Power system DNP3 data object security using data sets

Todd Mander a,*, Richard Cheung a, Farhad Nabhani b

a Ryerson University, Toronto, Canada
b University of Teesside, Middlesbrough, UK

Abstract

Power system cyber security demand is escalating with the increased number of security incidents and the increased stakeholder participation in power system operations, specifically consumers. Rule-based cyber security is proposed for Distributed Network Protocol (DNP3) outstation devices, with a focus on smart distribution system devices. The security utilizes the DNP3 application layer function codes and data objects to determine data access authorization for outstations, augmenting other security solutions that include firewalls, encryption, and authentication. The cyber security proposed in this article protects outstation devices when masters are compromised or attempt unauthorized access that bypass the other security solutions. In this article, non-utility stakeholder data access is limited through DNP3 data sets rather than granting direct access to the data points within an outstation. The data set utilization greatly constrains possible attack methods against a device by reducing the interaction capabilities with an outstation. The data sets also decrease the security complexity through rule reduction, thereby increasing the security applicability for retrofitted or process constrained devices. Temporal security constraints are supported for the data sets, increasing security against denial of service attacks.

© 2009 Elsevier Ltd. All rights reserved.

1. Introduction

Supervisory Control and Data Acquisition (SCADA) computer networks are used for critical national infrastructures including power systems. The demand for SCADA cyber security is escalating with increased number of cyber incidents, increasing power system automation that includes smart grids, and increasing stakeholder participation (SP800-82 Final Public Draft, 2008; Kropp, 2006; Schainker et al., 2006; Cleveland, 2008; Cai et al., 2008; Pollet, 2009). Until recently SCADA security has relied on security through obscurity (Cleveland, 2007). A commonly used SCADA protocol is the Distributed Network Protocol (DNP3), which is used for power, water, and gas utilities, and which has specified only authentication security (Draft DNP Application Note AN2005-001, 2006; DNP3 Specification, 2008a). This article proposes data access control security for DNP3, augmenting the DNP3 authentication security as well as security external to DNP3 that includes firewalls and encryption protocols. The data object security in this article utilizes the DNP3 data object library to create rule-based security, determining data authorization for transmission and reception operations (DNP3 Specification, 2007a,b, 2008b). The proposed security does not implement authentication or encryption, which can be implemented through the DNP3 authentication security, Transport Layer Security (TLS) for LAN DNP3, Internet Security (IPsec) for LAN DNP3, or security extensions that include bump-in-the-wire devices (Cleveland, 2007; DNP3 Specification, 2007c; RFC 4301, 2005; RFC 5246, 2008). Security risks for the SCADA networks are escalating due to the ongoing power system automation, particularly within the distribution system and for smart grids (Kropp, 2006; Schainker et al., 2006; Cleveland, 2008; Sweet, 2009).
ongoing utility automation provides significant improvements for power system integration and stability control, but increases the cyber risks to the infrastructure, i.e. there are numerous devices that can be affected by remote attacks from within the SCADA network. SCADA network security risks are increased further with the connections to the corporate networks (SP800-82 Final Public Draft, 2008; NISCC, 2005), e.g. attacks propagating from the Internet into the corporate network and then into the SCADA network. Although firewalls can isolate and protect SCADA networks from corporate networks or create electronic perimeters (Kropp, 2006; NISCC, 2005; CIP-005, 2006), firewalls do not protect the SCADA devices behind the firewall from compromised devices within the SCADA network. As a result of deregulation open access, and particularly with smart grids, the SCADA network will be directly accessible by numerous stakeholders including the system operator, electricity retailers, government agencies, and consumers. As a result of increased aggressive consumer demand side management (DSM), there may be potentially millions of devices within the distribution system, e.g. due to smart metering and dispersed renewable generation (Vojdani, 2008; Fan and Borlase, 2009; Meter Data Management and Repository (MDM/R), 2006).

There are two main vulnerabilities as a result of the numerous devices: device location and device access. SCADA devices used for DSM will be located in relatively unsecured locations and are therefore easier to compromise, e.g. consumers compromising smart meters to commit fraud. Multiple compromised devices can also be utilized to create organized attacks against the power system, e.g. cyber terrorists creating sustained power distribution problems such as outages and fluctuations. Therefore SCADA cyber security is critically required. However, DNP3 and TCP/IP security only provide security against compromised data transmissions and not against compromised devices.

The cyber security proposed in this article utilizes rule-based security to block unauthorized access to DNP3 devices from compromised devices within the distribution system and unauthorized access by stakeholders. The rule-based security is developed for power system characteristics, including long device life spans that require stringent interoperability and devices with limited processing capabilities that minimize deployment costs. The cyber security proposed in this article is a progression of previous work by the authors in Mander et al. (2007). The security in this article now restricts outstation access to data sets only for non-utility stakeholders, where previously the stakeholders had full data object access, and introduces temporal security constraints. This progression to data set only security results in increased security restrictions for the non-utility stakeholders and decreased implementation complexity. The cyber security emphasis on the data sets decreases security processing requirements, increasing efficiency and simplicity necessary for device long life spans and/or devices with minimal processing capabilities.

The rest of this article follows with Section 2 providing a brief overview of DNP3. Section 3 presents the security threats and the data object security basis for this article. Section 4 presents a support protocol to counter-act data set creation request threats. Section 5 presents the security rules and operations for the data set security, and includes performance results. Section 6 presents a data set security example for the security target application area, which is DSM, in comparison with conventional data object security. Section 7 presents the discussion and Section 8 the conclusion.

2. DNP3 overview

This section provides a brief DNP3 overview for those unfamiliar with DNP3. DNP3 can operate either in a master–slave or a peer-to-peer configuration, where the master stations control the outstation operations. The outstations can operate on a poll–response basis, and additionally provide unsolicited responses for event data to the masters. The DNP3 specification contains three protocol layers: application layer, transport function, and data-link layer (DNP3 Specification, 2007d,e,f). DNP3 also specifies the connection management layer for interfacing the DNP3 data-link layer with TCP/IP (DNP3 Specification, 2007c). The DNP3 data-link layer provides link connection services such as error detection, network addressing, and optional error control (DNP3 Specification, 2007f). The transport function is a pseudo transport layer used for fragmentation and reassembly of the application layer fragments only (DNP3 Specification, 2007e). The DNP3 application layer structures the data access requests for the masters and creates the data responses from the outstations. An application layer message is a complete data transmission to a device, e.g. the response to a master’s read access, and is fragmented into application layer fragments (DNP3 Specification, 2007d). The application layer does not fragment data objects across the application layer fragments.

