All About Eve: Comparing DNP3 Secure Authentication With Standard Security Technologies for SCADA Communications

Clifford Rosborough, *Exelon*
Colin Gordon and Brian Waldron, *Schweitzer Engineering Laboratories, Inc.*
2350 NE Hopkins Court, Pullman, WA 99163 USA, +1.509.332.1890

***Abstract*—This paper describes industrial control system (ICS) security problems that often require cryptographic solutions, investigates the central concepts that those solutions implement, and examines the tradeoffs and requirements for the selection of the best approach. Next, this paper introduces security protocols commonly used in ICS environments—Internet Protocol Security (IPsec), Transport Layer Security (TLS), and Distributed Network Protocol Secure Authentication (DNP3-SA)—and explains how these protocols are applied in common distribution communications architectures. Finally, this paper provides recommendations for how operational technology (OT) system owners and manufacturers can best implement cryptographic solutions.**

I. Introduction

Traditional discussions of data security begin with a simple scenario: Alice and Bob wish to communicate without Eve being able to intercept or manipulate the conversation. What techniques can Bob and Alice use to communicate securely?

In energy distribution networking systems, system reliability is the primary goal of securing data in transit. Ensuring that Eve cannot change or manipulate messages is a secondary goal. Conventional approaches to securing communications involve several forms of traditional cryptography methods. One popular method is tunneling (or virtual private network [VPN]), in which the system makes two ends of a communications link over an untrusted network appear as if they are on a local-area network (LAN) by hiding their Internet Protocol (IP) headers. Tunneling uses Internet Protocol Security (IPsec) to protect supervisory control and data acquisition (SCADA) and other communications by securing underlying transport mechanisms while leaving the protocol itself unaffected at the source and the destination. VPNs are popular in part because of how they compartmentalize the complexity of a security implementation and bring system security under the purview of communications system operators.

Recently, automation system engineers have expressed interest in SCADA protocols with secure extensions, such as Distributed Network Protocol Secure Authentication (DNP3-SA), and protocols that act as secure wrappers, such as Transport Layer Security (TLS). Although wrapper and integrated methods for securing SCADA communications are more complex for operational technology (OT) system operators to implement than cleartext protocols, they offer some specific benefits that are not available with VPN-only methods.

In this paper, we start by examining problems frequently solved by encryption techniques and how those problems relate to common SCADA architectures. We then describe the tradeoffs required to implement commodity cryptographic methods (i.e., mainstream cryptography methods used primarily for internet functions) in OT environments. Next, we look at examples of how IPsec, TLS, and DNP3-SA implement cryptographic concepts, investigating how those protocols map onto common distribution communications architectures. After examining real-world implementations of both IPsec and DNP3-SA, we make recommendations for OT system owners and manufacturers who wish to implement cryptographic solutions.

II. Understanding the Threat

Distribution network communications system designers often implement a hub-and-spoke architecture in which one or more secured metal cabinets communicate to a central location (a distribution substation or control center) over a wide-area network (WAN). This WAN is usually a type of wireless network and can be a public routable type, such as a cellular network.

The secured remote cabinets typically contain an "outstation" (usually a recloser control device), a battery, and a communications gateway device capable of passing traffic on a WAN. Fig. 1 shows an example of a "spoke" connected to the central "hub" of a system with hub-and-spoke architecture.

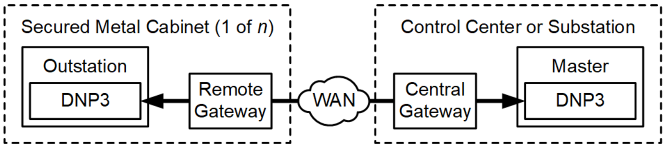
Secured Metal Cabinet (1 of *n*)
Outstation
DNP3
Remote Gateway
WAN
Control Center or Substation
Central Gateway
Master
DNP3

Fig. 1. Sample Hub-and-Spoke Architecture

For years, security practitioners have raised concerns about the vulnerabilities of geographically dispersed distribution equipment [1]. System owners generally respond to these concerns with physical precautions (such as secured enclosures and locks), and digital precautions (such as communications-securing gateways that are placed inside of locked enclosures).

However, some security provisions, including bump-in-the-wire (BITW) encrypting devices, can leave a physical attack vector between the outstation and the encryption device. Physical vulnerabilities are of particular concern in distribution networks because these networks are often located in unsupervised areas. The vulnerability is usually a standard network or serial cable that attackers can disconnect from the outstation and connect to an unauthorized device, as shown in Fig. 2. In some circumstances, an attacker who physically compromises a remote enclosure can obtain direct access to the master control center.

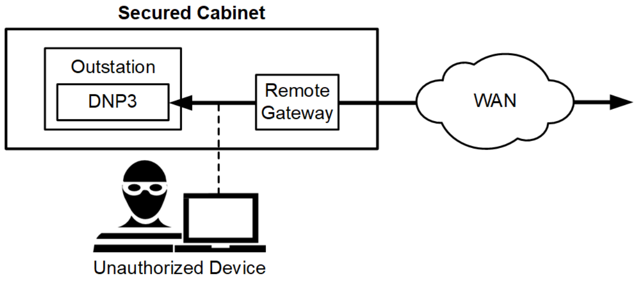

Fig. 2. Distribution Cabinet Threat Scenario

Reducing the physical attack surface of OT systems by moving encryption and security protections into outstation devices helps mitigate the physical cable vulnerability. System owners can implement this new security architecture with a complementary cryptographic solution. Having the cryptographic mechanism embedded directly into the outstation allows mutual authentication of the outstation device, gateway, and master. This solution prevents an attacker from inserting an unauthenticated device into the network, spoofing the outstation, and leveraging it to attack sensitive systems back at the head end of the network.

III. A Brief Cybersecurity Primer

The goal of applying cryptography is to increase the reliability of a system by mitigating threat actor attacks. Cryptographic systems achieve this goal by addressing one or more of the system attributes of confidentiality, integrity, and authentication (CIA). These attributes are often referred to as the CIA triad.

