Security Aspects Of Communications To Substations

Mark Adamiak
GE Multilin
King of Prussia, PA

Herb Falk
SISCO
Sterling Heights, MI

Security Aspects of Communications to Substations

Mark Adamiak
GE Multilin
King of Prussia, PA

Herb Falk
SISCO
Sterling Heights, MI

Abstract

The security of data and information transmitted either point to point or through network access that utilizes an Internet or intranet infrastructure has recently become a major concern to all. The data communication industry, however, has been cognizant of the issues and has been quite active in determining the various "attack" modes and creating mechanisms to address potential weaknesses. In particular, the Internet has driven such innovations such as Secure Socket Layer (SSL), Internet Protocol Security (IPSec), and Virtual Private Network (VPN).

SSL encryption and authentication can be used between a remote site and the user's browser to ensure that the data is secure. SSL is used by the online banking industry to insure secure transfer of data & information. A hard token with a rolling password provides an extra measure of security for critical applications with control.

The VPN security appliance encrypts the data to create a "virtual tunnel" between the substation equipment and a specific company's PC. This technology is very useful for protecting serial data streams. Firewalls can be used to prevent external access to the data source.

This paper reviews the general issues of secure communications (including recently released NERC guidelines) and addresses the solutions to providing secure substation network connections on the Internet or an intranet. It will also review existing work in progress that deals with utility-to-utility and utility-to-substation communication security.

Introduction

The rapid migration of the digital society into the utility enterprise has resulted in the establishment of communication interfaces with most utility protection, control, and monitoring devices. This rapid and pervasive penetration of communications has raised many concerns as to the security and integrity of the data being communicated and the consequences of inadvertent access. The tools and general knowledge to potentially "attack" utility systems are readily available. The utility industry, to date, has been mostly immune from cyber attacks as most communications occur on private networks and through the "security through obscurity" principle, however, most utility security departments are demanding more security.

Over the past several years, several surveys and studies have been conducted in order to determine the communication and informational security concerns of the global utility industry. The results are primarily based on information provided by utilities located

within the United States or from the United States Department of Energy. The Electric Power Research Institute (EPRI) has commissioned several such studies, and the major concerns prior to 911 are quite similar to the concerns for post 911. The top ten security concerns are:

1. Bypassing Controls
System flaws or security weaknesses that are intentionally attacked.

2. Integrity Violation
Information is created or modified by an unauthorized entity.

3. Authorization Violation
An entity authorized to use a system for one purpose that uses it for another unauthorized purpose.

4. Indiscretion
An authorized person discloses restricted information to a non-authorized entity.

5. Intercept/Alter
A communication packet is intercepted, modified, and then forwarded as if the modified packet were the original. This is a typical man-in-the-middle scenario.

6. Illegitimate Use
An action, control, or information retrieval is performed by an individual authorized for one action, but an action is completed for which the individual is not authorized.

7. Information Leakage
An unauthorized entity acquires restricted information. Typically this term is for non-eavesdropping acquisition of the information (e.g., through other means of disclosure).

8. Spoof/Masquerade
An attack against a communication dialog in which the attacker attempts to assume the identity of one of the communicating partners.

9. Denial of service (Availability)
Action(s) that prevent any part of an information system from functioning in accordance with its intended purpose. Usually flooding a system with messages to prevent it from servicing normal and legitimate requests. A PING attack, where the server is bombarded with requests for a simple echo command, can result in a denial of service.

10. Eavesdropping
An attack against the security of a communication in which the attacker attempts to "overhear" the communication – similar to wire tapping.

As with any type of attack, typically, a defense can be found to defeat the attack. Table 1 summarizes the security concerns discussed above and lists the defenses that are typically implemented to mitigate these concerns.

