

## **Uninterruptible Power Systems and Cybersecurity**

By: Michael A. Stout, Vice President Engineering Falcon Electric

The recent number of cyber-attacks and their level of sophistication have demonstrated the inadequate network security measures employed by many large corporations, government, and military agencies. Time is on the hackers' side. They only have to find one unsecure computer or device on a segment of a corporate or governmental network, and they can use any number of methods to eventually gain access to critical data. Should they not be able to find an unsecured computer, they simply have to send a cleaver e-mail containing a one-off designer backdoor virus that will evade many corporate level antivirus software and firewalls—and again they are in. WikiLeaks is a prime example of the amount of data an insider can obtain from a secured network and the damage that can result. In the ever-evolving hacker wars, many corporations and government agencies do not have a high enough level of protection for their most sensitive data. Recently, the hacker group "Anonymous," or "AntiSec," released a 7.4-GB file containing the e-mails and personal information obtained from the supposedly secure computers of 56 different law enforcement agencies.

Allowing the violation of a corporation's data is unacceptable, but what if the hacker gains access to a corporate Supervisory Control and Data Acquisition System (SCADA)? SCADA systems are the very heart of a corporation's automated manufacturing or process control. SCADA systems are installed to control and monitor the entire manufacturing process for automotive production, food processing, oil and gas refineries, pharmaceutical production, power production and distributions facilities, and others too numerous to mention. The Stuxnet virus attack is a good example. It is unknown who wrote the Stuxnet virus, but it is highly suspected to be a government's creation. At this point, it appears the virus has had only one intended target, a nuclear fuel processing facility located in Iran. Stuxnet took over the computer automated system (SCADA) controlling gas centrifuges critical to the uranium enrichment process. The virus increased the centrifuges' speed to a point where they were destroyed. This occurred while the virus instructed computers controlling the centrifuges' speed to report their conditions as normal to engineers monitoring the process in the facility's control room. Stuxnet was released on the Internet and infected a large portion of the world's computers before finding its intended target. The handwriting is on the wall, and it is time for governments and corporations to make the security of their data and process control networks their number one priority. New technologies and security threats will continually be developed, making this priority a costly, ongoing battle demanding continuous risk assessment. The approach taken must be complete and all-encompassing as the network security chain is only as strong as its weakest link.

Every network connected device in a data or SCADA network is a potential backdoor into the network, or at a minimum a security risk. For instance, an uninterruptible power supply (UPS) powering a programmable logic controller (PLC) responsible for controlling a key controlled substance mixing process on a pharmaceutical production line may be subject to outside sabotage through its unsecured SNMP/HTTP network interface. A UPS connected to the company's Ethernet network for the purpose of remote monitoring and management could be compromised through the collusion between an inside employee and a hacker friend outside the company. The unsecured UPS IP address could allow the UPS to be shut down and restarted remotely to cover thefts of a small amount of the controlled substance.

The UPS units are essential should there be a power outage to the SCADA RTUs, as they must apply the brakes on large overhead crane motors to prevent floor workers from being killed or injured by falling loads. As the UPSs are the RTU's sole source of power, they are essential to assure the crane is powered until it is in a safe state. One can imagine the damage that could be caused by a disgruntled employee or hacker acquiring the Internet Protocol (IP) addresses to the UPS units and having the ability to turn their outputs on and off at will and without warning.

Once a hacker has gained access to a moderately secured network, they can easily determine the IP addresses of every device on the network. Using port scans, they then can determine if the device communicates through HTTP, SNMP, Telnet, MODBUS, etc. Once the communications protocol has been established, the hacker will first attempt to determine if the device has any further security. In the case of a device supporting HTTP protocol, if unsecured, it is a simple matter to use any web browser to communicate directly with the device, often by displaying a menu of options. The critical selection and proper configuration of a UPS SNMP/HTTP agent option is vital to network security, but often an afterthought. This prompts the question "What security features should a UPS SNMP/HTTP agent support?"

The world is running out of IP addresses under the old 32-bit IPv4 format, which has prompted the development of a new world standard IPv6 that supports 128-bit IP addresses. In addition to adding a virtually unlimited number of IP addresses, IPv6 has Internet Protocol Security (IPsec) built-in. When used, IPsec secures the IP communications across the network by authenticating and encrypting each IP data packet. IPsec uses a shared key to accomplish authentication. IPv6 support is essential in the selection process.

The SNMP/HTTP agent should be able to turn off unused communications ports in addition to the ability to reassign port numbers. A typical agent may support BootP/DHCP, Ping Echo, Telnet, SSH connection, HTTP, HTTPs, UDP, three SNMP versions, UPnP, and SMTP protocols. All of these protocols are assigned differing port numbers and can, if unsecured, identify themselves should a port scan be performed. Some of the ports could provide backdoor access to the agent and the associated UPS unit. It is a good practice to turn off unused

communication protocol ports and to use communications protocols that have adequate security.