The DNP3 data parameters are named points, and related points are grouped together into a point type, e.g. analog inputs, analog outputs, digital inputs, digital outputs, and counters are all different point types (DNP3 Specification, 2007d). Specific points within the point type is accessed by contiguous index values that groups all related points together within the outstation, i.e. when a master requests a range of indexes from a point type within an outstation it is not requesting data from individual applications, but from an outstation ‘database’. The application layer function code defines the interaction between the master and outstation, e.g. a master may use function codes to read or write data, control operations or applications, and transfer files.

The data object defines the data and its attributes between masters and outstations. The application layer object header defines the properties of the data objects, and consists of the object type, qualifier, and optional range fields (DNP3 Specification, 2007d). The object type field consists of two fields: the object group and the variation fields. The object group field indicates the point type, e.g. digital outputs, and what the data represents within the point type, e.g. current value or a frozen value. The variation field defines the data-encoding format for the data object, either as a primitive data type, e.g. a 16-bit integer, or as a sophisticated data object format, e.g. data structures. The object type and variation used for a data transmission varies with the function code, e.g. file transfer function codes would only use file transfer data objects. The
qualifier and the range fields indicate which point type indexes are included in the application layer fragment and how those data objects are packed. There may be zero, one, or more different point types within an application layer fragment, e.g. digital outputs and analog inputs. The group number, variation, and point index provides many combinations for accessing outstation data that need to be secured from unauthorized access. This security problem is further exasperated by the fact that all outstation data is accessible from the DNP3 application layer.

Data sets provide the capability to collect related or unrelated point type data together for simpler data management at the master (DNP3 Specification, 2007g), e.g. providing the power consumption data (counter) with the voltage and current readings (analog input). The data sets are referenced by an index number in the same manner as the points. Data sets are unique for each master–outstation association, and therefore index values for the same data may vary within the same outstation. The data set prototype defines data set templates that can be used by the data set descriptors. The data set descriptor defines the attributes and structure of a data set used between a master and outstation. A data set point type is defined for the current data, and is used for accessing or operating on points within the outstation. A data set point type is also defined for reading event data. Data sets therefore provide third-parties the ability to access DNP3 device data without complicated security associations required for each individual point within an outstation.

DNP3 defines authentication security, but does not support encryption for confidentiality (DNP3 Specification, 2008a). The authentication utilizes an Advanced Encryption Standard (AES) key wrap algorithm and defines a set of authentication keys for each user communicating with an outstation, utilizing a master key and a session key (DNP3 Specification, 2008a). DNP3 does not specify any further security, but recognizes that data or RBAC security may be required to limit authorized access to an outstation (DNP3 Specification, 2008a). DNP3 supports two authentication procedures: normal and aggressive modes. The normal mode is a challenge-response mode where the master or an outstation will challenge the authenticity of critical data transmissions, e.g. control commands. The challenged device will respond with the authentication data. The aggressive mode includes the authentication data within the application layer fragment, reducing the protocol overhead. However, this mode is not considered as secure by DNP3 (DNP3 Specification, 2008a).

Although a user may be authenticated, there are no user data access restrictions unless security such as proposed by this article is implemented.

3. **Data object security**

3.1. **Data object attack vulnerabilities**

There are many possible attacks on the power system, with a broader example of attacks presented in (Ten et al., 2007). Many attackers are concerned with disrupting the entire power system, e.g. compromising multiple devices nearly simultaneously to create system stresses. However, other attackers are concerned only with localized attacks to compromise a device, e.g. consumers defrauding the distribution system operator or electricity retailer. These device compromise attacks can be implemented very effectively with power system data objects based on the simple attack tree shown in Fig. 1. The attack tree provided a guideline for the data set security development.

Fig. 1 shows three main attack methods for compromising a power system device using DNP3 function codes and data objects: device surveillance, denial of service (DoS) attacks, and directly controlling the device. The device surveillance monitors the device’s traffic, determining when the device can be physically attacked or is vulnerable to a denial of service (DoS) attack. For example, a device transmitting several unsolicited responses is likely undergoing a severe event and may be vulnerable to disruption with attacks such as DoS flooding. The DNP3 device attributes data objects can be accessed to determine the device capabilities and therefore it vulnerabilities. For example, the device may have a description providing its maximum ratings, allowing an attacker to determine the minimum current spike required to damage the device physically. The device’s operation values can be accessed to determine the types of attacks the device is vulnerable to, e.g. the operating point at which breakers will be operated. The device’s operation values also allow the attacker to determine their safety margins on influencing a device’s operations before there is a risk of detection, such as reading the trigger points in the deadband values.

DoS attacks disrupt a device’s operations at critical moments, causing the device to incorrectly operate, preventing the device from operating in a timely manner, or preventing the device from operating on received control commands. Using device surveillance intelligence, the attacker can transmit monitoring or control commands to the device at a critical moment, causing the device to divert resources to the handle the received data. As a result, the device may not respond quickly enough to an event or not transmit the event data quickly enough. Alternatively, the attacker can flood the device with data preventing the device from processing legitimate traffic, e.g. continuously transmitting function codes to read the current outstation response time in order to prevent control commands from being processed.

Attackers are capable of directly controlling device operations. The attackers can control the device’s physical operations, e.g. opening/closing relays, and altering the device’s behaviour, e.g. altering deadband triggers. Alternatively, attackers can turn on or off applications using the function codes and data objects. These attacks can severely disrupt power system operations. However, DNP3 authentication security authenticates the source of the message, but not the authorization of that source to implement control operations (DNP3 Specification, 2008a). External security is required to provide that authorization, such as with the data set security presented in this article. The security is especially critical, as illustrated by this article’s Demand Side Management (DSM) example, with multiple stakeholders accessing utility devices.

3.2. **Data object security profiles**

The DNP3 data object security can be implemented within the application layer or the connection management layer, which
is shown in the profiles in Fig. 2. There are advantages and disadvantages to each of the profiles, and therefore the data object security is developed layer independent to increase its implementation flexibility.