Concern Ranking	Concerns	
	Threat	Possible Counter-Measures
1	Bypassing Controls	Utility Policies, Strong Peer Authentication
2	Integrity Violation	Encryption, Message Authentication
3	Authorization Violation	Strong Peer Authentication, Privilege Levels
4	Indiscretion	Utility Policies
5	Intercept/Alter	Encryption, Message Authentication
6	Illegitimate Use	Utility Policies, Privilege Levels
7	Information Leakage	Encryption
8	Spoof/Masquerade	Strong Peer Authentication, Message Authentication
9	Availability (e.g. Denial of Service)	Appropriate Resource Management and fixing buffer issues.
10	Eavesdropping (e.g. Data Confidentiality)	Encryption

Table 1: Top ten utility communication and informational security concerns

Some details of these defenses are offered here:

Encryption

Encryption is the process of applying a "cipher" algorithm to input information, typically called "plaintext", that results in encrypted output data, typically called "ciphertext". The cipher algorithm scrambles the data based on a secret "key" that is exchanged between the communicating parties. There are numerous cipher implementations, however, the more common implementations are the Data Encryption Standard (DES), Triple DES or 3DES, and the Advanced Encryption Standard (AES). 3DES is quite well known due to its use in the Secure Sockets Layer protocol (see SSL description below). Basic DES uses a 56-bit key to encrypt the data. The basic encryption process is shown in Figure 1. The encryption process takes 8 bytes (64 bits) of data and splits it into two 32-bit pieces referred to al L_0 and R_0. The input 56-bit key is then broken into sixteen 48-bit keys.

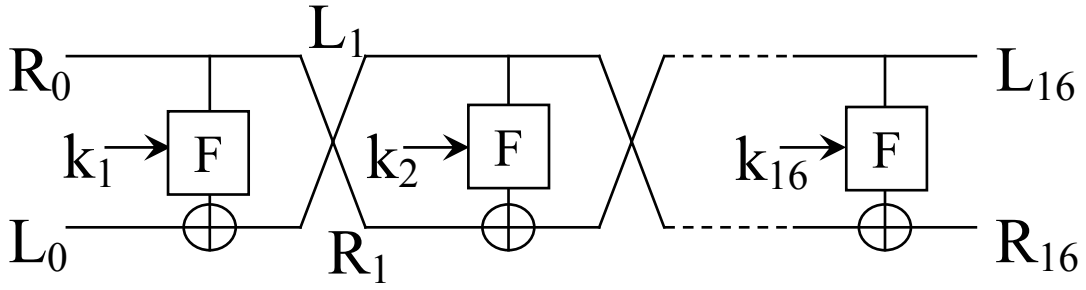


Figure 1
Data Encryption Standard (DES) Implementation

The data (R0 and L0) and key 1 is fed into the input of the cipher. The R0 data is fed into the function **F** and is operated on by key k1. The output of **F** is exclusive ored with the L0 data. The out of this operation becomes L1 and R0 becomes R1. This process is then repeated 16 times – once with each of the 48-bit keys that had been created. The result of this process is the encrypted data. Note that in 3DES, this process is repeated three times with three different keys. Since available computer power makes a 56 key somewhat decipherable (it actually has been cracked), the usual implementation is a triple implementation of encryption known as 3DES which, to date, has not been cracked. In this implementation, the key is 168 bits long and the above process is repeated three times with the three different 56 bit keys.

Secret Keys

Similar to physical security, cyber security is implemented by placing a digital "lock" on the secured information. To open the lock, one must have the appropriate "key". The security key system is based on a series of linked public/private key pairs. In one type of encryption algorithm, data that has been encrypted with one's public key can only be decrypted with the paired private key and visa-versa. There are a number of algorithms for sharing public keys (you never share your private key) and for creating new shared secret keys. 3DES requires that each party know the same "secret" so the key exchange algorithm goes about securely creating a shared secret. Just to make things more difficult for attackers, new keys are typically re-negotiated every 1 to 3 minutes.

