Michael J Martin, MA, MBA, Med, SCPM, PMP
Senior Managing Consultant, Broadband Networks
michael.martin@ca.ibm.com
Global Technical Services
Global Center of Excellance in Energy and Utilities.
3600 Steeles Avenue East
Markham, Ontario, L3R 9Z7Canada
416 478 3483 direct line
416 729 9991 cellular – Canada
720 626 8755 cellular – United States

Smart Grid: Cyber Security

Introduction

Smart grid security is a complex discussion. It is one that is not well understood. Every time I meet with a new Utility, I see differences in the way that security in understood and implemented. Placing proper security over a multimodal network is a daunting task. What security is needed and what are the impacts of apply this security? As the power grid evolves, security will need to change in cadence with the grid developments. This will not be an easy transition as most security experts within Utilities are from an IT background and the needs for OT can be in stark conflict to the classic IT approaches to security that are tried and true.

Recent events regarding security breaches teach us that proper security is not a destination to get to, but rather a never-ending journey that demands constant vigilance. Utilities need to be standing guard against attack and be at the ready with plans for fast turnaround actions to mitigate these attacks. The hackers and crackers strategies are evolving too, so Utilities must remain current and adjust methods, policies, governance, and train staff to maintain this ongoing battle at protecting the Utility's assets and customer information.

As smart grids evolve, more and more data will reside on the communication networks and may never get to the data centre. Some fear that content on the grid is at greater risk, but this need not be the case. I will repeat, protecting data is paramount. So, how do we protect the data and what tools, strategies and options are available to the network designer to ensure that the regulatory requirements are not only being met, but exceed.

In order to make this document more user friendly, it is provided out of order. Instead of listing all of the security tools and capabilities first and then providing the discussion related to them all, the discussion is provided first. It is assumed that many who might read this document already hold a firm grasp on these issues and are more interested in the applicability then the textbook definitions. However, for those readers who want more, the definitions are provided and follow this section.

Changes to Cyber Security on a Smart Grid Network

NERC now requires Utilities to define all BES Cyber Assets Low, Medium and High impact.

With NERC CIP Version 5, assets are categorized by impact levels: High, Medium, Low or Non-Impactful. The impact level then determines the level of protection required for CIP-003 through CIP-011, and these are specified in the standards.

It is likely that for those utilities with generation and transmission assets that NERC CIP V5 will translate into more assets that require compliance with the standards.

The NERC CIP 5 compliance deadline is April 1, 2016. Achieving full compliance can take two years or more. To avoid added costs and potential penalties, critical infrastructure utilities should start implementing a cyber security solution as soon as possible.

BES Cyber Assets are defined as those that "if rendered unavailable, degraded, or misused would, within 15 minutes of its required operation, mis-operation or non-operation, adversely impact one or more facilities, systems or equipment … "

Most likely, a responsible entity will be required to comply, at minimum, with the requirements associated with Low Impact assets. Many entities will be responsible for identifying Medium and/or High Impact BES Cyber Systems, which require additional protection.

Is NERC CIP 5 applicable to the distribution grid too? Generally it is believed that the answer is still, no. NERC CIP 5 provides a set of criteria for sizing of capacity by stating that the transmission line needs to carry power at 100 kV or more. Can this sort of line exist in a distribution grid? Yes, maybe, but rarely as typical North American distribution systems carry lower kV levels than 100 kV. But, if they do, then they would be applicable. Likewise, there is a secondary issue pertaining to assets that might be connected to these ≥100 kV lines, in some cases, the coupling to these protected assets will automatically include assets that might not otherwise be classified as CIP assets. So, the coupling plays a role too.

Depending upon how the assets are classified, and where they exist in the power supply chain, we should consider how to best protect them. Regardless of where they do reside, all Utility assets must be protected.

But, it is fair to say that different needs do exist in different points of the supply chain. Some security aspects can negatively exasperate performance aspects that are also required by NERC CIP. An example will be the added security aspects may add to the latency causing a critical transfer trip line in the transmission grid to exceed the 10 ms criteria for that capability. So, a balance is necessary.

As well, security can be very expensive to implement. So, selecting security that is appropriate to the risk is important. In the case of security, "one size does not fit all".

For example, in transmission, it is common practice to use encryption and a VPN to protect data. Regardless if the communication link is travelling over a public or private connection. These point to point links should be well protected. However, in the distribution grid, while encryption is desired, using a VPN on every connection can have negative impacts on the smart grid. This is especially the case for point to multipoint links where a VPN on every connection would be challenging from an administration and cost perspective. In some cases, such as over an IoT mesh network, there is likely insufficient data rate to even support the VPN and with each hop the burden for overhead increases. Again, encryption of the data is still required, but we should not look to a VPN on every connection and every hop.

