



White Paper

Revere SCADA Security Solution

Eric Smith, Tuck McAtee, Markku-Juhani O. Saarinen

RS-TR0120120103

Version: 1.4

Date: 2012-01-09

Securing Legacy Serial SCADA Communications – A New Solution

4500 Westgrove Drive
Suite 335
Addison, TX 75001
P: 972.930.7200
www.reveresecurity.com

1 Introduction

1.1 Purpose

The purpose of this document is to present a low cost retrofit solution that secures legacy SCADA (supervisory control and data acquisition) communications. The solution is transparent to the SCADA network and allows asset owners to gradually introduce security without disrupting operations. Current solutions are very invasive in that they introduce too much communications latency and require complex key management as well as, often, additional infrastructure.

1.2 Overview

The Department of Homeland Security (DHS) has identified security of legacy SCADA networks as a major issue and funded research to mitigate this issue. As recent research shows [1][2][10][13][14], these networks are vulnerable to known and published attacks using readily available commercial off the shelf (COTS) equipment. Several solutions have been proposed [10][16][18], but so far few have been adopted. This whitepaper explores why SCADA utilities are reluctant to adopt these proposed solutions and propose a far less invasive solution.

When SCADA networks were first established little, if any thought was given to communication security and malicious attacks that can destroy or disrupt equipment, cause environmental problems or lead to other threatening malfunctions. Early efforts were focused on building reliable devices built to withstand the harsh conditions physical commonly found in industrial locations. SCADA devices are built to last between 20 – 50 years. It is often not economically feasible to replace existing equipment with new, security ones. Therefore a retrofit solution is often necessary.

Leading the way, the American Gas Association (AGA) established a working group to develop an open standard for serial communication links. Their recommendation for migrating security into SCADA networks was to develop a “bump-in-the-wire” (BITW) device capable of encrypting and authenticating the communication channels. Such a device would be inserted right next the modem on both the master and slave ends. The AGA-12 working group completed their tasks in 2006 and is currently in the process of becoming an IEEE standard (IEEE P1711). AGA-12 part 2 established ten security cipher suites for implementing security onto these BITW devices.

In 2007, DOE committed more than \$10 million across five collaborative projects including Schweitzer Engineering Laboratory’s (SEL) Hallmark Project [18]. One of the goals of Hallmark was to take the Secure SCADA Communication Protocol (SSCP) from an initial research idea to a commercialized product. This was achieved with the SEL-3025. Currently work is underway to develop a centralized key management and access control system. The Hallmark team also works to integrate the SSCP specification into the IEEE P1711.

Unfortunately very few entities have adopted any solution at all. The reasons for non-adoption are based on three issues: latency, complexity and cost.

2 Challenges

2.1 Latency

A recent paper [6] summarized a number of surveys and interviews with asset owners by deducing that the introduction of security should not affect polling beyond a 20% reduction in frequency. Soon after, the Pacific Northwest National Laboratory (PNNL) evaluates the reliability of BITW devices that conformed to the AGA-12 standard [11]. Their testing showed that baud rates less than 9600 introduced a significant amount of latency. For instance, at 1200 baud, with a polling frequency of two seconds (which is common in the electric industry), the AGA-12 low latency solution (PE mode) reduced the polling frequency by 70%. That would undoubtedly adversely affect the reliability of communications and therefore the efficacy of the control system. The surprising result was that the AGA-12 low latency solution (PE Mode) did not outperform CTR mode as expected. CTR mode requires the decrypting module to buffer up and authenticate the entire message before forwarding it to the destination (this is often referred to as “hold-back”). In either mode, the latency is inadequate for universal acceptance.

In summary, PNNL was also asked to evaluate the performance of the BITW devices (and similar solutions) that conform to the SSCP specification [12]. Since the SSCP specification also requires “hold-back”, then the results are very similar to the AGA-12 solution.

2.2 Key Management

A report by the AGA-12 task group [3] and also a NIST publication called “Guide to SCADA and Industrial Control Systems Security” [15] recommend that utilities create information security (InfoSec) teams experienced in the areas of key management and secure policy creation. This may be an overwhelming burden on utility companies and still does not avoid an environment where the keeper of the keys can hold the utility hostage should he be terminated for example.

