INL/EXT-07-12635

Recommended Practice for Securing Control System Modems

James R. Davidson
Jason L. Wright

January 2008

The INL is a U.S. Department of Energy National Laboratory
operated by Battelle Energy Alliance

INL/EXT-07-12635

Recommended Practice for Securing Control System Modems

James R. Davidson
James L. Wright

January 2008

US-CERT Control Systems Security Center
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

ABSTRACT

This paper addresses an often overlooked "backdoor" into critical infrastructure control systems created by modem connections. A modem's connection to the public telephone system is similar to a corporate network connection to the Internet. By tracing typical attack paths into the system, this paper provides the reader with an analysis of the problem and then guides the reader through methods to evaluate existing modem security. Following the analysis, a series of methods for securing modems is provided. These methods are correlated to well-known networking security methods.

ACKNOWLEDGEMENT

This document was developed for the U.S. Department of Homeland Security to provide guidance for modem security for control systems. The author team consisted of subject matter expertise from the Idaho National Laboratory (James Davidson & Jason Wright)

For additional information or comments, please send inquires to the Control Systems Security Program at cssp@hq.dhs.gov.

CONTENTS

FIGURES

ACRONYMS

AT	Modem “Attention” Command
IDS	Intrusion Detection System
IED	Intelligent Electronic Device
IPS	Intrusion Prevention System
LAN	Local Area Network
MITM	Man-In-The-Middle
OS	Operating System
PBX	Private Branch eXchange
PLC	Programmable Logic Controller
PSTN	Public Switched Telephone Network
RTU	Remote Terminal Unit
VLAN	Virtual Local Area Network
VoIP	Voice over IP
WAN	Wide Area Network

Securing Control System Modems

1. INTRODUCTION

1.1 Scope

This recommended practice provides guidance on the analysis of methodologies for evaluating security risks associated with modems and their use in an organization. This document also offers useful methods for creating a defense-in-depth architecture that protects the system components that use modems for connectivity. It is assumed that the reader of this document has a basic understanding of vulnerabilities associated with modem and modem communications, as this information is available from other sources.[a]

Section 2 and 3 of the document discuss methods for assessing modem security, providing recommended resources for information and assessment tools and methods for identifying and analyzing modem connections. Section 4 provides options for implementing modem security according to the types of connections and/or devices being used. It also discusses methods such as authentication, logging, caller-ID filtering, and control system device security. Appendix A includes a list of resources used to create this document.

The methods presented in this document should be evaluated by each user for effectiveness within their operating environment. This analysis should include the capabilities and limitations of any hardware and/or software solution selected to implement these methods.

This document does not cover the physical security aspects of modem security. Physical security should be driven by the control system and its components. If the physical security of the control system and its components has been addressed appropriately, then the modems will be a part of this physical security perimeter.

1.2 Background

Modems represent an often overlooked "backdoor" to control systems. Modem security, if implemented at all, is often limited to a single method.

The use of modems is driven by the need for vendor support, periodic polling/control, and configuration of remote devices and for providing remote connectivity to these systems for engineering support. Modems can be configured for dial up, auto answer, or direct connection to provide a communication path into control systems.

There are two types of modem connection, dial up through the public switched telephone network (PSTN) and direct connection through a leased or dedicated line. Leased lines are analog compatible point to point connections and are often based on PSTN connectivity.

In general, the dialup PSTN is the least secure as it is exposes a modem to the equivalent of world-level Internet access. For an unsecured modem, the phone number of the modem correlates to an Internet-reachable IP (Internet Protocol) address. This is a phone number that can be reached from anywhere in the world. As a result, this communication point can be accessed from anywhere in the world by anyone with a modem and, thus, may be vulnerable to attack.

---

a. SecureLogix Chief Technical Officer Mark D. Collier has written a white paper titled: "Enterprise Telecom Security Treats" that can provide the reader with this information. http://download.securelogix.com/whitepapers.htm

To provide similar access to a leased line, the attacker must compromise some portion of the network that creates the leased line. This should be considered in the overall evaluation of modem security as a leased line is inherently more secure because of this layer of security. In addition the methods for discovery of the leased line require more sophistication than traditional war dialing efforts used for dialup modem discovery, an additional layer of security.

However, the traditional point-to-point leased line is a thing of the past. Analog switching centers have been replaced by digital switching centers that are susceptible to cyber attack. Many telephone company (telco) center's are now using Voice over IP (VoIP) for the long distance transmission of PSTN communications and more are considering it in the future. VoIP is in its infancy and many vulnerabilities have been published for these systems. This creates a larger exposure to attack than was afforded in the traditional PSTN leased line.

2. IP VERSUS MODEM SECURITY

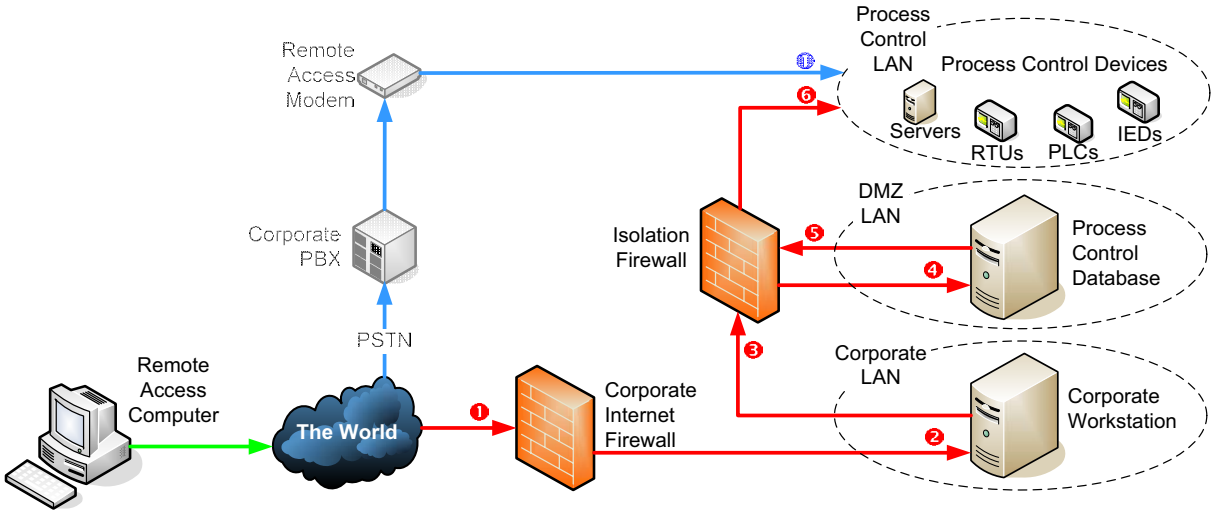
Ideally, similar sets of methods used for IP security should be used to properly secure modems in order to isolate a control system asset.

