Inside the Cyber-Security Perimeter

Steven Hodder
GE Digital Energy, Multilin

Dave McGinn
GE Digital Energy, Multilin

Dale Finney
GE Digital Energy, Multilin

1. Introduction

A common strategy for the provision of cyber security for electrical power transmission substations is to establish a single cyber security perimeter that includes all vulnerable devices in the station. This cyber security perimeter equipment is located inside the station's physical security perimeter to protect it from physical attack. A concern regarding this strategy is that it provides little or no cyber security against someone inside the physical perimeter. Proposals have been made to instead make each relay independently cyber secure, to limit access from inside the station to the internal unsecured LAN, and so on. However, anyone with malicious intent who has breached the physical security perimeter has numerous alternatives to cyber attack. Plugging this internal cyber hole would therefore result in little overall security improvement, and would present significant difficulties in comparison to a station wide-defence.

However, a cyber security concern that should draw more attention is security against employee errors. Such security would be invaluable in guarding against employees going about their assigned duties with no malicious intent, that through taking short-cuts or thorough unintentional error, negatively affect electric grid reliability. Many of the forms of cyber security discussed in the literature are ineffective against such undesired outcomes, as the employees are legitimately operating inside the cyber security perimeter. LAN-based protection and control systems can exacerbate this kind of problem, by making it easier to be working on a relay other than the intended one, or to incompletely block or restore a protection system.

This paper discusses the provision of cyber security at the relay level, and explores means to integrate security effective against employee error. Regulatory requirements are considered. Various sources of security threat are evaluated, and the value of the different security approaches against these sources is considered.

2. Security Overview

In order to discuss security in the context of protective relaying, it is first necessary to be able to break down, quantify and categorize security issues according to their risk and impact. Also, the impact of new technologies deployed in protection and control system within substations needs to be examined, with the intention of looking for vulnerabilities where a lack of suitable cyber security may have an undesired effect due to intentional or accidental user actions.

2.1 Security Risks

The nature of power systems and how they are constructed tends to make them a target for physical attacks:

- Assets (stations, towers) tend to be located away from densely populated areas, so there is very low risk of being seen by passers by.
- Utilities have undergone significant consolidation in past years, both in an attempt to reduce operating costs and also due to workforce attrition with the end result being most facilities are unmanned. Also, it is not common practice to provide 24 hour manned security at most stations.

Most large power apparatus (circuit breakers, transformers) are long lead time items, and transmission towers take a fairly long time to reconstruct. The physical destruction of these assets would not only result in potentially widespread outages, the repair/replacement time would make the duration of these outages unacceptably long.

This is not to say that there is not the potential for electronic-based attacks on key electricity assets, but the potential risks are greater and impacts are lower for an intentional, malicious electronic attack versus a corresponding physical attack. However, an internal security breach, caused by an inadvertent action of an internal user is far more likely.

2.2 Categorization of Threats

In evaluating the effectiveness of a security system, one should review the challenges that it might face. These may originate from two different source categories, either outside of or inside of the cyber-security perimeter that the utility community appears to be moving towards.

Sources from outside of the perimeter fall into many sub-categories.

Foreign Terrorists – With today's worldwide communications, it is quite conceivable for a foreign terrorist, bent on causing ruin to a western economy, to attempt to gain access to the computer assets of electric utilities. Once in, it is not difficult to cause major disruptions to electricity supply. Not only could geographically widespread blackouts be produced, taking many hours to recover from, but also damage to major equipment such as generators could result, taking weeks or months to recover from. It should not be assumed that foreign terrorists are unable to accomplish much with sophisticated modern protection and control equipment. They have a proven ability to acquire or develop the skills necessary for a complex operation. Such attacks would likely not produce the immediately visible impact that a physical attack would produce.

Domestic Terrorists – Domestic terrorists have opportunities and challenges similar to those of foreign terrorists, but being "in country", have the additional opportunity of attacking the physical perimeter. The strength of physical intrusion barriers is typically low, and in un-staffed rural transmission locations the response time to intrusion alarms is long. It would therefore seem less likely that domestic terrorists would attack the electronic cyber security barriers, or that having breached the physical security perimeter, that they would then mount a cyber attack rather than a direct physical assault.

Industrial Espionage – With open electricity markets, there is tremendous economic potential in having information not publicly available regarding the status of generators across the area, information that can be obtained from protection and control systems once the electronic security perimeter is breached. With this inside information, unscrupulous market participants can adjust their bids so as to control the market. Unlike previous categories, industrial spies would prefer that their intrusions go undetected in the long term, and so they would be unlikely to intentionally cause system disturbances or equipment damage with their cyber activities.

