Security Issues of Integrating a Stand-alone System into Corporate Network

Edward Jirak

Edward Jirak

GSEC

Version 1.3

original submission

SANS Conference
Vancouver

Nov.15 – 20 2001

Security issues of integrating a stand-alone system into corporate network

Summary

This paper describes some methods to improve security on systems that were originally designed as stand-alone or where security issues were ignored. It points out the weaknesses which have to be addressed before integration. It describes various channels into the system and explores ways on how to protect these pathways from being exploited.

Some implementations of Supervisory Control And Data Acquisition (SCADA) are such systems.

What is SCADA?

Supervisory Control And Data Acquisition is a top-level control system, which monitors and controls the company's means of production. This may be water management, traffic control, a fleet of vehicles, power delivery and distribution, operation of a pipeline, a group of factories, etc. (see "What is SCADA ?" or "SCADA primer" for a more eloquent explanation).

Security issues with some implementations of SCADA

The design of the software assumed that it would be run on dedicated hardware, so there is no provision for different users having different priorities. Casual users running a query have the same priority as the control program. The user's accounts are shared and in some applications the passwords cannot be changed by users. The passwords are usually easy to guess. The more people sharing a password, the simpler the password tends to be. If it is complicated, a lot of users will write the password somewhere close to their computer and compromise it that way.

SCADA software usually goes through a large amount of customizations. Many of the changes are done in the field and version control tends to be sloppy or non-existent. Developer UserNames and passwords are sometimes reused on multiple projects for different customers. So an employee of the vendor may have access to many different projects in which he is not directly involved. Because so much work is done in the field, a customer may discover the password and be able to access competitor's systems (they all have maintenance modems). This may be true with other applications to some extent, but due to the degree of customization and custom "glue" software required to make SCADA work with the existing equipment, it is more likely.

Data gathering

Since data gathering is the main purpose of SCADA system, it uses various methods for collecting data, some of which may not be normally used by corporate systems.