2.1 IP-Based Cyber Attack

Typical corporate networking security uses authentication, encryption, firewalls, routers, Virtual Local Area Networks (VLANs), access control lists, intrusion detection, and separate network segments to isolate a control system asset from the Internet. In order to access the control system, an attacker will need to gain access to one resource, compromise that resource, and use its permissions to attack the next component in the attack path.

An example of this type of attack is shown in Figure 1. This example is a simplified diagram that is not necessarily representative of a real-world network structure. The attack methods necessary for compromising some of the layers represented in this example would undoubtedly encounter additional layers of security. However, for the purpose of this paper, those demonstrated here are sufficient.

The Department of Homeland Security's Recommended Practice "Mitigations for Security Vulnerabilities Found in Control Systems" provides recommended network architecture for compartmentalizing communication and defense-in-depth. This network architecture is provided in Appendix B.



PBX = Private Branch Exchange; **PSTN** = Public Switched Telephone Network; **LAN** = Local Area Network; **DMZ** = Demilitarized Zone; **RTU** = Remote Terminal Unit; **PLC** = Programmable Logic Controller; **IED** = Intelligent Electronic Device

Figure 1. Simplified Network Attack Path

The following list of layers corresponds with the numbered layers shown in Figure 1:

Layer ❶: Corporate Internet firewall (authentication/rule-based filtering) with Intrusion Detection System (IDS)

Layer ❷: Corporate workstation access (userid/password) with security logs

Layer ❸: Isolation firewall (corporate workstation → process control database rules) with IDS

Layer ❹: Process control database access (userid/password) with security logs

Layer ❺: Isolation firewall (process control database → process control server rules) with IDS

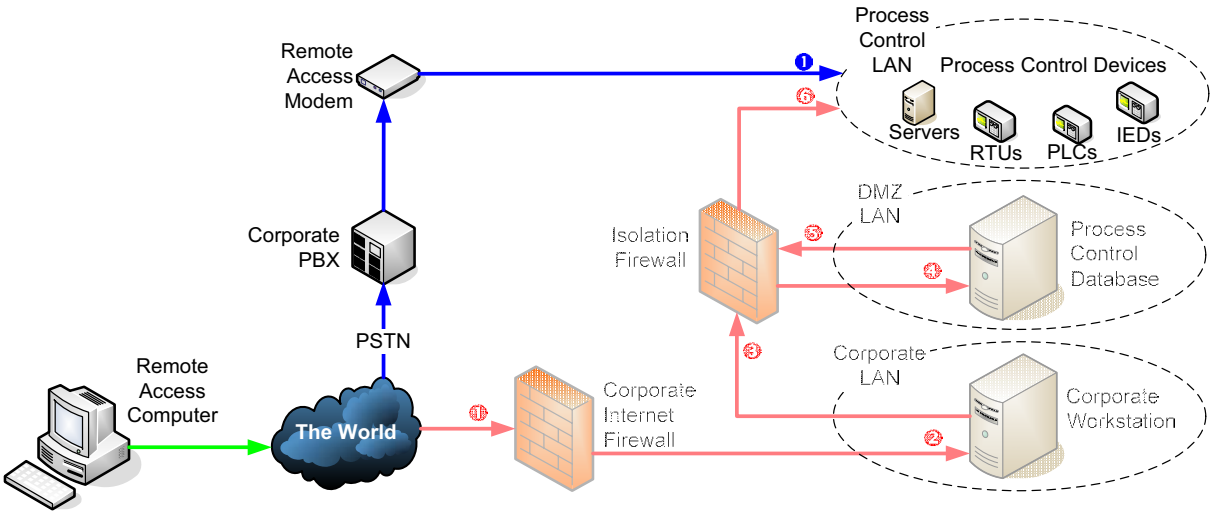
Layer ❻: Process control server access (userid/password)

Once the location of the control system component has been identified, it is necessary to start from an Internet access point and determine the number and type of security layers that are used to provide protection from an external attack on that asset.

2.2 Typical PSTN Attack Path

To properly secure the modem, it is necessary to provide functionally similar layers of security between the PSTN and the control system component. Currently, many facilities provide little or no security to the modem connection.

As illustrated in the example shown in Figure 2, the only protection in place for a PSTN attack is provided by the Process Control Server, which requires a userid/password combination to gain access. In some cases, primarily with older legacy components, the modem-connected device does not even provide this level of protection.



PBX = Private Branch Exchange; **PSTN** = Public Switched Telephone Network; **LAN** = Local Area Network; **DMZ** = Demilitarized Zone; **RTU** = Remote Terminal Unit; **PLC** = Programmable Logic Controller; **IED** = Intelligent Electronic Device

Figure 2. Simplified PSTN Attack Path

The following layer corresponds with a numbered layer in Figure 2:

Layer ❶: Process control server access (userid/password).

3. MODEM ASSESSMENT

3.1 Identify Points of Contact

Critical points of contact to use as resources include:

- Phone line provider
- Private Branch Exchange (PBX) operations personnel
- Control systems technicians
- Control systems engineers
- Control operations supervisors

3.2 Obtain Documentation

3.2.1 Company Level Documents

As a first step, obtain a copy of company security plan to determine the company mandated requirements.

Many companies do not have plans, policies, or procedures relating to modems on control systems, as they tend to concentrate on the corporate LAN and leave the control LAN to those responsible for the control system. In light of this, should a lack of corporate governance exist, the following items are considered the minimum security requirements for modems within a control system LAN:

- All modems incorporated into components inside the control system LAN should have a written justification of need, be registered in a central data base that identifies the person responsible for the modem, and require management-level approval.
- If the modem requires auto answer capability, then there should be a written justification of need and requirement of management-level approval. No auto-answer modem used with the control system should be allowed without some form of dialback security implemented.
- Periodic war dialing should be performed to detect rogue modems and to verify the existence of previously approved modems. Any deviation from the approved list should be investigated, and appropriate remediation (approval or removal) should be performed.
- A periodic review of approved modems should be performed to revalidate the need for the modem resource.
- A periodic review of installed analog phone lines should be performed to determine if any are used by modems. This is a way to discover modems that may not be detected using standard war dialing efforts.
- Any modem connected to a control system resource should undergo a defense-in-depth analysis, and, as a result of this analysis, the modem should be protected through the use of appropriate layers of security to protect that resource from remote access by unauthorized personnel. If the modem resource cannot meet this criterion, its removal should be mandated.