Hackers – There are people who will challenge security systems just because they are there. These people are more typically individuals, each acting independently, and thus not the same threat as a group with vast resources focused on a particular target. However, hacker communities exist that share techniques and other information that may be used by other more focused, malicious groups.

The above-mentioned threat categories originate from outside the electronic security perimeter, and for the most part can be countered with current cyber-security measures and technologies available in the computer networking industry. However, there is another category of threat that may not be receiving the attention it deserves relative to the threats previously discussed. In particular, threats posed by people who have been intentionally given legitimate electronic access to the system, and are inside the electronic security perimeter.

Disgruntled Employees – a conceivable source of attack is a utility worker whose normal job duties require access to the protected cyber assets, and who for some reason has decided to cause malicious harm or embarrassment to the employer, its customers, or to colleagues.

Employees can be a difficult challenge to security. They generally are well aware of the vulnerabilities of the power system, and have been given some degree of access in order that they can perform their intended functions. The limits to their access requirements are difficult to forecast – in an emergency the unforeseen often arises. As a result, access rights are often set wide with much attention paid to preparing for the unexpected.

This category could also include dismissed employees and employees involved in a labour dispute. An appropriate password management system could implement a policy that quickly removes the access privileges of this class of employees, and thereby promptly places them outside the electronic security perimeter. However, it should be kept in mind that such password management is effective only where it can be reliably implemented and there is foreknowledge of risk; there are many situations where is not possible to foresee the problem or not politically acceptable to take pre-emptive action.

Regular Employees – A threat category that deserves a much higher proportion of the attention the industry is giving to system compromise is that presented by regular employees going about their assigned duties, with no intention of causing any harm.

Such employees frequently make mistakes or take shortcuts that directly affect the security of the electric power system, most commonly by inadvertently tripping major generation or transmission assets. Comparatively little attention has been paid recently by the electric utility community as a whole to securing against the regular employee threat.

Typical mistakes and shortcuts a regular employ might make include:

- Isolating one subsystem for modification or test, and then inadvertently working on a neighboring system that has not been isolated.
- Isolating a subsystem and then inadvertently doing a test outside of the isolation boundary.
- Incompletely isolating a system so that a test results in some unplanned action.
- Isolating a subsystem to safely perform some job, then failing to completely remove the isolation when the job is finished.
- Making changes and then failing to properly verify that the change has been correctly executed.
- Making changes to facilitate some test activity, and then either forgetting to undo these changes when the work is complete, or undoing them incorrectly.
- Making changes that through error or inadvertence compromise the isolation of the system being worked on.
- Removing isolation before a subsystem that had been worked on completely resets.
- Installing a "backdoor" bypassing security to facilitate maintenance access.

While history has shown that the impact to power system security from regular employees is much less than intentional attacks potentially could be, history has also shown that regular employees cause incidents with an overwhelmingly higher frequency. Security risk can be defined as the cost of a security-related incident multiplied by the probability of that incident occurring. Using this definition to qualitatively compare the risk from regular employees to other threat classes, it can be seen that the comparison is between a very high cost multiplied a very low probability for a intentional incident against a low cost multiplied a high probability for an unintentional incident. As none of the values of these factors is known with any degree of certainty, the risks of each could very well be similar, so the effort expended on each should be similar.

Microprocessor technology presents a fantastic opportunity to greatly reduce the frequency in which this kind of security breach occurs. Unfortunately, the present momentum of security enhancements seems to be solely focused on defeating potential intruders and preventing regular employees from working outside of their discipline.

2.3 Effect of New Technologies

An additional incentive for expending more effort on securing against the threat posed by mishaps is the changing technology employed by protection and control systems. Over the long period of time previous technologies have been deployed, the design of the facilities and the work methods used have been tuned to provide relatively safe and secure means to perform the various activities needed. However, it appears that the future belongs to so-called station bus and process bus technologies. These communications network-based technologies present their own unique opportunities for commissioning and maintenance activities to affect the security of the power system.

Previous technologies provided many physical barriers to making the mistakes outlined earlier in this paper. For the most part, hardware is dedicated to particular and easily conceptualized functions. The hardware for different functions is located in physically separate locations. For instance, the protection relays for a line usually are on a panel or rack of their own. The protection relays for other power system elements, the RTU, the local control, the DFR, etc. are located elsewhere. The physical separation provides a barrier against worker activity affecting other equipment or functions. Re-testing following a change is limited to the equipment on that panel. Utilities often adopt a practice where temporary visual or physical barriers such as caution tape or plastic film are required to be installed masking off neighboring equipment prior to work. This forces focus on correctly identifying the equipment to be worked on while installing these barriers, and facilitates returning to the correct equipment after attention is temporarily diverted. Typically utilities provide all the test switches necessary to completely block the protection on the same panel as the relays, so that the worker can easily see that if all are open then the protection may be tested safely, and if all are closed the protection is restored. While these and other devices can lessen the security impact to tolerable levels, they are far from perfect.