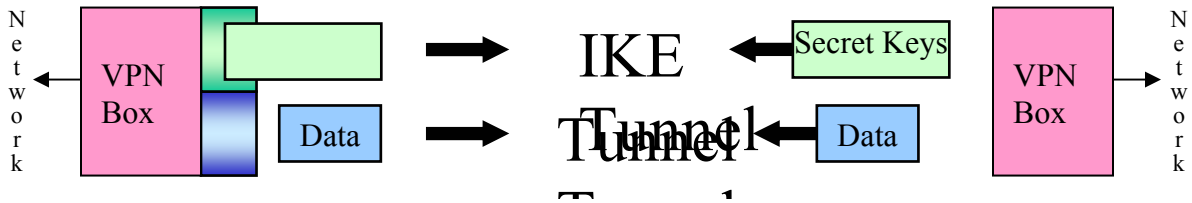
Authentication

Authentication is the security process that validates the identity of a communicating party. In the simplest implementation, this takes the form of a static password. Passwords can be easily compromised through indiscretion as discussed above and typically do not address "who" is entering the password. A variant of the static password is the rolling password as provided on a hard token. The hard token has a programmed sequence where the password changes every 1-minute. Many business enterprises use this technology for remote access to corporate networks.

Another variant of authentication is known as "**strong authentication**". In this implementation, authentication is provided by a "digital signature" which is an encrypted value provided by the entity requesting authentication that can only be decoded by the "public" key of the signature's owner.

Non-repudiation
A security service that prevents a party from falsely denying that it was the source of data that is did indeed create.

Security Implementations
The above tools are typically integrated together at create a "total" security solution. The first of these solutions is known as a "Virtual Private Network" or VPN. VPN creates a secure "tunnel" between two networks (Figure 2). The tunnel is established through the use of the Internet Key Exchange to establish secret keys between the ends of the communication tunnel. Once the keys are established, data is encrypted at one end of the tunnel, sent through the tunnel in the network, decrypted at the receiving end of the tunnel and sent into the remote end network. For added security, keys between the ends are periodically re-negotiated (for example, every 3 minutes) to add greater security to the connection.



A second implementation that incorporates the above tools is known as Secure Sockets Layer (SSL 3.0)/ Transport Layer Security (TLS). These implementations are similar to VPN technologies in that the both use a key exchange and similar encryption technology to VPN. The primary difference is that SSL/TLS are implemented at the transport layer of the communication profile (figure 3).

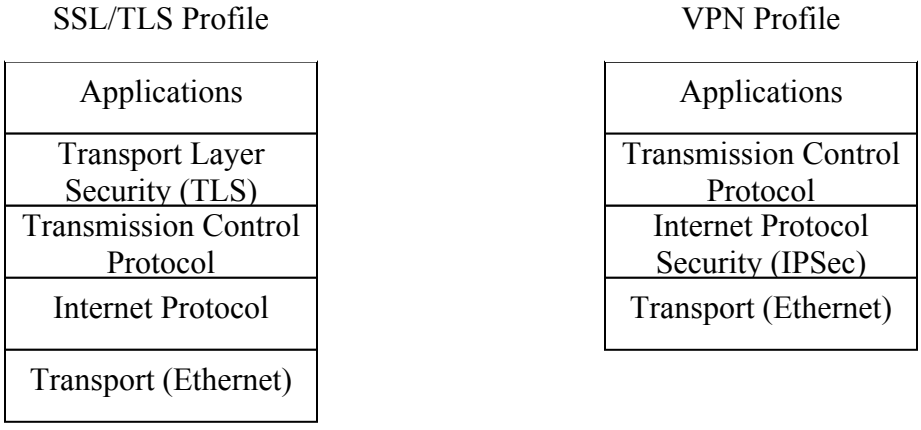


Figure 3
TLS and VPN Communication Profile Comparison

A third technology often employed for security is the firewall. As the name implies, a firewall is a go/no-go portal through with all data must pass in order to enter or exit a network. There are three basic techniques used to filter data through a firewall, namely, packer filtering, application gateway, and a stateful inspection.

A packet filter is the simplest form of firewall. A packet filter firewall will compare any IP packet that attempts to traverse the firewall against its Access Control List (ACL). If the packet is allowed, it is sent through. If not, the packet filter can either silently drop the packet (DENY) or send back an error response indicating "REJECT". Packet filters only look at five things: the source and destination IP addresses, the source and destination ports, and the protocol (UDP, TCP, and so on). These tests are very fast because each packet contains all the data (in the packet headers) necessary to make its determination. Due to its simplicity and speed, a packet filter can be enabled on your routers, eliminating the need for a dedicated firewall.