A. Confidentiality

Confidentiality is the protection of information from disclosure to, or interception by, unauthorized viewers [2]. Encryption provides confidentiality by using secure algorithms and secret keys to scramble information, making that information incomprehensible to threat actors.

B. Integrity

Integrity refers to the assurance that information has not been tampered with or altered. Integrity is checked by running information through a cryptographic algorithm to produce a unique value. If the message is altered in any way, then the unique value changes.

One type of unique value is a keyed hash-based message authentication code (HMAC), which is appended to the end of a message.

C. Authentication

Authentication provides proof of the identity of the message originator. Mutual authentication requires this to occur in both directions.

Discussions of authentication often cover the three types of identity evidence used to authenticate a human being: something you *have*, something you *know*, or something you *are*. The first of the three is a common way of proving identity over digital communications, as seen with public-key cryptography and digital certificates (something each person *has*). Authenticating a *device* instead of a human involves the same method, verifying something the device has, such as a key or one or more certificates, depending on the authentication scheme used.

Communications flows between master and outstation benefit when cryptographic systems use the CIA triad to ensure the integrity of commands and data.

D. Nonrepudiation

Nonrepudiation is often mentioned alongside the CIA triad, and it is directly mentioned in IEEE 1815-2012, Standard for Electric Power Systems Communications—DNP3. However, it applies less to the communications themselves than it does to accountability for actions taken on the system. Nonrepudiation is about intent and deception. These are characteristics unique to human actors and do not apply to the scope of this paper.

E. Replay Protection

Communications systems might encounter a threat where data can be recorded and replayed. However, most replays in real-world implementations are not signs of an attack but instead duplicate data associated with rapid Ethernet network reconfigurations.

Preventing a message from being captured and replayed onto the communications link at a time different from its original generation (whether the message is modified or not) is referred to as replay protection. Including a sequence number along with an HMAC at the end of a message is one example of replay protection.

IV. Three Common OT Cryptographic Methods

Tunnels (VPNs), wrappers, and protocol security extensions are three common methods of implementing cryptographic concepts in distribution networks.

A. VPN: IPsec

IPsec is a suite of protocols that provides security to Ethernet communications at the network layer [3]. It offers two basic modes: tunnel and transport. The tunnel mode provides a secure tunnel in the form of a VPN between two or more sites that already have a point-to-point or hub-and-spoke architecture by obfuscating the original IP header of the packet. The IPsec transport mode does not obscure the original IP header of the packet and generally does not fall under the definition of VPN; therefore, this paper discusses tunnel mode only.

IPsec adds a significant level of security. IPsec requires strong authentication, provides integrity verification, encrypts the traffic (for confidentiality), and includes a standards-based automatic key exchange. IPsec integrates tightly with routed network architectures by requiring that relationships called security associations are established between specific devices and networks. Without an established security association, the network cannot route communications.

VPNs tend to be data-agnostic so most Open System Interface (OSI) Layer 3 protocols and higher can be routed without extra complication.

Most IPsec gateways also provide additional security features such as port filtering, intrusion detection and prevention, and security logging. Common implementation examples for IPsec are available even for nonroutable protocols such as IEC 61850 GOOSE [4].

B. Wrapper: TLS

The primary goal of TLS is to provide a secure communications channel between two communicating peers on an existing network [5]. Unlike IPsec, TLS does not natively tunnel network traffic itself (i.e., it does not act as a VPN), but it is typically used as a method for encrypting existing applications and associated protocols. HyperText Transfer Protocol (HTTP) with a TLS wrapper pairing yields HTTPS; File Transfer Protocol (FTP) with a TLS wrapper pairing yields FTPS, and so on.

C. Protocol Security Extension: DNP3-SA

DNP3 offers a security extension in the form of SA Version 5 (SAv5) under the IEEE 1815-2012 DNP3 standard. Providing confidentiality is not the main purpose of SA in DNP3. Instead, SA is used to correctly identify the master and outstation that are communicating with each other (device authentication) and prevent both modification of transactions in transit (message integrity) and replay attacks (as defined by IEC 62351-2).

DNP3-SA uses a calculated HMAC; the outstation verifies the expected message or application service data unit (ASDU) with that HMAC. For example, a DNP3 master sends a binary output control for a critical operation to the outstation. The DNP3 outstation reply sends a challenge message to the DNP3 master. This causes the master to calculate an HMAC for the control operation and send it to the outstation. Once the outstation receives the HMAC, it calculates the HMAC value for the control operation and compares that HMAC value against the received value. If the HMAC values match, the DNP3 outstation executes the control. This behavior is shown in Fig. 3.

The master does not need to wait for the outstation to determine that an HMAC needs to be transmitted to the outstation for a particular DNP3 request or control. In Aggressive Mode, the DNP3 master simply includes the HMAC with the original DNP3 message. This is shown in Fig. 4.

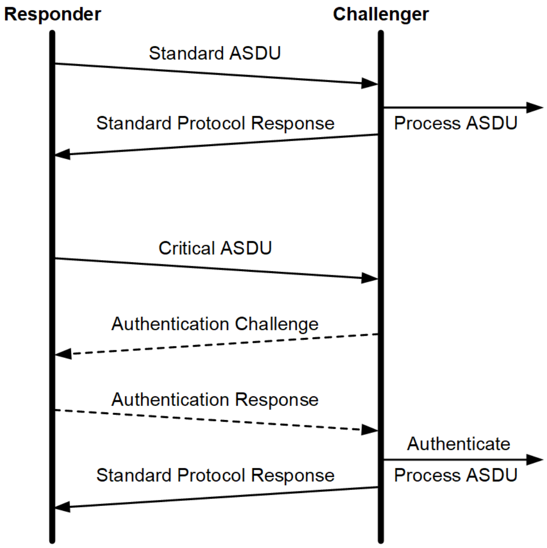

Fig. 3. Example of Challenge Response

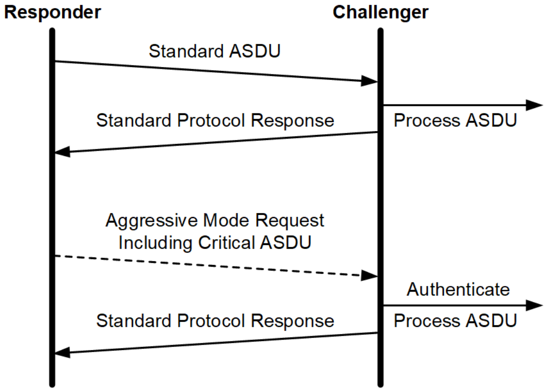

Fig. 4. Example of Aggressive Mode

The DNP3 standard stipulates that either Aggressive Mode or a challenge must be used with critical ASDUs. An ASDU is critical if an HMAC is required for the DNP3 message to be accepted and processed by the outstation (otherwise, the ASDU is standard).