Figure 1.
Security within new technology

With future technologies, many of the physical mechanisms used successfully with previous technologies become irrelevant. Physical separation is not provided to the same degree: an IED may protect multiple elements, and may in addition implement the RTU function, local control, DFR and more. If one is revising an RTU setting in an IED, there is a valid concern that the protection could be inadvertently affected. Is it then necessary to re-test the protection? A Merging Unit may supply data to three or more IEDs. If a change is made to a merging unit, is it necessary to take all three IEDs out of service and re-test them? Using caution tape to mask off neighboring equipment will have no value if access to the relay is via a LAN that could equally provide connectivity to another relay in the station. The worker may not even be at the station; changes may be initiated from a remote engineering office, in which case there is the concern whether a change or test is even to a relay at the correct station. FT type blocking switches are of course unusable on GOOSE trip signals. Equivalent blocking could be provided with the IED configurable logic, but can these be trusted when a new and therefore untested configuration is downloaded to the IED?

These future technologies can however provide other means to achieve or even surpass the security provided with previous technologies, provided these means are fully thought out and carefully implemented. For instance the IEDs and/or their setup programs could be designed such that setting modification or test initiation is permitted only after two different people have authorized the activity, a technique that in other industries is referred to as double custody. The immutable base firmware can be designed to implement independently of user settings virtual devices that completely and securely block the relay, and provide positive indication of the relay's blocked/unblocked state. Many activities may be disallowed by the IED when it is not blocked. Features may be provided that prevent the blocking being removed should doing so directly result in control action such as tripping. Even better, features may be implemented that remove the requirement for workers to access the system at all for many activities.

3. Standards Overview

World events over the past years have placed increasing focus on critical public infrastructures, like public works (water/waste water) and bulk electricity systems, and the importance of their security and availability. The events of September 11th, 2001 opened a whole new dimension of concerns for public infrastructure – no longer was interruption of these key systems solely the result of unexpected equipment failures or natural occurrences, but also intentional and malicious acts of human beings. Widespread power system outages, like the August 2003 Northeast blackout, heightened awareness of the necessity of a reliable bulk power system, and the ramifications that result when the power system is unexpectedly unavailable for long periods.

There are a number of standards, both officially published as well as in draft that deal with the issue of security of so-called electronic assets considered critical to the safe and reliable operation of bulk electricity systems. There are also a number of key industry working groups addressing issues related to cyber security for electric utilities

3.1 NERC Critical Infrastructure Protection (CIP)

NERC Critical Infrastructure Protection standards outline the security requirements for Critical Cyber Assets. Critical Cyber Assets are essentially any programmable electronic devices or communication networks that if damaged or otherwise made unavailable may impact the safe and reliable operation of the associated bulk electricity system[1]. Access to these Critical Cyber Assets is broken down into both the physical security of the installation housing these assets, as well as the electronic access (i.e. communications) to these assets.

NERC CIP is broken down into the following sections:

CIP Standard		Scope	Technical/Procedural /Documentation
CIP-002	Critical Cyber Assets	Identification & enumeration of critical cyber assets	D
CIP-003	Security Management Controls	Development of cyber security policy, including auditing	D
CIP-004	Personnel & Training	People authorized to access critical assets must be trained on security policy, having deeper background checks	P
CIP-005	Electronic Security	Electronic Security Perimeter and Electronic Access Controls	T,P
CIP-006	Physical Security	Physical security and access controls around Critical Assets	T,P
CIP-007	Systems Security Management	Security controls to detect/ deter/prevent compromise of Critical Cyber Assets	T,P
CIP-008	Incident Reporting	Identification, classification and reporting of Cyber Security incidents	P
CIP-009	Recovery Plans	Restoration of Critical Cyber Assets following compromise of the asset(s)	P

Table 1.
NERC Critical Infrastructure Protection Standards CIP-002 through CIP-009

In the above table, the focus of each section can be classified as Documentation, Technical or Procedural. Documentation refers to exercises in identifying or enumerating key pieces of information related to critical cyber assets. Sections with a Technical focus deal with actual functionality of devices and technologies within secure cyber assets. Procedural sections speak to organizational and process requirements for utilities and how personnel deal with and access secure cyber assets.