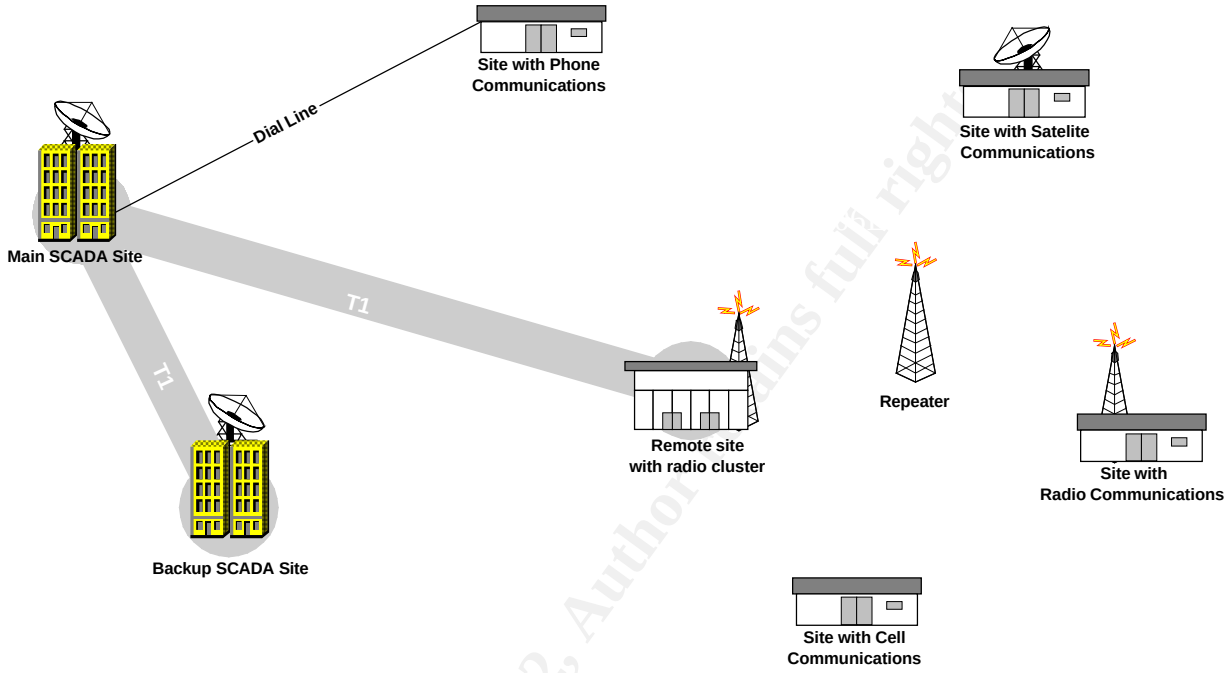

Figure 1 - Communication Means

Communications between major sites are via T1 links. A remote site (master) may have a cluster of minor sites (slaves) associated with it. It communicates with the cluster via VHF radio. The master initializes the communications and slaves answer only when addressed. The master forwards the slave's and it's own data to the main site via T1 link.

The dial lines are used for sites with Telephone company (Telco) service, where T1 link is not justified, or not available.

At locations where wired service is not available, but has a cell phone coverage a cell modem is used. Otherwise a satellite link has to be used.

The following table lists some security issues associated with the data gathering.

Pathway	Security Issues
Direct connection	secure

Pathway	Security Issues
Local Area Network•• (LAN)	normal security issues associated with LAN communications, usually under control of the corporate Information Technology (IT) department
Wide Area Network (WAN)	normal security issues associated with WAN communications, Telco and IT responsibility
Dial-up line	Security issues: denial of service by blocking the line, unauthorized access to the equipment, Trojan horse dial out.
Radio	Security issues: eavesdropping, denial of service, unlawful takeover of devices. Easy prey for denial of service attack, but also easy to locate the source of attack.
Cell phone	Security issues similar to radio communication.
Satellite	Relatively safe from casual snooper.

Data security

Various communication protocols are in use to share data. Older equipment uses proprietary protocols as each manufacturer tried to force customers to buy only his equipment. Over the past ten years, there has been a trend towards open protocols such as MODBUS, BSAP, EtherNet/IP and others. Interoperability is great, but widely published protocols are sometimes perceived as less secure.

Most of the installations communicate in the clear. The common wisdom is that the data by itself may have very little value and would not make sense to any outside person. The problem is, that by analyzing the traffic (even in proprietary protocols) from radio intercepts, one can easily discern the structure of commands. One argument is that it may not be possible to determine what the actual target device is for a command. Unfortunately even without this knowledge it is possible to cause extensive damage with possible fatal consequences.

SCADA integration into corporate network

Why integrate?

The time for decisions is getting shorter. A few years back, a daily report may have been sufficient to run a business effectively. Now it may be 15 minutes, or shorter. If the report

takes ten minutes to print and three hours to deliver, it is not much good.

SCADA provides up-to-the-minute information about the state of a most important part of an enterprise, that which is actually earning money. Making the information available to decision makers will result in a more efficient operation.

In the past, some business needs led to add-hoc interfaces into the SCADA system from the corporate side. Such action, endangers the security of both networks. The most perceived attacks actually originated with the "experts" on corporate side, hell bent on "improving" the SCADA system.

Historical differences

This may seem irrelevant, but because of the diverse development of corporate and industrial computer systems, one should be aware of the differences to minimize potential pitfalls during integration of the two branches.

Corporate computing

Information technology (IT) is driven by business needs, such as accounting, financial and human resources record keeping.

Security and confidentiality were always very important in these fields and were taken into account in the systems' design and operation.

These systems were, in most cases, originally based on extremely expensive mainframe computers, requiring air-conditioned, clean rooms so the physical security of the systems was important and easy to accomplish.

Generally, the computer usage spread from top down in a controlled manner, with little variation in hardware and software at anyone time.

Industrial computing

Industrial controls have their origin in mechanical devices such as a centrifugal governor, then progressed to single purpose stand-alone devices, such as pneumatic controllers, relay panels, current loop controllers, Proportional, Integral and Derivative (PID) loop controllers. The advent of Distributed Control Systems (DCS) and Programmable Logic Controllers (PLC) led to the integration of control functions into a single control system. In enterprises with widely scattered production facilities utilizing these control systems, there was a need to aggregate information collected at individual locations for

systemic supervision and control. This led to development of SCADA systems.

