

SCADA SECURITY FOR REMOTE OPERATIONS IN THE WATER & WASTEWATER INDUSTRIES

By: Kevin L. Finnan, vice president, marketing, CSE-Semaphore

INTRODUCTION

Operators of water and wastewater SCADA systems are facing up to the fact that their systems are no longer sailing under the cyber security radar.

History has largely been to the contrary. The industry has been able to point to only a single attack, which took place in Australia in 2000. The Maroochy Shire council sewage computer system was hacked by a disgruntled, former employee of the contractor who had installed the system.

While this attack illuminated numerous, potential vulnerabilities in SCADA systems, many operators focused on the fact that the hacker was an insider and prioritized on personnel measures over cyber security.

The industry has also taken note of the Stuxnet attack, which targeted a SCADA system. Yet, a common perception is that such a well-funded, covert operation is unlikely to be used against assets in the water or wastewater industries.

A more recent incident, reported in November, 2011, is of perhaps greater concern. It was first reported as a security breach in which hackers from Russia obtained passwords and operated a pump in an Illinois system. Investigators soon determined that there was, in fact, no security breach.

Why should this particular incident be cause for concern? The problem with the Illinois scenario – as it was initially reported – is its feasibility. It is far more practical than Stuxnet. It resembles the Australia attack to the extent that hackers take control of pumps. The key difference is that it is not an inside job. It is also the sort of scenario that security experts often demonstrate in “friendly” hacks.

With SCADA security now prominent in the news, operators are reviewing their assessments and measures to date. What are they doing, now, to enhance SCADA security?

Today, technology exists to design and implement measures within remote terminal units (RTUs) and SCADA networks. The following such measures, all of which have been put into practice, will meet emerging industry requirements:

- Password maintenance
- HTTP security
- Firewall
- Virtual Private Network (VPN)
- Authentication

PASSWORD MAINTENANCE

Security consultants continue to be amazed at the number of systems that operate using default passwords without account maintenance. Protecting account information and maintaining passwords are the minimum security measures and should collectively be first on the list to implement, immediately.

HTTP SECURITY

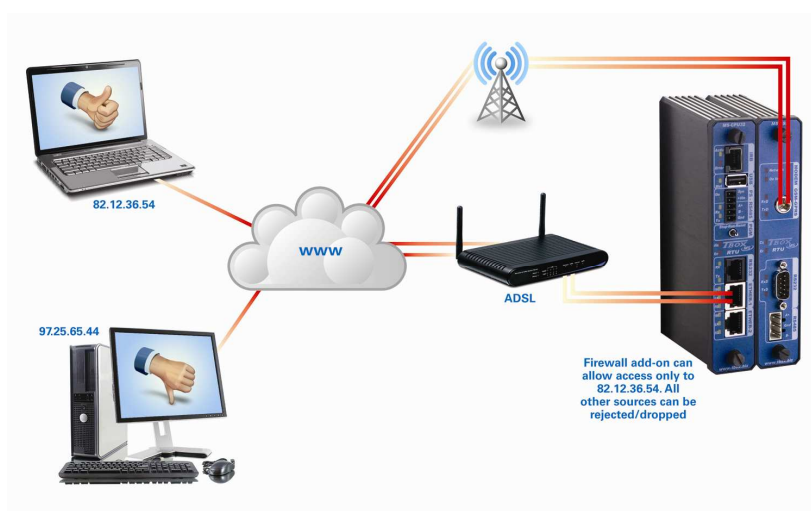
The fact that many RTU devices on today's market feature integral web servers substantially increases security concerns. HTTP log-in using a password is the minimum measure. Account maintenance practices should follow the same process as non-HTTP password maintenance.

HTTPS, or "HTTP Secure," is the hypertext transfer protocol with encryption using the SSL or TLS protocol. It is available as an add-on, which allows access to the integral web server in the RTU using HTTPS. Simple menu interactions allow the user to configure the TCP ports for HTTP and HTTPS, whether HTTP is blocked, and to specify a certificate file name.

FIREWALL

A firewall is a device or software capability that is designed to allow or deny network transmissions based upon a set of rules. The firewall is used to protect networks from unauthorized access while allowing legitimate communications to pass.

Firewalls are finding their way into the more sophisticated RTU products on the market. The firewall provides access protection for any incoming or outgoing IP connection. Ethernet ports and cellular, e.g. GPRS connections can be protected using the firewall. Menu interaction allows the user to define one or more rules to allow or deny access. Users are warned to be sure that they completely configure firewalls; otherwise, an outside party might still be able to access the network.



In this example, access to the RTU is allowed only to a PC with a specified IP address.