Within the application layer, the data object security can directly interact with the application layer to minimize processing overhead, e.g., the application layer can specifically indicate which data objects are within the application layer fragment to the data object security. There would be a larger processing overhead to provide the same level of service for each data object within the connection management layer. However, data object security within the connection management layer creates easier device retrofitting for TCP/IP operations. A restriction of one data object per application layer fragment is therefore required for the connection management layer security profile to avoid intensive security processing. This restriction precludes the use of the DNP3 authentication security in the non-critical aggressive mode (DNP3 Specification, 2008a).

3.3. Stakeholder classifications

This article classifies authorized utility stakeholder access to outstations with four classes: primary master, secondary control, secondary limited control, and secondary monitoring. The primary master is defined as any authorized utility user accessing the SCADA network. The secondary control master is defined as a stakeholder that has authorized access to control specific operations in a device, but not with the degree of control as the utility. Examples of the secondary control masters, presented in the Section 6 DSM example, are the consumer and the electricity retailer. The limited secondary control master is equivalent to the secondary control master except for increased access restrictions. An example of the limited secondary control master, presented in Section 6, is the device manufacturer. The secondary monitoring master is defined as a stakeholder with no authorized access to device control operations; they are limited to device monitoring only (read-only access). Except for the primary master, masters may only directly access the device via the Internet (or local connection) and indirectly through the SCADA network at the utility’s discretion and terms.

3.4. Function code security

Function codes indicate the operations that are to be performed on the data objects, e.g., read and write (DNP3 Specification, 2007d). The function codes therefore highly enable the attacks shown in Fig. 1, including surveillance, DoS, and directly controlling device operations. The data object security presented in this article uses the function codes as a coarse granular security selector for compromised communication, compromised masters, or stakeholders attempting unauthorized access to a device. With the coarse granular security selector, the data object security quickly discards received data that can be used in the attacks indicated in Fig. 1. For masters with limited access requirements, potential DoS attacks are prevented by discarding any data from masters accessing files, assigning classes, requesting time responses, or turning on/off unsolicited responses. Additionally, masters

![Fig. 1 – Simple attack tree for compromising a DNP3 device.](image1)

![Fig. 2 – Various data object security profiles.](image2)
are prevented from using control operations (select/operate function codes), from controlling applications or device availability (start/stop device and application function codes), or from controlling measurement values (freeze function codes). The function code rules are summarized in Table 1 for various master types discussed in Section 3.3.

In Table 1, the primary master, e.g. the distribution system operator, will require all function codes. As a result, the function code coarse security selector cannot be used for the primary master, and therefore there are no function code restrictions for the primary master. The control secondary master has full control over specific aspects of the DNP3 device, e.g. a consumer turning off their main breaker. The control secondary master is prevented from accessing functionality that is useful for DoS attacks (e.g. time response measurements), and control operations (e.g. freeze commands). The limited control master is limited to only altering device parameters, and is therefore prevented from accessing physical properties of the device. The monitoring secondary master is prevented from exercising any control over the outstation. The monitoring secondary master therefore has limited capability to implement DoS attacks and is prevented from implementing any device control attack.

The function code security does not provide security against a master abusing a function code that they have authorization for, e.g. writing values to unauthorized points. Therefore the data object finer granularity security selector is required.

### 3.5 Data objects

Data objects define the properties and structure of the data that is accessed or operated on in conjunction with the function codes, such as binary or analog I/O (DNP3 Specification, 2007a,b, 2008b). The data objects therefore refine the attacks on DNP3 devices that were shown in Fig. 1, including surveillance, DoS, and directly controlling specific device operations. The data object security presented in this article uses the data objects as a fine granular security selector for compromised communication, compromised masters, or stakeholders attempting unauthorized access to a device.

To properly implement security access for a DNP3 data object, security rules must be created for each allowed combination of function code, group number, variation, and index per master. Defining security for only the point type without the application layer header group number for that point type would allow a compromised master to access unauthorized values or operations, e.g. a master would be able to access all of the analog inputs instead of allowing access to only analog input event values. Without security for the variation, compromised masters would be able to have unauthorized access to detailed information, e.g. device attributes or logs. Without security for the indexes, compromised masters would be able to access any data within a point type that they had access to.

Defining security rules for every allowed function code, group number, variation, and index creates an immense number of rules that need to be defined and processed by an outstation as illustrated in this article’s DSM example. The number of security rules that need to be defined to protect an outstation from the attacks in Fig. 1 can be greatly simplified with data sets. The data sets can contain any data required by a master, and allows both monitoring and control operations with only four group numbers (DNP3 Specification, 2007g). The data object security operations are therefore simplified to discarding any application layer fragment that does not contain the following groups: data set descriptor (group 86), static data sets (group 87), event data sets (group 88), and authentication (group 120). The data set prototype is not included to simplify the security operations.

An important facet of the DNP3 data sets is that their index values are unique only to a particular master–outstation connection (DNP3 Specification, 2007g). Therefore no security rules have to be implemented for the index values, further simplifying the security operations. Table 2 indicates the allowed function code and data object pairings for the security implementation. The term data set security is used for the remainder of the article to provide differentiation with conventional data object security. The data sets use attributes to indicate if the data set is readable, writable, or controllable, providing an inherent security check to the function code operations.

The allowed function code/data object pairing in Table 2 provides strong security against comprised secondary masters at the cost of reduced functionality, e.g. a secondary master is unable access the time response function codes. As a result, the primary master, i.e. the utility, requires access to nearly all function codes, object types, variations, and points to ensure proper control over the DNP3 device to counter-act the constraints on the secondary masters. This would create an immense number of security rules for the primary master, contrary to the article’s objective of reducing the number of required security rules. Therefore, the primary master security overhead for the outstation is shifted onto the primary master. This creates a permit-all basis for the primary master in the outstation, reducing the implementation overhead and thereby