Industrial systems are rugged, designed to operate in hostile environments with easy access for maintenance and troubleshooting.

Use of industrial computing grew from the bottom up, in a rather haphazard way. Due to a long lifespan of the industrial equipment, systems are made up of a patchwork of various generations of devices. Some of these devices are obsolete, with insufficient documentation and support.

Until recently, security was not an issue. The general attitude toward cyber security was, that if somebody wants to do real damage, there are more efficient and destructive ways to do it, than by attacking a control system. A disgruntled employee may cause much more serious damage by sabotaging a piece of equipment he has expertise with, rather than a control system he is not as familiar with. As for the external attacker, blowing up a pipeline or a high voltage line is a much more spectacular way to let the world know about the chip on his shoulder.

Hardening of SCADA system

Educate employees

There is some valuable material available on the web aimed at control system specialists to educate them on the security issues. I would recommend a series of articles and slide presentations written by Joseph Weis: Information Security Primer, Information Security Needs for the Electric Power and Other Process Industries, Information Security Issues for Industrial Control Systems, by Eric J. Byres, P. Eng: NETWORK SECURITY IN PROCESS CONTROL ENVIRONMENTS, DESIGNING SECURE NETWORKS FOR PROCESS CONTROL. There are many others, for example: 5 Steps to a More Secure Network, Critical Infrastructure Protection - Physical distribution sector, SCADA makes you a target for terrorists.

Monitor emerging standards

Don't try to go it alone. If you recognized a problem, many others in your industry are probably aware of it and lots of ground is already covered (Natural Gas Utilities and Infrastructure Security). Excellent articles are available at http://www.riptech.com/securityresources/whitepapers.html. If the industry is vital to national security, government sites may be valuable sources of information (National Infrastructure Protection Center).

Find the suitable equipment

Locating equipment with all the bells and whistles for a new installation is not difficult (SCADA security is a critical issue, Intellution Enhances HMI/SCADA Security,). It is much more difficult to find equipment which would work within an existing infrastructure.

Protect communications

Data encryption

There is some new equipment coming up with the encryption capabilities built-in (see Encryption Provides Low-Cost SCADA Operating Security). This is however the most difficult safeguard to retrofit:

- Most of the existing equipment can't do it, so the additional devices would have to be purchased, software modified, people trained and it could take years to implement, due to the sheer numbers of devices of various models in the field.
- It would greatly complicate the commissioning, maintenance and troubleshooting of remote sites.
- Unacceptable costs to mitigate a vulnerability which is not considered serious enough.

Auto-answer modem protection

Auto-answer modems are used in some remote areas. SCADA calls them periodically for updates. They are also used at the main SCADA site for maintenance purposes. They could be simply switched off when not in use, but that is either not practical (remote sites) or unreliable (people forget). If the site is equipped with a Private Branch eXchange (PBX), it may be worthwhile to explore its security features, for modem protection. Otherwise the optimal solution may be an inexpensive call processor (for example The Stick, Versalink). These devices have multiple ports, each protected by a password (some have one port without password protection as default). They may effectively hide the modem from casual war dialing. There is a problem though, in that the modem number may already be known. The phone number should be changed, which is not always possible. The spare ports should be connected to a honeypot PC. This PC can be an obsolete type because the load is minimal.

Authentication

There is a big problem with some software designed for SCADA and similar systems in that, the UserNames are shared, so the security policy is tied to UserName and workstation name. This is inconvenient, since you either log in with the highest security, or login as a different user each time to be able to carry out various functions. Sometimes an application's licensing verification implementation can force the same limits at the operating system level. So at the server (and sometimes even on the host) the user must use a particular UserName.

The individual actions are not traceable, only the UserName is, and since UserNames are shared, auditing is impossible. The vendor may be unable or unwilling to modify his product in reasonable time and for a reasonable price.

One solution is to do authentication of an individual at the network level. Logging of individuals is possible only at the network. The internal users are authenticated by the corporate network log-in procedures.

The external users are authenticated by the password server. Instead of dialing directly into a SCADA network, the user would connect to a Public Key Infrastructure (PKI) password server and identify himself by means of proof-of-possession, such as Smart Card, or tokens like SecurID or iKey. Choice of the device will depend on what is already used by the corporation. If nothing is in use so far, this may be a nice pilot installation, but you will get stuck administering the tokens. IKey seems easiest and cheapest to implement. It is small and does not need specialized reader because it plugs directly into USB port.