Typical key management systems require certificate authorities (CAs) or trusted third parties to create, destroy, and escrow keys. This solution can be costly and there is still an element of trust required. Additionally, CAs or trusted third-party systems cannot be easily adopted into closed-circuit serial networks. The costs of managing keys and enforcing security policies will most likely be the most expensive component in securing SCADA communications. Such high management and employment burdens discourage end users from adopting this technology.

2.3 Cost (BITW Encryption Market)

The price for BITW devices is typically greater than \$500 per unit. A multitude of units is required for each site installation. Schweitzer, for example, sells three BITW products: SEL-3021-1 [7], SEL-3021-2 [8], and SEL-3025 [9] at a cost of \$540.00, \$540.00, and \$900.00 respectively. The SEL-3021-1 provides confidentiality only with no integrity protection. The SEL-3021-2 provides both encryption and authentication conforming to the AGA-12 specification. The SEL-3025 also provides encryption and authentication conforming to the SSCP specification, which was developed under the Hallmark project.

A competing company, SEQUI, sells a BITW device [17] that conforms to the AGA-12 specification at the cost of \$595.00.

However the cost of the BITW alone does not take into account the costs for additional hardware and software required to implement a key management infrastructure, not to mention the cost of hiring and training constantly available personnel to create and enforce key management policies.

3 The Solution

We propose a low latency, plug and play, serial encryptor that alleviates the need for users to handle key management tasks and that is engineered to low cost targets as well. This solution ensures confidentiality, but also that messages cannot be forged, modified, spliced, reordered or replayed. Naturally the target cost is less than \$500 per device. The solution will require very little training for utility personnel and will impose a negligible amount of latency on their networks.

The encryption keys remain hidden within the devices themselves and will never be revealed to anyone. It does not require key management services so employees do not have to replace keys in the devices. The solution further provides significant improvements in avoidance of latency, complexity and cost. It is FIPS compliant with 128-bit key strength and enhanced by a proprietary cryptographic primitive and key management protocol to attain the needed performance.

The solution consists of two components; a low-cost terminating (SECTERM) end and a security server (SECHOST). The security server is a rack-mounted, hardened device that is able to host multiple serial connections. SECHOST has Ethernet connectivity for connection monitoring, statistics and configuration. Two SECTERM devices are able to secure a single line without the aid and of a SECHOST.

3.1 Latency Solution

Our solution builds on the recommendations of AGA-12, which prescribes a special mode of operation (PE mode) [10] incorporating AES and guaranteeing error propagation. It leverages existing CRC to ensure message authentication. Discarding of messages with failed CRC's is a feature that is already built-in to the existing SCADA framework. Normally CRC is used to detect transmission errors. However, the PE mode considerably assures that any tampered message will have a failed CRC.

Unfortunately, PE mode imposes 32 byte-times of latency. This is because the underlying primitive driving PE mode is AES, which has a block size of 16 bytes. Therefore there is a 16 byte delay for the receiving module and an additional 16 byte delay for the sending module for a total of 32 byte-times. We propose to greatly reduce the latency with the incorporation of the Hummingbird-2 (HB-2) encryption algorithm [19], which has a block size of 2 bytes.

Hummingbird HB-2 is a word-based cipher that is ideally suited to solving this problem. The small word size (2 bytes) greatly reduces latency. In addition, Hummingbird HB-2 has built-in message integrity protection via a message authentication code (MAC) functionality. These properties are ideal for this scenario and achieve the same security objectives as PE mode.

Hummingbird HB-2 has survived rigorous examination by the world's leading cryptographers. However, to create a very high security margin we propose a double encryption. On the first pass, we encrypt with the AES CTR mode and follow up with a second pass with Hummingbird HB-2 (using CTR mode in this fashion does not require hold-back). Since CTR mode is byte oriented, this does not cause additional latency. With the slow bandwidth of commonly used serial lines (300 to 115200 bps), there is more than enough clock cycles available to keep up with real time.

