SECURE ACCESS CONTROL FOR DISTRIBUTION SYSTEMS

Alex WANG
Cisco Systems – USA
alexwang@cisco.com

Walid ALI
Alstom Grid – Canada
walid.ali@alstom.com

Rik IRONS-MCLEAN
Cisco Systems - UK
rironsmc@cisco.com

ABSTRACT

The modernization of the power grid has great potential to improve operational efficiency with distributed intelligence and automation. However, with more and more control systems being interconnected, there is also greater risk that distribution systems could be compromised if not protected properly. This paper describes a comprehensive secure access control scheme to mitigate cyber incidents. The ultimate goal of the proposed solution is to ensure grid reliability via proper cyber security protections.

Security risk is the product of threat, vulnerability and consequence. Threat has been ever increasing as control functions expand to systems that are deployed on publicly accessible premises. The data network that supports distribution automation usually focuses on system connectivity. This could introduce vulnerability if security is not built into the design at the early phase of planning. Even more concerning is the fact that many existing deployments will continue to operate. These legacy systems are not capable of securing themselves, nor upgradeable. Adverse attacks could take advantage of these vulnerabilities and cause service disruption as well as information leaks. Modern cyber penetration technique makes it easy to present rogue devices as legitimate ones. System availability and operation privacy will be at danger when a system is compromised or a rogue device gains network access.

Vulnerabilities of distribution systems should be addressed holistically. A user accessing remote services, especially from public locations, should be authenticated by network. Two-factor authentication provides more secure safeguard than traditional single authentication scheme. For automation devices that do not have security capability, the network can profile these systems and establish security baselines. Operations of these legacy systems will be controlled based on the information learned by the intelligent network. The essence of this mechanism is device sensor capability as the network performs content inspection. In conjunction with operation policy management, insecure legacy systems are protected by the secure network.

Among the security triad CIA (Confidentiality, Integrity, and Availability), availability is more critical for distribution systems. Many are concerned about security complexity and potential service disruption due to tighter security measures. This paper describes a practical approach that could smoothly transition from an un-secure state to a relatively secure state. The introduction of security mechanisms are planned and deployed via several phases. Each phase adds new measures upon a previous baseline setup and situation awareness level.

INTRODUCTION

Today's electrical utilities face the demands of a rapidly transforming industry, including increasingly stringent security regulations and power grid management requirements. Identified as critical national infrastructure by most nations, utilities are under pressure to assure 24x7 reliability and availability of the power grid. As more and more control devices are interconnected in electrical power transmission and distribution networks, cyber security vulnerability from adverse attacks and unintentional operation mistakes become increasingly concerning. To meet these needs, utilities are focusing on improving grid security. And secure access control is a fundamental element to gain visibility and controls.

A number of security frameworks and guidelines exist today that should be incorporated into distribution systems designs [1-3]. Cyber security regulations for utilities further mandate strict security measurements in order to safeguard installations. The NERC CIP standards [4] in North America are the most prominent example. As of today, many power grids inherit security practice through obscurity. Admittedly, this principle suits for standalone proprietary systems. When distributed intelligence and controls involve multi-vendor systems, standards-based deployment becomes an important means to achieve interoperability between systems and devices. This is true for grid communication as well as for grid security.

SECURE MOBILE USER ACCESS

Distribution and transmission data communication is undergoing convergence of the SCADA and IT services network. For example, field technicians need to connect mobile PC or tablets to the secondary substations or AMI aggregation nodes for troubleshooting. In order to gain access to the network, field technicians need to be authenticated and authorized. An open connection without proper access controls allows malicious attacks to be launched easily. Even for authenticated users, human mistakes could cause unintended operations.

Therefore, it is critical to apply Role-Based Access Control (RBAC) so that the authenticated users are only given permissions defined by their job roles.

IEEE 802.1X is a prominent industry standard for port-based network access control. Until a user’s credentials and identity are successfully validated, the connected network port is disabled. This scheme is considered as a security best practice that un-used network access ports should deny services as the default setting; it has been adopted by relevant power grid security standards. IEEE 801.1X is based on a two-tier framework.

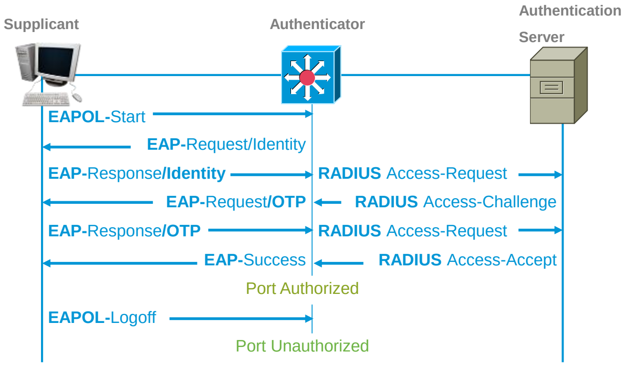


Figure 1 IEEE 802.1X

Within the 802.1X handshaking interactions, the user or client that wants to be authenticated is called a supplicant. The actual server doing the authentication, typically a RADIUS server, is called the authentication server. The device in between is called the authenticator. Most common credentials used by clients are user name and password which are centrally administered.

In certain high risk and high impact situations, a password alone is not secure enough. There are a number of techniques to crack or steal passwords. Two-factor authentication is a stronger approach to authenticate an identity using any two of these schemes: by something the user knows (such as a password or personal identification number), something the user has (a security token or smart card) or something the user is (a physical characteristic, such as a fingerprint, called a biometric). Examples include hardware tokens, digital certificates, and smart cards. Two-Factor authentication can also be provided by the use of PIN and phone to receive the one time passcode, without the complication of deploying hardware tokens and smartcards.

In today's diverse applications supported by distribution network, technicians, SCADA engineers, IT staff or even vendors need to access network resources over the same data network. Although IEEE 802.1X authentication secures the internal network by requiring employees to present valid credentials before accessing the network, provision must also be made for users without IEEE 802.1X supplicants.

Used as a fall-back mechanism to IEEE 802.1X, Web Authentication (WebAuth) provides supplemental authentication while maintaining the benefits of an IEEE 802.1X-protected network.

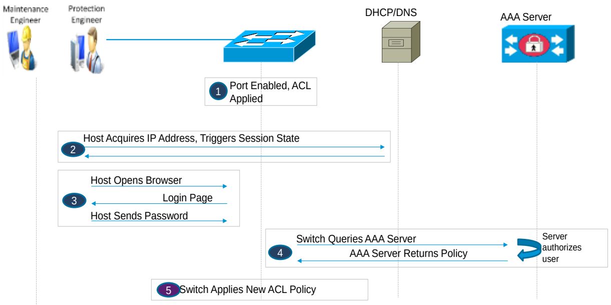

Maintenance Engineer
Protection Engineer
DHCP/DNS
AAA Server
1 Port Enabled, ACL Applied
2 Host Acquires IP Address, Triggers Session State
3 Host Opens Browser
Login Page
Host Sends Password
4 Switch Queries AAA Server
AAA Server Returns Policy
Server authorizes user
5 Switch Applies New ACL Policy

Figure 2 Web Authentication

With an IEEE 802.1X-enabled network, WebAuth begins after IEEE 802.1X authentication times out or fails. The network access node opens the port for configurable traffic types (for example, DHCP and DNS) required for WebAuth. The host requests and receives an IP address, triggering the session state on the port. The client host needs to open a browser. The network access node intercepts the host's HTTP traffic and presents the host with a login page. The user enters credentials on the login page. The network access node sends these credentials to the authentication, authorization, and accounting (AAA) server. The authentication server validates the credentials and sends back the user-specific policy that should be applied to the port. After this new policy is applied to the port, the host can access the network according to the assigned policy. Lastly, the access node redirects the host to the original web page.

WebAuth requires a web browser and there are multiple interfaces involved to get the authentication to complete. However, WebAuth is a viable alternative solution when IEEE 802.1X is not supported by the client host.

DEVICE ACCESS CONTROLS

The essence of any grid automation solution is to provide near real-time information about the status, the health and performance of various assets within the power grid. The captured data is composed of operational and non-operational data. Operational data such as volts, amps, MW, MVR Circuit Breaker status, and switch position which indicates the status, loading and overall performance of the power apparatus. This data is time critical and is used to monitor and control the power system (e.g. opening of Circuit breakers, indication equipment failure). Non-operational data consists of information that indicates the overall health of the equipment (e.g. Circuit contact wear information). The data can be in the form of oscillographic event reports, sequence of events records, and security events. Non-operational data is used by the maintenance group for preventative, predictive maintenance, and condition monitoring of the power equipment. Due to the importance and the criticality of the data and the need to access it from various personnel with different roles such as SCADA Engineers, Protection Engineers and Relay technicians, the data needs to be transmitted and accessed in a secure and reliable manner. This should be done on a "need to know basis" and hence some kind of mechanism for authentication, authorization, auditing is needed before giving access to automation devices in the field, and the transmitted data needs to be encrypted to guarantee its integrity.

Transport Layer Security (TLS) is one of the Extensible Authentication Protocol (EAP) types. This protocol is similar to SSL (Secure Sockets Layer) and the way encryption is formed between automation devices and network access nodes. EAP-TLS is an IETF (The Internet Engineering Task Force) standard, and uses X.509 certificates. One major benefit of EAP-TLS is that it provides the ability to support mutual authentication, where the automation devices must trust the AAA server's certificate, and vice versa.

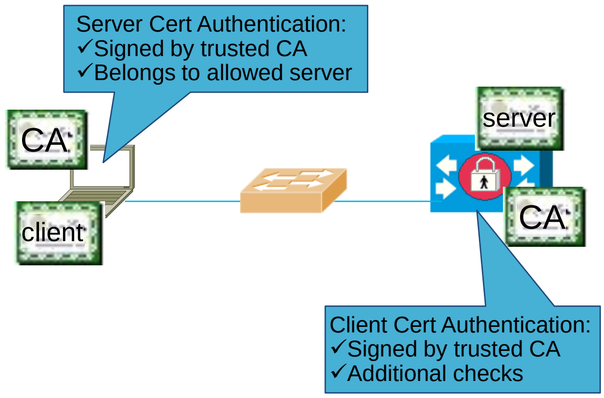

Server Cert Authentication:
✓Signed by trusted CA
✓Belongs to allowed server
CA
client
server
CA
Client Cert Authentication:
✓Signed by trusted CA
✓Additional checks

Figure 3 EAP-TLS

EAP-TLS authentication involves two elements of trust: The EAP-TLS negotiation establishes client trust by validating, through RSA signature verifications, that the client machine possesses a keypair that a certificate signs. This process verifies that the client is the legitimate keyholder for a given digital certificate and the corresponding user identification in the certificate. However, trusting that a client possesses a certificate only provides an identity-keypair binding. The second element of the trust chain in the EAP-TLS process is a mutually trusted third-party. Using a third-party signature, usually from a CA (Certificate Authority), the information in a certificate is verified.

EAP-TLS authentication is based on the 802.1X/EAP architecture. Many automation devices are not capable to support IEEE 802.1X due to firmware constraints or service disruption during an upgrade. An alternative solution to lack of 802.1X support is MAC Authentication Bypass (MAB). MAB is a MAC-address-based authentication mechanism. MAB uses the MAC address of the connecting device to grant or deny network access. To support MAB, the AAA server utilizes a database of MAC addresses for devices that require access to the network.

MAB requires an asset database as authentication repository. Until a central MAC address database of distributed system is fully populated and enabled, port security could be set on individual access node. With port security, network ingress traffic limits the MAC addresses that are allowed to send traffic into the port. At each access node, the permitted MAC addresses are specified and saved in a local data store. The access nodes do not forward ingress traffic that has source addresses outside the group of defined addresses.

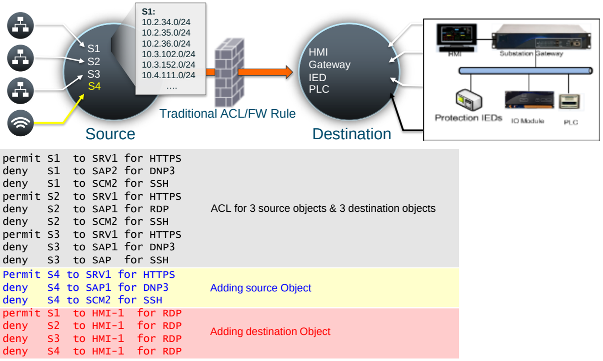
SERVICE-ORIENTED CONTROLS

The access control mechanisms described so far are safeguards which either deny or permit network access. The current industry trend is to apply RBAC (Role-based Access Control) based on identity. Its objective is to limit what services an authenticated entity is allowed to access.

One technique to support RBAC is dynamic VLAN assignment that places an authenticated user/device into a specific VLAN based on its credentials. Assigning clients to a specific VLAN is handled by a RADIUS authentication server. The IETF standard on the RADIUS protocol specifies a method for communicating information between the authenticating device and the RADIUS server by using the vendor-specific attribute (attribute 26). This attribute is used to transport assigned VLAN ID or name to the authenticator as part of the RADIUS return message.

Access enforcement policy can also be implemented via downloadable Access Control Lists (dACL). After authentication, the AAA server pushes the pre-defined ACLs to the access node. As soon as the access node downloads all the ACLs from the AAA server, it will try to get an IP address for the client. After it gets the IP for the host (using either DHCP snooping or ARP snooping), it will associate the downloaded ACLs to that specific IP address.

Both dynamic VLAN and downloadable ACL solutions are suitable for small size deployments where the number of VLANs and ACLs are manageable. When the size of the distribution network becomes large, it will be challenging to administer the individual access policies efficiently.

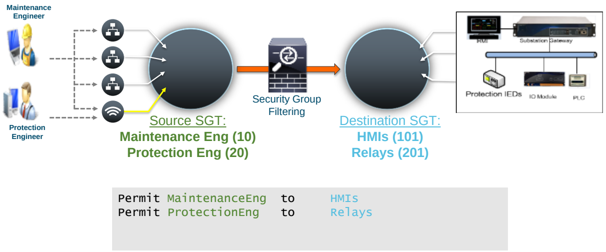


```
permit S1  to SRV1 for HTTPS
deny   S1  to SAP2 for DNP3
deny   S1  to SCM2 for SSH
permit S2  to SRV1 for HTTPS
deny   S2  to SAP1 for RDP
deny   S2  to SCM2 for SSH
permit S3  to SRV1 for HTTPS
deny   S3  to SAP1 for DNP3
deny   S3  to SAP  for SSH
Permit S4 to SRV1 for HTTPS
deny   S4 to SAP1 for DNP3
deny   S4 to SCM2 for SSH
permit S1  to HMI-1  for RDP
deny   S2  to HMI-1  for RDP
deny   S3  to HMI-1  for RDP
deny   S4  to HMI-1  for RDP
```

Figure 4 ACL-based Access Controls

As shown in a simple deployment above, the number of entries in the ACL becomes difficult to maintain. And the ACL continues to grow as more sources and destinations are introduced.

Security Group Access (SGA) is a technology which overcomes the shortcomings of the traditional approaches to policy administration. When a user connects to the network and tries to access an application, the access node automatically profiles the user and finds out the user's ID, device being used, location, and time of access. The access node then tags all traffic coming from the user's device based on the RBAC policy for the user's profile.



```
Permit MaintenanceEng  to     HMIs
Permit ProtectionEng   to     Relays
```

Figure 5 Security Group Access

The Security Group Tag (SGT) is a numerical value and is either manually assigned to the access nodes or automatically administered through a central management application. With central STG management, the assigned tag information is distributed across the network. Every data packet from the authenticated user's device is tagged. Authorization based on the tag is enforced by a filter node in the network. Typically, the switch connected to the server where the application or database resides enforces access based on a utility's access policy.

PROTECTING LEGACY SYSTEMS

Many distribution automation devices are controlled via serial-based protocols. There is a trend that many utility's data communication networks are gradually migrating to Ethernet/IP. During the transition, a protocol gateway is commonly used as a way to bridge serial and Ethernet/IP. One example of such a gateway device is to perform IEC 60870 T101 to IEC 60870 T104 protocol translation. The serial-IP gateway allows the IP-based control center to serve as the master in the network when communicating with the protocol gateway. The gateway serves as a proxy master station for the control center when it communicates with the serial-based RTU. Basically, the protocol gateway performs the following functions:
-Receive data from RTUs (T101) and relay configuration commands from the control center (T104) to RTUs.
-Receive configuration commands from the control center and relay RTU data to the control center.
-Terminate incoming T104 requests from the control center, when an RTU is offline.
Such protocol gateways can effectively function as a security proxy that automation devices only communicate with the rest of network via the gateway. The advantage of this approach is that there is no need to upgrade or replace the serial-based automation devices.

There are also legacy systems which require immediate network access without having to spend time on exchanging authentication messages with the network. While this requirement is legitimate and must be supported, a key adaptation is required to identify and classify these automation devices through the proper device sensing.

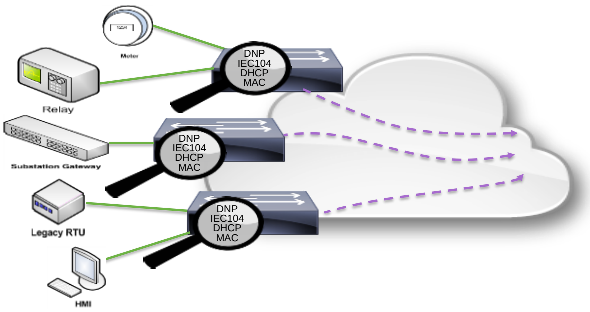


Figure 6 SCADA Device Sensors

Device Sensor is a network access node feature, used to gather raw endpoint data from connected devices, such as Modbus, DNP3, and T104. The end device type can be classified locally or can be offloaded to a central policy server via an access session. To support automation device profiling, the device sensor module is introduced and enabled on the network access nodes. The device sensor is SCADA protocols aware, and is capable of intercepting or querying the connected automation devices to retrieve the device identification.

A common goal of profiling the connected automation devices is to maintain visibility about assets and system behaviors. Although access control can be expressed based on the device information discovered, it is recommended to monitor the device behaviors for a prolonged period before full access control is turned on.

DEPLOYMENT CONSIDERATIONS

Authentication and Authorization is usually thought of as binary in nature. A device is either granted or denied access. Activation of access control on a large scale network at once might cause service disruption as the unexpected issues are practically inevitable. It is recommended to use a three-phase deployment approach which security levels tune up gradually. With a phased rollout scheme, a utility can begin with the monitor mode which is a process to allow network admission regardless of authentication results. The objective for the monitor mode is to gain network visibility on endpoints, and build an asset database. It is not uncommon that a number of devices are discovered without previous knowledge of their existence in the network. The second phase of the deployment is the low-impact mode where the network permits all traffic once a device has successfully authenticated and the failed authentication devices still get limited access. Usually, high impact services should be protected from access for failed authentications. Lastly, the closed mode of access control is to provide zero network access to devices without authentication, and then provide RBAC to those who have been authorized.

CONCLUSIONS

Access control is an essential component of securing the electrical grid which is undergoing modernization. While distributed intelligence improves grid operations, there are also security threats that must be addressed holistically including access controls for both users and systems. A security design for electrical grid must also consider the systems that do not support built-in security features. Finally, reliable operation is an ultimate goal for the electrical grid. Security deployment must take incremental steps to avoid potential service disruption.

REFERENCES

[1] National Institute of Standards and Technology, "Framework for Improving Critical Infrastructure Cybersecurity"

[2] National Institute of Standards and Technology Internal Report 7628, “Guidelines for Smart Grid Cyber Security”

[3] International Electrotechnical Commission (IEC) 62351, “Power systems management and associated information exchange - Data and communications security”

[4] The North American Electric Reliability Corporation, “Critical Infrastructure Protection”