Microsoft Windows 2000 operating system provides the Smart Card PKI logon capability. A Unix server could also be used, but Windows provide better support for the less experienced. Not perfect, but better than nothing.

Intrusion detection

If the modem connection is via PBX, monitoring may be handled there.

If the modem is connected via call manager, decoy modems can be plugged into spare ports and then to a honeypot PC. The honeypot would run an intrusion detection program.

If the Password server is used, it should also provide intrusion detection.

Auditing capability

Due to the poor design of some applications, the logging information is limited. The applications provide their own event logging by UserName / Workstation. This is not very good, but it can be improved by limiting authorized users to the absolute minimum. One way is to replicate the SCADA databases to a server on another network for use by casual users.

Database replication

A bright spot is that the data flow is only one way, from SCADA to the corporate database. As long as the rest of the company can access the data elsewhere, it has no need to communicate with the SCADA system itself. We want to provide access to the operational data to various authorized users, without allowing them direct access to the operational databases. Most of the office users require just a raw data returned by an SQL query, but the field personnel need associated live graphics such as schematics and trends provided by the Human Machine Interface (HMI), which is a part of the SCADA package. An additional license for SCADA will have to be purchased, just to drive the HMI displays required by the field personnel. Another way to provide information from this server, is to publish it on the company's Intranet.

Modified system

Due to the poor security of the original installation, I don't dare show it to the public. Similar systems are probably still in use elsewhere and I don't want to give the bad guys any ideas.

To keep the schematic reasonably simple, only basic components are shown. The real SCADA installation would be fully redundant.