One problem with packet filters is that they generally do not look deeply enough into the packet to have any idea what is actually being sent in the packet. Though you might have configured a packet filter to allow inbound access to port 25, the Simple Mail Transfer Protocol (SMTP) port, a packet filter would never know if some other protocol was used on that port. For example, a user on one system might run his Secure Shell (SSH – another secure communication protocol) application on that port, knowing that the traffic would be allowed by the packet filter, and would be able to communicate through the firewall against policy.

A second and more thorough filter is an application gateway. An application gateway goes one step beyond a packet filter. Instead of simply checking the IP parameters, it actually looks at the application layer data. Individual application gateways are often called *proxies*, such as an SMTP (Simple Mail Transport Protocol) proxy that understands the SMTP protocol. These proxies inspect the data that is being sent and verify that the specified protocol is being used correctly. Given the creation of an SMTP application gateway, the proxy would need to keep track of the state of the connection: Has the client sent a HELO/ELHO request? Has it sent a MAIL FROM before attempting to send a DATA request? As long as the protocol is obeyed, the proxy will shuttle the commands from the client to the server.

Since application gateway must understand the protocol and process both sides of the conversation, it is a much more CPU-intensive process than a simple packet filter. However, this also lends itself to a greater element of security. You will not be able to run the previously described SSH-over-port-25 trick when an application gateway is in the way because it will realize that SMTP is not in use. Additionally, because an application gateway understands the protocols in use, it is able to support tricky protocols such as FTP that create random data channels for each file transfer. As it reads the FTP command channel, it will see (and rewrite, if necessary) the data channel declaration and allow the specified port to traverse the firewall only until the data transfer is complete.

Often there is a protocol that is not directly understood by your application gateway but that must be allowed to traverse the firewall. SSH (Secure Shell) and HTTPS (Hyper Text Transfer Protocol Secure) are two simple examples. Because they are encrypted end to end, an application gateway cannot read the traffic actually being sent. In these cases, there is usually a way to configure your firewall to allow the appropriate packets to be sent without interference by the firewall. This configuration is often called a *plug*.

The third filter technique often employed in firewalls is called stateful inspection. Stateful inspection firewalls are a middle ground between application gateways and packet filters. Rather than truly reading the whole dialog between client and server, a stateful inspection firewall will read only the amount necessary to determine how it should behave.

Industry Efforts

The International Electotechnical Commission (IEC) Technical Committee (TC) 57 Working Group (WG) 15 (e.g. IEC TC57 WG15) was formed to address security concerns for communication protocols for which IEC TC57 was the standards forming and maintenance body. The EPRI report was submitted to WG15 as base research for use in the evaluation, in additional to the NIST Common Criteria (ISO/IEC 15408), of the security issues regarding the Inter Control Center Protocol ICCP/IEC 60870-6-TASE.2, IEC 60870-5 (and its sibling DNP), UCA/IEC 61850, and DMS/IEC 61134, and others.

WG15 was tasked with analyzing the threats, potential risks, and to recommend security work item proposals, as required, to secure the TC57 protocols. Additionally, WG15 represents the core competency for security of TC57 and is to assist in the creation of the security mechanisms for the relevant protocols.

WG15 began its task prior to 911. It determined that the highest risk protocol was ICCP/IEC 80870-6-TASE.2 since it is wide scale deployment for 60-80% of utility control centers within the United States and the percentage of deployment worldwide is increasing dramatically. Additionally, the ICCP/TASE.2 protocol is used to convey control, generation schedules, and financially sensitive SCADA information. These factors, plus the perception of control centers being exposed to cyber attacks made the securing of ICCP/TASE.2 the highest WG15 work priority.

It is worthwhile to note that several of the countermeasures listed in Table 1 involve the utility developing appropriate policies and software/equipment vendors implementing appropriate access privilege levels. These issues are clearly outside the scope of WG15, however, this does not minimize their importance. Part of the scope of WG15 was to determine recommended security communication topologies and how to achieve Strong Peer Authentication, Encryption, and Message Authentication across those topologies. Another dimension to the TASE.2 work was knowledge that UCA/IEC 61850 and DMS/IEC 61134 specified similar protocols for use (being ISO 9506/MMS or a derivative). Therefore, one of the design objectives of WG15 became to develop common security specifications for these three protocols when possible. Such work

would allow securing of communications between control centers, control centers to meters, control centers to substations, and internally to a substation.