Telnet has been used for decades by network administrators to manage remote devices, but its security is very weak and, in the case of a hacker, non-existent. SSHv1 protocol offered a much more secure option as it has strong authentication protections in addition to encrypting the communications across the network. SSHv2 was developed as it was determined that hackers could bypass security and execute code at the root level on UNIX-based systems. SSHv2 also supports the Triple Data Encryption Standard (3DES) in addition to AES, making it essential for a secure SCADA network.

Simple Network Management Protocol (SNMP) is used by larger companies to remotely monitor and manage most network devices like managed switches, printers, UPS units, fileservers, computers, modems, etc. SNMP provides a very robust means of monitoring any number of devices from one central workstation having network management software (NMS) installed such as SolarWinds or OpManager. Each device industry has developed a standard set of management instructions specific to the type of device referred to as a RFC Standard Management Information Base (MIB). The MIB for the applicable device is supplied in file format by the device manufacturer. The MIBs for all of the devices to be monitored are installed into the NMS, allowing the remote monitoring and management of the device. There are presently three versions of the SNMP protocol: SNMPv1, SNMPv2, and the latest and most secure SNMPv3. It is strongly advised to turn off SNMP protocol all together if it is not going to be used to manage a UPS. The default setting for most UPS manufacturers SNMP/HTTP agents has SNMPv1 selected and active. SNMPv1 supports a minimal single level password. Typically, agents are shipped from the UPS manufacturers with a default password making unauthorized access through SNMP child's play. SNMPv3 security supports hashing algorithms for secure multi-level password protection in addition to full data encryption, supported using differing shared keys. SNMPv3 should also be configured to limit access to one or two management workstation IP addresses and exclude all other addresses. This is usually the same IP addresses as the assigned SNMP trap receivers.

Hypertext Transfer Protocol (HTTP) with regards to a UPS SNMP/HTTP agent is a very unsecure protocol incorporating a couple of unencrypted, single-level user logins and passwords. It allows access to the main menu of the agent by anyone entering the agent's IP address into a web browser's URL line. It is recommended to turn off the HTTP port if the protocol will not be used. Hypertext Transfer Protocol Secure (HTTPs) is the preferred choice when web browser access is desired. HTTPs incorporate HTTP with SSL/TLS security. Even with the added security, it is suggested to use HTTPs in conjunction with a Remote Authentication Dial In User Service (RADIUS) server and enable the RADIUS support on the agent. RADIUS can effectively limit access to Internet, wired, and wireless networks.

Universal Plug and Play (UPnP) protocol is primarily used to support automatic configuration of residential networks devices. It should always be turned off in the UPS agents, as it allows easy detection of the agents configured on a network. It poses a real security risk in corporate or governmental networks.

Simple Mail Transfer Protocol (SMTP) supports the e-mail transmission over Internet Protocol and is used to send e-mail messages from the UPS agent upon specified UPS detected events. When configured, it can send e-mail to IT staff after normal working hours, in the event of a critical situation like a UPS failure. Again, it is best enabled in conjunction with RADIUS to provide additional security.

It is convenient for IT staff to use the Ping command to determine if a device is communicating with the network. Unfortunately, pinging for computers and devices over the Internet is the hacker's first act in finding unsecured computer and network devices. It is then a simple matter of entering the detected IP address into a "whois" domain look up on the Internet to determine what corporation or government agency the IP address is registered. They next run port scans of the IP address to determine if there are any open ports and their port number. The port number will indicate the type of communications port they have accessed. They next communicate with the port in its own language and attempt to gain access. This entire process is over in minutes. Once a device has been properly configured on a network, the Ping Echo support must be turned off in the device. Without a ping response from the agent, in addition to unused ports being turned off, it assures the agent is more stealthy and harder to detect on a network.

User Diagram Protocol (UDP) is used primarily by the UPS SNMP/HTTP agent to facilitate remote real-time firmware updates. It is a very unsecure protocol and should be turned off when not needed unless RADIUS is configured where UDP must be turned on.

In conclusion, it is essential to understand the security features and versions available in a specific UPS SNMP/HTTP agent as they can differ widely depending on the UPS manufacturer. Some manufacturers may not support IPv6, while others may not support SSHv2, SNMPv3, or RADIUS. UPS agent security features alone may not yield the level of security desired without the ability to turn off unused communications ports. The overall security of data and SCADA networks requires the careful selection of network-enabled devices, meticulous IT procedures, along with vigilant IT and network security departments. The UPS is a vital part of a resilient SCADA network; however, the SNMP/HTTP agent option selected may be critical to the continued reliability and safety of your process control. The level of network security required must be weighed against the level of security demanded by the application.

Learn more about Falcon Electric, Inc.