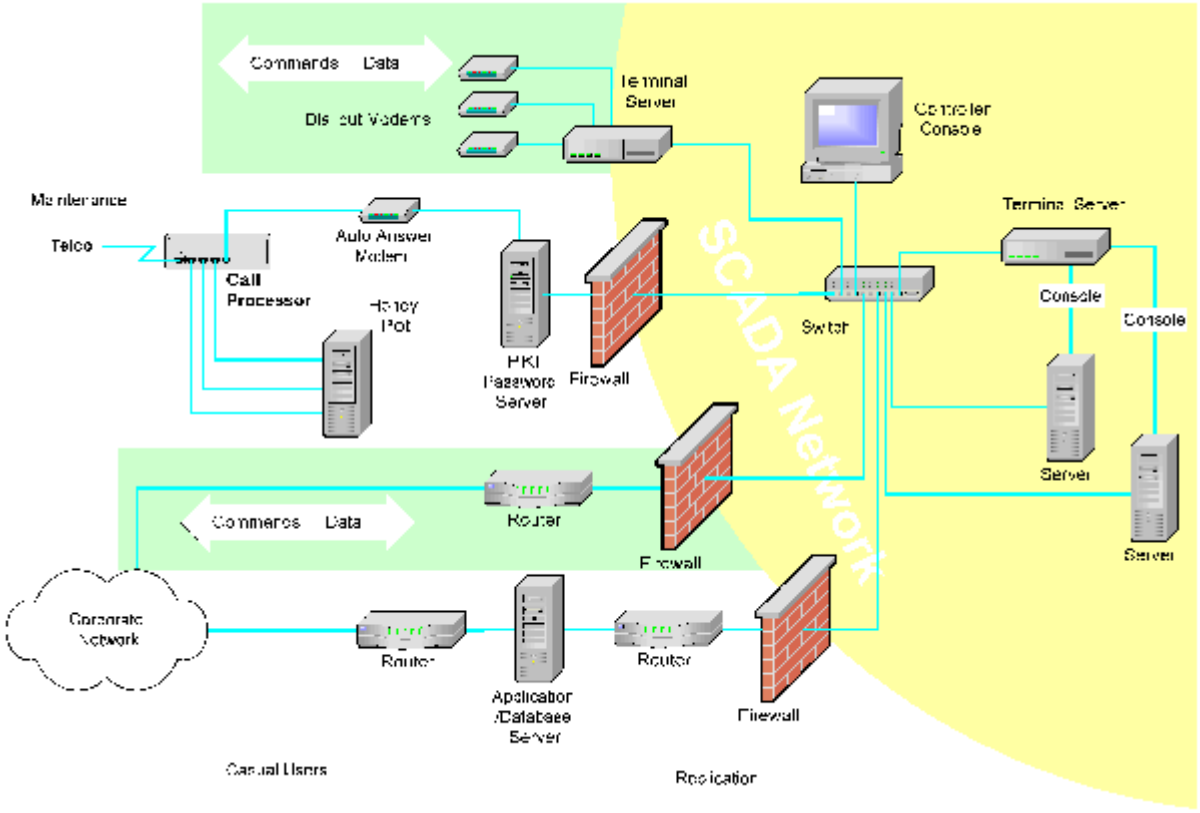

Figure 2 - Secured SCADA Installation

Notes

Corporate Network

Entire corporate network, such as LANs, WAN, T1 links and corporate security implementation.

The Commands / Data is on a separate network segment from the user's segment.

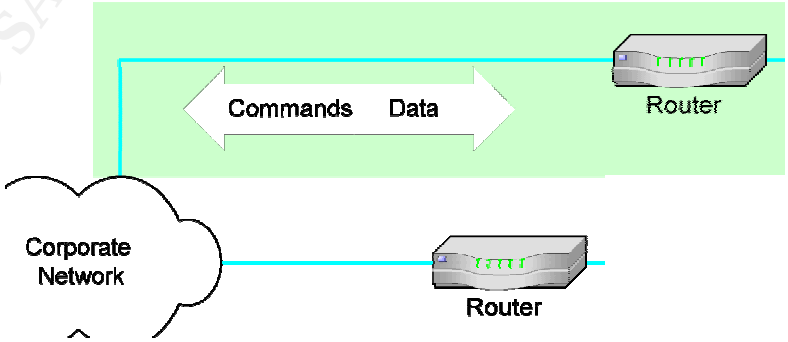

Figure 3 - Corporate network interfaces

Data gathering

The main vectors for data communications at the central site are:

- SCADA utilizes T1 links to exchange data with larger stations via the corporate network structure
- For the sites which do not have a T1 connection, regular phone lines are used. All data gathering modems are dial out only. SCADA initializes all calls. Terminal (a.k.a. Access) server allows sharing of an Ethernet line by multiple modems and has security features such as Access Control List (ACL), IP filtering, dial back etc.

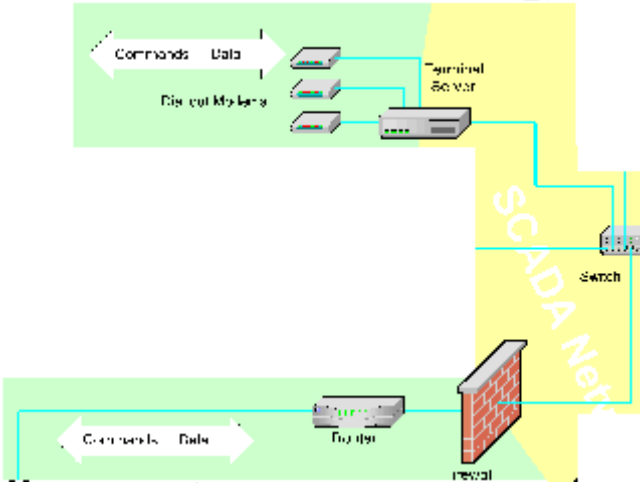

Figure 4 - Data gathering

Dial in provisions

For security reasons the corporate policy prevents RAS and VPN access to SCADA via the corporate network for third parties. It is a bit shortsighted, to facilitate the maintenance and troubleshooting of SCADA, auto-answer modems had to be installed directly into the SCADA system. These modems however, represent a dangerous entry point. To mitigate the possible threat, the following actions had to be taken:

- Each authorized user is supplied with a token, which provides both authentication and encryption.
- PKI login server screens the users, decrypts the traffic, proxy, auditing and Intrusion Detection (there should not be any intrusion past the call processor).
- Call Processor screens incoming calls and redirects the calls with the incorrect passwords into the honeypot

server. The similar setup is implemented at the remote stations containing auto-answer modems.