The communication topologies addressed were the use of microwave, frame relay, internet, dial-up, and other wireless media (including satellite). In general, the use of well understood security technologies was found desirable. The OSI Reference Model clearly indicates that encryption is a Presentation function (e.g. transforms local representation into encrypted information) and is not an Application Protocol function. However, Strong Peer Authentication can only be accomplished at the Application level. Additionally, Message Authentication needs to be accomplished at the Transport or Network layer (figure 4).

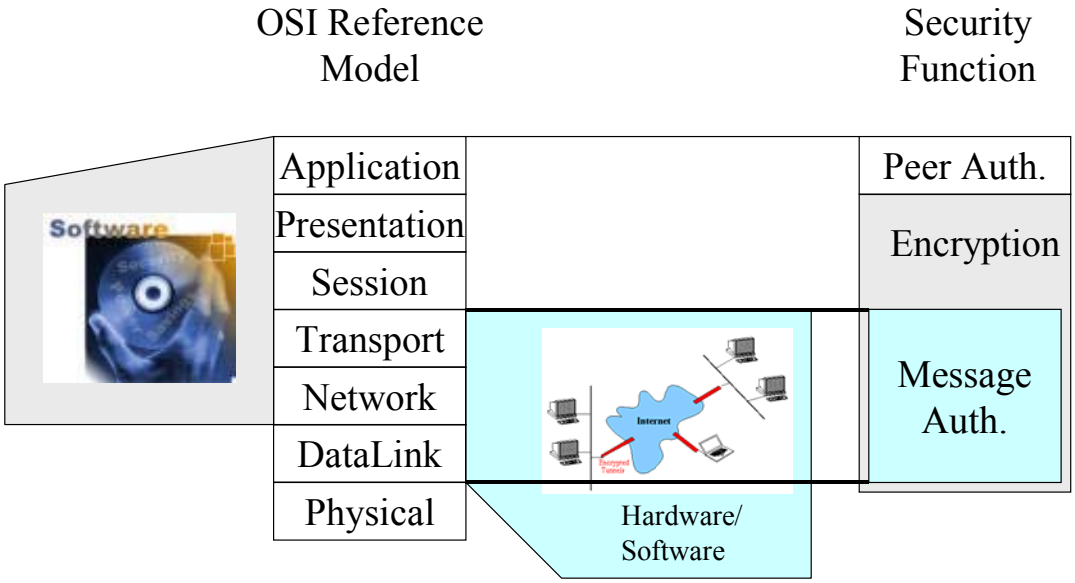


Figure 4

Possible Security Solutions

Both TASE.2 and UCA/61850 make use of standard networking technologies (e.g. TCP/IP) and therefore there are potential hardware (e.g. VPN and Firewall) solutions that can provide Encryption and Message Authentication functions. However, there are software solutions that can also provide this capability. WG15 recommended a solution that allowed combination of hardware/software solutions to exist in order to accommodate different trust levels (e.g. Internet vs. Intranet). In this regard, WG15 has recommended that TASE.2 be secured through the use of SSL/TLS (Transport Layer Software) that provides encryption and message authentication. Additionally, WG15 has recommended that backward compatibility with non-secure implementations needs to be provided (e.g. no SSL/TLS) and that the use of SSL/TLS needs to be a configuration issue. These recommendations result in the following capabilities at the transport level:

- The ability to use VPN/Firewall technology to provide secure tunnels between implementations that are not using SSL/TLS and thereby providing a "secure" environment for non-secure TASE.2/61850 transport connections.

- The ability to use VPN/Firewall technology in conjunction with "secure" TASE.2/61850 transport connections (e.g. SSL/TLS).

- The ability to use the "secure" TASE.2/61850 transport connection solely.