Is there a difference approach to public versus private networks? Yes, most definitely, we should apply stronger protection to public networks, and adequate protection to the Utility's own private networks. This statement assumes that there is an air-gap between the private and public networks.

As we build NOCs (network operation centres) we should consider a NOC just for security. This cyber security NOC would support both IT and OT needs, and would be collocated with the Network Management Systems NOC.

NISTIR (National Institute of Standards and Technology Interagency Report) is a set of security guidelines for the smart grid industry. The published standard is *NISTIR 7628, entitled, Guidelines for Smart Grid Cyber Security*. NISTIR 7628 presents an analytical framework that organizations can use to develop effective cyber security strategies tailored to their particular combinations of Smart Grid-related characteristics, risks, and vulnerabilities.

Clearly, the convergence of the information and communication infrastructure with the electric power grid introduces new security and privacy-related challenges. However, the introduction of these technologies to the electric sector also presents opportunities to increase the reliability of the power system, to make it more capable and more resilient to withstand attacks, equipment failures, human errors, natural disasters, and other threats. Greatly improved monitoring and control capabilities must include cyber security solutions in the development process rather than as a retrofit.

A few examples of potential risks associated with the evolution of the Smart Grid include:

- Greater complexity increases exposure to potential attackers and unintentional errors;
- Networks that link more frequently to other networks introduce common vulnerabilities that may now span multiple Smart Grid domains and increase the potential for cascading failures;
- More interconnections present increased opportunities for “denial of service” attacks, introduction of malicious code (in software/firmware) or compromised hardware, and related types of attacks and intrusions;
- As the number of network nodes increases, the number of entry points and paths that potential adversaries might exploit also increases; and
- Extensive data gathering and two-way information flows may broaden the potential for compromises of data confidentiality and breaches of customer privacy, and compromises of personal data and intrusions of customer privacy.

The convergence of both IT and OT over a common network fabric can add complexity to the security picture. While it is desired to integrate IT and OT, caution must be taken to respect the differences of these two domains and to ensure that adequate protection is in place to ensure that problems in one network do not create vulnerabilities in the other network.

NERC CIP should be applied just where it is required. Due to the costs to the Utility, it would be excessive to apply NERC CIP to all aspects of the supply chain. This is not to say that the security would be relaxed or lessened in the distribution grid, just that it would be applied in a manner to reflect the lower risk aspects of parts of the communication network within the distribution grid compared to the critical aspects of the transmission grid where the Bulk Electric System resides.

Order 791 and CIP Version 5 Standards use a new methodology based on whether a Bulk Electric System (BES) Cyber System has a low, medium, or high impact on the reliable operation of the bulk electric system.

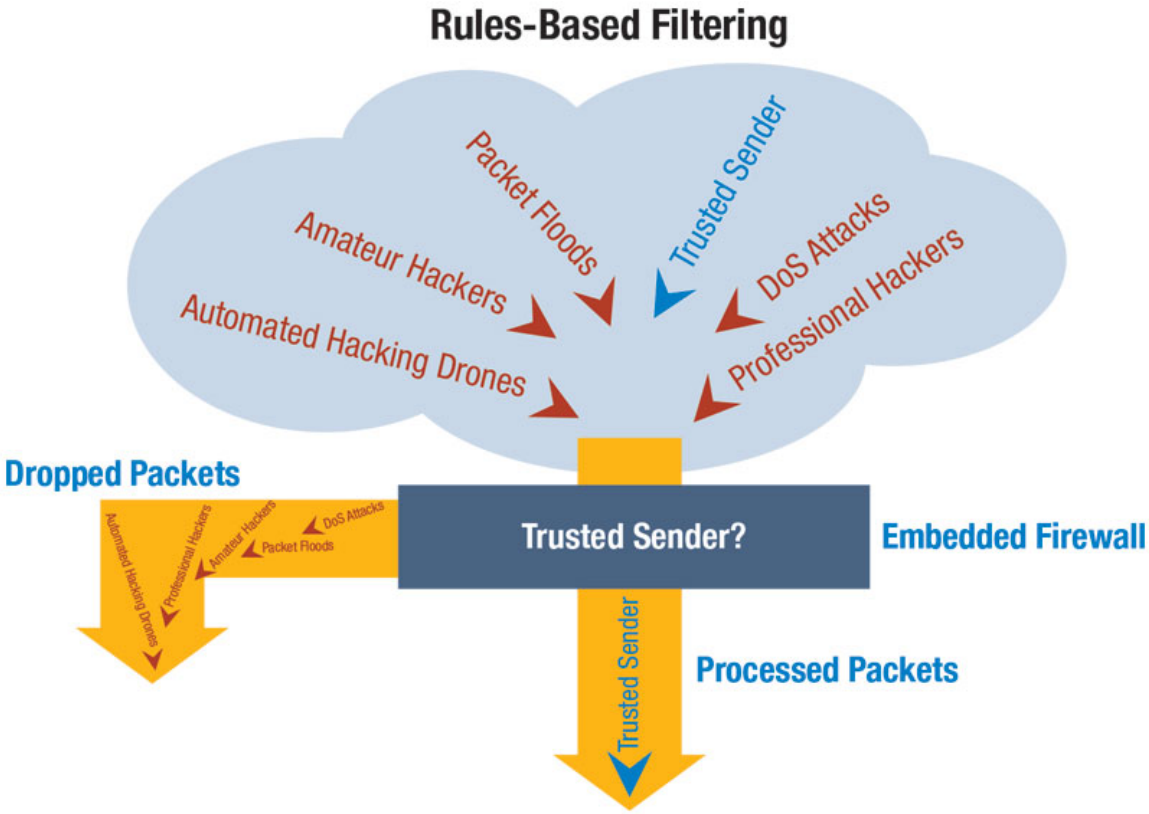
Time is short as the requirement for Medium and High Cyber assets is April, 2016. Low Cyber assets take effect in April 2017.