VIRTUAL PRIVATE NETWORK (VPN)

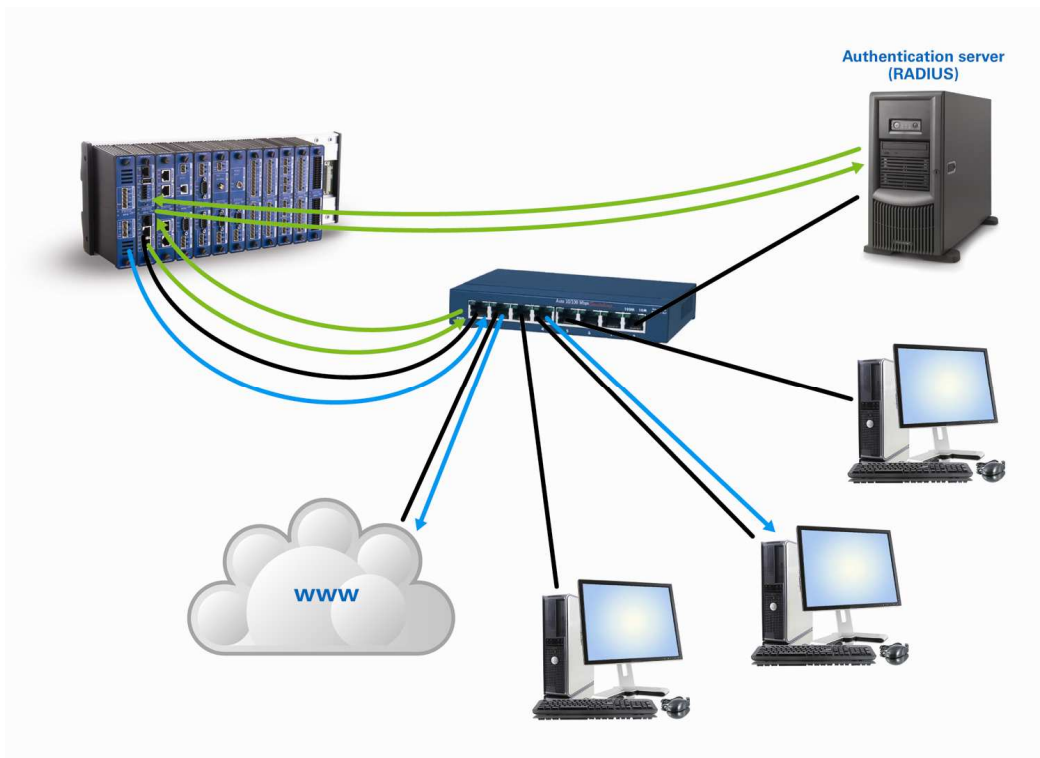
Vulnerabilities specific to SCADA networks result from their coverage of broad, geographical areas and use of the Internet or public networks. One security measure SCADA operators have implemented is a virtual private network. A virtual private network, or VPN, uses authentication to deny access to unauthorized users and encryption to privately transport data packets over networks that are, otherwise, unsecured. An alternative to a firewall, a VPN allows users to bypass such Internet restrictions.

AUTHENTICATION

Two of the authentication methodologies that have recently been put into practice in the RTU world include IEEE 802.1X and DNP3 Secure Authentication.

IEEE 802.1X

IEEE 802.1X, a standard for port-based, network access control, addresses a key security risk, spoofing, which many operators have uncovered in vulnerability assessments. IEEE 802.1X provides authentication for devices wishing to access a local area network (LAN). It prevents rogue devices from attaching to the LAN or RTU port. That, in turn, prevents unauthorized access to proprietary information and the ability to download parameters or commands.



Using IEEE 802.1X, each device on the network must identify itself to an Authentication Server.

DNP3 SECURE AUTHENTICATION

The DNP3 User Group Steering Committee has ratified a security extension that mandates the authentication of master devices through the use of one-way cryptographic hash functions employing a shared key in order to access critical DNP functions. DNP3 Secure Authentication is an extension to the existing DNP3 standard incorporating IEC62351 Version 2.0 authentication on top of the DNP3 communication protocol. According to the DNP3 User Group, the purpose of this specification is to define a protocol mechanism that:

- A DNP3 outstation can use to unambiguously determine it is communicating with a user who is authorized to access the services of the outstation.
- A DNP3 master can use to unambiguously determine that it is communicating with the correct outstation.

DNP3 Secure Authentication uses a challenge process. When a command, e.g. to operate a pump is received from the server (blue arrow in the accompanying diagram), the RTU challenges the server to be sure it is a legitimate node on the network (yellow arrow in the accompanying diagram).

The Server responds with an authentication message. If the server authenticates correctly, only then will the RTU perform the action (green arrows).



Caption: Only when the server authenticates correctly does the RTU perform the requested action such as operating a pump.

The authentication key is updated at regular intervals in order to prevent old keys from being stolen and re-used. If an RTU does not receive a new key within a specified time limit, it will mark the key as stale and ignore commands until a new key is provided.

CONCLUSION

Authentication, firewalls, password security and virtual private networks are among the technologies being implemented, today, in order to prevent SCADA security breaches. These measures must be incorporated into an operator's overall implementation plan that meets standards in the industry.

For the water and wastewater industries, best practices are provided by the "Roadmap to Secure Control Systems in the Water Sector," which was released by the Water Sector Coordinating Council

Cyber Security Working Group in 2008. The vision is that “in 10 years, industrial control systems for critical applications will be designed, installed and maintained to operate with no loss of critical function during and after a cyber event.”