<table>
<thead>
<tr>
<th>Master</th>
<th>Allowed function codes (FC)</th>
<th>Allowed range encoding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary</td>
<td>All</td>
<td>FC ≥ 0</td>
</tr>
<tr>
<td>Control secondary</td>
<td>Confirm to direct operate no response</td>
<td>0 ≤ FC ≤ 6</td>
</tr>
<tr>
<td></td>
<td>Authentication request and authentication error</td>
<td>32 ≤ FC ≤ 33</td>
</tr>
<tr>
<td></td>
<td>Response to authentication response</td>
<td>129 ≤ FC ≤ 131</td>
</tr>
<tr>
<td>Limited control secondary</td>
<td>Confirm to write Authentication request and authentication error</td>
<td>0 ≤ FC ≤ 2</td>
</tr>
<tr>
<td></td>
<td>Response to authentication response</td>
<td>32 ≤ FC ≤ 33</td>
</tr>
<tr>
<td></td>
<td>129 ≤ FC ≤ 131</td>
<td></td>
</tr>
<tr>
<td>Monitoring secondary</td>
<td>Confirm and read Authentication request and authentication error</td>
<td>0 ≤ FC ≤ 1</td>
</tr>
<tr>
<td></td>
<td>Response</td>
<td>32 ≤ FC ≤ 33</td>
</tr>
<tr>
<td></td>
<td>Authentication response</td>
<td>FC = 129</td>
</tr>
<tr>
<td></td>
<td>Authentication response</td>
<td>FC = 131</td>
</tr>
</tbody>
</table>
increasing utility efficiency. To compensate for the decreased security between the primary master and the outstation, the utility is responsible for implementing additional security measures to prevent unauthorized access to the SCADA devices, such as role based access control (RBAC) security. This security simplification eliminates the single data object per application layer fragment constraint in Section 3.2 for the primary masters, increasing utility efficiency.

### 3.6. Temporal constraints

The data set security prevents or limits various DoS attacks. However, it is difficult to prevent compromised masters from implementing DoS attacks using data that they are authorized to access, e.g. implementing an DoS attack shown in Fig. 1 for accessing or controlling the device at critical moments. These risks can be mitigated with the additional data set temporal security. Various power system data is typically only accessed at specific times or only at a maximum rate. For example, kWh measurement values are typically accessed at maximum every 15 min (Meter Data Management and Repository (MDM/R), 2006). The data set security can therefore limit data access to once every 15 min, limiting the effectiveness of the DoS attacks. Other point types are rarely accessed, e.g. disconnecting the home or generation from the grid in this article’s DSM example. The data set security can therefore either discard transmissions that exceed a maximum limit and/or warn the primary master of a possible attack on the DNP3 device.

The optional temporal security requires additional security rules that bind the data set indexes to the temporal constraints. The inclusion of the temporal security constraints increases the security operation complexity since each index in the application layer fragment must now be examined using the qualifier and range fields discussed in Section 2. Without the temporal constraints, the index values can be ignored by the data set security operations. Therefore, in this implementation, the temporal constraints can be bypassed during lower threat risks and used for elevated threats. This increases the security operation efficiency, as demonstrated in Section 5, since temporal constraints can perceptibly degrade performance.

The master requests are the greater security threat to the SCADA network operations rather than the outstation responses in regard to the data set security. Therefore, the temporal constraint processing is further simplified by examining only incoming application layer fragments to the outstation. The application layer fragments from the masters contain the list of requested data sets indexes only while the outstation response would include the filled data objects associated with the index. With the Section 3.2 one data object per application layer fragment rule, the security operations only need to read the list of requested indexes within the first transport function fragment. The qualifier field value used to request all data sets is supported by the data set security, but is not recommended. Any data set temporal constraint violation will cause the entire application layer fragment to be discarded.

### 4. Data set security protocol

Data sets provide an effective method for highly restricting access to DNP3 devices, either limiting or eliminating the threats shown in Fig. 1. However, compromised masters are capable of circumventing the data set security by creating data sets that contain data that they are not authorized to access. Therefore, the data set creation capabilities are disabled for secondary masters in this article. This reduces the quality of service for secondary masters since they are no longer able to create or re-arrange data sets to best suit their requirements. As a result of outstations not being capable of creating the data sets without device restarts (DNP3 Specification, 2007g), the primary master must create and administer the data sets for the secondary masters. The protocol in Fig. 3 is used to provide the necessary primary master support for secondary master data set creation.

In the protocol shown in Fig. 3, the secondary master will read its data sets from the outstation to determine which data it has access to and the available data set indexes. The secondary master will then create the new data set, containing data compiled from the currently defined data sets. The new data set is written to the outstation as application data, which is accessed by the primary master periodically polling the outstation. The secondary master is restricted to only one data set creation request at a time, reducing the potential for DoS attacks resulting from multiple data set creation requests. To determine when the primary master has responded to the data set creation request, the secondary master will periodically poll the outstation to read back the application data that was used for the creation request. If the data set had been processed by the primary master, the application data containing the data set will have been cleared. The secondary master will then read the data set descriptor for the desired data set. If the data set has been approved by the primary master, the outstation will respond with the data set. Otherwise, the outstation will respond with the normal parameter error indication if the data set does not exist and therefore had not been approved by the primary master.
5. Data set security operations

The data set security operations are shown in Fig. 4, with the security rules formalized in Section 5.1 and performance results for the security operations presented in Section 5.2. In Fig. 4, the data set security differentiates between the primary and secondary masters, as well as among secondary master types, to determine the applicability of the rules. The function code coarse granularity security selector and the data object fine granularity security selector are then applied to determine if the function code and the function code/data object combination is allowed. Finally any temporal constraints for the data are applied if defined. The data set security implementation includes additional security that is not shown in Fig. 4 or presented in the formalized rules. For example, the data set security will ensure that request function codes are not transmitted by an outstation or that the Confirm request function code, used for application layer error management, does not contain any data. These security checks provide redundancy for the application layer operations.

5.1. Formalized security rules

Rule 1: Data object usage is unrestricted between an outstation and the primary master, e.g. the utility control center, and the subsequent rules do not apply as shown in Fig. 4.

Rule 2: Application layer fragments received or transmitted by an outstation will contain only one data object.

Rule 3: The outstation shall not issue a response to data discarded by the security operations, i.e. the data is treated as corrupted data, decreasing DoS attack potential. The application layer header of a discarded data transmission is logged for the primary master.

Rule 4: The function codes shall implement the first stage coarse granularity security selector shown in Fig. 4. Only application layer fragments containing the secondary master functions codes in Table 1 will be accepted for the specific type of secondary master. All other application layer fragments will be discarded.

Rule 5: The data objects shall implement the second stage fine granularity security selector shown in Fig. 4. Only the specific function code, group number, and variation combinations in Table 2 for the master type will be accepted.