End to end encryption should be implemented rather than applying discrete encryption for each leg of the network.

Security Tools and Capability Review

Let's review the main security tools for wired and wireless networks. This article is a collection of definitions of these security tools by respected industry thought leaders who are cited at the end of the page. The discussion to consider the impacts of these security tools is above and is the core content provided for your consideration.

Firewalls

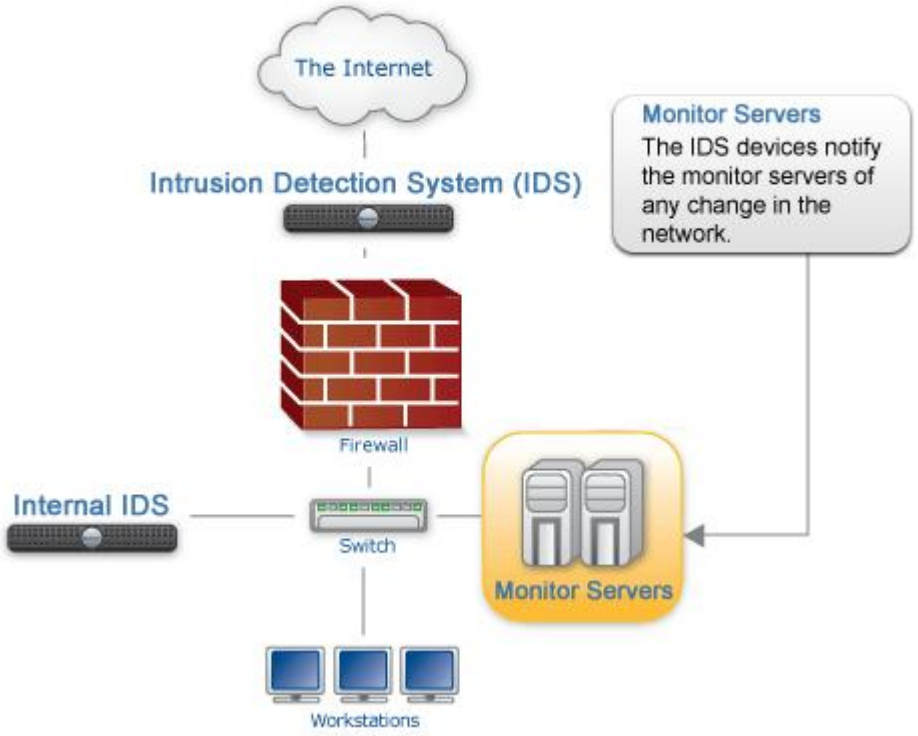


Everyone knows the term "firewall" but do we all understand what a firewall does for a Utility? Firewalls have been hardware devices that sit in front of a network device and perform functions based upon some predefined settings. Traditional firewall techniques such as port blocking and NAT still play a massive part; however on their own they do not have the in depth power to stopping today's threats. The primary job of a firewall is to protect the Utility's network from threats and to enforce company security policies. The security policy will dictate what applications, services, ports and IP addresses are allowed and disallowed via the firewall. Utilities are in need of firewalls that do not only consist of advanced protection tools, but also have other built in advanced capabilities for other uses, such as VPNs, WAN Optimisation, Failover and high availability, VLAN support, Dynamic routing, logging and reporting and other very handy utilities [1].