3.2 IEEE Power Engineering Society (PES)

Following the release of the NERC CIP standards, and the certification of NERC as electricity reliability organization for North America by the Federal Energy Regulatory Commission there has been a significant amount of activity from several Subcommittees within the IEEE PES.

Power System Relaying Committee (PSRC)

The Power System Relaying Committee Working Group C1 is developing a report covering issues related to cyber security for electronic communications access for protective relays. The document is intended to educate those individuals implementing or using electronic communications to access protective relays.

Power System Substations Committee (PSCC)

The Power System Substations Committee Working Group C1 is currently finalizing Standard P1686: Standard for Substation IED Cyber Security Standards. This standard defines the functions and features needed to accommodate critical infrastructure protection programs. In particular, it outlines the security requirements for access, configuration, upgrading and data retrieval for substation IEDs (including RTUs) and presents a compliance table for users to include in RFI/RFP documents.

Power System Communications Committee (PSCC)

The purpose of the PSCC Security Assessment Working Group has been established to develop methods for utilities to assess information security risks. These efforts will be closely coordinated with the on-going work on security standards for power system communications in other standards activities.

3.3 IEC Technical Committee (TC) 57

IEC TC57 WG15 has been commissioned to recommend or supply standardized security enhancements as needed to other TC57 WGs, to secure the information exchange for tele-control applications through enhancements to the IEC TC57 protocols including IEC 60870-5 and its derivatives (e.g. DNP), IEC 60870-6 TASE.2 (a.k.a. ICCP), and IEC 61850.

4. Authentication

Authentication is the process by which the identities of the parties involved in a transaction are verified by some trusted source or mechanism, and to establish which privileges those parties have within the transaction. In the context of protective relaying, the real goal of authentication is two-fold:

1. Verify the identity of the user who will be accessing the protective relay in question, and to define what features and functions they will be allowed to access or execute.

2. Verify the identity of the end relay that the user wishes to access and work with.

Authentication is a typical function of life in modern society. Examples of user authentication in day-to-day life include logging in to a computer network at the office, accessing voicemail messages and banking via an ATM. All of these examples feature the same two-step identification: the user must provide both a "name" (login ID, voicemail box, ATM card) and a secret piece of information or "key" (password, PIN) that is associated with the name given that proves the individual requesting access must be the true individual.

Typically, the process of authentication involves establishing a session, where the two parties exchange identification credentials and create a trusted communications channel between them. A key feature of most sessions is the inclusion of an expiry time that requires the parties to re-establish their credentials in order to resume communications. This prevents potentially malicious parties from using an old set of credentials to initiate communication sessions by posing as a trusted party.

Authentication mechanisms can be very simple, as the user ID/password schemes above, or they may be very complex, multi-realm distributed authentication schemes such as Kerberos.

A simple analogy to describe Kerberos is riding on most public transit systems. The first step in the authentication process is to provide a set of valid credentials, in this case a transit pass and photo ID. This validates that the rider is (1) who they claim to be and (2) that they have a valid fare to ride the system. Once inside the system, a transfer can be obtained that allows the rider to go between different routes (say from a subway to a bus) without having to provide all of the initial credentials each time. The transfer normally includes a time stamp that invalidates the transfer after a preset time and forces the rider to "re-authenticate" to re-enter the transit system and prevents other users from riding the transit system using a discarded transfer.

4.1 Authentication for Power System Protective Relaying

The Requirements for an Authentication Mechanism

Authentication, as defined previously, is any mechanism for ensuring that the parties involved in a communication transaction are identified correctly. In the case of protective relaying, this would predominantly be engineering or maintenance staff accessing IEDs to load or update settings, commission or re-verify protection or download diagnostic information. It is therefore necessary, for the reasons discussed in previously, to absolutely verify both the identity of the person who wishes to access the IED and the correct IED has been accessed. Again, for the purposes of this discussion it is assumed that the individual requiring authentication is already within the electronic security perimeter of a given station.

Authentication is typically done by comparing information sent by one party against information generated internally by the other party, using some secret information based on an agreed upon algorithm. The secret information would not be easily discernable by an outside party by altering the information sent via the communications link based on an agreed upon algorithm.

Any authentication mechanism within protective relays must meet the following requirements and constraints:

- Any authentication algorithm running within the IED must not impact the fundamental performance of protection elements, logic execution and high-speed, time critical, communications (e.g. IEC61850 GOOSE).

- The addition of any authentication algorithms must be tested to ensure that the above requirement is not violated. This test must be done on an IED with the maximum feature set configured and running, with the injection of meaningful signals including AC quantities, contact inputs and communications messages a must. Tests should be run both in the steady state as well as for typical fault cases with performance verified for each case.