Rule 6: Temporal constraints will be implemented for selected data sets, shown in Fig. 4, if the temporal constraint selector is not bypassed.

Rule 7: The primary master determines the data sets for the secondary masters. Secondary masters must use the data set security protocol in Section 4 for further data set creations.

5.2. Data set security operation performance

Typically performance metrics are implemented on the most state-of-the-art device that can be accessed for the best possible results. However, utilities are more concerned with device reliability and potential ‘bugs’ within the device. This concern arises from the need to ensure critical infrastructure reliability and the long device life spans that may be in the range of 15–20 years. As a result, typical utility devices are much more primitive than the state-of-the-art technology. Therefore, the data set security performance and operation testing utilized non-state-of-the-art technology to provide results comparable to what a utility may use within the field. A 300 MHz Intel Celeron running Windows 98 was therefore utilized for the evaluation of the data set security source code. The performance results were to only ensure that an acceptable performance
margin existed for deployment to less than state-of-the-art technology. There was no data set protocol performance testing, since this is not a priority utility operation that can be executed at a convenient time for the utility.

The code implementation tested was based on an application layer security profile, which differed from a connection management layer profile by the number of offset bytes to read the function code and data object. For the data set security to recognize the primary master data and bypass the security operations averaged 0.2 ns. The data set security is therefore unlikely to adversely affect the utility’s SCADA network performance and system operations.

For the data set security to complete the previous security operation and to recognize that the data was from an unauthorized master averaged 7.7 ns. For the data set security to recognize that the data is from an authorized master but a master using an unauthorized function code averaged 7.7 ns as well. Therefore the determination of an authorized master does not impact the data set security operation performance. The previous security operations and the data object fine granular security selector to determine that an unauthorized combination was received averaged 8.8 ns. Therefore, depending on the timing requirements, the function code coarse granular security selector may not be required for the data set security since checking the full combination did not add significant delays.

The previous security operations and bypassing the temporal security for authorized data averaged 1.0 ns. The data set security therefore does not adversely affect the performance of normal authorized stakeholder communication with an outstation. For the security to determine if an authorized qualifier field value was used for the temporal constraints, and including the previous security operations, averaged 8.3 ns. To complete the security operations with a failed temporal constraint check averaged 326.3 ns and 282.9 ns for a passed temporal constraint. The temporal constraints therefore may create performance issues for slower architectures or for a carefully orchestrated DoS attack, where the attacker accesses all of the indexes consecutively to delay critical outstation responses (causing the temporal constraint security operation time to accumulate). However, with the data set temporal constraints, attackers have much fewer opportunities in which to carry out an effective DoS attack, e.g. an opportunity once every 15 min to carry out an attack.

### 6. Security example for advance demand side management

This section provides an example for the proposed data set security. The example utilizes consumer based demand side management (DSM), which is the primary application area for the proposed security. However, the data set security is applicable to any application area where the utility is required to severely limit independent device access, e.g. limiting manufacturer remote access to substation equipment.

#### 6.1. Demand side management configuration

A smart distribution system is used to illustrate the effectiveness of the data set security for preventing or limiting the attacks as shown in Fig. 1 as well as limiting the number of required security rules. In the example shown in Fig. 5, data is accessed from a DNP3 SCADA device within a consumer’s home that operates smart metering functions, controls renewable power generation functions (e.g. solar power), and controls local or community power storage functions (e.g. fuel cells) (Nourai and Schafer, 2009). Multiple stakeholders, including the distribution system operator (utility), electricity retailer, consumer, device manufacturer, and the government access the SCADA device. The distribution system operator accesses the device via the SCADA network. The consumer is able to access the DNP3 device locally or through the Internet. The electricity retailer, manufacturer, and government access the DNP3 device via the Internet. The consumer, electricity retailer, manufacturer, and government can alternatively access the data from the SCADA device through the distribution system operator’s data historian via the Internet (shown as direct connections in Fig. 5). The distribution system operator is the primary master while all other stakeholders are secondary masters. The consumer and electricity retailer are secondary control masters, the device manufacturer is a limited secondary control master, and the government is a monitoring secondary master. Other security measures, such as firewalls, are neglected.

All secondary master access to the data historian is read-only, avoiding control command congestion within the SCADA network that may be employed to create DoS attacks against the utility. The data historian provides additional security for the power system since remote access to the DSM device can
be disabled by the primary master during elevated threats, protecting the device from all compromised masters.

6.2. Data point types and indexes

The cyber security example is simplified by considering only a few point types and data points and is derived from the author’s example in Mander et al. (2007) using similar data points.

6.2.1. Binary output point type

Index 0 is a grid disconnect, disconnecting the residence from the system and is controlled by the distribution system operator only, but is accessible by the consumer and electricity retailer. Index 1 and 2 are grid disconnects for the generation and storage respectively, and is controlled by the distribution system operator only, but is accessible by the consumer. Index 3 and 4 are local disconnects for the generation and storage respectively, and is controlled by the consumer but is accessible by the distribution system operator. Indexes 0–4 are accessible by the government. Indexes 0–4 are local disconnects for the generation and storage respectively, and is controlled by the distribution system operator. Indexes 5–7 are used to initiate device diagnostics for troubleshooting and maintenance. Index 5 (smart meter) is accessed by the distribution system operator and manufacturer only. Indexes 6 and 7 (generation and storage) are accessible by the distribution system operator, consumer, and manufacturer.

6.2.2. Counter point type

Index 0 provides the kWh consumption for the current price rate. Index 1 provides the total kWh consumption for the day. Index 2 provides the total kWh consumption for the previous day, and Index 3 provides the kWh consumption from the last billing date. These indexes provide the revenue parameters to the stakeholders, and are therefore accessed by all stakeholders except the manufacturer. Index 4 provides the kWh generation for the current price rate. Index 5 provides the total kWh generated for the day. Index 6 provides the total kWh generated for the previous day, and Index 7 provides the kWh generated from the last invoicing date. Indexes 4–7 are accessible by the distribution system operator, consumer, and government. Indexes 4–7 are the combined generation from the renewable generation and storage devices.

6.2.3. Analog input point type

Index 0 monitors the consumer’s real-time power consumption from the distribution system, and is accessible by the distribution system operator, electricity retailer, and consumer. Index 1 monitors the total real-time power generated by the residential consumer into the distribution system, and is accessible by the distribution system operator and consumer. Index 2 monitors the total power generation of the renewable generation, and is accessible by the distribution system operator, consumer, and manufacturer. Index 3 monitors the current power generation capacity of the storage, and is accessible by all stakeholders except the electricity retailer. Index 4 monitors the current power generation capacity of the storage, and is accessible by all stakeholders except the electricity retailer. Index 5 indicates to the consumer when the electricity storage has reached its minimal set point at which it has sufficient stored electricity to be made available to the distribution system, and is accessible by the distribution system operator, consumer, and government.
6.2.4. Analog output type

Index 0 controls the set point at which the storage ceases to generate electricity into the distribution system and begins to store electricity, and is accessible by the distribution system operator and consumer. Index 1 is used to control the minimum set point for the electricity storage at which it has sufficient stored electricity to be made available to the distribution system, and is accessible by the distribution system operator and consumer. This point ensures that the electricity storage cannot be fully discharged by index 0 during emergencies. Index 2 indicates the electricity purchasing rate from the distribution system operator, and is accessible by all stakeholders except for the manufacturer. Index 3 indicates the current rate for the consumer to sell electricity at, and is accessible by the distribution system operator, consumer, and government. Index 4 indicates the current contractual rate for the consumer to purchase electricity from the retailer, and is accessible by all stakeholders except the manufacturer.

6.3. Data set security rule reduction comparison

The data set security is compared to simply using a security rule for each allowed function code, group number, variation, and index combination (called conventional data object security in this article). This section clearly illustrates the advantage of data set security since the rules are independent of which data is accessed or even the number of data sets contained within a DNP3 device (except for temporal constraints). The data set security rule quantity is consistent and can be applied to any device without modification since the rules are not dependent on the actual accessed data. In comparison, the conventional data object security is device dependent, with the rules directly bound to particular data points. As a result, as device access increases, so do the number of required rules.

Table 3 summarizes the differences between the number of security rules needed for data set security and conventional data object security for the function codes defined in Table 1, and for the point types and indexes defined in Section 6.2. In both cases there has been no security rule optimization. Regardless of optimization, the data set security is consistent in the number of required security rules (except for any additional temporal constraints), which will be fewer than the conventional data object security.

Table 3 is a trivial example for the distribution system operator since the outstation data set security has shifted the security overhead onto the primary master. A similar option is possible for the conventional data object security, creating an equivalent number of security rules for both the data set and conventional data object security implementations.

With the conventional data object security, security rules are required for each combination of function code, group number, variation, and index. As shown in Table 3, this can lead to a significant number of security rules. Creating and maintaining these security rules, or applying optimization techniques to reduce the number of rules, may cause incorrect security coverage, i.e. unintended authorized data access. With the data set security, all authorized data is separate and independent of any other data point. A compromised consumer’s access is therefore unable to circumvent security rules to access similar but unauthorized data within the same point type, e.g. it is more difficult to create unintended access to the binary output indexes used exclusively by the distribution system operator. The security rules for the secondary master access to the historian are much less than the direct access to the DNP3 device since all control function codes have been disabled.

6.4. Data set security operation analysis

The data set security analysis for the DSM example is discussed in this section with respect to the security threats shown in Fig. 1. The previous section presented data set security rule reduction in comparison to the conventional data object security. This section discusses the effectiveness of the data set security in reducing unauthorized device access.

6.4.1. Distribution system operator

The data set security does not prevent a compromised primary master from accessing data and functionality that should be accessible by the consumer only, e.g. the utility controlling the storage device. However, given that a compromised primary master can implement more effective attacks on the power system, e.g. by directly disconnecting the residential home from the grid, accessing consumer only functionality would not be a priority target. Therefore, trading-off lower security for higher efficiency with the data set security is an acceptable risk. Regardless of the type of data security utilized, it is difficult to prevent or limit attacks from a compromised primary master since it has a high degree of control over a device’s operations.

6.4.2. Consumer

The consumer is classified as a control secondary master. The consumer is therefore capable of controlling specific aspects of the DNP3 device, including the renewable generation and storage operations. The consumer data set security increases the outstation’s security against compromised consumer remote and local connections or consumers attempting to defraud the utility.

The consumer is prevented from using specific function codes, such as the application control and file transfer function codes. As a result, the consumer or compromised consumer connection is prevented from executing application control attacks shown in Fig. 1 attack tree. Function codes that

<table>
<thead>
<tr>
<th>Stakeholder</th>
<th>Data set (historian)</th>
<th>Data set (historian)</th>
<th>Data set (historian)</th>
<th>Data set (historian)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distribution system operator</td>
<td>0</td>
<td>667</td>
<td>–</td>
<td>–</td>
</tr>
<tr>
<td>Consumer</td>
<td>26</td>
<td>593</td>
<td>21</td>
<td>534</td>
</tr>
<tr>
<td>Electricity retailer</td>
<td>26</td>
<td>165</td>
<td>21</td>
<td>149</td>
</tr>
<tr>
<td>Manufacturer</td>
<td>26</td>
<td>113</td>
<td>21</td>
<td>105</td>
</tr>
<tr>
<td>Government</td>
<td>18</td>
<td>153</td>
<td>18</td>
<td>153</td>
</tr>
</tbody>
</table>
are not supported by the data set security, and which may typically be required for a secondary master, are either handled by the primary master or substituted through the data sets. For example, the assign class and enable/disable unsolicited function codes can be handled by the primary master for the secondary master, thereby limiting potential DoS and control attacks on the device. The consumer is able to utilize the timestamps within the data sets to provide equivalent capabilities as the function codes used to gather network response statistics.

The data set security effectiveness in comparison to the conventional data object security is more apparent at the data object level. At the data object level, the data set security prevents the consumer from directly accessing the points. This prevents the consumer from unauthorized access of specific points and variations within the same point type (group) that can be used for extensive surveillance and DoS attacks. This security is more apparent for the other stakeholders than the consumer in this DSM example.

