



by Herb Falk, SISCO, USA

# The evolution of threats is occurring rapidly in cyber security.

## Cyber Warriors: Learning from Physical Warfare

Valid issues are often raised about the cost of implementation of cyber security. However, if you continue to read the article there are some non-high tech actions that can be taken in order to provide better protection. In this regard, the issues of cyber security are often the same issues as physical security:

- How do you detect that a person is not who they claim to be? In both the physical and cyber security realms, this is referred to as Identity establishment or Authentication.
- How do you identify that a person has the right to access certain facilities? Access control and privilege management are very similar.

*Certain information needs to be hidden.*

So why is the need for cyber security so hard to convince people or companies? The answer may be found in something as simple as the history of human warfare. Human physical aggression or war has been evolving since there has been more than one human being. The reality is that the evolution of physical security, and its acceptance, has been millenniums in the making. In comparison, cyber security has only really been an issue since the advent of the computer digital modem (circa 1958). However, the evolution of threats is occurring more rapidly in cyber security than it did in regards to physical security. Therefore, the world has less experience in dealing with cyber security and the need to counter new threats occurs at a more rapid rate. The concepts

to counter cyber security threats are re-treads/re-casting of concepts developed from physical security but using different technological solutions.

### Perimeter Security is not enough

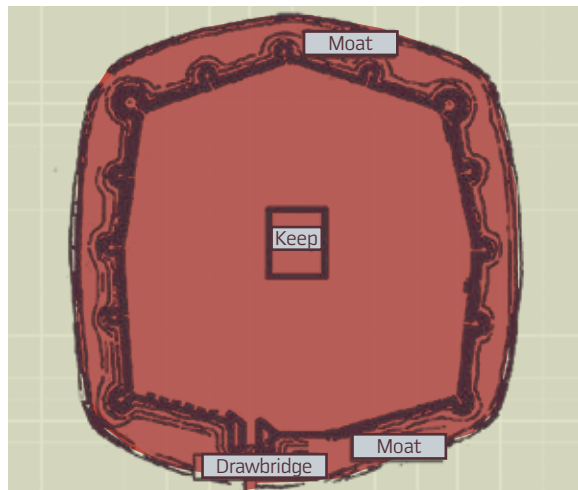
The North American Electric Reliability Corporation (NERC) issued a set of Critical Infrastructure Protection (CIP) Cyber Security Standards. Although these are North American standards (Canada and Mexico are indirectly affected), the core premise of these standards is to define security perimeters and to implement security methods/technologies at those perimeters. However, medieval castles offer a historical reference of why perimeter defense is not enough. (Figures 1,2)

Castles were designed to allow smaller forces to defend it from much larger assault forces. Original castle design, for better or worse, started out with a two perimeter defenses: the moat and a rampart. However, designers quickly found that a single perimeter was not sufficient. As their designs evolved, interlocking parapets were added and there were inner and outer sets of walls created. This was done so that the inner wall could lend support to the defenders of the outer wall. The side benefit of the onion approach was that attackers were required to mount a more complicated assault utilizing more resources. If you had a choice to defend yourself in one of the two castles shown in the figures, which would you choose?

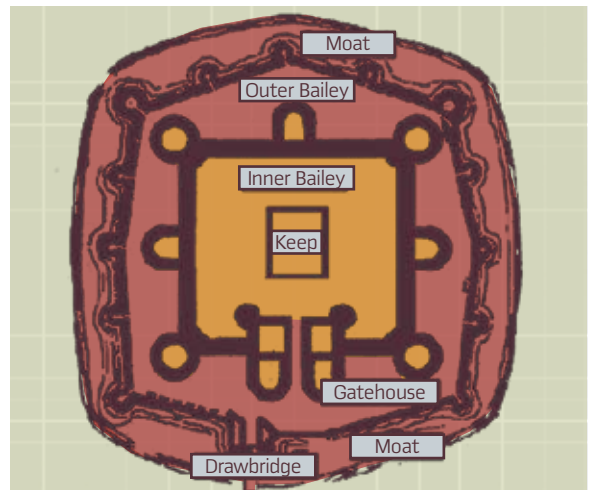
The analogies between cyber security and castle defense are too obvious to be ignored:

- Properly designed defenses can allow smaller forces to defend their domains against superior forces that have more resources, in addition to time and the element of surprise on their side.
- Diligence is required. Sentries must be on the lookout for signs of a possible attack.
- It is rare that the best defensive system can withstand a sustained attack. Resources are drained, and weaknesses are usually discovered and exploited.