- The authentication mechanism must prevent an unauthorized user from using historical data to decode the secret information used in the authentication mechanism, or from using past authentication credentials to masquerade as a valid user to gain access to the IED.

- The authentication mechanism should not only use key secret information about the user to be authenticated, but ideally information for both the user and the given IED to generate a set of credentials for the transaction.

- The IED configuration and access software should require these credentials to be valid for the given IED before allowing the user to connect to the device. Credentials that are not valid for the desired IED should prevent the user from connecting to the device.

- The IED should keep track of the credential information used for each access session. The information should allow forensic examination of the individuals that accessed the IED based on the credentials.

It is possible to use the basic principles of cryptography to take key pieces of information and use simple cryptographic algorithms to generate these secure credentials for authentication. While the algorithms and keys themselves may not be as strong as those typically found in the world of computer security, additional strength can be obtained by the relative obscurity of the IED secret information used in the creation of credentials.

4.2 IED Passwords for Security and Authentication

Passwords for Security

Many standards mandate the use of "strong" passwords within IEDs as an absolute requirement for security. These strong passwords are usually defined as having at least 8 characters, with a mix of upper case letters, lower case letters, numbers and special characters. While this mandate makes sense at first glance, there are a number of issues that need to be considered before simply assuming that strong passwords will be the panacea for security issues.

- Strong passwords, by their very nature, must not be easily associated with any human discernable information to prevent compromise via dictionary attacks or so-called social engineering attacks. This also means that the password is not easily remembered by the human beings that are required to use it, the end result of which is that the password will likely be written down somewhere thus violating a fundamental rule of password security.

- Passwords, strong or otherwise, should be unique for each IED within a given station. In a small distribution station there may be only a few IEDs but in a large transmission station there may be hundreds of individual IEDs and therefore potentially hundreds of individual passwords. Even if the passwords were not strong, it is unlikely that any human being would remember every password and therefore the result is again passwords being written down.

Password management also presents a number of issues.

- In order for passwords to be truly a mechanism for security, they should be changed periodically or in the event of staff turnover. This proves to be a significant challenge to execute in a real-world utility. As an example for calculation, say a given utility has a total of 100 critical stations, and an average of 100 IEDs in each of these critical stations. Assume that the average time to drive between any two stations is 2 hours and that each password change takes 10 minutes, including the time to actually change the password plus fill out the required documentation. Also, assume that one full-time employee (FTE) is defined as 1920 hours/year (40 hours/week, 48 weeks/year). The total time required for password management is 1865 hours/year, or 0.97 FTE. In other words, one employee would do nothing for the entire year, year after year, but drive between stations and change passwords. This is assuming there is only one password to change, but the reality is there are often multiple passwords within IEDs, and therefore the amount of labour involved in password management increases accordingly.

- The solution to the above issue would seem to be somewhat alleviated through the use of remote password management, however there are a number of issues with this strategy. The loss of communications between a remote site and the password management system renders the system ineffective. Additionally, any system used for remote password management must be at least as secure as the system where the passwords are to be managed. A compromise of the remote password management system could result in the compromise of all of the IEDs managed by the system, potentially making it impossible for any legitimate users from accessing the IEDs.

4.3 Passwords for Intrusion Detection

Often, the strength of passwords within protection IEDs is a source of debate and specification games. One could argue the perceived strength of one password paradigm versus another and the absolute superiority of one over the other. In reality, regardless of the password paradigm chosen, having relatively strong passwords does have certain advantages, particularly in terms of improving the probability of Intrusion Detection (ID) systems detecting unauthorized access attempts from internal and external hackers attempting brute force attacks (e.g. dictionary attacks).

As the number of password permutations is increased, eventually the point is reached where the increase in security does not justify the increased difficulty of use. Calculation of the probability that a time-limited attack is defeated is illuminating. Consider the following three password paradigms:

	Type 1	Type 2	Type 3
Password Length:	6	8	10
Characters:	10 (Digits Only)	70 (Alphanumeric)	10 (Digits Only)
Number of Permutations:	1×10^6	5.8×10^{14}	1×10^{10}
Time/Attempt:	60 seconds		
Attack Duration:	1 month		
Probability Attack Defeated:	95%	99.999999994%	99.9996%

Table 2.
Examples of password paradigms

In the table above, the assumption is that the attacker tries passwords in some sequence that avoids repetition. The Time/Attempt is chosen to ensure that any invalid password monitoring functions within the target IED will not be asserted. Some IEDs implement a function to detect a certain number of invalid password attempts within a given time window. This function will typically generate an alarm event that can be passed to a SCADA or Network Management System and may even close the affected communications port for a given time, thus increasing the amount of time needed to break the IED password.