These combinations allow maximum deployment flexibility by a utility so that issues of cost and performance may be addressed as appropriate.

The graph in figure 5 attempts to illustrate that the probability of a successful attack increases with time if security methods are not changed. In the case of encryption, the longer a single key/algorithm is in use, the higher the likelihood that the encryption will be cracked.

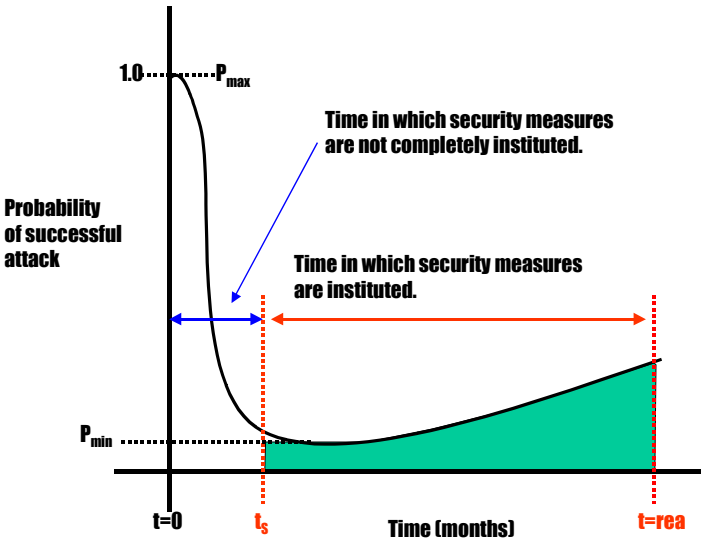


Figure 5

Therefore, WG15 has recommended a minimum key re-negotiation period based upon time and number of packets, whichever occurs first. This mechanism is specified as part of a "secure-profile". This capability may not be available in all VPN/Firewall implementations.

WG15 has also rejected certain SSL/TLS supported cipher suites since the suites do not offer what is perceived to be enough protection. Additionally, it has mandated a set of cipher suites that must be supported thereby allowing interoperability to be achieved. One of the cipher suites that is mandated is AES, thereby allowing some performance concerns to be addressed.

The Strong Peer Authentication, recommended by WG15, supports the use of certificates and username/passwords. Both formats are digitally signed and sealed so that a replay of the connection sequence will not result in a connection.

WG15 has recommended that the end application (e.g. TASE.2/61850) must allow for the configuration of multiple combinations of incoming connections:

- NON SECURE: Neither transport encryption or application authentication is to be used. This provides backward compatibility and would need to be used over a VPN if any security is desired.

- AUTHENTICATED: Only application authentication is to be used.

- SECURE: Both transport and Application level security is to be used.

The current status of the WG15 work is that IEC TC57 WG07 (the group responsible for TASE.2) is in the process of evaluating the recommendations to become a Technical Report specifying how to secure TASE.2. It is expected that this decision will be positive since three vendors are already implementing the recommendations and since WG07 comments have already been addressed in the current recommendations. In addition to the WG07 recommendations, WG15 has created a similar work item to address the similar issues and solutions for UCA/61850.

Securing Remote Access to Electronic Control and Protection Systems

In January of 2003, the North American Electric Reliability Council released a draft guideline for securing access to Electronic Control and Protection Systems (ECPS). The guideline is aimed at communications to electronic relays, substation automation and control systems, power plant control systems, energy management systems, SCADA, and Programmable Logic Controllers where the remote connection is anything other than a direct connection. The a summary of the guidelines are as follows:

1. Establish policies and procedures governing the use of remote access to ECPS systems including identifying responsible parties. Periodic review and updates should be schedules
2. Remote Access should only be enabled when required, approved, and authenticated
3. Multi-factor authentication (2 or more factors) should be used. Factors include passwords, phone numbers, IP addresses, biometrics, GPS location, etc.
4. Automatically lock account access after a preset number of consecutive invalid password attempts.
5. Encryption should be used when traversing unsecured networks
6. Approved Remote Access authorization lists should be established and periodically reviewed
7. DO NOT use default passwords. Use meaningful but non-descriptive passwords
8. All remote access hardware and software should be approved and installed per policy
9. Remote access connections should be logged (and periodically reviewed)
10. Consider the risk to the process when allowing remote access.

Security Architectures

Given the above tools and security guidelines, there are several security architectures that can be developed. Two of these are suggested below.

First, there is the architecture where a secure VPN tunnel is created from the utility headquarters network into the substation network (figure 6). This architecture implements a single secure point of entrance into the substation and does not burden the existing hardware with encryption/decryption overhead. The drawback to this implementation is that there are still authorization issues to address. This could partially be addressed through the addition of a firewall in series with the VPN tunnel. The firewall would only allow authorized computers to pass requests through the firewall. Ultimately, the IED will need to provide authentication of a user.

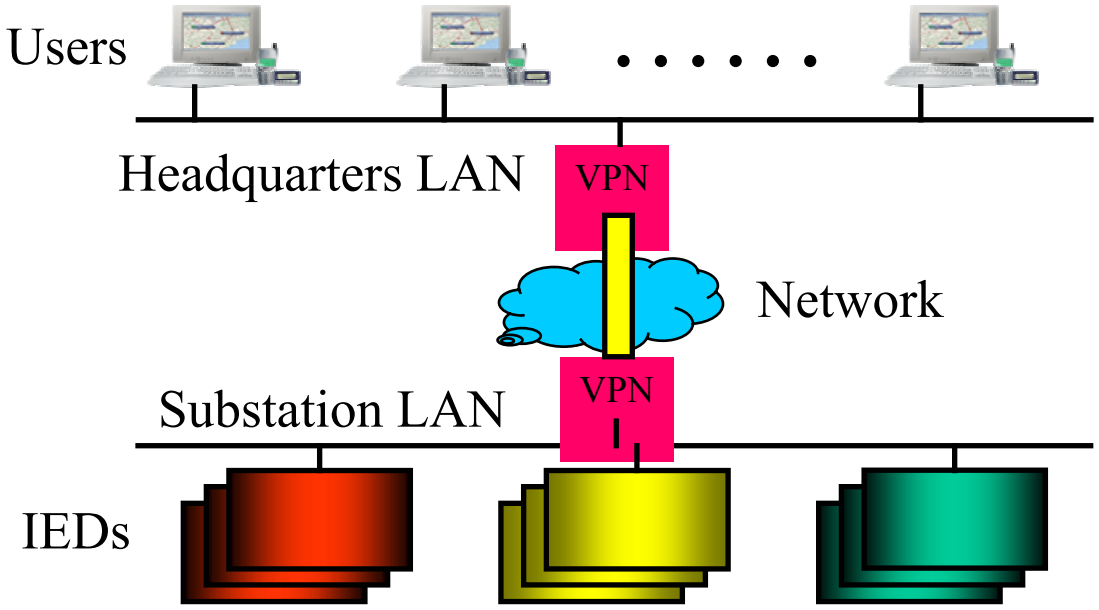


Figure 6
Secure Substation Architecture via VPN

The second architecture, which results from the IEC WG15 recommendations, is an SSL/TLS based solution. In this implementation, TLS/SSL is inserted as the presentation layer of the client-server protocols. In the case of a UCA implementation, the resulting protocol profile is shown in figure 7.

Standardization of such architectures will be required in the future in order to facilitate inter-operability. Work is underway to develop such an Integrated Energy and Communications System Architecture (IECSA) that will detail implementations from the energy traders to the thermostat (see reference 6).

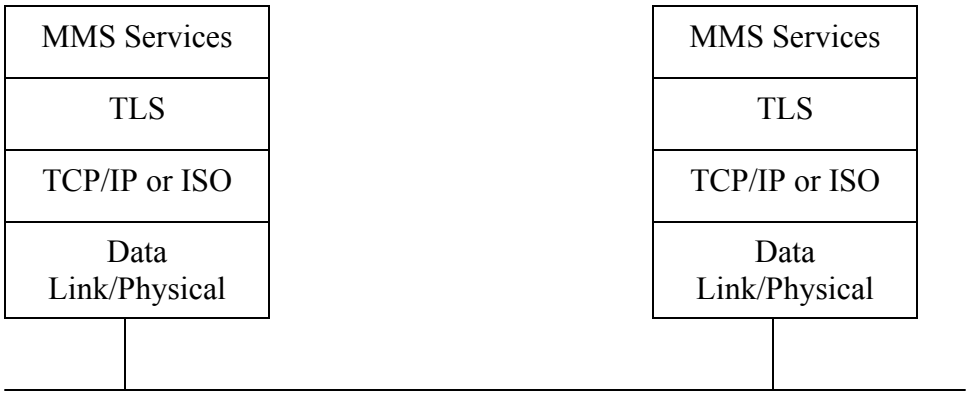


Figure 7
Secure Communications Architecture between UCA Based Client and Server

Conclusions

Security in all forms is becoming a requirement in our society. Communication security concerns have been identified by EPRI, NERC and others and can be addressed with available software and procedures. The industry has responded with recommendations of application of TLS/SSL and VPN in the utility communication infrastructure. Although these software solutions are strong and effective security tools, they are only part of the total equation. True security requires many such tools *and* a comprehensive plan to employ them.

Bibliography

1. SSL and TLS Essentials – Securing the Web, Stephen A. Thomas, Wiley Computer Publishing, 2000.

2. VPN Fundamentals, Chuck Semeria, Juniper Networks, Sunnyvale, CA., Part # 200012-001 3/01.

3. Security Guidelines for the Electricity Sector; Securing Access to Electronic Control and Protection Systems, North American Electric Reliability Council; version .3, January 15, 2003.

4. ICCP (TASE.2) Security Enhancements Volume 1, EPRI, Palo Alto, CA, 2002. 1001642.

5. 3DES and Encryption, Kenneth Castelino; http://kingkong.me.berkeley.edu/~kenneth/courses/sims250/des.html

6. Integrated Energy and Communications System Architecture; www.IECSA.org

Biographies

Mark Adamiak received his Bachelor of Science and Master of Engineering degrees from Cornell University in Electrical Engineering and an MS-EE degree from the Polytechnic Institute of New York. From 1976 through 1990, Mark worked for American Electric Power (AEP) in the System Protection and Control section where his assignments included R&D in Digital Protection and Control, relay and fault analysis, and system responsibility for Power Line Carrier and Fault Recorders. In 1990, Mark joined General Electric where his activities have ranged from development, product planning, and system integration. He is presently Manager of Advanced Technology Programs and is responsible for identifying and developing next generation technologies for the utility and industrial protection and control markets. In addition, Mr. Adamiak has been actively involved in developing the framework for the implementation of the MMS/Ethernet peer-to-peer communication solutions for next generation relay communications and is currently the Principle Investigator on the EPRI/E2I Integrated Energy and Communication Systems Architecture (IECSA) project. Mark is a member of HKN, a Senior Member of IEEE, past Chairman of the IEEE Relay Communication Sub Committee, a member of the US team on IEC TC57 - Working Group 11 on Substation Communication, and a registered Professional Engineer in the State of Ohio.

Herbert Falk - Project Manager: Mr. Falk has been involved in numerous projects involving the application of information systems technology and real-time communications technology to automated manufacturing, electrical distribution and automation and power quality monitoring. Mr. Falk is a recognized expert on MAP, OSI, UCA, information integration technology, distributed object technology, and the Manufacturing Message Specification (MMS) having served on and chaired numerous industry technical committees. He has been a involved in the determination of communication security needs and standardization since 1996. In 1998, Mr. Falk prepared the security specification for UCA. Shortly thereafter, Mr. Falk assisted in the design and implementation of SISCO's first suite of "secure" communication products. In 2000, Mr. Falk completed an EPRI security assessment of the United States Electric Utility Infrastructure. Additionally, Mr. Falk is a technical leader within IEC TC 57 WG15 whose scope is "Data and communication security in the field of IEC/TC 57". The scope includes assisting in the assessment and standardizing of communication security for ICCP/TASE.2, IEC 870-5, DNP 3.0, IEC 61850, and other IEC TC57 protocols and their potential derivatives.