The expected latency will be 4 byte-times plus the cost of the cryptographic header for a total of 6 – 10 byte-times of latency.

3.2 Key Management Solution

In many respects key management is more difficult than encryption. An adversary is far more likely to attack the key management than the encryption algorithm. Storing keys securely and preventing access to unauthorized parties is an ongoing problem. Human involvement exacerbates the problem and thus policies must be rigorously enforced to ensure that employees who have access to keys or passwords do not leave them lying around or hand them out for convenience sake. Even the most scrupulous employees can be fooled into giving up their keys by sophisticated hackers using social engineering. When employees are terminated or voluntarily leave, passwords and keys must be changed to prevent retribution. Also, disgruntled employees who have access to keys may attempt to extort the utility. This threat may be more realistic than threats from a terrorist organization.

We propose a key management solution whereby keys are not revealed at all. Rather they are shared only by the BITW devices and a security hardened server to remain hidden inside the devices. The critical event is the key establishment. How do all of these devices securely agree on a key?

For key agreement we rely on a Diffie-Hellman (DH) key exchange. DH allows for keys to be exchanged over an insecure channel. However, since these BITW devices are willing to perform a DH exchange with anyone, there is no way to assure that a malicious party has not established himself as a connection point between both the two intended parties. This is known as a man-in-the-middle attack. To prevent this we provide a very novel and inexpensive way to assure no third party has intervened in the key exchange.

There is no need for key fill devices or to generate and install complex pre-shared keys and the system does not require integration with a PKI system. A unique shared secret of sufficient entropy is automatically generated for each connection. Man in-the middle attacks are deterred by out-of-band verification of a human-readable numeric string derived from the automatically generated shared secret.

For the solution Revere Security has designed SESLP (Self-Enabled Secure Link Protocol), a light-weight but robust session handshake and transport security protocol designed for use with serial devices.

In SESLP "anonymous" ad-hoc handshake mode, the two communicating parties establish their shared secret using the Diffie-Hellman key exchange protocol. All keying material for encryption, decryption and message integrity protection is derived from this shared secret.

Upon initialization, a special serial-synchronized Diffie-Hellman handshake is performed in the Elliptic Curve group P-256 and the group generator G defined in section D.1.2 of FIPS PUB 186-3, "Digital Signature Standard (DSS)" (NIST, June 2009). Both parties generate their 256-bit secret values A (for Alice) and B (for Bob) using a cryptographically secure PRNG. Alice performs scalar multiplication $X=A*G$ and transmits X to Bob. Bob conversely transmits $Y = B*G$ to Alice. After appropriate checks both parties are then able to derive their unique shared secret Z from $Z = A*Y = B*X = A*B*G$.

After initialization, the shared secret is detained in nonvolatile memory together with nonce counters and pools of randomness. The handshake is performed again only if the connection needs to be reset for some reason.

A human-readable 4-8 - digit decimal numeric code is derived from the shared secret and optionally displayed on the device itself (on a LCD display). This code is manually checked on both devices to deter any man-in-the-middle attacks. The Diffie-Hellman handshake mode has been especially designed to produce a secure short authentication code.

3.3 Cost Solution

We propose to design these BITW devices such that they only solve the problem they are built for. Unlike other vendors who create additional functionality into their devices to perform a multitude of processing and communications tasks, we have engineered a security only solution from the ground up with low cost, high speed and low power in mind. Our solution does not have wireless capability, which not only drives up the cost, but also creates another attack vector. It also allows us to power the devices from the serial line itself, thus eliminating costs for power adapters. Serial lines for these applications have as much as 5V available, which is enough to power them. However as a failsafe feature, devices contain a battery in case the power drops to an unacceptable level. The batteries can then be re-charged during periods of inactivity.

Texas Instruments offers an extremely low power microcontroller called the CC430. The CC430 has a hardware AES module which makes it ideal for this application. The CC430 can also perform an HB-2 encryption at 333 clocks which should be adequate to keep up with the fastest baud rates available on these serial connections.