Again referring to the table above, the attacker is limited to the maximum time duration shown to prosecute the attack. A hacker must open a communications port continuously during the attack. The risk is that this open communication port to the outside world may be detected as suspicious by an ID system. The best result for the hacker is that the port is closed and access is no longer available; the worst result is the communications are traced back to the origin and the hacker is caught.

In the above example, it would appear obvious from first glance at the number of permutations that Type 2 is the best password mechanism, with Type 3 being a distant second and Type 1 apparently completely useless. Often individuals will state this to be the case, however before judging the suitability of these password models, one must consider the whole system and process for accessing IEDs, including in the context of ID systems. Looking at the probability that an attack is defeated, it can be seem that the advantage of Type 2 over Type 3 is a negligible 0.0006%, and that even the simple Type 1 scheme gives pretty good security.

4.4 Passwords for IED Authentication

A different perspective on passwords would be to look at them as an authentication mechanism not to identify the human user, but rather authenticate the identity of the end IED that is to be accessed. The rationale behind this is simple: a user may be able to access any IED within a station via a local substation network such that the user may not even be in front of, or potentially in the same building as the protection to be worked on. Without clear authentication of the end IED to be accessed, it is quite possible that the user may inadvertently connect with an IED other than the intended one. The result may be maintenance actions performed on the wrong protection leading to unexpected power system outages, or settings being loaded on to the incorrect relay potentially causing either a failure to trip or overtripping.

By assigning unique passwords to each device, a level of protection against this type of security breach can be obtained. In order to have unexpected or undesired outcomes from relay setting and maintenance, the user must not only connect to the incorrect device but also provide the password for the same incorrect device. Inadvertently connecting to the wrong device and providing the password for the correct device will generate an error that forces the user to closely examine the connection they are attempting.

5. Encryption

Encryption, by contrast, is a set of mathematical algorithms that are used to encode information to be transmitted over communications media so that the information is unusable except for those parties involved in the transaction. There are two methods of providing encryption: symmetric (private key) and asymmetric (public key). This is done to ensure confidentiality and integrity of the data transmitted.

Symmetric encryption uses a common secret key that both encrypts and decrypts the information to be transmitted securely over an insecure communications link. The secret key can only be used to decrypt the information if an associated secret (i.e. a password) is provided by each key owner.

The risk in symmetric encryption is that the key used for decryption must be transmitted over a potentially insecure link, making it possible to hijack the key during transmission creating what is known as a “man-in-the-middle” attack.

Asymmetric encryption, on the other hand, uses two separate cryptographic keys – one that is freely distributed and one that is kept secret. The public key is always used to encrypt the data and the private key is always used for decryption. The strength of asymmetric encryption lies in the fact that the public key can be easily generated when the private key is known, but it is computationally impractical to derive the private key by only knowing the public key.

The major disadvantage of public key encryption is that the private key must be securely stored and backed up, preferably in several locations. This is necessary as the private key (the actual electronic file) can never be recreated – if it is lost then a new private key must be created and a new public key derived and distributed.

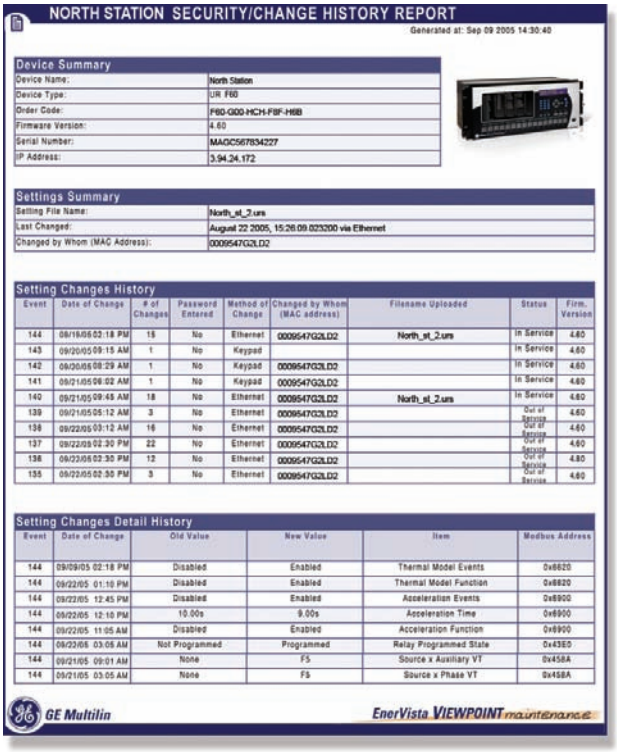
Real-time encryption and decryption of all communications between a user and an IED is not likely practical due to performance constraints, and within the electronic security perimeter its necessity is arguable.

6. Security Audit Trail

A sound security policy will minimize the possibility of unwanted access to the IED. Even so, it is necessary to plan for the unexpected. NERC CIP-003 mandates that electric utilities must have a process for managing changes in critical cyber assets, including hardware and software changes. In the case of power system protective relay IEDs, an electronic log within the IED that is dedicated to storage of security events is an essential tool for detecting configuration changes and an aid in the post-mortem analysis of a breach or recording the results of a penetration test. The following events should be time-stamped and logged:

- Attempted and failed access
- Password change
- Download of settings
- Download of firmware
- Deletion of a record (sequence of events, etc.)
- Security log retrieval
- Time and date change
- Factory service access
- IED out-of-service / IED-in-test
- IED powered down / IED powered up

Access to this log should be restricted with a separate password required for retrieval. It should not be possible to delete the log under any circumstances even through a firmware upgrade.


NORTH STATION SECURITY/CHANGE HISTORY REPORT

Generated at: Sep 09 2005 14:30:40

Device Summary

Device Name:	North Station
Device Type:	UR F60
Order Code:	F60-G00-HCH-F8F-H6B
Firmware Version:	4.60
Serial Number:	MAGC567834227
IP Address:	3.94.24.172

Settings Summary

Setting File Name:	North_st_2.urs
Last Changed:	August 22 2005, 15:26:09.823200 via Ethernet
Changed by Whom (MAC Address):	0009547G2LD2

Setting Changes History

Event	Date of Change	# of Changes	Password Entered	Method of Change	Changed by Whom (MAC address)	Filename Uploaded	Status	Firm. Version
144	08/18/05 03:18 PM	15	No	Ethernet	0009547G2LD2	North_st_2.urs	In Service	4.60
143	09/20/05 09:15 AM	1	No	Keypad			In Service	4.60
142	09/30/05 08:29 AM	1	No	Keypad	0009547G3LD2		In Service	4.60
141	09/21/05 06:02 AM	1	No	Keypad	0009547G2LD2		In Service	4.60
140	09/21/05 09:48 AM	18	No	Ethernet	0009547G2LD2	North_st_2.urs	In Service	4.60
139	09/21/05 05:12 AM	3	No	Ethernet	0009547G2LD2		Out of Service	4.60
138	09/22/05 09:12 AM	16	No	Ethernet	0009547G2LD2		Out of Service	4.60
137	09/22/05 02:30 PM	22	No	Ethernet	0009547G2LD2		Out of Service	4.60
136	09/23/05 02:30 PM	12	No	Ethernet	0009547G2LD2		Out of Service	4.60
135	09/23/05 02:30 PM	3	No	Ethernet	0009547G2LD2		Out of Service	4.60

Setting Changes Detail History

Event	Date of Change	Old Value	New Value	Item	Modbus Address
144	09/09/05 02:18 PM	Disabled	Enabled	Thermal Model Events	0x8820
144	09/22/05 01:10 PM	Disabled	Enabled	Thermal Model Function	0x8820
144	09/22/05 12:45 PM	Disabled	Enabled	Acceleration Events	0x8900
144	09/22/05 12:10 PM	10.00s	9.00s	Acceleration Time	0x8900
144	09/22/05 11:05 AM	Disabled	Enabled	Acceleration Function	0x8900
144	08/22/05 03:05 AM	Not Programmed	Programmed	Relay Programmed State	0x43E0
144	09/21/05 09:01 AM	None	F5	Source x Auxiliary VT	0x458A
144	09/21/05 03:05 AM	None	F5	Source x Phase VT	0x458A

GE Multilin

EnerVista VIEWPOINT maintenance

Figure 2.
Security audit trail's found in software such as GE Multilin's Viewpoint Maintenance, can automatically track the details of settings changes to your relays.

7. Permission from a Controlling Authority

It is a common practice among utilities today that work is carried out in the substation only with the permission of a controlling authority, and usually work is scheduled and approved weeks in advance. Even so, events can arise in the power system at the last minute such as a forced outage of a transmission line that can make the approved work an unacceptable risk. The controlling authority is the sole entity with the required information on the overall status of the power system needed to make such assessments at the time the work commences.