Within the binary output point type, the consumer is prevented from overriding the utility’s grid disconnect operations, which may affect system stability, power equipment (overloading), and human safety (maintenance personal). Additionally, the consumer is prevented from accessing the smart metering maintenance operations, where a consumer could create utility reliability issues. The consumer is still capable of accessing a significant amount of data within the device that can be used for surveillance and DoS activities. The most significant potential DoS attack is to rapidly cycle on and off the equipment disconnects, damaging equipment. Typical binary output point type access can be expected to be infrequent. Therefore temporal constraints can be employed to reduce the risk of the DoS attacks. Repeated device access to damage the device, and deny or delay device access, can be eliminated by limiting access frequency, e.g. once every 15 min. Although the access/control device operations at critical moments DoS attack is still possible, the threat is reduced since attack opportunities are more limited. Additionally, the consumer can employ a local physical lock-out switch to prevent remote access and reduce the security threat further.

Within the counter point type, the consumer is restricted to read operations only, and is therefore prevented from price tampering by altering the reported consumption and generation readings. The consumer is incapable of exercising any of the device control attacks in Fig. 1 for the counter point type. The consumer read access to the counter values remains unabated, and therefore has full device surveillance and DoS capabilities. The DoS attacks can be limited with the temporal constraints used for the binary output or counter point types. The set points parameter attack threats are lessened but not eliminated due to the control over the set points. The consumer read access to the analog output values remains unabated, and therefore has full device surveillance and DoS attack capabilities. The more significant DoS attack is to rapidly alter the set points in order to damage equipment. Access to the analog output point type can be expected to be infrequent, and can therefore use the same temporal constraints as the counter point type. The set points can be further constrained by local physical lock-outs.

6.4.3. Electricity retailer

The electricity retailer is classified as a control secondary master. The electricity retailer is therefore capable of controlling a very limited aspect of the DNP3 device, dealing with electricity price rate charged to the consumer. Security is critical for the electricity retailer since control threats are possible. The data set security can be used to ensure that only one data set can be used for the select/operate function codes, thereby reducing the data access security risks. The electricity retailer security for the function codes is the equivalent to the consumer. The data set security increases the outstation’s security against compromised retailer remote connections or retailers attempting to defraud the utility or consumers.

Within the binary output point type, the electricity retailer is unable to control any operations. As a result, the electricity retailer is unable to affect distribution system operations or human safety. The electricity retailer can only read one point, and therefore has very limited capability to implement surveillance and DoS attacks. Retailer competition reduces a retailer’s attack capabilities since there will be fewer data sources on which to determine surveillance patterns for DoS attacks. The DoS attacks can be handled for the electricity retailer in the same manner as for the consumer’s counter point type.

Within the counter point type, the electricity retailer is restricted to read operations only, and is therefore prevented from price tampering. The electricity retailer is incapable of exercising any of the device control attacks in Fig. 1 for the counter point type. The electricity retailer is limited in the amount data that it can access, and therefore has limited surveillance capability on the DSM operations within the residence, e.g. breach of consumer privacy. The DoS attacks can be handled for the electricity retailer in the same manner as for the consumer’s counter point type.

Within the analog input point type, the electricity retailer is restricted to read operations only except for the deadband values. The deadband values provide alert triggers to the consumer. As a result, any control device operation parameter attacks in Fig. 1 will affect the consumer only in this DSM example. This type of attack can be handled with a lock-out for remote deadband access. As with the other point types, the consumer read access is unrestricted and therefore the surveillance remains unabated for this point type. The DoS attack threat resulting from device reads can be reduced with the temporal constraints used for the binary output or counter point types.

Within the analog output point type, the consumer is prevented from overriding the utility’s and electricity retailer’s price rates, which would allow the consumer to misreport their billing/invoicing information. The control device operation parameter attack threats are lessened but not eliminated due to the control over the set points. The consumer read access to the analog output values remains unabated, and therefore has full device surveillance and DoS attack capabilities. The more significant DoS attack is to rapidly alter the set points in order to damage equipment. Access to the analog output point type can be expected to be infrequent, and can therefore use the same temporal constraints as the counter point type. The set points can be further constrained by local physical lock-outs.
The analog input point type is the only point type that the electricity retailer has some control over. Within this point type, the electricity retailer is prevented from overriding the utility’s price rates, which would allow the retailer to influence the consumer by misreporting the utility’s prices. However, competitors compromising electricity retailer connections can unduly influence consumers by misreporting the retailer’s price rates. However, this attack effectiveness will be limited since the price rate is informational only and is not used for the actual billing. The device surveillance and DoS attack threat is very limited. The DoS attacks and the overriding of the retailer’s prices can be further limited with the same temporal security constraints as the counter point type.

6.4.4. Manufacturer
The manufacturer is classified as a limited control secondary master. As a result, the manufacturer is much more constrained than the control secondary masters. The manufacturer cannot access the physical operations of the device via the select/operate group function codes. The data set security ensures that the manufacturer cannot control the grid connections or the generation capabilities, including the electricity storage. The manufacturer is limited to simple control operations that have much less threat potential. The manufacturer’s capability to create new data set requests can be disabled by the primary master for enhanced security. The data set security increases the outstation’s security against compromised manufacturer remote connections.

Within the binary output point type, the manufacturer is unable to control any operations except the device maintenance initiation. As a result the manufacturer is limited in its capability to disrupt distribution system operations or endanger personal safety. The manufacturer is only capable of reading one point. As a result, the manufacturer’s capability to implement surveillance and DoS attacks is very limited and can be further limited with temporal constraints, e.g. limiting access to once a day.

The manufacturer has no access to the counter or analog output point types. As a result, the manufacturer is unable to implement any attack shown in Fig. 1 for these point types except for the communication surveillance. The manufacturer connection is therefore unable to influence any of the power consumption/generation readings or pricing information that can be used to defraud a stakeholder or create conflict among stakeholders.

Within the analog input point type, the manufacturer connection is restricted in the same manner as the binary output point type. There is no control capability for affecting the power consumption/generation readings to create fraudulent values. The manufacturer is only able to access real-time power consumption and generation readings. Therefore, the manufacturer has limited surveillance and DoS capabilities that can be further limited using the same temporal security constraints as the binary output.

6.4.5. Government
The government is classified as a monitoring secondary master. As a result, the government has no control over any of the DSM device operations, eliminating the device control attack threats shown in Fig. 1 for all of the point types. The government connection is unable to control the connections/disconnections of the device equipment, affect the consumption/generation data or pricing rates. However, the government connection is vulnerable to the surveillance and DoS attacks since most of the points in the DSM example are accessible by the government. The DoS attack potential can be lessened by using the same temporal security constraints used for the consumer. Disabling unsolicited responses for the government decreases the capability to create DoS attacks or to implement responsive device surveillance threats, e.g. quickly responding to device difficulty notifications received from unsolicited responses.