- Honey pot server logs all the failed connection attempts.

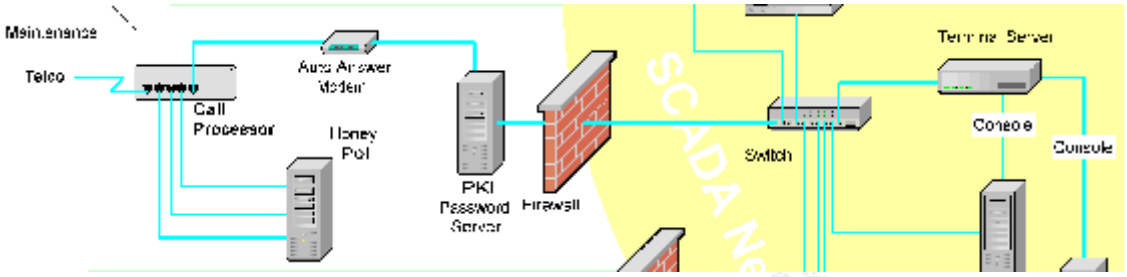

Figure 5 - Dial-in provisions

Some of the systems commands must be performed from console ports. The Terminal server allows access to the console port from the network.

Data reporting

The SCADA database is replicated to the isolated server. In addition to the database, the server is running the SCADA package to provide an HMI services to provide graphical information and/or the Intranet server.

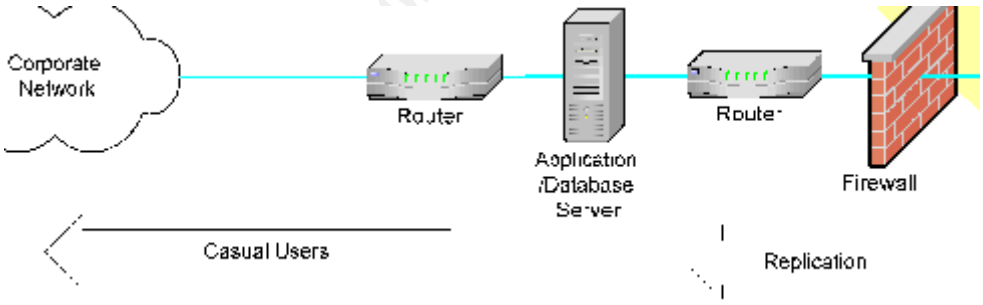

Figure 6 - Application and database server

Conclusion

This paper attempted to show what has to be addressed before a stand-alone system could be incorporated into the rest of corporate network and explored various means which could be used to provide essential security features. The main thrust was to limit number of users with access to the system. Where the access had to be allowed, the entry points were hardened to minimize possibility of unauthorized entry and to improve auditing capabilities of the system.

References

Infrastructure security

NIPC,, National Infrastructure Protection Center,,,17-Jan-02, http://www.nipc.gov/ ,Home, 01/20/02

Favley, Tom, "Securing Physical Distribution Sector", Commission on Critical Infrastructure Protection,,, http://www.ciao.gov/PCCIP/ac_physd.pdf,, 01/20/02

Schoenberg, Steve , "Sharing information with heightened security", InTech Online,,26-Oct-01, http://www.isa.org/journals/intech/opinion/1,1163,390,00.html, Home >> InTech Magazine >> Opinions >> Article ,01/20/02

Felton , Bob, "Assessing the e-threat to manufacturing", InTech Online,,06-Dec-01, http://www.isa.org/journals/intech/feature/1,1162,694,00.html, Home >> InTech Magazine >> Features >> Article,01/20/02

Call processors, Terminal (Access) servers

Faxswitch,, "Faxswitch.com - Automatic Telephone Switches Save Money",,,20-Jan-01, http://www.faxswitch.com/, Home,01/20/02

iTouch communications,, "Terminal Serving Products",,, http://www.itouchcom.com/products/product_cats.cfm?cid=termserv, Home > Products,01/20/02