## 1 Original Castle Design



## 2 Improved Castle Design



*Defenses are built to protect critical resources.*

However, there are differences between castles, or forts, and cyber security. The greatest difference is the size of the geographic areas that need to be defended. Within a vast geographic area, there are defendable assets such as substations, generation stations, and control centers. There are mitigating factors that need to be considered as well.

#### Properly Designed Defenses

**TRUE or FALSE:** Is it truly possible to secure ALL of one's cyber assets in a utility environment?

This is a simple testing example of a TRUE or FALSE question. In basic test taking skills, students are often told to be careful about words like ALL, NEVER, ALWAYS, or IMPOSSIBLE, when the answer is almost always FALSE. Just as in test taking, there are no absolutes in the cyber security arena. Besides the absolute testing rule, there are several factors that contribute to the answer of FALSE in regards to cyber security. One of the most important assumptions, for cyber security, is that the communicating devices are physically secure. With the exceptions of utility control centers, what type of physical security is really available or implemented? Can we claim that utility cyber assets are physically secure (*this is a rhetorical question*)?

The cyber assets within a control center and generation stations have the highest probability of being physically secure. These are the castles of a utility. Control centers mimic the rings of physical access. There is the entrance to the control center (e.g., the Drawbridge). There is a lobby (e.g., the Gatehouse) where visitors must be given clearance to proceed beyond the first ring of physical security. Once past that ring of security, critical assets typically are locked in a further restricted asset control room (e.g., the Keep).

Can we make claim that substations are physically secure? Substations typically have fences, a padlocked gate, and, if you are lucky, video surveillance cameras. Can we honestly believe that these "weak" solutions really constitute physical

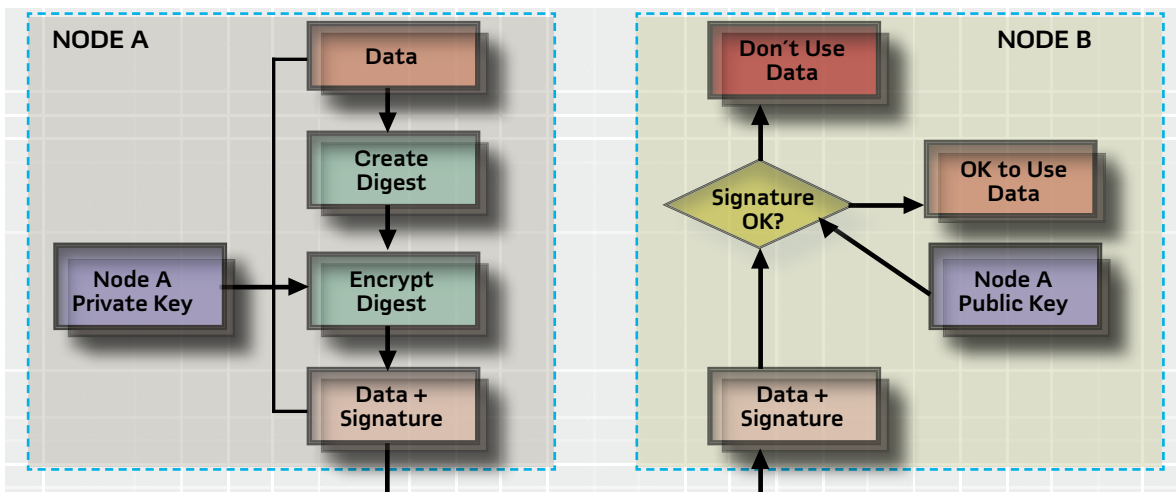
security? If one truly evaluates the situation, we know that padlocks and fences can be easily cut or breached. Typically, video cameras are not monitored by personnel in real-time. In many cases, the forensic evidence collected by video cameras can be used to prosecute the perpetrators only if they are caught. Although the situation seems like doom and gloom, there are some simple low-technology solutions that can be used to improve the substation physical intrusion detection problem. Since it would be very costly to prevent physical intrusion, it is important to be able to detect the intrusion and to react as rapidly as possible. To accomplish the objective of detection, we need to consider monitoring the access points into the substation, substation buildings, and automation panels. There are already communicating assets, or we wouldn't be concerned about cyber security, that are probably more than capable of monitoring a couple of additional inputs and sending this information to the SCADA or other peer client system.