7. Discussion
The data set security presented in this article reduces the number of security rules that need to be implemented within an outstation, thereby reducing the processing overhead for outstations that contain minimal processing capabilities. The number of security rules remains constant regardless of the amount of data accessed from an outstation by a secondary master, except for data sets implementing temporal constraints. The data set security was developed to limit the effectiveness of insider or compromised master attacks that can exercise unconstrained device operation control shown in Fig. 1. The data set security severely limits secondary master interactions with the outstation by restricting access to only specific data points rather than with the more complex association for each data point using a group number, variation, and index. As a result, a compromised master is, at worst, only able to affect the data that it is authorized to access. A compromised secondary master threat is further mitigated by temporal constraints, which implement constraints on when or how frequently a secondary master is able to access specific functionality, such as reading the kWh counters in the DSM example.

The data set security was designed to be layer independent to support the profiles shown in Fig. 2. Depending on the profile, the data set security can be enhanced to provide more extensive security. Within the application layer, the data security can handle multiple data objects within a single application layer fragment. This provides support for the DNP3 authentication security aggressive mode, and increases efficiency for transmitting several objects at the same time. Alternatively, the data set security within the connection management layer can provide security coverage for the data-link layer and transport function. For example, the data security can provide security for the data-link function codes, providing security against DoS attacks using the request link status function code (DNP3 Specification, 2007f).

Although the data set security provides strong security against compromised secondary masters, it does not provide security against a compromised primary master. In addition, the preeminence of the distribution system operator over all other stakeholders, including the consumer, is assumed in this article. In situations where greater security or privacy is required against compromised primary masters, or where the consumer has preeminence, more complex security...
implementations are required. A hybrid data set security implementation may be used in this situation, with the primary master using more conventional data object security. This hybrid would retain its simplicity for the secondary masters while increasing security against a compromised primary master. To reduce the number of implemented security rules, a permit-all with exception basis instead of a deny-all basis can be used. However, the hybrid system may create further complications for the data security, e.g. the utility would be blocked from accessing consumer only data but the utility’s data historian would have full device access. Alternatively, RBAC based security created by the authors can be implemented (Mander et al., 2009). The RBAC security is more flexible, handling a wider range of security requirements, but at the cost of increased complexity and overhead. This complexity and overhead may not be suitable for devices with limited processing capability or devices being retrofitted for security.

The cyber security proposed in this article implemented a security solution for DNP3 devices, instead of simply providing a security threat assessment without a specific security solution (Cleveland, 2007; CIP-005, 2006; Ten et al., 2007). The proposed security provided a security capability beyond simply using commercial authentication and encryption security. In addition, security is provided against compromised masters within the SCADA network or ‘electronic perimeter’ that are not dealt within other security specifications, e.g. behind the firewall (SP800-82 Final Public Draft, 2008). The proposed security was designed specifically for independent access to utility devices that has only begun to be recognized by the utilities.

8. Conclusion

Authentication, encryption, and firewalls do not provide sufficient security for large SCADA networks with multiple stakeholders. Security focus has been on the interface to the SCADA networks, e.g. firewalls, and do not provide as much security within the SCADA network. The majority of the stakeholders will access the SCADA devices directly, e.g. through the Internet or locally with the consumer, rather than indirectly through a data historian. The number of SCADA devices, which may be potentially millions of devices, will be difficult to protect with only authentication, encryption, and firewalls. Many of the devices will be accessible by numerous parties, and are therefore likely to be compromised, e.g. a consumer compromising smart metering functions in the DSM example to defraud the utility. The SCADA security must be focused on providing security for each device, rather than for the SCADA network as a single entity, through security such as the proposed data set security in this article.

The data set security in this article is developed for DNP3 outstations. The security provides access control to a device’s operations and data using the application layer function codes and data objects. The security rules define the authorization for which data is allowed to be received or transmitted by the outstation to the secondary masters. The data sets simplify the security implementation, minimizing the security overhead for the outstation, which may be critical in retrofitting outstations with security or for outstations with minimal processing capability. The data security also shifts the primary master security from the outstation to the primary master, further decreasing the security overhead. This requires aggressive security within the primary master, such as with RBAC, to protect the outstations from unauthorized access from the primary master. The security shift from the outstation to the primary master decreases the data rights of other stakeholders, primarily the consumer. More complex and aggressive security may therefore by required to decrease vulnerabilities from primary masters and to ensure increased data rights for the consumer, e.g. hybrid data set security.

The cyber security proposed in this paper provides critical access control security against compromised devices, similar to some firewall operations. The cyber security does not replace data transmission security such as encryption and authentication, but augments it. Firewalls, authentication, and encryption are additionally required for robust SCADA network security solutions.

References


Cleveland F. Enhancing the reliability and security of the information infrastructure used to manage the power system. IEEE Power Engineering Society (PES) General Meeting (Tampa, Florida); June 24–28, 2007.


NISCC good practice guide on firewall deployment for SCADA and process control networks. National Infrastructure Security Coordination Centre (NISCC); February 2005.


RFC 4301: security architecture for the Internet. Internet Engineering Task Force (IETF); December 2005.

RFC 5246: The transport layer security (TLS) protocol version 1.2. Internet Engineering Task Force (IETF); August 2008.


SP800-82 final public draft: guide to industrial control systems (ICS) security. National Institute of Standards and Technology (NIST); September 2008.


Todd Mander received his doctorate from the University of Teesside in a joint program with Ryerson University on power system advance computer communication and protocol research. His current post-doctorate research interests at Ryerson University include power system infrastructure development including smart grids, security, resource management optimization, and distribution system collaborative computing.

Richard Cheung is Professor in electrical engineering at Ryerson University. His research interests include electric machine drives, generation excitation system, nuclear power generation design aspects, power electronics, and power system protection, control and monitoring. He is president of RCPC Inc. and is currently under contract to Siemens for Bruce Power Restart Projects.

Farhad Nabhani is Professor in Biomechanics and Manufacturing at the University of Teesside. His research interests include biomechanics, manufacturing systems and design process, ERP implementations, six sigma, benchmarking, materials process technology lean manufacturing. Professor Nabhani work has resulted in publication in many international journals and he is currently the course leader for several Master courses at the Teesside University.