The IEEE 1815-2002 DNP3 standard lists DNP3 requests that require HMACs to be compliant with DNP3-SA. Some implementations allow supported messages to be configured as either standard or critical ASDUs. Depending on the configuration of the intelligent electronic device (IED), only some DNP3 messages might use SA or all messages exchanged might use SA. Processing power and bandwidth consumption are common factors that determine which messages are used with SA.

In addition to verifying an HMAC when processing a message, DNP3-SA can implement user roles. These user roles define whether the master is authorized to read data, operate controls, change configurations, allow a local login, and so on. However, most devices only implement certain actions for user roles: recognizing monitoring data, operating controls, or transferring data files.

Three types of keys are used in a typical DNP3-SAv5 scenario: short-term session keys, medium-term update keys, and long-term authority certification keys. Session keys perform the bulk of the cryptographic operations because they are used to generate and verify the HMAC on critical controls. After the system owner configures the update key in the outstations and master (using out-of-band transfer methods), the session keys are automatically initialized, distributed, and regularly changed without human operator intervention.

DNP3-SA also allows automatic updates of the update key through the use of the authority certification key and either symmetric or asymmetric X.509 certificate methods. DNP3 does not offer an automated update system for authority certification keys. Depending on the system owner and key-management preferences, this can create challenges when scaling and managing keys. However, once the initial update key and authority certification keys are commissioned on the master and outstations for DNP3-SA, the authority certification key rarely needs to be updated to meet standard recommendations.

1) Advantages to DNP3-SA

DNP3-SA simplifies troubleshooting and integration with intrusion detection systems (IDSs) and intrusion protection systems (IPSs) because all DNP3 commands are in cleartext.

The implementation of user roles with DNP3-SA also allows an outstation to define which master connections it permits. Outstation user roles restrict the ability of masters because an outstation only processes request types that suit its user role.

When security extensions are built into the protocol, as with DNP3-SA, an IED can keep track of how many successful connections are made, how many unsuccessful attempts are made, and when keys are updated. It can then report these statistics through the protocol connection. Also, when the security is built into the application protocol, the bandwidth consumed between the master and outstation is significantly less. This particularly benefits remote connections where bandwidth may be limited.

An advantage to DNP3-SA that is not often discussed is hardware cost. At crucial substation locations, SCADA connections can easily warrant the additional cost of a security-related appliance for a VPN. The data concentrator at a substation is also likely to support TLS or another encryption-based protocol. However, devices in remote locations are less likely to support TLS and other protocols, and at connections to remote locations with one or just a few IEDs, it is not always cost-efficient to purchase security appliances. DNP3-SA is beneficial in these situations because most remote IEDs support DNP3 , and adding support for DNP3-SA to a device is less expensive than adding TLS support or an additional security appliance.

2) Disadvantages to DNP3-SA

The data exchanged between the master and the outstation are not encrypted. While this allows for easy troubleshooting, it also allows easy access to view exchanged information, which can include I/O status and configuration changes to power system IEDs.

Another disadvantage to DNP3-SA is that it is not very mature from a usage standpoint, compared to other encryption protocols such as IPsec and TLS. IPsec was created in its first form, a peer-to-peer tunneling protocol, in 1996. TLS started in 1994 as Secure Sockets Layer (SSL) and is the primary protocol used for encryption between browser and web outstations. Industry-standard encryption protocols such as TLS and VPN have had in-depth penetration testing for decades, with many protocol revisions and large installation bases consisting of millions of users.

This is not to say that DNP3-SA has not received any testing or independent examination; however, the testing and installation base of DNP3-SA cannot compare to the testing and installation bases of TLS and other industry-standard cryptographic methods.

V. Cryptography Tradeoffs in OT Environments

Because of the system reliability advantages that cryptography can bring, the authors recommend its evaluation by OT system owners and operators. If system owners are interested in implementing cryptography, they must consider the tradeoffs when doing so. They should perform well-informed risk analyses to determine if and where cryptography should be used in industrial control systems (ICSs). Furthermore, OT operators should be acutely aware that the emphasis on system reliability and availability makes changing settings, keys, and firmware on embedded devices rare. Thus, operators must take extra care to ensure cryptographic solutions are implemented correctly. The following subsections discuss several concerns to consider when adopting a cryptography system.

A. Frequent Changes to Standards and Best Practices

Frequent cryptographic standard changes by both private industry groups and government entities are problematic for OT environments. For example, because of both pressure from vulnerability researchers and support for commodity hardware accelerators, TLS 1.2 was ratified within two years of TLS 1.1 [6]. Even though the gap between TLS 1.2 and TLS 1.3 was ten years (August 2008 to August 2018), changes were made in March 2011 to update supported cipher suites and remove backward compatibility with previously supported versions [7]. The lag time between a standard's ratification and its implementation by OT manufacturers and system owners can be considerable, with some new firmware upgrades already out-of-date by modern cryptographic standards by the time those upgrades reach the endpoint IEDs.

Best practices for implementations can change with or independent from standards, because security practitioners are always honing guidance for cryptographic system implementations due to changing threats or advances in research. Either way, the effect is the same: a requirement to update field devices. One example of a recent change involved suggestions from the National Institute of Standards and Technology (NIST) on secure password implementation, specifically, shifting from an emphasis on password complexity to an emphasis on longer "passphrases" [8]. This change was echoed by a recent critique of the IPsec standard, wherein researchers suggested that preshare key implementations of IPsec should be 19 random ASCII characters or longer [9]. With these updated recommendations, implementations of commodity cryptographic protections that use passwords previously considered secure are now considered nonsecure applications by the industry, without any standards changes, known implementation flaws, or technical vulnerability discoveries. Furthermore, advances in computational power can obsolete existing cryptographic standards.

A key design goal for OT is to simplify designs to minimize the number of technologies in use. This includes using standards not subject to frequent changes that are associated with infrastructure built for different end goals.

B. *OT Secure Key Management*

Security key management in OT is notoriously difficult. A general rule of thumb in ICS is that without automated key-management systems in place, it is safe to assume that security keys will not be changed after commissioning for the lifetime of the device. The reasons for this are out of the scope of this paper; however, the cost of manual key management by paid administrators is generally considered a major factor. Therefore, a key design goal is to simplify this administration and avoid it where possible.

C. *The Complexity-Patching Cryptography Tradeoff*

Well-implemented cryptography adds reliability to the power system it protects at the cost of additional complexity within the communications system. It is axiomatic in the cybersecurity industry that additional complexity creates opportunities that threat actors can exploit [10] [11]. Researchers have discovered thousands of vulnerabilities in cryptographic implementations and standards [12]. Probably the most well-known example is the Heartbleed vulnerability [13], which affected most implementations of the popular OpenSSL library and allowed attackers to remotely read raw memory out of thousands of affected implementations and millions of devices.

This issue can be severe for systems that integrate feature-rich commodity cryptographic libraries because the sheer size and number of features included in these libraries can require frequent patch updates. The availability requirements for the average distribution energy system are vastly greater than the availability requirements of the average information technology (IT) system. Because of these strict availability requirements, there is an order-of-magnitude difference for patching consequences when IT-based cryptographic functions are implemented in OT devices. As a result, a key design goal for OT is to minimize patches.

D. *Cryptography Demands Expertise*

The security and cryptographic expertise of an organization is usually based within the realm of IT subject-matter experts. Smaller organizations without IT experience can commit grave errors when configuring commodity cryptographic systems in OT environments. OT system owners who are intimidated by "thou shalt" patch mandates and IT-based vulnerability enumeration engines generally avoid enabling commodity security solutions directly into IEDs (when made available by manufacturers). Enabling commodity security solutions can require the involvement of an outside organization and lead to associated pressures from the organization business unit. This IT and OT divide is often "solved" by demarcating the IT and OT equipment into separate physical devices, with IT security governance falling on the communications gateway equipment at the outstation location, and OT owning the actual IEDs (Fig. 1 illustrates this division).

A highly complex security solution can also lead OT personnel to bypass security devices due to frustration or lack of training. For these reasons, a key OT design goal is to minimize the expertise needed to securely apply the technology.

E. *Standard-Mandated Encryption*

Technical working groups design commodity encryption standards for the internet, where the primary goal of cryptography is to provide confidentiality. In ICS environments, the main goals are authenticating devices on the wire and ensuring the integrity of commands to prevent spoofing of data or devices. In ICS environments, not only is there less emphasis on confidentiality, but cleartext protocols are sometimes preferred for functions such as diagnostics or IDS and IPS systems, which require cleartext SCADA protocols to analyze out-of-place commands or operations and perform stateful protocol analysis. Many functions of ICS intrusion-detection technologies are based on evaluating cleartext SCADA protocols and providing inline intrusion prevention functions that come into conflict with the confidentiality of the data stream. TLS 1.3 mandates confidentiality and prevents data recovery using perfect-forward secrecy mechanisms that are not well-suited for ICS environments [5].

Not all scenarios in OT environments are similar with respect to their susceptibility to threat scenarios; distribution environments, for example, require confidentiality because of the geographically dispersed devices and communications networks involved. A key design goal for OT is to apply encryption (confidentiality) only where it is necessary.

F. *Heavy Computational Requirements*

Modern cryptographic standards presume modern central processing unit or hardware cryptographic accelerators are available. Many modern cryptographic methods are ill-suited for embedded environments, particularly legacy IEDs without cryptographic accelerators. For some ICS systems, cryptographic implementations optimized for embedded devices (such as streaming encryption ciphers) are ill-suited because of a lack of required message integrity. Many legacy systems also lack the required entropy (randomness) sources to establish strong cryptographic sessions. Therefore, system owners should evaluate what types of cryptographic functions are suitable for their available hardware resources.

G. *Application Performance Demands*

Modern cryptographic methods can add some overhead to existing communications links. Most modern cryptographic standards assume high-speed internet connections, while in the ICS space, high-latency (300+ milliseconds) and small-bandwidth (25 kilobytes per second) connections are still the norm. Cryptographic systems that require multiple round trips to establish a valid cryptographic session can have negative impacts on shared-medium links.

Because of existing ICS infrastructure, a key design goal for OT systems is to ensure that system performance is acceptable under worst-case conditions.

VI. Cryptographic Architectures for Distribution Networks

When evaluating how to integrate cryptographic systems into distribution networks, system owners should consider the three different types of secure communications architectures: BITW, bump-in-the-stack (BITS), and hybrid BITS plus BITW architecture.

A. *BITW: Commonly Used With IPsec*

In BITW systems, hardware devices (such as network gateways) at the master and the outstation add security functions to existing communications going over a WAN. An example of BITW architecture is shown in Fig. 5.

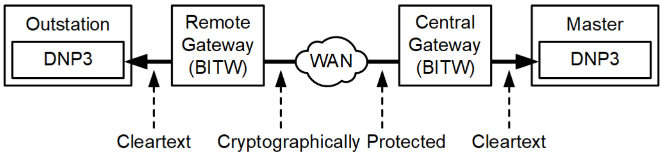

Fig. 5. Common BITW Cryptographic Implementation Architecture

BITW systems are present in both Ethernet-based OT systems and legacy serial systems (albeit less widely implemented there). BITW systems typically manifest as an IPsec VPN in the former and a serial wrapper protocol (such as IEEE 1711.2, Secure SCADA Communication Protocol) in the latter.

1) *Advantages of BITW Systems*

OT operators can implement BITW systems without changing or replacing existing OT systems, devices, protocols, or functions.

The complexity of the security change management lifecycle is also factored out from OT devices. At larger organizations, IT tends to own the communications devices, and BITW security features are built into those devices.

Having a separate security device conforms to best-practice defense-in-depth cybersecurity models. Best-practice security calls for implementing a separate device to segment security between functioning security layers because, for the outstation to be compromised, the BITW must first be compromised. BITW devices are generally purpose-built for security functions (rather than automation, protection, and other OT functions) with hardware both tailored for cryptographic operation and tested for defense against cybersecurity threats.

2) *Disadvantages of BITW Systems*

Without additional security methods in the IED, BITW devices leave a "last mile" of physical cable that is vulnerable to threat actors who have physical access to the secure outstation enclosure. (Note that some BITW systems integrate a hardware module directly into the IED chassis and do not have this physical vulnerability.)

BITW systems also generally require additional hardware and device management overhead.

Another disadvantage is that, because of the knowledge base needed, the implementation of and maintenance for BITW systems typically requires input from IT personnel.

In addition, BITW devices usually require accelerated patch cycles because of the larger attack surface that IT-based devices bear.

B. *BITS: Commonly Used With TLS*

In a BITS system, such as the example in Fig. 6, the outstation IED implements necessary data security functions as part of a separate software application or integrated hardware implementation. That module is both directly accessible by the embedded IED operating system (OS) and transparent to other applications on the same device.

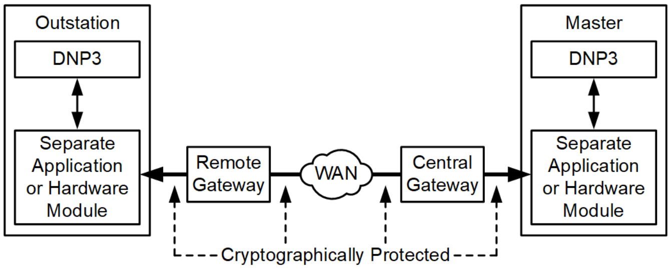
Outstation
DNP3
Separate Application or Hardware Module
Remote Gateway
WAN
Central Gateway
Master
DNP3
Separate Application or Hardware Module
Cryptographically Protected

Fig. 6. Common BITS Cryptographic Implementation Architecture

An example of a BITS security system might involve using host-based software VPN applications. Because the software VPN program is accessible and controllable by the OS and transparent to other programs (e.g., DNP3), it can be classified as a BITS security system. BITS systems typically use wrapper protocols such as TLS. Another example of a BITS system is the remote intelligent gateway program implemented by the California Independent System Operator (CAISO) corporation. That system requires TLS when DNP3 is used over a public network [14].

A BITS system must be an integrated solution that is directly accessible only within the chassis of the outstation or device. The BITS system should not be connected to peripheral I/O ports and should not be easy to manipulate physically. It must be difficult to physically compromise a BITS security system.

1) *Advantages of BITS Systems*

Because all cryptographic operations take place within the physical chassis of the IED, there is less of a last mile physical security problem with a BITS system if the outstation enclosure is compromised. Data integrity is maintained all the way back to the IED.

A system using only BITS security at the outstation typically has decreased costs of ownership because a BITW security device might not be required. Compared to scenarios where BITW security devices are necessary for each IED (for example, recloser control scenarios), BITS hardware costs can be less than or equal to 50 percent of the BITW cost.

BITS system owners can update the cryptographic functions separately from the application protocol, allowing underlying protection and automation functions to remain untouched. This can reduce the testing burden necessary with third-party test sets because the protocol itself might not be changed by the update.

2) *Disadvantages of BITS Systems*

Many WAN transport protocols require modem-like devices in the outstation enclosure to keep up with rapidly changing wireless communications technologies. Because each outstation enclosure typically requires at least one communications gateway device, overall hardware capital and operational expenditures might not be much lower than in BITW architectures where the BITW functionality is contained in the gateway.

Integrating commodity BITS programs and wrapper protocols into the outstation IED can require IT security governance over aspects of the outstation IED functions.

Security key management on ICS IEDs is also notoriously difficult. Although good security practices (and some standards) mandate regular key changes, it should be assumed that the administrative cost of performing key changes is high without automated key-management systems.

Another disadvantage to this system is that pushing commodity BITS programs and wrapper protocols to outstation IED devices can increase patch frequency due to the expanded attack surface.

Note that poor outstation OS security can also undermine some BITS implementation benefits. If easy OS exploits make the IED vulnerable, it can be trivial for an attacker to bypass the security afforded by the BITS scheme. The compromise of other physical ports to bypass encryption, or the compromise of a vulnerable application on the device, can lead to a compromise of the common memory space and allow attackers to steal encryption keys from the device [15]. Much onus is placed on OT device manufacturers to make sure that the IED OS is properly protected. Solutions such as application whitelisting and secure memory partitioning are recommended.

C. *Hybrid BITS Plus BITW: Commonly Used With IPsec*

A hybrid BITS plus BITW system is most often used in Ethernet distribution architectures. Fig. 7 shows an example architecture.

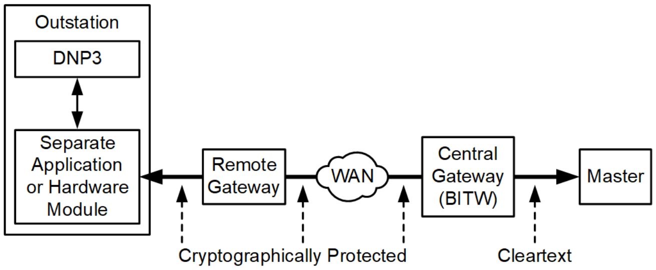

Fig. 7. Common Hybrid Cryptographic Implementation Architecture

In this system, the outstations implement the cryptographic functions inside the physical chassis and the master device adds security to the protocol using a separate BITW device. This architecture has several benefits over a pure BITS or BITW system.

1) *Advantages of Hybrid Systems*

The master typically has a more expensive operational cost than the outstations, so leaving the application in the master untouched is more desirable. The BITW system simply adds the security functionality to the communications layer and terminates directly in the remote outstation.

Because the location of the master system typically has much higher levels of physical security controls, there is less risk of a threat actor compromising any cleartext channel between the master and the BITW device at the head end of the network.

2) *Disadvantages of Hybrid Systems*

The hybrid approach brings some of the downsides of both BITS and BITW approaches. The cost may not be much lower than BITW architecture given defense-in-depth requirements, and BITS architectures may require increased patching frequency due to the push of wrapper protocols to the outstation device.

D. *Integrated: Commonly Used With TLS or DNP3-SA*

An example architecture for an integrated system is shown in Fig. 8.

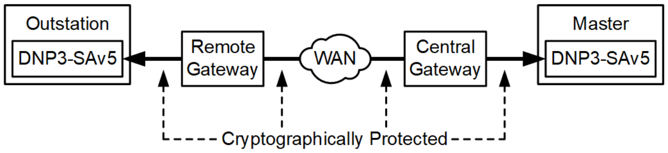

Fig. 8. Common Integrated Cryptographic Implementation Architecture

In an integrated cryptographic system, the end application is aware of the security methods and either calls a separate wrapper protocol (e.g., with HTTPS, the application performing HTTP invokes TLS) or has a version of the primary application that directly includes security extensions, such as DNP3-SA.

1) *Advantages of Integrated Systems*

Integrated systems with security extensions can provide security event logging and alerting information directly rather than relying on that function to be provided by the BITS or BITW entities.

Integrated protocols are easier to make transport-neutral, because the protocols and associated security mechanisms can be conveyed over different types of communications mediums, including both serial and Ethernet cables.

Bandwidth consumption is also lower because security is embedded into the application protocol. This is due to directly embedded cryptographic functions that do not rely on encapsulation provided by separate protocols.

TABLE I
CAPABILITIES OF CRYPTOGRAPHIC IMPLEMENTATIONS

Protocol Capability or Name	IPsec VPN	TLS Wrapper	DNP3-SA
Communication session authentication	Yes	Yes	No
Spoofing protection (device authentication)	Yes	Yes	Yes
Eavesdropping protection (message confidentiality)	Yes, with encapsulated security payload (ESP)	Yes; required in Version 1.3	No (yes for key updates only)
Modification protection (message integrity)	Yes	Yes	Yes, configurable on a per-message basis
Open System Interconnection layer	Layer 3; Layer 2 with L2TP	Layer 4	Layer 7
Message replay protection	Yes	Yes	Yes
Valid message holdback and flood protection	No	No	Yes, except for Aggressive Mode
Out-of-order message protection	No	No	Yes
Initial handshake required	Yes	Yes	No
Symmetric key support	Yes	No	Yes
Asymmetric key support	Yes	Yes	Yes (version 5 only)
Perfect-forward secrecy support	Yes	Yes, required in Version 1.3	Yes
Transport neutral	No (Ethernet only)	No (Ethernet only)	Yes (serial and Ethernet)

2) *Disadvantages of Integrated Systems*

Integrated systems that have protocols with security extensions cannot have security updated without affecting the underlying availability of power system functions unless the integrated system is using a wrapper protocol.

Some integrated systems with wrapper protocols use more than one variant of the same cryptographic wrapper protocol. For example, an integrated HTTPS application might use TLS implemented in OpenSSL 1.0.2q while an integrated FTPS application on the same device uses an older OpenSSL 1.0.2n. Devices with multiple integrated applications only get the benefits of a small overall code base if they use the same undifferentiated wrapper protocol.

A comparison of all three cryptographic methods discussed in this section is shown in Table I, along with the protocol capabilities of each system.

VII. REAL-WORLD IMPLEMENTATIONS

A. *Integrated Architecture With DNP3-SA*

In an integrated architecture cybersecurity system, Pepco, a subsidiary of Exelon, deployed approximately 100 outstations running DNP3-SAv5 on four IP networks with radio backhaul. This system was installed to verify the SA feature.

DNP3-SA was challenging to deploy because the adoption of the protocol has been light; the lack of interoperability testing between OT manufacturers puts the burden on the end user. Device support and interoperability limitations required working directly with the manufacturers to achieve successful communications. There were also version issues to overcome. Different versions, such as DNP3-SAv2 and DNP3-SAv5, are not compatible and device manufacturers typically only support a single version.

Based on experience from this implementation, key management in an integrated cybersecurity system needs to be worked out prior to deployment. The end user can choose between symmetric shared keys or asymmetric public-private keys. A centrally managed key and certificate authority is generally preferable to manual key installation.

The maintenance of the outstation and outstation communications also needs to be planned upfront. If the authentication of all commands is required by the outstation, then the current encryption keys need to be installed in the DNP3 test equipment. Fortunately, the devices can be configured to require authentication for individual commands. The DNP3-SA standard “critical” defaults were a good starting point for the outstation. To achieve the full security benefit of the protocol, the master should require authentication for all commands. This increases the traffic on the communications path because each command sent by the master must be authenticated first.

Using DNP3-SA over IP proved to be an issue when communicating over poor or overprovisioned communications systems. Only a handful of poorly functioning devices can cause a denial of service condition for other devices on the network. The authors’ experience shows that DNP3-SA over IP requires a stable network with the adequate bandwidth to handle operations and device management.

One portion of the test included a network of 20 to 40 outstations that communicated via Ethernet over a power line to a backhaul radio. All commands from the master were authenticated using asymmetric keys. In this mode, several extra packets were exchanged for every command with authentication. Those extra packets led to cascading failures over time because when communications became erratic, the master devices sent out retries, causing additional outstations to fail to communicate. The system should have reduced the retry attempts. DNP3-SA configurations need to be carefully tweaked for various communications conditions to prevent this kind of behavior.

B. BITW Architecture and Hybrid BITS Plus BITW Architecture With IPsec

IPsec proved to be a reliable method of securing thousands of devices in the Exelon environment. Most of the distributed devices were deployed with IPsec using two of the methods mentioned earlier: with IPsec built into the outstation and with separate BITW devices.

The IPsec built into the outstation (BITS) architecture provided superior protection to the network and back-end systems. With this protection, fewer physical and operational controls were required to thwart physical threat actors, reducing operations and maintenance costs. When the BITW devices were used, additional alarming, physical controls, and operational controls were required to mitigate physical threats to the outstation enclosure.

The latency of the network was also important for internet key exchange rotations. Keeping the round-trip time under 1 second allowed time to establish reliable and efficient security associations. However, a round-trip time that exceeds 3 seconds for any single device on a network can cause a denial of service. In this implementation, dead peer detection was configured to recover devices that had rebooted or lost their security associations prior to the keys expiring. Most utilities with thousands of devices to terminate should consider a tiered architecture with multiple remote VPN concentrators.

VIII. Summary of Security Model Considerations

System owners with the following concerns should consider implementing a BITW cybersecurity system:

- Direct network access to more than one outstation network host is necessary.
- Minimal security change controls on IEDs are required.
- Existing IEDs cannot be upgraded with BITS or integrated cryptographic support due to cost, technical hurdles, or reliability concerns.
- Defense-in-depth is a system requirement.
- Cryptography subject-matter experts are already present among the telecom or IT personnel who govern the communications infrastructure devices (gateways) for the organization. Note that this does not excuse OT system owners from educating themselves on proper security applications and functions.
- Unencrypted traffic inspection (typically in the form of an intrusion detection application) is required prior to allowing SCADA protocols to egress to an outstation device.

System owners with the following concerns should consider implementing a BITS cybersecurity system:

- Physical attack surface minimization (cleartext cabling) is required at the outstation.
- More than one specific protocol or application is needed on the outstation device (a BITS implementation can include VPN functions to secure the entire network layer).
- Authentication must be granularly traced to the individual outstation device.

System owners with the following concerns should consider implementing an integrated cybersecurity solution:

- Physical attack surface minimization (cleartext cabling) at the outstation is required.
- Authentication to the individual application on the master and outstation is required.
- A transport-neutral security implementation that works with existing serial and Ethernet systems without costly infrastructure upgrades is required.
- An entire system needs to be upgraded without the costly purchase of additional BITW devices, and the system already supports security, e.g., DNP3.
- The ability to secure a specific protocol command or operation is needed and adding IPS devices is not feasible.
- Bandwidth concerns are high, and high assurance is only required for specific commands, not the entire protocol communications session. Integrating authentication of all commands results in high bandwidth usage.

A. Combining Architectures

System owners can combine cybersecurity architectures to gain additional benefits. For instance, combining gateways that implement BITW solutions with IEDs supporting BITS or integrated solutions provides last mile physical link mitigation and conforms to defense-in-depth best practices. Combining BITS (TLS) with integrated solutions such as DNP3-SA provides many of the benefits of the protocol plus security extensions and additional strong confidentiality across untrusted networks.

B. The "Trust Boundary" Argument

Some security researchers argue that common SCADA protocol standards are large enough that many flaws exist among the different implementations [16]. This could lead to a false sense of security. If a manufacturer simply adds security extensions to an existing protocol that already has flaws, an end user might implement that single cryptographic method without any other security controls and use only that flawed protocol when tunneling communications over untrusted networks.

For example, if a system owner implements DNP3-SA as shown in Fig. 8 without additional cryptographic protections, such as TLS or IPsec, then any attacker on the untrusted WAN can damage the master or the outstation devices by "fuzzing" or manipulating the DNP3-SA protocol itself, attempting to exploit flaws in the protocol. This example illustrates what happens when a system owner puts DNP3 outside the trust boundary, exposing a protocol with many flaws to an attacker.

In contrast, using a simpler wrapper protocol (such as TLS) to protect the DNP3 protocol puts the SCADA protocol inside the trust boundary because any attack against the TLS-wrapped DNP3 protocol falls against the security of the small wrapper implementation which (in theory) has fewer flaws. If a system owner does not trust the SCADA implementation of a manufacturer, using a well-vetted wrapper protocol instead, on as many SCADA protocols as possible, minimizes the code footprint and the possible exploitation of flaws in the other protocols.

IX. Conclusion

The advent of ubiquitous SCADA communications in remote cabinets has changed the threat landscape to the point that cryptography presents a compelling solution to the physical security problem. System owners should discuss cryptographic solutions with fellow OT system owners and with device manufacturers. Increasing knowledge about cryptographic processes and functions among OT owners, operators, and manufacturers is a good first step, because forays into evaluating cryptographic solutions should begin with good security education for personnel.

A. Next Steps for System Owners

Any critical security discussion should begin with a threat analysis: how vulnerable is the system to threats that can affect reliability? Not all distribution communications architectures are the same. In populated areas, quick responses to physical security alerts can eliminate the need for cryptographic protections inside of secure outstation enclosures. Even in geographically isolated areas with long response times for truck rolls, system owners can mitigate threats of command injections from physical attacks (such as scripts that disable input from remote outstations for a period of time) with digital methods.

Owners should discuss threats identified by their organizations with the appropriate security personnel. If cryptographic protections are deemed necessary, then the tradeoffs of cryptographic implementations in OT devices should be discussed. Cryptography can be difficult to implement, enable securely, and maintain. If personnel education, cost, or scalability are of concern, then continuing with existing and reliable noncryptographic solutions in outstation IEDs might be a better option.

If a cryptographic solution is necessary and still acceptable after weighing the tradeoffs listed in Section V, then system owners should meet with device manufacturers to determine the most reliable cryptographic option for each system. Device manufacturers should then develop cryptographic solutions with reliability and safety as primary goals.

B. Final Recommendations

It can be difficult for system owners to objectively weigh the benefits and downsides of integrating cryptography into environments that are not expected to change for a decade or more, given that there are already many obstacles to implementing long-term cryptographic systems. The following list of conditions should be considered when implementing any cryptographic system into an outstation device in a geographically dispersed distribution network:

- Minimize code size and complexity for cryptographic implementations.
- Monitor the integrity of executing code using whitelisting or other security techniques.
- Use the security features of the platform to protect sensitive data, such as credentials and cryptographic keys, from unauthorized access or modification.
- Simplify or automate cryptographic key management as much as possible.
- Consider using feature-reduced versions of cryptographic library "forks" that are minimized for embedded systems.
- Provide additional security controls to detect and alarm on physical tampering so that an attack with physical access to the IED cannot easily bypass BITS or integrated schemes.

X. References

[1] E. Byres, "DNP3 Vulnerabilities Part 1 of 2 – NERC's Electronic Security Perimeter Is Swiss Cheese," Tofino Security: Practical SCADA Security Blog, November 2013. Available: https://www.tofinosecurity.com/blog/dnp3-vulnerabilities-part-1-2-nerc%E2%80%99s-electronic-security-perimeter-swiss-cheese.

[2] D. Whitehead and R. Smith, "Cryptography: A Tutorial for Power Engineers," proceedings of the 35th Annual Western Protective Relay Conference, Spokane, WA, October 2008.

[3] S. Frankel and S. K. Ericsson, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," Internet Engineering Task Force (IETF) Request for Comments (RFC) 6071, February 2011. Available: https://tools.ietf.org/html/rfc6071.

[4] P. Jafary, O. Raipala, S. Repo, M. Salmenperä, J. Seppälä, H. Koivisto, S. Horsmanheimo, H. Kokkoniemi-Tarkkanen, L. Tuomimäki, A. Alvarez, F. Ramos, A. Dede, and D. Della Giustina, "Secure Layer 2 Tunneling Over IP for GOOSE-Based Logic Selectivity," proceedings of the 2017 IEEE International Conference on Industrial Technology (ICIT), Toronto, ON, Canada, March 2017.

[5] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF RFC 8446, August 2018. Available: https://tools.ietf.org/html/rfc8446.

[6] J. Salowey, A. Choudhury, and D. McGrew, "AES Galois Counter Mode (GCM) Cipher Suites for TLS," IETF RFC 5288, August 2008. Available: https://tools.ietf.org/html/rfc5288.

[7] S. Turner and T. Polk, "Prohibiting Secure Sockets Layer (SSL) Version 2.0," IETF RFC 6176, March 2011. Available: https://tools.ietf.org/html/rfc6176.

[8] P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid, W. Burr, and J. Richer, "Digital Identity Guidelines: Authentication and Lifecycle Management," *NIST Special Publication 800-63B*, June 2017. Available: https://pages.nist.gov/800-63-3/sp800-63b.html.

[9] K. Matthews, "Security Gaps Found in IPsec," Hacker Noon, August 2018. Available: https://hackernoon.com/security-gaps-found-in-ipsec-5a075b44609e.

[10] C. Perrin, "The Danger of Complexity: More Code, More Bugs," TechRepublic IT Security blog, February 2010. Available: https://www.techrepublic.com/blog/it-security/the-danger-of-complexity-more-code-more-bugs/.

[11] A. Bessey, K. Block, B. Chelf, A. Chou, B. Fulton, S. Hallem, C. Henri-Gros, A. Kamsky, S. McPeak, and D. Engler, "A Few Billion Lines of Code Later: Using Static Analysis to Find Bugs in the Real World," *Communications of the Association for Computing Machinery (ACM)*, Vol. 53, Issue 2, February 2010, pp. 66–75. Available: https://cacm.acm.org/magazines/2010/2/69354-a-few-billion-lines-of-code-later/fulltext.

[12] MITRE Corporation, "CVE Search Results (Keyword = SSL)," Common Vulnerabilities and Exposures List, January 2019. Available: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=SSL.

[13] Synopsys, Inc., "The Heartbleed Bug," April 2014. Available: http://heartbleed.com/.

[14] California Independent System Operator, "CAISO RIG Acceptance Test (RAT) Procedures," September 2016. Available: https://www.caiso.com/Documents/RIGAcceptanceTest_RAT_Procedures.pdf.

[15] DNP Users Group, "DNP3 Security Notice SN2017-001: CrashOverride/Industroyer Malware," DNP.org, August 2017. Available: https://www.dnp.org/DNP3Downloads/DNP3%20SN2017-001%20CrashOverride_Industroyer%20Malware.pdf.

[16] A. Crain, "DNP3 SAv5 and TLS: Different Trust Boundaries," Automatak, April 2013. Available: https://automatak.com/blog/2013/04/08/dnp3-sav5-vs-tls-different-trust-boundaries.html.

XI. Biographies

Clifford Rosborough is a principal cybersecurity architect with Exelon. He has 40 years of utility experience in engineering, programming, integrating, and securing energy management systems. He started his career in Rockwell International's Automation division as part of the team that installed, integrated, and maintained Pepco's first system-wide supervisory control and data acquisition (SCADA) implementation. He continued his career with Pepco, Pepco Holdings, and Exelon.

Colin Gordon is a lead application engineer at Schweitzer Engineering Laboratories, Inc. (SEL) in the wired communications division, specializing in communication and cybersecurity solutions and services for critical infrastructure. His work experience includes secure network design, implementation, testing, and regulatory compliance integration for utilities and asset owners in North America and abroad. He joined SEL in January 2008 as a product management intern, and he holds a bachelor's degree in computer engineering from the University of Idaho.

Brian Waldron is a lead automation engineer with Schweitzer Engineering Laboratories, Inc. (SEL) in Pullman, Washington. He has several years of experience in designing and troubleshooting automation systems and communications networks. He has authored several application guides focusing on integrating automation products. He has represented SEL at IEC 61850 interoperability demonstrations organized by Utility Communications Architecture (UCA) and frequently teaches engineering design and the application of IEC 61850 solutions. Brian graduated from Gonzaga University with a B.S. degree in electrical engineering.

20190131 • TP6910