Once the peer system is delivered the information, having trained personnel to react to the intrusion alarms is equally important to the monitoring inputs. Grid operators (e.g., EMS Operators) are not responsible for this type of activity, as their responsibilities are related to the proper operation and stability of the electrical transmission or distribution networks. Therefore, this type of monitoring needs a dedicated staff trained to respond to un-scheduled intrusions.

It is clear that the personnel that supervise, and are trained to monitor for the intrusion, are not the same individuals that will be the on-site initial responders to the intrusion. The on-site responders will be maintenance depot personnel or geographically, local law enforcement. In order to minimize the time of reaction of the initial responders, closely coordinated procedures need to be developed between the utility and the initial responders. In the case of substations and distributed cyber resources, what is the equivalent to

Herb Falk has worked on numerous projects from the application of information systems and real-time communications technology, to automated manufacturing, electrical distribution and automation & power quality monitoring. He has been involved in the determination of communication security needs and standardization since 1996. In 1998, Mr. Falk prepared the security specification for UCA. Shortly thereafter, he 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. He is actively involved in security efforts within IEEE .

### 3 Digital signature algorithm



the castle's keep? This represents the last line of defense. These are the actual cyber assets themselves, the intelligent electronic devices (IEDs). Once there is physical access to the IEDs and/or the communication infrastructure, there is no more physical security (e.g. the castle keep is being attacked). However, there could still be tamper detection provided.

Consider that your security perimeter has been breached. Even with detection and "quick" initial response, cyber assets may be exposed, especially the communication infrastructure itself. For utilities, it is important to protect access to the communication infrastructure. This is very similar to protecting access to paths of trade routes in olden days.

**Diligence**

Castles and forts have guard towers and sentries. There are several purposes for the sentries that have a direct correlation to functionality in the cyber security world.

One of the jobs of sentries is to challenge approaching people and to insure that their identity is established. Once the identity is established (e.g., friend, foe, or other), the sentries determine which physical security perimeters the person is granted access to or what alarms/alerts to generate. The concepts of challenge, identity establishment and access control all have equivalents in the cyber security world

**Identity Establishment**

In order to challenge and establish the identity of a communicating entity, there needs to be a method of establishing identity. In medieval times, establishing a person's identity was based upon prior knowledge or official papers/credential of introduction. Of the two methods, the use of the digital equivalent to official papers of introduction is the most interesting. Each type of "credential" has an equivalent challenge mechanism.

Username and password credentials are challenged through the use of a login challenge. The degree of security achieved with a password is directly related to the size of the password and the procedures implemented to respond to failed username/password logins. Cracking of username/passwords takes time. However, like castle sieges, the password will eventually be cracked. The appropriate designed defense is to prolong the attack, alert the sentries, and

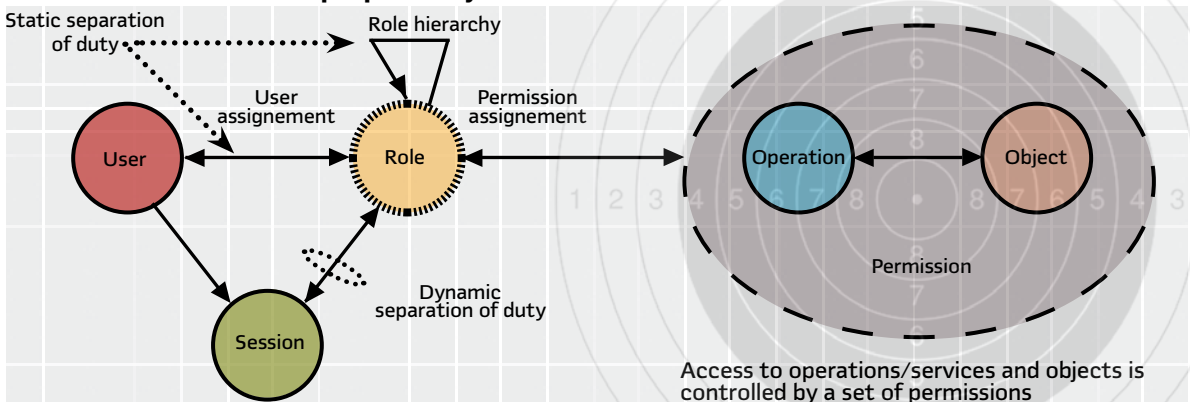


wait for the cavalry to arrive. To accomplish this, a pre-defined number of consecutive failed login attempts should trigger a delay for further login challenges for the challenged node. Simultaneously, some type of alarm needs to be generated. There need to be trained personnel that monitor for such alarms, and are responsible for generating the initial response. Such a defensive strategy provides adequate protection for username/passwords. However, username/passwords are useful for humans, but more appropriate digital techniques need to be used for cyber asset to cyber asset challenging.

The equivalent to a login for peer cyber asset challenging, is the Challenge Handshake Authentication Protocol (CHAP). There are various forms of CHAP but all have similar characteristics to PPP Challenge Handshake Protocol (RFC 1994). CHAP is used for the purposes of securing IEC 60870-5 and DNP. It works well for IEDs with low processing resources. The vulnerability window in using

Division of responsibility needs to be used to help recognize that access is based upon roles - commonly known as Role Based Access Control (RBAC).

**4 Current RBAC model proposed by IEC TC 57**



## 5 Explanation of Windows Vista Password Policies

Realtime  
community  
"Leading the Convergence" Vista

From: [http://www.realtime-vista.com/administration/2007/03/password\\_security\\_policy.htm](http://www.realtime-vista.com/administration/2007/03/password_security_policy.htm)

certificates are X.509 Certificates. The use of such certificates solves the formatting issues normally associated with the shared key in CHAP. However, work is still ongoing in order to manage the exchange of update of certificates for IEC 61850 and IEC 60870-6 TASE.2/ICCP.

### Access Control

In the medieval times guards, or sentinels, established the identity of a person and then either allowed or disallowed that person from gaining access to the physical asset that they had been commanded to protect. In the cyber world, access to cyber assets, information contained by those assets, and the services exposed by the assets also need to be guarded or protected. As in the olden times, division of labor/responsibility needs to be used to help categorize to what assets they could have access. As times have progressed, it has been recognized that access is based upon roles; not necessarily the social/military level achieved. This concept has been translated into what has commonly become known as Role Based Access Control (RBAC).

IEC TC57 WG15 is undertaking the work to attempt to standardize concepts in RBAC for the telecontrol protocols standardized within TC57. In the RBAC model, access to services and objects is controlled by a set of permissions. It is easy to think of permissions as categories such as the ability to read the contents of an object or write information of the object, determine the existence of information or to perform actions through the object. IEC TC57 WG15 is considering adding additional permissions such as the ability to: configure a device, create additional information objects, remove information that was created, assign permissions or security roles. The final set of standardized permissions may be expanded as needed by various standards. Permissions on objects are grouped into what is known as a role. Users are then enrolled to be members of a particular role/group.

Figure 4 depicts the hierarchy of roles/groups. What is unclear is that there is still ongoing discussion regarding whether the hierarchy implies inheritance. Inheritance of roles/permissions allows easier administration but also may allow unintended security holes. Consider the following example where Security Administrator role inherits privileges from the Configuration role - Table 1. Note that the Security Administrator role inadvertently has the read and write privileges. In order to prevent such holes from being created, new RBAC methodologies have users being members of multiple roles, instead of roles inheriting from each other. The same thought process applies to not having permissions inherit from the granting of other permissions.

### Alarms and Alerting

Medieval guards/sentinels reported "all clears" or issued alarms based upon intrusion or unauthorized access. In the



Many different utility assets can be the target of cyber attacks.

CHAP, is during the period of time between challenges. There are two other disadvantages to the use of CHAP: the disruption of normal communication flow (e.g., delays) while challenges are being resolved, and there is no easy mechanism to manage or formats for the shared keys required in order to make CHAP work. In order to close the window of vulnerability, CHAP morphed into the use of Digital Signatures. Digital signatures are the equivalent to responding to a challenge, but without an explicit challenge protocol. If one closely evaluates the algorithms for Digital Signature creation, the similarities with CHAP can be seen. However, the hash is signed through encrypting the hash with a private encryption key. The encrypted hash, normally referred to as a secure hash (SHASH), is then transferred along with the information over which the original hash was created. The receiver of the SHASH then uses the sender's public key to decrypt the SHASH in order to re-constitute the sender's original hash. The receiver calculates its own hash, using the same algorithm, and then compares the calculated versus re-constituted hash. If the two hashes match, the authenticity of the information and sender is established.

This digital signature methodology is used in the generation of the Message Authentication Code (MAC) that is used as part of the Transport Layer Security (TLS) Application Process authentication for IEC 60870-6 TASE.2 (e.g., ICCP) and IEC 61850, and others. Additionally, Digital Certificates provide an effective mechanism to transfer the required key information. The most prevalent standard format for digital



## IEC TC57 WG15 is attempting to standardize concepts in Role Based Access Control (RBAC).

cyber world, how can utility devices issue alarms and who will hear their screams for help?

Utility devices must “yell” or alert the fact of cyber intrusion through some form of communication protocol. Whatever is chosen, personnel must be present 24/7 to receive and respond to the alerts. Most utilities have an IT staff that is responsible for 24/7 monitoring/repair of enterprise level communication infrastructure. However, some utilities differentiate responsibilities for teleprotection communication to some other set of resources. Typically, it is the IT department that has the 24/7 monitoring capability. Therefore, utilities should evaluate having the IT monitoring center be responsible for monitoring for cyber intrusions in the protection/control world as well.

IT staffs are typically armed with network management tools. The tools typically use versions of the Simple Network Management Protocol (SNMP) to monitor routers and equipment. SNMP is typically used to monitor network infrastructure statistics (e.g., bandwidth use, hop delay, which Ethernet ports are active, etc). This is accomplished through the use of management agents that define the information to be exposed via SNMP. This combination allows the agent to monitor for local information and to report to the management tool. It is possible to conceive of security agents that detect cyber intrusion information and convey that information via telecontrol protocols or SNMP. At a minimum, the security agents/telecontrol protocol combination would need to have well defined standardized information that would be able to be converted into, and monitored by, IT network management tools. Currently, the standardized information definitions don't exist within field devices, and most IEDs do not implement the function of a security agent.

IEC TC57 WG15 is working to establish a standard set of security related information that should be monitored and captured by the local security agents. The intent would be that this information is then mapped into the appropriate protocol objects so that they can be communicated to the IT staff leaving the need to create a telecontrol protocol object

information into information that a network management tool can access. Many of the management tools allow plug-ins to be written. Either approach will provide the critical link required for cyber security intrusion monitoring in the far reaches of a utility.

### Resources and Time

A utility's business is to provide services and power to its customers, not to invest all of its money for cyber security. This simple truism leads to an alarming fact; cyber attackers may have more modern resources than utilities. Utilities must amortize and depreciate costs for cyber assets and utility devices. Attackers do not have this encumbrance. This means that cyber attackers will probably have better computational cyber attack resources than utilities have to defend their assets. This seems like a dire situation. However, planning and providing protection against future attacks is also a business function. Unfortunately, this planning of needs for the next 5-10 years typically doesn't occur for cyber security assets. There are several reasons that lead to this trend: threat vectors and cyber attack technologies change more rapidly than computational technologies. These make prediction of future cyber problems difficult. Through the appropriate selection of password lengths, encryption key sizes, and encryption algorithms, cyber warriors can make choices that may be viable for several years; However, there are poor choices as well.

How long are your passwords? There is a large difference in the time it takes to crack a six character password versus a fourteen character password. The computer security groups for most financial portals require at least eight characters and the password needs to include letters and numbers. By increasing the number of characters and character selection for passwords, your protection goes up dramatically. It is probably advisable to start asking IED vendors to allow up to the maximum Microsoft Windows password size and character set. It is also important to evaluate how often IED passwords need to be changed as most IEDs don't force a time based change (Figure 4).

Besides mandating larger passwords that are changed more frequently, a cyber warrior can also select more modern encryption algorithms with larger than needed encryption keys. Several standards are taking a proactive action. As an example, IEC 62351-4 and IEC 62351-6 specify different levels of protection based upon internal substation use and external substation communication. Both specify the more modern, higher protection, less computational resource, Advanced Encryption Standard (AES). However, it is specified that AES256 be used for external substation communications. The standards also prescribe that AES128 may be used within the substation. The selection of the larger encryption key adds additional protection to the information conveyed over the communication links (e.g., possibly the internet) where attackers could leverage the most computational resources. The difference in cost, to implement AES128 or AES256, within an IED is low. The difference in the levels of protection is immense over the

**table 1** Example of Inheriting Permissions

Role	Desired permissions (rwvxcdes)	Permissions based on security from configuration role
Configurationstm	rwv-c--	
Security Administrator	--v-c--s	rwv-c-s

Security Administrator role inherits privileges from the Configuration role.