Popular firewalls are made by well known brands in the networking business including Cisco, Checkpoint, HP, Fortinet, SonicWALL, Watchguard, Netgear, Juniper and Palo Alto. Firewalls can be hardware based or software based. Open source code for firewalls is now available too. Some radio vendors offer basic firewall functionality within the radio itself. There are some lightweight firewalls meant for home or consumer use. Utilities need trusted firewall solutions. Popular Utility firewalls for the wired and wireless networks include Cisco and Checkpoint. It is common to see multimillion dollar firewalls from Juniper at the data centre.

Lower end firewalls need to be controlled locally. So, it is better and far more cost effective to use firewalls that can be controlled centrally by pushing a new image over the network to the remotely located devices. This saves truck rolls for security staff to the substations or to some irregular placed firewalls on poles, rooftops, or towers.

Unified threat management (UTM) is an approach to security management that allows an administrator to monitor and manage a wide variety of security-related applications and infrastructure components remotely through a single management console. UTMs, which are typically purchased as cloud services or network appliances, provide firewall, intrusion detection, anti-malware, spam and content filtering and VPN capabilities in one integrated package that can be installed and updated easily. UTMs for enterprise customers may also include more advanced features such as identity-based access control, load balancing, quality of service (QoS), intrusion prevention, SSL and SSH inspection and application awareness. The principal advantage of a UTM product is its ability to reduce complexity. The principal disadvantage is that a UTM appliance can become a single point of failure. UTM appliances are sometimes referred to as next-generation firewalls [2].



IDS (Intrusion Detection System)

An intrusion detection system (IDS) monitors network traffic and monitors for suspicious activity and alerts the system or network administrator. In some cases the IDS may also respond to anomalous or malicious traffic by taking action such as blocking the user or source IP address from accessing the network.

IDS come in a variety of flavours and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. There are IDS that detect based on looking for specific signatures of known threats- similar to the way anti-virus software typically detects and protects against malware- and there are IDS that detect based on comparing traffic patterns against a baseline and looking for anomalies. There are IDS that simply monitor and alert and there are IDS that perform an action or actions in response to a detected threat.

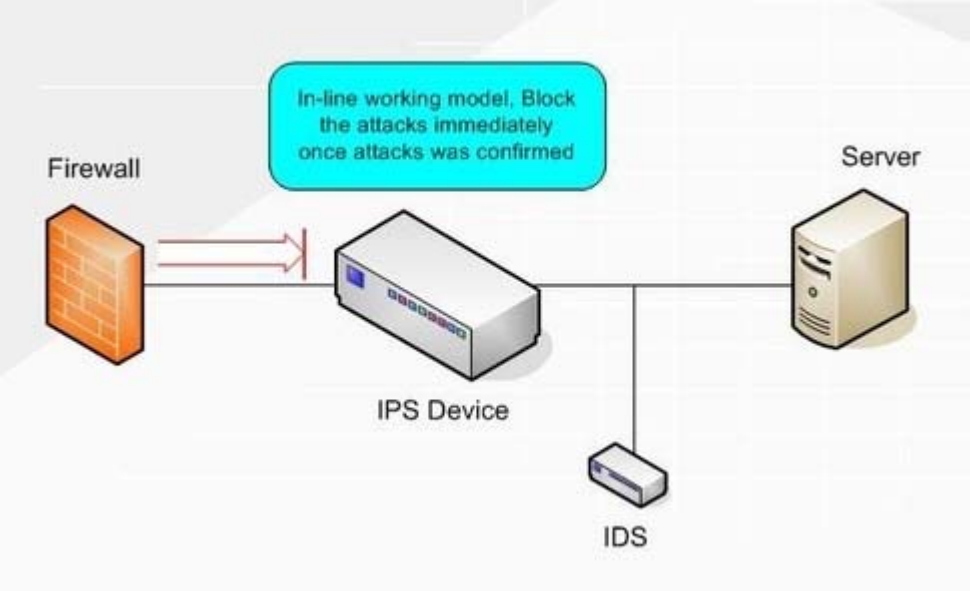
A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. This is similar to the way most anti-virus software detects malware. The issue is that there will be a lag between a new threat being discovered in the wild and the signature for detecting that threat being applied to your IDS. During that lag time your IDS would be unable to detect the new threat.

An IDS which is anomaly based will monitor network traffic and compare it against an established baseline. The baseline will identify what is "normal" for that network- what sort of bandwidth is generally used, what protocols are used, what ports and devices generally connect to each other- and alert the administrator or user when traffic is detected which is anomalous, or significantly different, than the baseline.