PKI, Proof-of-possession

Microsoft Corporation, "Prerequisites for Implementing PKI", Planning Your Public Key Infrastructure,,2001, http://www.microsoft.com/WINDOWS2000/techinfo/reskit/en/Deploy/dgch_pki_kvsq.htm, MSDN Home > MSDN Library > Security > ,01/20/02

Microsoft Corporation,, "Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon", 27/Apr/00, http://www.microsoft.com/WINDOWS2000/techinfo/administration/security/smrtcrdtr.asp, Windows 2000 > Technical Resources > Administration ,01/20/02

Microsoft Corporation,, "Smart Card Enrollment Control", Microsoft Platform SDK,,2002, http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/scenr_portal_71np.asp, MSDN Home > MSDN Library > Security > Certificate Services and Components,01/20/02

Rainbow Technologies,, "Windows® 2000 Logon", About USB Smart Tokens and Smart Cards,, 2012/04/01, http://www.rainbow.com/ikey/win2000logon.html,, 01/20/02

RSA Security,, "RSA Keon UNIX Platform Security",,,2000, http://www.rsasecurity.com/products/keon/whitepapers/ups/KUPS_WP_0400.pdf, RSA Security Home > Products > RSA Keon ,01/20/02

RSA Security,, "SecurID", Securing Your Future with Two-Factor Authentication,,, http://www.rsasecurity.com/products/securid/demos/SecurIDTour/RSASecurIDTour.html, RSA Security Home > Products > RSA SecurID ,01/20/02

Smart Card Alliance,, Home page,,,2002, http://www.smartcardalliance.org/,, 01/20/02

Honeypots

Lance Spitzner, Honeypots, http://www.enteract.com/~lspitz/honeypot.html

Last Updated: July 24th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Riyadh July 2019	Riyadh, SA	Jul 28, 2019 - Aug 01, 2019	Live Event
SANS July Malaysia 2019	Kuala Lumpur, MY	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Boston Summer 2019	Boston, MAUS	Jul 29, 2019 - Aug 03, 2019	Live Event
SANS Melbourne 2019	Melbourne, AU	Aug 05, 2019 - Aug 10, 2019	Live Event
Security Awareness Summit & Training 2019	San Diego, CAUS	Aug 05, 2019 - Aug 14, 2019	Live Event
SANS London August 2019	London, GB	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Crystal City 2019	Arlington, VAUS	Aug 05, 2019 - Aug 10, 2019	Live Event
SANS Prague August 2019	Prague, CZ	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS Minneapolis 2019	Minneapolis, MNUS	Aug 12, 2019 - Aug 17, 2019	Live Event
SANS San Jose 2019	San Jose, CAUS	Aug 12, 2019 - Aug 17, 2019	Live Event
Supply Chain Cybersecurity Summit & Training 2019	Arlington, VAUS	Aug 12, 2019 - Aug 19, 2019	Live Event
SANS Virginia Beach 2019	Virginia Beach, VAUS	Aug 19, 2019 - Aug 30, 2019	Live Event
SANS Amsterdam August 2019	Amsterdam, NL	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS Chicago 2019	Chicago, ILUS	Aug 19, 2019 - Aug 24, 2019	Live Event
SANS MGT516 Beta Three 2019	Arlington, VAUS	Aug 19, 2019 - Aug 23, 2019	Live Event
SANS New York City 2019	New York, NYUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, DK	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Hyderabad 2019	Hyderabad, IN	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Philippines 2019	Manila, PH	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Brussels September 2019	Brussels, BE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Canberra Spring 2019	Canberra, AU	Sep 02, 2019 - Sep 21, 2019	Live Event
SANS Munich September 2019	Munich, DE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Network Security 2019	Las Vegas, NVUS	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, NO	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS Dubai September 2019	Dubai, AE	Sep 14, 2019 - Sep 19, 2019	Live Event
SANS Raleigh 2019	Raleigh, NCUS	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Paris September 2019	Paris, FR	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Rome September 2019	Rome, IT	Sep 16, 2019 - Sep 21, 2019	Live Event
Oil & Gas Cybersecurity Summit & Training 2019	Houston, TXUS	Sep 16, 2019 - Sep 22, 2019	Live Event
SANS Bahrain September 2019	Manama, BH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
DFIR Summit & Training 2019	OnlineTXUS	Jul 25, 2019 - Aug 01, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced