kaspersky software had been uninstalled, information continued to be sent from the laptop. What was thought to be anti-virus software was actually a form of malware.

In addition to detecting the Kaspersky malware, iSecure Protector was able to automatically block data so no unauthorized traffic, including traffic to Kaspersky’s home location, was able to leave the network.

> “ **Coming under attack from IP addresses** all over Russia and Europe with hackers trying to access our server was a real wake-up call for us. With the help of iSign, we stopped all these attacks and are now confident our system is fully protected from hackers. Knowing that hackers had invaded our email server gives me serious concerns that they may have done the same to utilities across the country and may be much closer to attacking the power grid than anyone thought possible. My experience with iSign tells me their system can quickly and easily identify these hackers, block them from stealing our data and stop future attacks. We will be using the iSign system and will help in introducing it to other electric cooperatives/utilities to protect the American Power Grid. America’s electric coops and hopefully all utilities will make every effort possible to protect the electric power grid and utility systems so uninterrupted services can continue for our members.”

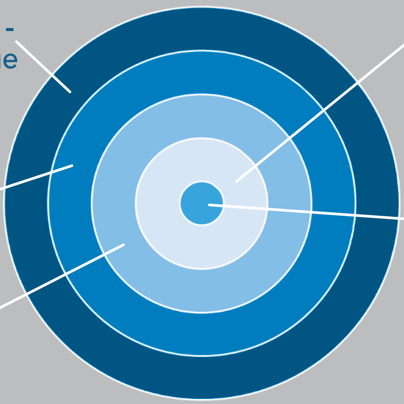
Rick Condren,
IT Manager at SWEC

iSign CyberSecure Solutions

Combining ease-of-use with the highest level of security to keep you safe from cyberattacks, iSign can:

IDENTIFY rogue activity on your network, including on IoT devices
BLOCK unauthorized inbound and outbound networks connections
PROTECT you from external and internal attacks immediately stopping all network breaches

Signing into the iSign system is secured by its proprietary **AI Security Protocol** (see below).



Application & Server Authorization - Applications are validated with unique ID's and keys before communication links are established to prevent unauthorized access.

GEO Recognition - GPS-tagging allows iSign to reject any transmission that comes back from a location different from where it was sent.

Device Learning - Proprietary technology automatically pairs your phone with your computer. If an unknown device tries to connect, it is rejected.

Dynamic PKI Encryption - iSign’s proprietary Dynamic PKI constantly changes the key pairs, making each end-to-end communication highly encrypted and un-hackable.

Biometric Signature - Faster, easier, & more secure than 2-factor authentication, Biometric Signature leverages artificial intelligence (AI) to learn physical signature patterns (angles, speed, acceleration, and discontinuities) which are practically impossible to reproduce. AI knows that two signatures from the same person are never exactly the same so if it detects two identical signatures, it knows it's not you.

iSign Partner Network

At iSign, we recognize that to deliver world-class solutions for our clients, it takes more than building world-class products. That's why we partner with the top hardware, distribution, and manufacturing companies in the world.

BlueStar
Your Solutions Distributor

cradlepoint

ZEBRA

To consult with our experts please call 206.992.8141 or email info@isignintl.com