A passive IDS simply detects and alerts. When suspicious or malicious traffic is detected an alert is generated and sent to the administrator or user and it is up to them to take action to block the activity or respond in some way.

A reactive IDS will not only detect suspicious or malicious traffic and alert the administrator, but will take pre-defined proactive actions to respond to the threat. Typically this means blocking any further network traffic from the source IP address or user [3].

IPS (Intrusion Prevention Systems)

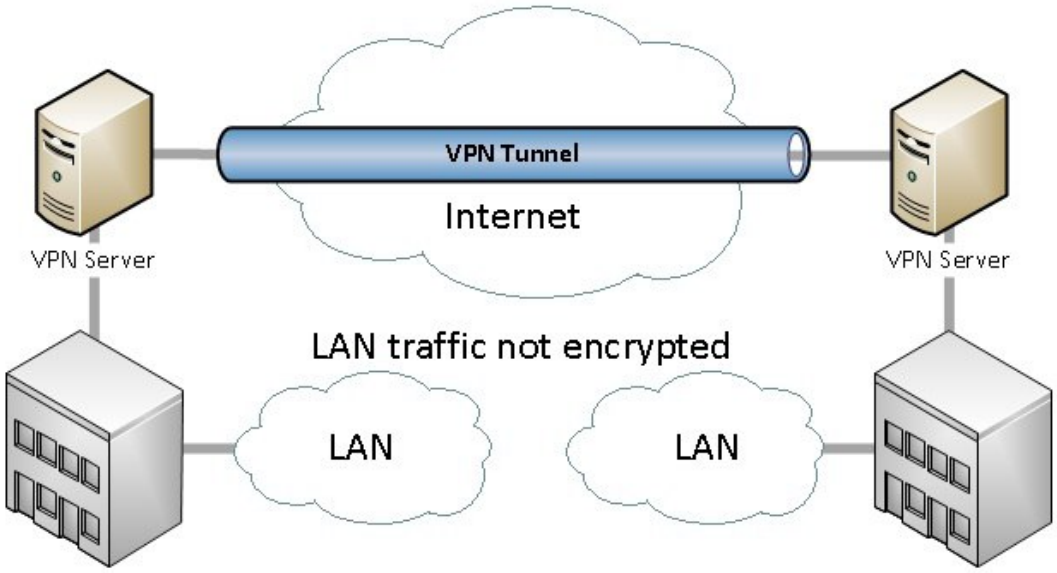


IPS (Intrusion Prevention System) systems are deployed in-line and actually take action by blocking the attack, as well as logging the attack and adding the source IP address to the block list for a limited amount of time; or even permanently blocking the address depending on the defined settings. Hackers take part in lots of port scans and address scans, intending to find loop holes within organizations. IPS systems would recognize these types of scans and take actions such as block, drop, quarantine and log traffic. However this is the basic functionality of IPS. IPS systems have many advanced capabilities in sensing and stopping such attacks [4].

An IPS can be either implemented as a hardware device or software. Ideally (or theoretically) and IPS is based on a simple principle that dirty traffic goes in and clean traffic comes out.

Intrusion prevention systems are basically extensions of intrusion detection systems. The major difference lies in the fact that, unlike intrusion detection systems, intrusion prevention systems are installed are able to actively block or prevent intrusions that are detected. For example, an IPS can drop malicious packets, blocking the traffic an offending IP address, etc. [5]

VPN (Virtual Private Network)



A Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network such as the Internet or a private network owned by a service provider. Utilities use VPN technology to enable remote users to securely connect to a private network.

In order to gain access to the private network, a user must be authenticated using a unique identification and a password. An authentication token is often used to gain access to a private network through a personal identification number (PIN) that a user must enter. The PIN is a unique authentication code that changes according to a specific frequency, usually every 30 seconds or so.

There are a number of VPN protocols in use that secure the transport of data traffic over a public network infrastructure. Each protocol varies slightly in the way that data is kept secure.

IP security (IPSec) is used to secure communications over the Internet. IPSec traffic can use either transport mode or tunnelling to encrypt data traffic in a VPN. The difference between the two modes is that transport mode encrypts only the message within the data packet (also known

as the payload) while tunnelling encrypts the entire data packet. IPSec is often referred to as a "security overlay" because of its use as a security layer for other protocols.

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) use cryptography to secure communications over the Internet. Both protocols use a "handshake" method of authentication that involves a negotiation of network parameters between the client and server machines. To successfully initiate a connection, an authentication process involving certificates is used. Certificates are cryptographic keys that are stored on both the server and client.

Point-To-Point Tunnelling Protocol (PPTP) is another tunnelling protocol used to connect a remote client to a private server over the Internet. PPTP is one of the most widely used VPN protocols because of its straightforward configuration and maintenance and also because it is included with the Windows operating system.

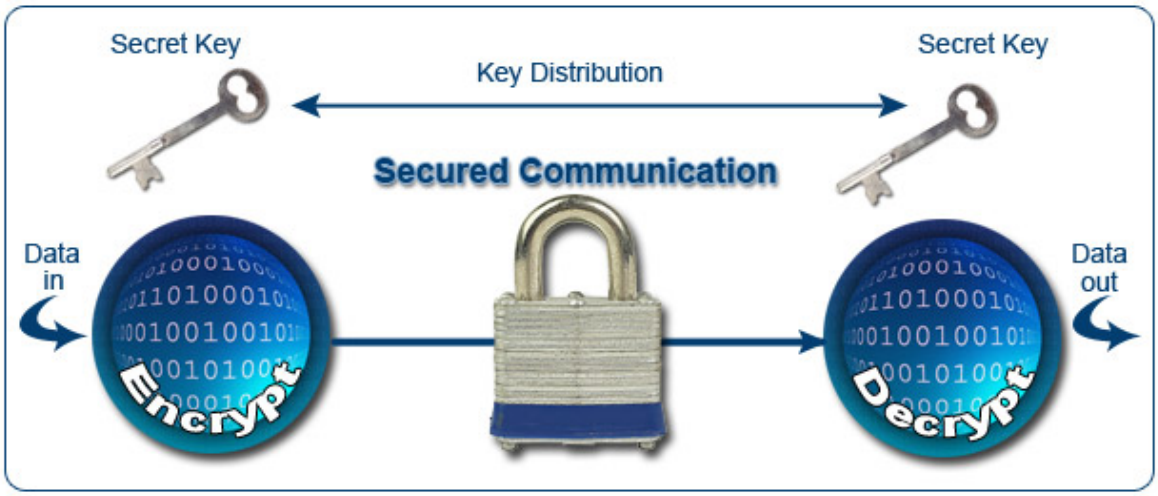
Layer 2 Tunnelling Protocol (L2TP) is a protocol used to tunnel data communications traffic between two sites over the Internet. L2TP is often used in tandem with IPSec (which acts as a security layer) to secure the transfer of L2TP data packets over the Internet. Unlike PPTP, a VPN implementation using L2TP/IPSec requires a shared key or the use of certificates.

VPN technology employs sophisticated encryption to ensure security and prevent any unintentional interception of data between private sites. All traffic over a VPN is encrypted using algorithms to secure data integrity and privacy. VPN architecture is governed by a strict set of rules and standards to ensure a private communication channel between sites. Utility network administrators are responsible for deciding the scope of a VPN, implementing and deploying a VPN, and ongoing monitoring of network traffic across the network firewall. A VPN requires administrators to be aware of the overall architecture and scope of the VPN to ensure communications are kept private.

A VPN is an inexpensive effective way of building a private network. The use of the Internet as the main communications channel between sites is a cost effective alternative to expensive leased private lines. The costs to the Utility include the network authentication hardware and software used to authenticate users and any additional mechanisms such as authentication tokens or other secure devices. The relative ease, speed, and flexibility of VPN provisioning in comparison to leased lines makes VPNs an ideal choice for Utilities who require flexibility. For example, a Utility can adjust the number of sites in the VPN according to changing requirements.

There are several potential disadvantages with VPN use. The lack of Quality of Service (QoS) management over the Internet can cause packet loss and other performance issues. Adverse network conditions that occur outside of the private network are beyond the control of the VPN administrator. For this reason, many Utilities pay for the use of trusted VPNs that use a private network to guarantee QoS. Vendor interoperability is another potential disadvantage as VPN technologies from one vendor may not be compatible with VPN technologies from another vendor. Neither of these disadvantages has prevented the widespread acceptance and deployment of VPN technology.

Cryptography



In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.

Within the context of any application-to-application communication, there are some specific security requirements, including:

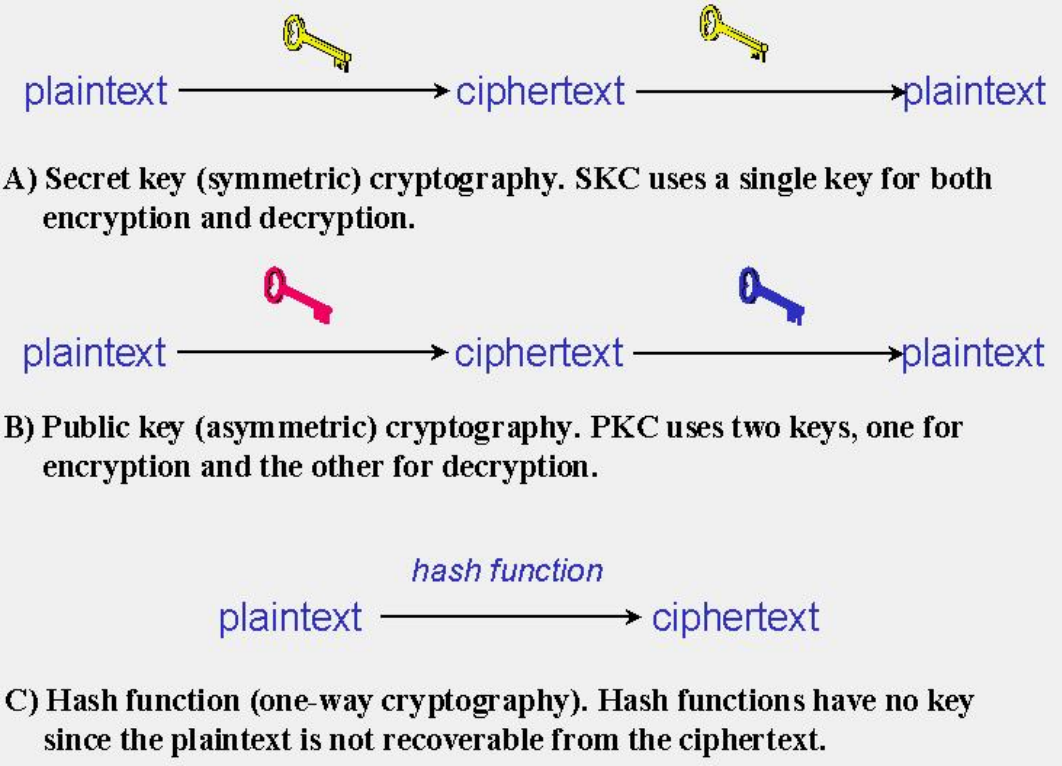
- *Authentication:* The process of proving one's identity. (The primary forms of host-to-host authentication on the Internet today are name-based or address-based, both of which are notoriously weak.)
- *Privacy/confidentiality:* Ensuring that no one can read the message except the intended receiver.
- *Integrity:* Assuring the receiver that the received message has not been altered in any way from the original.
- *Non-repudiation:* A mechanism to prove that the sender really sent this message.

Cryptography, then, not only protects data from theft or alteration, but can also be used for user authentication. There are, in general, three types of cryptographic schemes typically used to accomplish these goals: secret key (or symmetric) cryptography, public-key (or asymmetric) cryptography, and hash functions, each of which is described below. In all cases, the initial unencrypted data is referred to as *plaintext*. It is encrypted into *ciphertext*, which will in turn (usually) be decrypted into usable plaintext.

There are several ways of classifying cryptographic algorithms. For purposes of this paper, they will be categorized based on the number of keys that are employed for encryption and

decryption, and further defined by their application and use. The three types of algorithms that will be discussed are (Figure 1):

- Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption
- Public Key Cryptography (PKC): Uses one key for encryption and another for decryption
- Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information



So, why are there so many different types of cryptographic schemes? Why can't we do everything we need with just one?

The answer is that each scheme is optimized for some specific application(s). Hash functions, for example, are well-suited for ensuring data integrity because any change made to the contents of a message will result in the receiver calculating a different hash value than the one placed in the transmission by the sender. Since it is highly unlikely that two different messages will yield the same hash value, data integrity is ensured to a high degree of confidence.

Secret key cryptography, on the other hand, is ideally suited to encrypting messages, thus providing privacy and confidentiality. The sender can generate a *session key* on a per-message basis to encrypt the message; the receiver, of course, needs the same session key to decrypt the message.

Key exchange, of course, is the main application of public-key cryptography. Asymmetric schemes can also be used for non-repudiation and user authentication; if the receiver can obtain the session key encrypted with the sender's private key, then only this sender could have sent the message. Public-key cryptography could, theoretically, also be used to encrypt messages although this is rarely done because secret-key cryptography operates about 1000 times faster than public-key cryptography [6].

NERC CIP

The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the reliability of the bulk power system in North America. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel. NERC's area of responsibility spans the continental United States, Canada, and the northern portion of Baja California, Mexico. NERC is the electric reliability organization for North America, subject to oversight by the Federal Energy Regulatory Commission and governmental authorities in Canada. NERC's jurisdiction includes users, owners, and operators of the bulk power system, which serves more than 334 million people [7].

NERC's Reliability Standards became mandatory within the three countries. These mandatory Reliability Standards include CIP standards 001 through 009, which address the security of cyber assets essential to the reliable operation of the electric grid. To date, these standards (and those promulgated by the Nuclear Regulatory Commission) are the only mandatory cybersecurity standards in place across the critical infrastructures of the United States. Subject to FERC

oversight, NERC and its Regional Entity partners enforce these standards, which are developed with substantial input from industry and approved by FERC, to accomplish NERC's mission of ensuring the security and reliability of the electric grid. NERC's current nine mandatory CIP standards address the following areas:

- CIP-001: Covers sabotage reporting;
- CIP-002: Requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System;
- CIP-003: Requires that responsible entities have minimum security management controls in place to protect Critical Cyber Assets;
- CIP-004: Requires that personnel with authorized cyber or unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness;
- CIP-005: Requires the identification and protection of the Electronic Security Perimeters inside which all Critical Cyber Assets reside, as well as all access points on the perimeter;
- CIP-006: Addresses implementation of a physical security program for the protection of Critical Cyber Assets;
- CIP-007: Requires responsible entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the other (non-critical) Cyber Assets within the Electronic Security Perimeters;
- CIP-008: Ensures the identification, classification, response, and reporting of cyber Security incidents related to Critical Cyber Assets; and
- CIP-009: Ensures that recovery plans are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices [8].

By most accounts Version 5, currently pending approval by the Federal Energy Regulatory Commission (FERC), is a significant enhancement over the current Version 3. In fact the changes are significant and impactful enough that many believe the in-between, not-yet-in-effect Version 4 standards will never see the light of day. FERC has noted that NERC's proposed Version 5 CIP standards represent an improvement over the current CIP Reliability standards, and extend the scope of systems protected by the CIP Reliability standards.

From a security perspective, Version 5 "ups the ante" on data protection, creating hard requirements for items that were previously only mentioned in guidelines. In order to better safeguard assets in certain situations, Version 5 of NERC CIP 005 (Cyber Security – Electronic Security Perimeter(s)) mandates the use of security techniques including encryption and strong authentication based on technologies such as Public Key Infrastructure. Encryption, which transforms data into an unusable form, has evolved over the years from niche usage to common practice and is a core component in data protection and IT security strategies. PKI too has become pervasive for many use cases, including authentication of users and systems as part of an access control strategy. In both cases, care must be taken to safeguard and manage associated private key material against compromise.

And although Version 5 primarily consists of updates to previous standards, it also includes a brand new standard, NERC CIP 011 (Cyber Security – Information Protection), focused on data security. The requirements in this standard specify the need to identify information in accordance with its sensitivity; to have procedures to protect and securely handle such information in storage, transit, and use; and tracking of encryption, deletion, or other means of preventing unauthorized retrieval of data [9].

----------**MJM**----------

Michael Martin has more than 35 years of experience in broadband networks, optical fibre, wireless and digital communications technologies. He is a Senior Executive Consultant with IBM's Global Center of Excellence for Energy and Utilities. He was previously a founding partner and President of MICAN Communications and earlier was President of Comlink Systems Limited and Ensat Broadcast Services, Inc., both divisions of Cygnal Technologies Corporation. He holds three Masters level degrees, in business (MBA), communication (MA), and education (MEd). As well, he has diplomas and certifications in business, computer programming, internetworking, project management, media, photography, and communication technology.

References

- [1] Security and Firewall Features, http://www.internet-computer-security.com/Firewall/Firewalls.html
- [2] Unified Threat Management (UTM), http://searchmidmarketsecurity.techtarget.com/definition/unified-threat-management
- [3] Introduction to Intrusion Detection Systems (IDS), http://netsecurity.about.com/cs/hackertools/a/aa030504.htm
- [4] IPS (Intrusion Prevention System) and IDS (Intrusion Detection Systems), http://www.internet-computer-security.com/Firewall/IPS.html
- [5] Intrusion Prevention Systems, http://www.techopedia.com/definition/15998/intrusion-prevention-system-ips
- [6] An Overview of Cryptography. http://www.garykessler.net/library/crypto.html
- [7] NERC, http://www.nerc.com/Pages/default.aspx
- [8] CIP Compliance, http://www.nerc.com/pa/CI/Comp/Pages/default.aspx
- [9] John Grimm, https://www.thales-esecurity.com/blogs/2013/october/understanding-nerc-cip