Under a typical scenario, a maintenance person arrives at the substation. He notifies the system operator, usually by telephone, of his arrival and requests permission to carry out some activity on a particular system, nowadays taking the form of a multifunction IED. The activity can involve removing the IED from service. The activity can also require some actions by the system operator such as opening a particular breaker or taking a particular line out-of-service. During the maintenance period the system operator may inhibit alarms or status associated with the IED under maintenance. The IED itself may provide some indications to the operator of its operational state (out-of-service, critical failure, etc.) although this is often not the case with older systems. On completion of the task, the maintenance person will contact the operator to indicate that the system has been restored to service.

A serious exposure arises when the maintenance person, through negligence or inexperience, carries out his activity on the wrong system. The consequences of such a mistake can result in an element of the power system being left unprotected. Alternatively, it can result in an unexpected false trip of a system element that is currently in-service. Such events have been known to result in the loss of the entire substation (e.g. a station is fed from two lines – one line is removed from service for maintenance – the maintenance personnel mistakenly initiate a test trip on the line that remains in-service). Finally, the IED may be configured with the wrong settings, resulting in a subsequent failure-to-trip or false trip. The problem becomes more likely in the case that IEDs may be controlled or configured over a substation LAN allowing access to any IED in the substation. Requiring unique passwords for each IED in the substation could mitigate this problem.

A proposed improvement to this solution is to place the IED access control function under SCADA supervision. Such a scheme can be readily implemented in modern IEDs. A command from SCADA opens a time-window within the IED wherein passwords are accepted and access to the IED is granted. Outside this window, access to the IED is rejected, regardless if the correct access password is provided. The window would expire after a fixed period of time (say 8 hours). Under such a scenario, the maintenance person informs the operator of the device to be accessed. The operator sends a command to the IED via SCADA. All other IEDs in the substation reject any access attempts. Access to the wrong IED would require both the operator and the maintenance person to make the same mistake. A failure of SCADA would prevent password access to any of the IEDs in the substation, however, in this instance, arguably the primary concern should be the timely restoration of the SCADA system.

Importantly, this solution also provides an additional layer of security against malicious attacks. The SCADA system typically utilizes a secure, dedicated communications network which is unlikely to be compromised by an external hacker or accidentally through misadventure of internal personnel. It is also highly improbable that a hacker would initiate an attack on a particular IED at the same time that maintenance is occurring.

8. Inherent Limitations of IEDs

Microprocessor-based protective relays can be considered as highly specialized embedded systems, optimized for the execution of specific tasks, primarily to run power system protection algorithms and associated programmable scheme logic with high speed and determinism. This often forces other services, including non-critical communications to run at lower priorities than the main protection tasks. Many factors must be balanced, including processor clock speed (related to heat dissipation), processing margin and available data memory. This balancing essentially forces limitations on any advanced communications functions, such as secure session management and data encryption. Even in the fastest microprocessor designs, assuming there is adequate processing margin, these functions may add significant and unsatisfactory delays to the speed at which communications can occur.

This is not to say that certain key concepts from the realm of security, including authentication and cryptography, can not be applied to the existing installed base of protection IEDs.

8.1 Restrictions on Traditional Authentication Mechanisms

Often, it is assumed that use of industry standard security mechanisms are either impractical, or impossible to implement in protective relaying IEDs. This in the sense of certain mechanisms, for example strong encryption of communications messages, may impose too great a demand on microprocessors resulting in degraded system performance. One could argue that new IED technology may render some of these arguments obsolete. However the current state of most utilities is that there are hundreds, even thousands of protection IEDs based on current technologies to which these arguments will still apply. It is not practical, both in terms of economics and timely execution, to assume that existing protection IEDs would be swapped out immediately should a new technology be available tomorrow, next month or next year.

It is possible to provide reasonably good security and authentication in protective relaying IEDs without necessarily trying to apply existing technologies and mechanisms from the computer security world-at-large. Rather, the underlying principles and paradigms for these mechanisms should be examined and then a new set of technologies and mechanisms developed that can be applied to current and future protective relay technologies without requiring significant hardware upgrades or change-outs of existing IED installations.

9. Conclusions

All power systems are potentially vulnerable to compromise, both physical and electronic, resulting in undesired effects on power system stability and reliability. Potential activities may originate from either internal or external sources, and may occur due to malicious intent from unauthorized individuals or an inadvertent action on the part of legitimate users. Security from external electronic threats outside of the electronic security perimeter can be achieved using current computer security technologies but a separate mechanism is needed to prevent legitimate users from accidentally compromise protection systems. While modern IEDs may not be capable of implementing advanced authentication and encryption technologies, the basic principles that these technologies are based on can be adapted to be applied on existing protective relay technology to prevent power system disruption through legitimate user misadventure.

10. References

[1] NERC Critical Infrastructure Protection Standards CIP-002 through CIP-009.