The optional security host device (SECHOST) is a rack-mounted OEM network appliance with appropriate serial and Ethernet connectors. It runs a hardened version of Linux or NetBSD operating system to control and monitor the operation of terminating devices, generating alerts if necessary.

The greatest cost savings come in the form of human capital though. Our plug and play key management solution does not require trained staff and requires very little sophistication from current employees. Additionally, maintenance cost will be lower due to the reduced complexity in key management.

4 Conclusion

We propose a low latency serial encryptor that has plug and play capabilities, hides key management from the end users and is engineered for low cost. In a document published by DHS entitled “Cyber Security Procurement Language for Control Systems,” [16] three security objectives are listed in order of importance: availability, integrity, and confidentiality. Here we introduce two more security objectives: cost and simplicity. By including these, we can mitigate some of the barriers to SCADA security.

References

1. President’s Information Technology Advisory Committee, Cyber Security: A Crisis of Prioritization, Report to the President, National Coordination Office for Information Technology Research and Development, Arlington, Virginia, 2005.
2. V. M. Ijure, S. A. Laughner, and R. D. Williams, “Security issues in SCADA networks,” *Computers & Security* Vol. 25, pp498-506, 2006.
3. AGA, Cryptographic Protection of SCADA Communications, Part 2: Retrofit Application, AGA Report No.12, Part 2, 2006.
4. IEEE, Trial Use Std. for Retrofit Cyber Security of Serial SCADA Links and IED Remote Access, P1689, Draft, 2007.
5. IEEE. Trial Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links, P1711, Draft, 2007.
6. P.P. Tsang and S.W. Smith, “YASIR: A Low-Latency, High-Integrity Security Retrofit for Legacy SCADA Systems,” *The IFIP TC 11 23rd International Information Security Conference*, 2008.
7. Schweitzer Engineering Laboratories, Inc. SEL-3021-1 datasheet. http://www.selinc.com/datasheets/3021-1_DS_20060929.pdf.
8. Schweitzer Engineering Laboratories, Inc. SEL-3021-2 datasheet. http://www.selinc.com/datasheets/3021-2_DS_20070109.pdf.
9. Schweitzer Engineering Laboratories, Inc. SEL-3021-2 datasheet. <http://www.selinc.com/SEL-3025/>
10. Andrew K. Wright, John A. Kinast, and Joe McCarty. Low-latency cryptographic protection for scada communications. In *ACNS*, volume 3089 of *Lecture Notes in Computer Science*, pages 263–277. Springer, 2004.
11. M. D. Hadley, K. A. Huston, T. W. Edgar, AGA-12, Part 2 Performance Test Results, Pacific Northwest National Laboratories, 2007.
12. M. D. Hadley, K. A. Huston, Secure SCADA Communication Protocol Performance Test Results, Pacific Northwest National Laboratories, 2007.

13. Energy Sector Control Systems Working Group (ESCSWG), *Roadmap to Achieve Energy Delivery Systems Cybersecurity*, Sponsored by the U.S. Department of Energy, September, 2011
14. S. Hong and S.-J. Lee, "Challenges and perspectives in security measures for the SCADA system," in Proc. 5th Myongji-Tsinghua University Joint Seminar on Protection & Automation, 2008.
15. K. Stouffer, J. Falco, K. Kent, Guide to supervisory control and data acquisition (SCADA) and industrial control systems security, Special Publication NIST-SP-800-82-2006, National Institute of Standards and Technology (NIST), 2006.
16. G. Finco et al., "Cyber Security Procurement Language for Control Systems", Idaho National Labs, 2007, <http://www.msisac.org/scada>.
17. SEQUI, EncryptorPak L datasheet. <http://www.sequi.com/SEQUI-EncryptorPak-L.pdf>
18. Hallmark Project, 2010. www.oe.energy.gov/DocumentsandMedia/4-Hallmark.pdf
19. D. Engels, M.-J. O. Saarinen, P. Schweitzer and E. M. Smith: "The Hummingbird-2 Lightweight Authenticated Encryption Algorithm", In A. Juels and C. Paar (Eds.): RFIDsec 2011, LNCS 7055, pp. 19-31, Springer, Heidelberg (2011)