If the company's plans, policies, and procedures do not cover modems on control systems, then they should be added. The methods provided in this document can help define what is appropriate for a specific organization.

3.2.2 Regulatory Level Documents

Obtain a copy of any required regulatory standards. As an example, the North American Electric Reliability Corporation (NERC) has a set of standards for securing control systems within the electricity sector. These Critical Infrastructure Protection standards include some criteria for modem use.

3.2.3 Equipment Level Documentation

Gather together easily locatable manuals, specifications, and configurations for the equipment that exist, such as modems, attached devices, and any other equipment that is in the communications path established between the remote connection and the control system component. As the evaluation of the system, proceeds it may be necessary to track down additional materials.

3.3 Tools of the Trade

Before attempting to secure modems, it is a good practice to equip the organization with some common tools that will help with evaluating modem security. Many of these same tools may be used by an attacker to gain access to modem-connected resources.

3.3.1 War Dialing

The most important tool for modem detection is a war dialer. SearchSecurity.com[b] provides this definition of a war dialing program:

> *A war dialer is a computer program used to identify the phone numbers that can successfully make a connection with a computer modem. The program automatically dials a defined range of phone numbers and logs and enters in a database those numbers that successfully connect to the modem. Some programs can also identify the particular operating system running in the computer and may also conduct automated penetration testing. In such cases, the war dialer runs through a predetermined list of common user names and passwords in an attempt to gain access to the system.*
>
> *A war dialer usually obtained as freeware, is typically used by a hacker to identify potential targets. If the program does not provide automated penetration testing, the intruder attempts to hack a modem with unprotected log-ins or easily cracked passwords. Commercial war dialers, also known as modem scanners, are also used by system administrators, to identify unauthorized modems on an enterprise network. Such modems can provide easy access to a company's intranet.*

The war dialer can be used to detect dialup modems within an organization that are auto-answer enabled. There are methods covered later in this document that can be used to mask these modems from war dialing efforts. Using the war dialer against these known modems is a means to determine the effectiveness of these masking methods.

The following is a list of some war dialer resources:

- iWar, http://www.softwink.com/iwar/, Freeware – Unix/Linux OS
- ModemScan, http://www.wardial.net/default.html, Freeware – Windows OS

---

b. SearchSecurity WWW site: http://searchsecurity.techtarget.com/.

- PAW, http://www.wyae.de/software/paw/, Freeware – Unix/Linux OS
- PhoneSweep, https://www.sandstorm.net/products/phonesweep/, Commercial – Windows OS
- TeleSweep, http://www.securelogix.com/modemscanner/index.htm, Freeware – Windows OS

For a more comprehensive description of war dialing, an excellent paper on the subject is available from SANS.[c]

3.3.2 Modem Diagnostics

Modem diagnostics are used to query the modem about its configuration, connectivity, and, in some cases, about the last valid phone connection. A modem supplier may have provided diagnostic and configuration software with the modem to automate this task. Examine what the supplier delivered; any electronic media may contain useful software.

One form of modem diagnostics is a simple communications program, such as the Windows-based HyperTerminal that can access the communications port the modem is on. With the modem disconnected, and access to a good reference on the AT ("attention") commands for the modem users can obtain a wealth of information, such as the default configuration, non-volatile RAM configuration, last phone number dialed, and length of the last call. Some of this information can be useful for post-attack analysis.

If using the modem on a computer running a Microsoft Windows Operating System (OS), the control panel provides some built-in diagnostics that can be used to help evaluate the modem connections. Other OSs may have similar capabilities.

3.3.3 Modem Monitoring Software

Many operating systems provide software to monitor the attached modem. This can be installed to create modem logs, read caller ID information from the modem, and control connectivity. In addition, the modem company itself may provide modem monitoring software that can use. In some cases, this software can act like a local PBX with many of the same capabilities.

3.4 Modem Identification

The goal of this section is to identify every modem with the potential to affect process control.

3.4.1 Known Modems

Using corporate documentation, identify all known modems and faxes. This list will be used as a baseline for comparison. Working with communications personnel, identify and document all analog phone lines in the facility that could support a modem or fax connection. This list will be used in a war-dialing exercise. Determine if the PBX has capabilities to use the digital lines for analog transmission. Realize that if it does, the number of potential phone numbers that could use modems will be significantly expanded. These lines should also be included in the war-dialing exercise list. Identify and document all leased phone lines, as these may use direct-connect modems that will not be detected in a war-dialing exercise.

3.4.2 Modem Discovery

Schedule a war-dialing exercise at your facility.

---

c. SANS War Dialing Paper: http://www.sans.org/reading_room/whitepapers/testing/268.php.

Exclude critical phone numbers where modem discovery could impact safety, operations, or emergency services. Phone numbers to be queried by this exercise should be reviewed by all organizations that might be impacted and the final list approved by senior management.

Create a contingency plan should a critical system inadvertently be overlooked. This should include contact information for the individual responsible for the war-dialing effort.

Inform all personnel of the date, time, and time span of the exercise to reduce the impact on operations. Include the contingency plan in the notification. Be aware that some individuals may disconnect modems to avoid discovery.

It is better to run two separate exercises: one during business hours and one after hours. Computers with attached modems are more likely to be on during business hours. The after hours exercise will reduce the impact caused by busy telephones that share a line with a modem.

3.4.3 Finalize List

The result of the war-dialing exercise is a list of known functioning modems. This list must be compared with the corporate list to identify discrepancies. In addition a determination as to whether this modem is needed should be addressed. Often these modems are put in place for a short period of time and then forgotten when they are no longer needed. Removing these unneeded modems reduces modem footprint, making it easier to secure system.

A modem that responded to war dialing but didn't show up in the corporate list may be undocumented, may be unauthorized, or may have been moved from another location (line). A modem that was documented but didn't respond to war dialing may have been removed, not configured to answer automatically, unplugged, or on a busy shared line.

Refine the list by visiting the supposed location for discrepant modems and review documentation to resolve differences. As this may require time and effort, remember that these modems present the most significant vulnerability to operations.

For each modem, determine whether the physical connection is located in an area that could allow a modem connection to a control system; all others are outside the scope of this document. In addition to comparing lists and resolving discrepancies, investigate the physical location of all analog phone lines that could have a modem attached. It is not uncommon for an analog phone line to be in place for occasional use with a modem creating an open invitation to use this connection to "get the job done," possibly exposing the control system to an external attack. These lines should be added to a refined list as if they were modems. Next, locate the phone connections for leased lines, determine if a modem is attached, and include these modems in the list. Finalize the list by determining which modem connections or lines in areas near control systems do or may perform control system-related functions. These are the modems that require security evaluation.

As part of this evaluation organization have the opportunity to identify unneeded modems and analog phone lines and remove them, thereby reducing exposure to external attack.

3.5 Analyzing the Modem Connections

The finalized list of modem connections is the basis for the rest of the work. Look carefully at commonalities and differences of the modem assets now identified. If there is a large quantity of modems, consider some form of centralized management to simplify their maintenance.

Use modem diagnostics software to examine the configuration and manuals to determine the security capabilities of each modem. Keep in mind that just as typical corporate network security uses authentication, encryption, firewalls, routers, virtual LANs, access control lists, intrusion detection, and separate network segments to isolate a control system asset from the Internet; modems should also enjoy a defense-in-depth approach that is periodically reevaluated for network security issues.

4. MODEM SECURITY METHODS

This section describes methods of applying defense-in-depth principles to modem connections. Determine which of the suggested methods are applicable and appropriate for a particular installation.

Modem security challenges of password management, authorized user lists, and modem database maintenance grow with the number of modems employed in control systems operation. These issues require workable plans, policies, and procedures. They also require end user awareness in order to avoid modem abuse and potential process alteration.

As an example of modem abuse, consider a situation in which a control system operator, faced with work computer use limitations imposed by his employer, uses a control system modem to access the Internet through a personal Internet Service Provider account. While this connection allows the operator to bypass unwanted limitations, it grants the same privilege to would-be attackers, negating many defense-in-depth countermeasures associated with the network implementation.

4.1 PBX System

From a defense-in-depth perspective, the PBX is the first place to consider security countermeasures. Safeguards applied here are particularly effective for organizations with numerous modems as they will provide central management for all PBX connections.

Determine the modem security settings that exist on the PBX. Many of these security settings can limit the hour of the day and days of the week that a phone line is active, some can limit the phone numbers that can connect to a modem line, and some may block calls based on caller-ID lookup. Some provide active logging capabilities that may be used in an IDS for modem connections. Any or all of these security settings should be considered for use, depending on the operational requirements of the control system.

4.1.1 Networking Equivalent

The PBX is roughly equivalent to a core networking router. Some routers have the programmed ability to impose firewall access control lists based on time of day in addition to the normal function of enforcing policy based on combinations of source and destination addresses. Routers can also produce logs for successful or attempted network accesses. Where the destination address (the modem's extension) is a reliable indicator, the source address (the incoming caller ID) is not as reliable. Caller ID can be faked or completely absent.

4.1.2 Limitations

Because PBX settings can protect modems, it is also important to consider the security of the PBX itself. As these systems are geared more towards standard telephony applications, such as call forwarding and voice mail, they are often not considered in the overall security profile of the company. For more information on PBX security, comprehensive security reviews and suggestions are published elsewhere.[d,e] At a minimum, however, keep the following in mind:

---

d. NIST developed a PBX vulnerability analysis that can be use to understand these systems. NIST SP 800-24 PBX Vulnerability Analysis: http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf.

e. A checklist for securing a PBX system is provided by ATT's "ATT Security Statement" document. ATT PBS Security Checklist: http://images.bimedia.net/documents/ATT_Security_Statement.doc.

- PBX systems are rarely upgraded to the newest technologies. This is analogous to using outdated and/or unpatched networking components.
- PBX may not provide the level of control to meet security goals.
- Many PBXs have vulnerabilities that could impact overall PSTN communications.

4.2 Telephony Firewalls

If modems go through a PBX system that does not provide the level of control necessary to meet security goals, consider an upgrade and/or use telephony firewalls. These systems are normally placed between the PSTN and modem. They can provide voice-level capabilities similar to the data-level capabilities of network firewalls in use today. A diagram showing the installation of a telephony firewall in a typical system is shown in Figure 3. Keep in mind that the firewall can be located on either or both sides of the PBX depending on security needs.

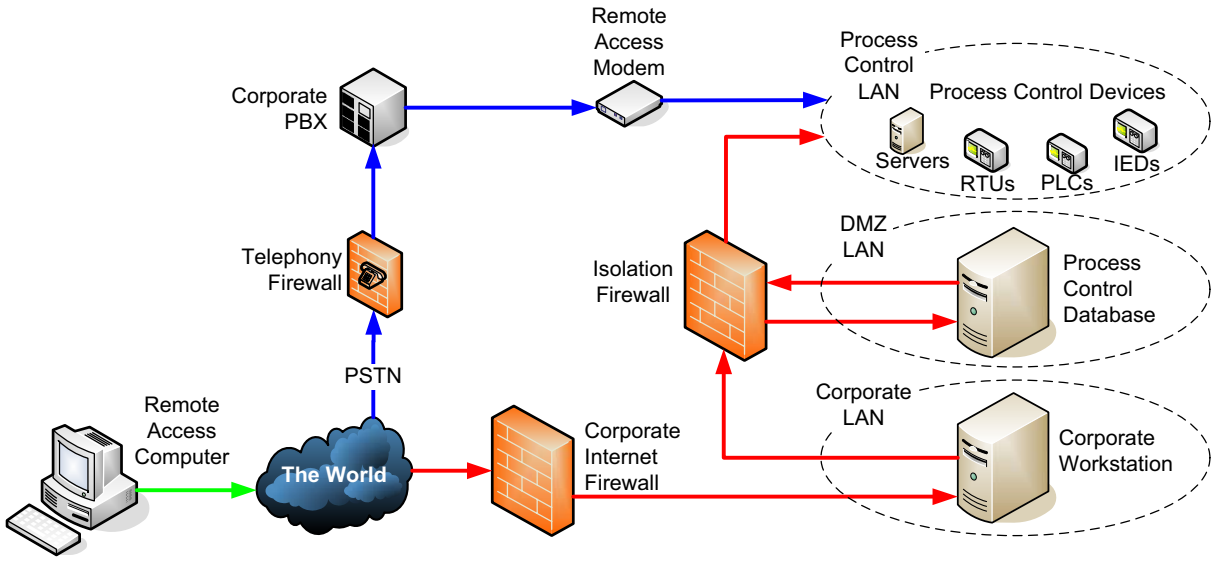


Figure 3. Telephony firewall installation.

Consider this type of hardware to be the equivalent of the corporate Internet firewall for PSTN connections. It is designed to protect a voice system from "phreakers," the PSTN equivalent of a hacker.

Some telephony firewalls include the ability to monitor phone line traffic to detect communication from internal modems. Once this has been discovered, the firewall can compare the modem traffic to a list of authorized modems. If the modem is not included on the authorized list, the firewall can automatically block the modem, alarm the existence of an unauthorized modem, and/or add it to the list. This ability makes voice firewalls invaluable tools for the detection of unauthorized modems that may not be discovered using typical war-dialer techniques such as those that are connected irregularly and those on leased lines.[f]

f. A resource for information on telephony firewalls can be found on the Talisker WWW site. Talisker WWW Page on Telephone Firewalls: http://www.securitywizardry.com/firetel.htm.

4.2.1 Networking Equivalent

The best analogy to a telephony firewall is an Intrusion Prevention System (IPS). These systems sit inline between two network points and control access bidirectionally. IPSs can be viewed as completely passive devices, as long as policy is not being violated; traffic between the two sides of an IPS is inspected and passed, without modification, to the other side if it is not flagged as suspect. Just like an IPS, a telephony firewall has the ability to block connection to a phone line if specific criteria are not met.

4.2.2 Limitations

There are three potential limitations associated with telephony firewalls: cost, PBX usage, and compatibility.

Cost may be a concern with this type of system. However, the initial cost of such a system may be justified over its life cycle. It simplifies and reduces costs of the management of modems and modem security resources and avoids costs associated with recovering from damages incurred by modem misuse.

The use of a telephony firewall with a legacy PBX may not protect for the following reasons:

- Some PBX systems aren't compatible with analog dialup modems
- Phone lines in remote facilities may be connected directly to the service provider and not go through the PBX

If there are direct phone line connections from the phone company instead of a PBX, a voice firewall is necessary for each and every connection.

4.3 Telephony Authentication

One interesting technology is telephony authentication. With this technology, hardware keys reside on the PSTN side of the modem, not between the modem and serial device as is typically done with in-line encryption/authentication devices know in the industry as "bump-in-the-wire." When two phones attempt to connect, the master key must validate the slave key before a PSTN connection is allowed. Because it is on the PSTN side, it should block modem discovery during a war-dialing exercise. An example of this hardware token technology with one primary key and many slave keys can be found at http://www.cpscom.com/gprod/challp2.htm.

With this system the primary key resides on the control system and the slave keys exist external to the system. The primary key manages a list of valid slave keys that will allow access. This allows for easy rejection of slave keys that have been issued but are no longer allowed access.

4.3.1 Networking Equivalent

Some virtual private network (VPN) technologies provide bump-in-the-wire modes; key exchange takes place out of band in these systems. The analogy goes further when incorporating hardware tokens, which are similar to the tokens used in SecurID tokens.

4.3.2 Limitations

This technology has not been tested for throughput and the possible impact on the modem connection. If a slave key were compromised, stolen, or lost and not removed from the valid key list on the master, then an unauthorized user could use this slave key to obtain access to the modem.

4.4 Logging

The logging of information such as phone calls, connection attempts, time of connection, and failed login attempts can be a valuable tool in the overall security of these systems. Modems often lack significant logging capabilities; most will, at least, provide details about the last connection. The control device that the modem is connected to may provide significantly more information than a modem. If a PBX or a telephony firewall is being used, then these logs can be useful. However, they will be of little use if they are not examined.

Automated monitoring of these logs can be used to develop an IDS for modem connections. Using logs can provide the ability to alarm on specific connectivity configurations. By monitoring these logs and alerting on specific items using software such as the freeware Swatch[g], it is possible to build an IDS for the PSTN remote access connections. Two examples of log analysis for intrusion detection are as follows:

- **Logged Event 1**: a call comes in but hangs up before a login attempt is made.
  - **Possible Attack**: war dialing effort to detect modems.
- **Logged Event 2**: n number of invalid login attempts.
  - **Possible Attack**: attempt to break into a system.

A value of n that is greater than 1 reduces false positives from people who mistype their login credentials. However, the value of n should never be greater than 3, the number of acceptable failed logins allowed for in most standard IT security recommended practices.

If the systems has logging capabilities on multiple devices within the communication flow, comparison of these logs by correlating alarm signatures can reduce the number of false positives for this type of intrusion detection.

Where other methods for logging may be unavailable, technology exists that provides an in-line-logging system. This hardware add-on is inserted between the modem and the serial device and allows configurable logging functions that can be monitored. An example of this type of line logging can be found at http://www.cpscom.com/gprod/tlc.htm.

4.4.1 Networking Equivalent

The concept of logging data for audit and analysis is common place on a network. Applying IDS analysis to telephony is the key here. The techniques used in large IDS deployments rely on correlation from multiple points to reduce false-positive indicators and provide a holistic view of the network. As shown in Section 4.4 each event taken separately may be benign, but if combined, the events represent a higher likelihood of malicious behavior.

It may be possible to leverage an investment in logging analysis software already available to the corporation by configuring the telephony gear to send its log information to a central logging server. The analysis software used to provide networking event correlation for the corporate network can be applied to the telephony data as well.

4.4.2 Limitations

Legacy modems and modem-connected devices may not have logging capability.

---

g. http://swatch.sourceforge.net/

Creating signatures for attacks that minimize false positives will require expertise that may not exist "in house," however, if IDS specialists are available, their experience can be used to develop workable solutions.

Centralized management of logs may not be possible due to the remote locations of some modem connected devices. Adding the capability to transmit logs from remote devices might expose system components to a different line of attack. If centralized transmittal of logs is not possible then the log information obtained may only provide forensics.

4.5 Dialup Modem Connections

One of the best methods to secure a modem is to connect it only when necessary and disconnect it as soon as the period of use concludes. This limits system exposure time and reduces the likelihood of an attacker identifying the modem via war dialing.

4.5.1 Modem Power

One method for controlling the modem's connections is to control its power supply. This can be done manually by either using the power connection (cord and plug) or the power switch on the modem. For this method, a control system contact is tasked with powering the modem up for use and powering it down when access is no longer required. While power manipulation is an effective security control, employee work loads may lead them to omit disconnecting the modem from power when it is no longer in use. This issue can be resolved by placing a timer on the power line. This timer is set according to a period of use that must accompany all requests for access. The timer automatically disconnects the modem as the determined period expires.

Whether modem power is controlled by physical access or through a remote power control system is not important. However, physical access is not feasible in all cases, such as situations requiring automated modem connectivity or modems that are not physically accessible. In these circumstances a remotely managed power relay, in which an electronic signal turns the power on and off, is more effective.

Unfortunately, typical remote control power systems available on the market today do not have timer-like functionality. Therefore, when using these systems, it is imperative that the responsible control system contact disconnect the modem power when it is no longer needed. The ideal solution may involve integration of a remotely controlled power relay into the control system operator's control console, and programming a timer into the system logic. This would allow the operator to remotely enable the modem for only the requested period of use.

4.5.2 Modem Phone Line

Another method for isolating the modem is to disconnect it from the PSTN. This method, similar to limiting power to the modem, can be done physically by unplugging the connection or logically by programming the PBX to accept calls to modem lines only during specific times. While PBX time-window programming is not as effective as manual intervention, it does put technology to work to save effort and mitigate the risk of human neglect or forgetfulness. In addition, similar to remote modem power control, PBX control could be built into the control system operator console.

4.5.3 Networking Equivalent

The closest network analogue of using power to secure a modem is the use of power to secure an Ethernet hub. By removing power, the network connections are severed, preventing this method of ingress.

The closest network analogue of disconnecting the phone line to secure a modem is the removal of the network uplink cable from an Ethernet hub. By removing the uplink cable, the network is severed, preventing this method of ingress.

4.5.4 Limitations

While controlling dial up modem connections reduces the window of opportunity an attacker would have to connect to a modem, it makes no provision for validating the identity or authorization of the entity attaching to the modem.

4.6 Dial Back

Dial back helps eliminate the challenge of modem use authorization. Instead of answering to any caller, the modem is programmed to hang up when it receives a call from any number and call the number programmed into its memory. This method works well when only one line or location is needed to communicate with a modem.

4.6.1 Multiple Dial Back

Where multiple call back numbers are required to address multiple users and/or multiple call back numbers, modems are available that can be configured to support this requirement. In this case sets of userid/password combinations are linked to specific call back numbers. As with all userid/password sets, these should follow company mandated guidelines for password complexity and aging with all default userid/password combinations removed or reprogrammed.

With login credentials and dial back capability, this method provides two layers of security.

4.6.2 Networking Equivalent

There is no direct networking equivalent to dial-back and multiple dial-back systems. The closest correlation is authentication and validation. For single dial back systems the best correlation is validation. For multiple dial back capabilities the best correlation is authentication and validation.

4.6.3 Limitations

As with any security method, there are ways to break the security of such systems. Hackers have developed methods called “dial-back spoofing” where a fake dial tone is presented to the modem and the hacker just ignores the call-back process and maintains the connection. This is mitigated somewhat when the modem requires a userid/password combination for the dial back and/or final connection.

When a company has multiple dial-back modems within the control system environment, there is an additional burden of managing userid/password sets. These modems typically do not have the same capability, with respect to password management, as most computer systems do. When implemented at the modem level, there are very limited, if any, automated management controls that can be placed on password age, complexity, history, and failed login lockout.

Some dial back enabled modems do not provide password capability. For modems that do implement password access there are often have limitations on password complexity that may not meet the company mandated guidelines.

4.7 Caller ID Filtering

If caller ID is available from the phone service, this capability can be used with some modems to add another layer of security. Modems exist that can read the caller ID, compare it to a preprogrammed list of valid phone numbers, and then allow/deny access based on this comparison. A second choice is a caller ID server that compares the caller ID with a preprogrammed list. This service is placed in line with the modem or uses a modems caller ID capability to respond in a manner that blocks an unauthorized connection. Another useful security layer created by using caller ID is that it blocks most typical war dialing efforts to discover the modem.

Many modems are considered caller-ID compliant; however, this does not mean that the modem will block unauthorized phone calls. Rather, this means that the modem can report the results of the caller ID to some other piece of software, and it is up to the software to look up the number and determine if the connection should be maintained.

4.7.1 Networking Equivalent

Caller-ID can be used to provide the source address (phone number) of the other end of a connection. Creating access control lists based on this address is directly analogous to creating a firewall Access Control List (ACL). However, in this case, as described in Section 4.7.2, the address is not completely reliable or can be misleading.

4.7.2 Limitations

It is becoming a common practice for corporations to block or provide a baseline phone number as a caller ID from all phones within their organization. Some of this is driven by the PBX systems they use and some of it is based on a corporate security and/or privacy philosophy. If the caller ID is blocked, then this security method would block access. If they use a common phone number for all calls originating from their corporation, then the usefulness of this security feature is limited.

Additionally, it is possible for an attacker to spoof the caller ID number to indicate a number different from the originating phone.

4.8 Leased-Line and Dialup Modems

This section covers methods that can be used for both leased-line and dialup modems.

4.8.1 Authentication

With any remote connection, it is preferred that the two end points know with whom they are talking. The key to this is some form of authentication. In many cases the modem connection provides access to direct control of an element of a control system. Many of these components, such as Remote Terminal Units (RTUs), Programmable Logic Controllers (PLCs), and Intelligent Electronic Devices (IEDs) may not require any authentication for connection. Password authentication for use with dialup modems does not work well or is impractical with leased-line modems.

Modems can be purchased that can be embedded with keys that are verified during modem negotiation. If the keys do not match, the modem disconnects.

In addition, there are add-on hardware keys that can be added to existing modems. These devices are placed between the serial port and the modem.

4.8.2 Encryption

Often associated with authentication keys is the addition of encryption as part of the process. Encrypted modems are available that can provide this level of security. An evolving field of in-line-encryption (bump-in-the-wire) devices is being rolled out to act as an intermediary between the serial port and the modem. A diagram of the installation of such a device is illustrated in Figure 4.

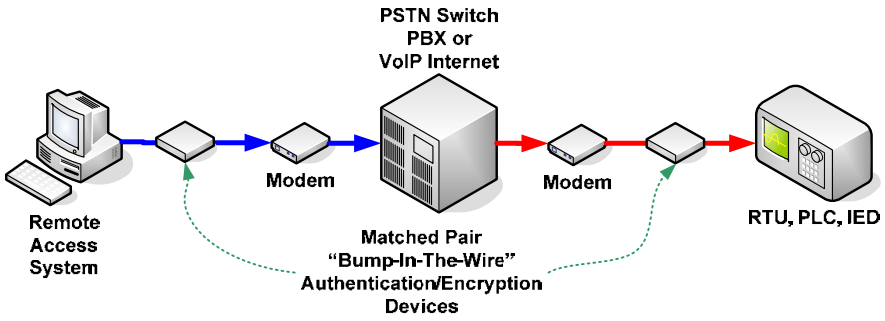


Figure 4. Bump-in-the-wire installation.

Encryption becomes very important if the communication between devices uses a clear text (non-encrypted) protocol for data transfer between modems. With clear text protocols, an attacker can interject themselves into the communication stream, read userids and passwords, and/or act as an intermediary between the two connection points. As an intermediary, the attacker intercepts traffic from one end, changes the data and forewords it on to the receiving device, which is known as a Man-In-The-Middle (MITM) attack. This MITM attack could originate within the public telephone system, the internal PBX system, or through a VoIP communication path. A diagram of such an attack is shown in Figure 5.

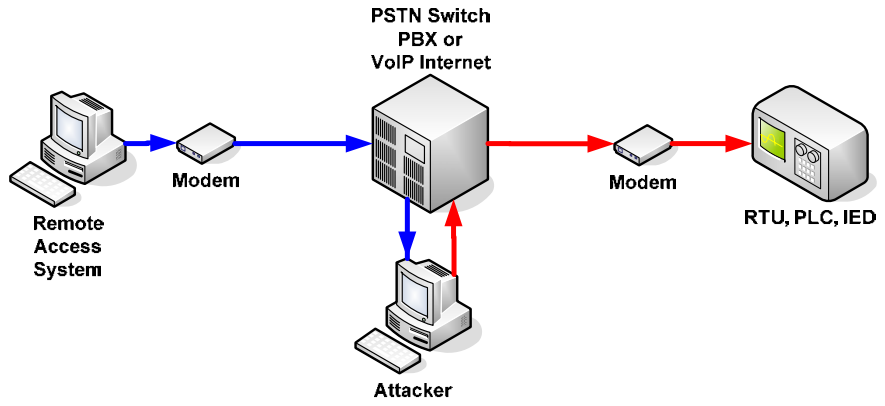


Figure 5. Man-In-The-Middle attack on modem communications.

Many phone companies are using VoIP technologies to move phone calls between long-distance locations. In addition, there is an increasing demand for VoIP at the corporate level, both due to costs and the loss of support for traditional PSTN phone lines. VoIP could provide access to phone lines via Internet transmission of these signals. A recent search of the Internet with the keywords "VoIP Vulnerabilities" returned over 5 million hits.

Use of secure modems or bump-in-the-wire devices with authentication and/or encryption will help mitigate this vulnerability.

4.8.3 Networking Equivalent

There are several security products providing equivalent functionality in the network arena. The closest match to the functionality discussed here is Internet Protocol Security (IPSec). IPSec provides strong authentication of network endpoints. It also provides authentication of individual packets sent between the endpoints and can also encrypt the protocol data. The authentication of packets provides a positive assurance that the endpoint is what it claims to be, whereas the encryption prevents successful eavesdropping.

4.8.4 Limitations

Both ends of the communication path must have the same encryption/authentication device (normally make, model, and revision-level compliant) to use these techniques. Some of these technologies do not allow a master/slave relationship where the master (the control system component) can connect to multiple slaves (the remote access component).

On slower baud rate connections (normally 1,200 bps or less) the handshaking to establish the encryption can exceed the time-out of the modem, causing it to hang up prematurely. The encryption can reduce overall throughput of the connection. However, there are vendors that claim a throughput increase when using their systems.

Before using these technologies test them with a representative system to make sure they do not introduce a connectivity or throughput problem.

4.9 Control System Device Security

Control system device security is an issue that is usually addressed when the resource is a computer. Userid/password policies can be included as a part of the operating system and managed from a central location. Other remote monitoring and control devices such as RTUs, PLCs and IEDs often have userid/password combinations as part of the device security.

4.9.1 Networking Equivalent

The use of userid/password combinations on control system devices provides a similar layer of security as their implementation on standard IT devices found on corporate networks

4.9.2 Limitations

Remote monitoring and control devices such as RTUs, PLCs, and IEDs may only allow for very simple passwords using a restricted subset of the ASCII characters. This limits the effectiveness of this layer of security. The default passwords can often be found using an Internet search. It is imperative that these devices have the default password(s) replaced. For this layer of security to be effective, these passwords be changed on a regular basis. As the complexity of the control system increases, the quantity of these devices increases. As the quantity increases, implementing good userid/password policies such as expiration date, complexity, etc. may become unmanageable. If centralized device management is not available for these devices, plans, policies, and procedures outlining password policies may not be practical. In this case, use additional layers of security as outlined in this document.

4.10 Modem Escape Sequence Vulnerability

One vulnerability that exists in many Hayes-compatible modems concerns the breaking out of a connected environment to the command mode. A typical +++ escape prefix on an AT command will allow the attacker to control the modem through its own command structure. As an example, the string +++ATH0 escape sequence can cause the modem to hang up. Other AT command strings can be sent in this manner that could change the modem's configuration commands such as "hang up and dial another number" or "changing the dial type."

4.10.1 Modem Escape Sequence Mitigation

This can be resolved by changing the S2 register value from its default, 43 (+), to a value from 128 to 255. This changes the defined escape character to an invalid ASCII value, disabling the +++ sequence.

The impact of the mitigation for this vulnerability limits troubleshooting capabilities because the escape sequence is often used to troubleshoot an active modem connection. Some modem monitoring software use this technique to create modem logs while the modem is connected. Disabling the escape sequence will prevent either of these functions from working.

5. CONCLUSION

Whatever methods are used, more than one of the previously listed methods should be considered for providing in-depth security needed for modems.

In the original example explained in Section 2.1 and shown in Figure 1, there were six layers of security between the Internet and the control system server. The techniques used to build layers of security in the network included firewalls, IDS systems, userid/passwords, and critical-logging functions. The example of the modem connection (see Figure 1 and Section 2.2) showed a single userid/password layer of security. To properly secure the modem in this example, the user should add similar capabilities in the modem connection. Ideally, since there are at least six security layers in the example networking communication chain, a similar set of security techniques should be provided for the modem connection using methods such as those suggested in this paper.

Where a direct correlation between networking and modem security methods does not exist or is not available in a system, consider methods listed in this document to add alternative layers of security.

Remember, the overall security of a control system is only as good as its weakest link.

Appendix A

Resources Used in Creating this Document

Appendix A

Resources Used in Creating this Document

During the creation of this document, numerous WWW sites were visited for research and to determine the technologies available to secure modems. This portion of the document lists the resources used and provides WWW links. This is not a detailed list of all available resources and technologies that could be applied to the issue of modem security.

Modem WWW Sites Visited

Data-Linc Group – Industrial Modems, Multiplexers, and Systems

General DataComm – Modems; Secure Dial-up and Private Line Access

OneAccess Telindus – Aster 5 Modem

StarComm – Password and Caller ID Security Modems

Telenetics – Data Modems

Voice Security WWW Sites Visited

Timberline Technologies – Alphabetical List of Dialup Security Products

Computer Peripheral Systems, Inc. – Dial Security Products

SecureLogix – Voice Firewall, Voice IPS, Modem-Security

Teltone – Serial/IP Technologies for Phone Line Sharing, Integrated Firewalls, Authentication, and Encryption

Other Equipment WWW Sites Visited

Aegis Technologies, Serial Encryption/Authentication, Log Monitoring, Centralized Management

Data Comm for Business, Inc. – Serial Encryption Transceiver

Schweitzer Engineering Laboratories, Inc. – Serial Encryption Transceiver

Verano, Industrial Defender – Security Event Monitoring, Firewalls, NIDS, HIDS, SNMP

Reference Papers from WWW Sites Visited

An Analysis of Dial-Up Modems and Vulnerabilities; Peter Shipley, Simson L. Garfinkel; 2001

Enterprise Telecom Security Threats; Kirk Vaughn; Secure Logix Whitepaper; 2004

Modem over IP; Mindspeed Technologies Whitepaper, 2002

Outsourcing and the Increased Dangers of 'Dial Up' Access; Paul Jenkinson; SANS Whitepaper; 2001

PhoneSweep, The Corporate War Dialer; Greg Hodes; SANS Whitepaper; 2001

Tools for Protecting Electric Power Systems from Electronic Intrusions; Paul W. Oman, Jeff Roberts, and Edmond O. Schweitzer; Schweitzer Engineering Laboratories; 2002

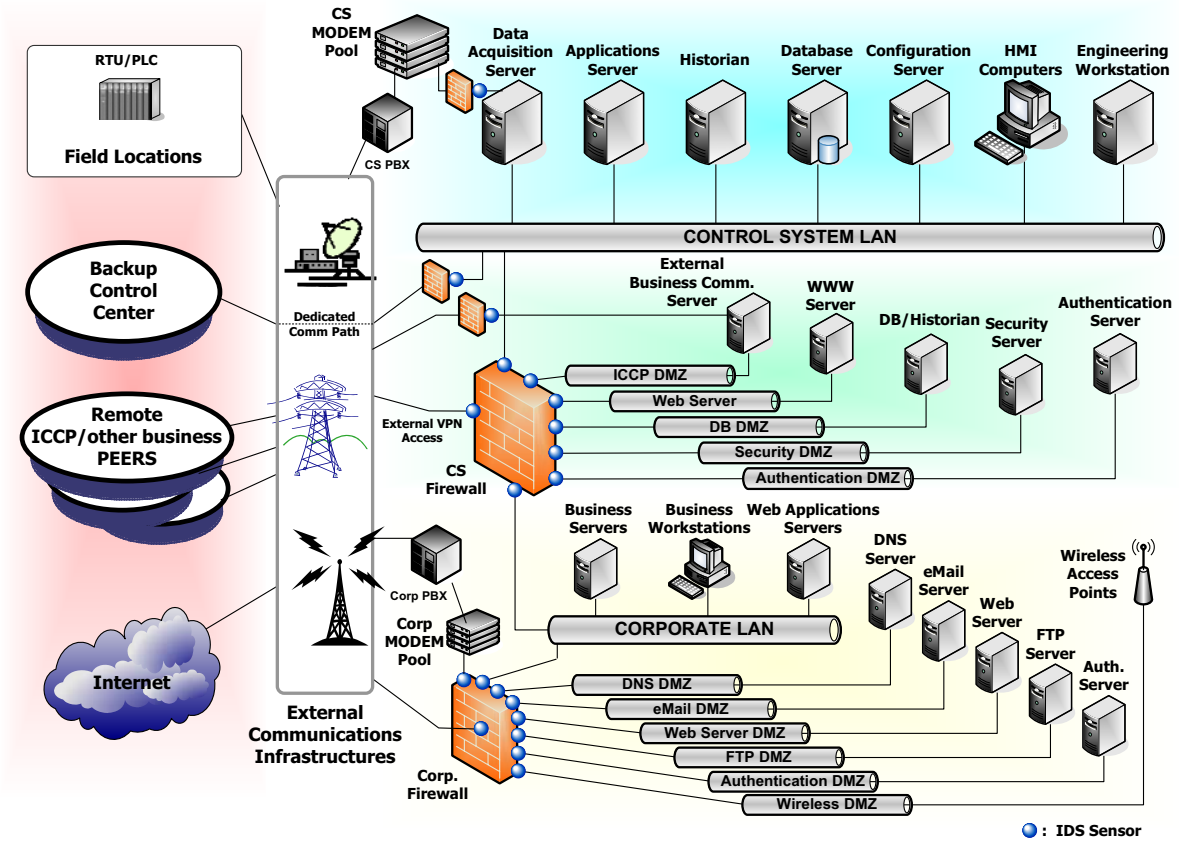
Voice Network Management Best Practices; Secure Logix Whitepaper

VoIP: Making PSTN Modems Work on IP Networks; Keith Chu and Michael Metzger; CommsDesign March 12, 2003

Appendix B

Recommended Network Architecture

Appendix B



DHS Recommended Network Architecture Design for Control System Security.[h]

h. DHS Control Systems Security Program, Secure Architecture Design