Global Information Assurance Certification Paper

Security Issues of a Power Plant Control System Implementation

James Morrow

18 September 2002

GSEC v1.4 Option 1

Abstract

This paper deals with security issues of an automated control system developed by two federal agencies operating in the electric power industry. The control system, the general nature of the electric utility industry, and some of the collateral issues related to the system implementation will be introduced. After examining the threat, an outline for managing the risk will be presented. The paper is intended to serve as a discussion piece for those responsible for system security. Key points of discussion will be procedural and policy issues in a deployment across jurisdictional boundaries.

The Control System

The particular system being addressed here is the Generic Data Acquisition and Control System (GDACS) as developed by the U. S. Army Corps of Engineers (USACE) and The Bonneville Power Administration (BPA) for use at multiple USACE hydropower generation facilities in the Pacific Northwest. A write-up on the system appeared in the March 2002 Hydro Review magazine.

To summarize, GDACS is a scalable system built on top of commercial, off-the-shelf software and running on Intel hardware. There is custom software to provide the functionality required for the application, but the key feature making this a generic application is the use of standardized interfaces between proprietary components, i.e. TCP/IP over Ethernet.[1] The generic features that made it economically attractive as a control platform also make it attractive as a data collection platform for other users. This is the source of one problem, but definitely not the only one.

The data used as input to the control system has value beyond the control function. It makes economic sense to collect data once and minimize handling in route to the end user; therefore it is best to automate the collection and dissemination of the information. Since the Internet connection is a common media for all parties, it is the logical distribution method. It is also the common media for millions of other people, some with less than noble intentions. While the Internet connection is a potential security threat, it is not the only threat that needs to be addressed when reviewing system security.

The Environment for Implementation

The term critical infrastructure as used here is consistent with the definition resulting from the Presidential Commission on Critical Infrastructure Protection convened by the Clinton administration in 1998. The findings of that commission were the basis of a Presidential Decision Directive (PDD-63), creating the Critical Infrastructure Assurance Office (CIAO) within the Department of Commerce.[2] The major initiatives of the CIAO include assessing threats, raising awareness, and coordinating efforts between the public and private sectors.[3]

Another development that resulted from the Presidential Commission on Critical Infrastructure Protection was the formation of the National Infrastructure Protection Center (NIPC) within the Department of Justice's FBI. Predating the issuance of PDD-63, and the companion PDD-62 focusing on unconventional threats, NIPC is the government lead in a joint public/private sector effort to assess vulnerabilities and respond to attacks on the critical infrastructures.[4]

Beyond critical infrastructure assurance, individual government agencies developed their own programs tailored to address their information assurance needs. Within the DOD, Department of Army, and USACE there are a number of programs that impact this system implementation. While these programs must be complied with, they can present their own challenges to a security program.

In a broader sense, because this system inter-connects with the BPA system, which falls under the jurisdiction of the Department of Energy (DOE), there are potential impacts from that agency's security programs as well.

During the time all of this was happening, the industrial control market also experienced many changes. Customer demand is forcing the industry away from proprietary systems and components and toward more industry-standard based equipment. This has resulted in adoption of protocols such as TCP/IP for networking in spite of its limitations and vulnerabilities. In some cases brute-force application of hardware is used to offset the performance limitations, but in the push to achieve specified performance levels, security issues are often marginalized until after installation.

Beyond the push to achieve specific performance criteria required of real-time control systems, the system designers are faced with adapting to the new technology they are working with. The concept of security isn't new to the designers but the full implications of the security impacts of the new technology are not openly advertised or quickly appreciated.

Compounding the problem in the electric utility industry are regulatory factors. Industry deregulation requires more open access to the power grid. In order to operate the grid in a reliable manner, there will be more control system interconnections. The interconnections add security vulnerabilities.

The Threat

The first thing to do when discussing cyber threat to the control system is check conventional logic at the door. The common threats are the result of what most people would consider unconventional thinking or motivation. When people are involved, either insiders or outsiders, they usually count on routine and predictable behavior to do their damage. Other threats, such as those to the physical plant, can also result from excessively conventional thinking. It is essential to think outside the box when evaluating the matter of threats.

Common usage has made the term hacker synonymous with the concept of cyber threat. Most characterizations of the hacker community portray a pyramid with the broad base of "script kiddies" or novice hackers and the peak representing the few very knowledgeable or elite hackers. The pyramid portrays not only a wide range of skill level, but also a spectrum of motivation ranging from intellectual curiosity to pathological behavior. While many discount the threat of the generally clueless majority, Crume makes a good point that it should be feared for lack of skill as much as the criminal genius is feared for mastery of the craft.[5]

Although it is relatively easy to stop most novice hackers at the perimeter of the system, this doesn't work for the insider. Whether the action is ignorance or malicious intent, the threat is just as real. Facts are lacking, but some reports attribute more damage to insiders than outside forces.

Because the information used for the control system reflects what is happening real-time in the production environment it has value beyond its initial intended use. Economics does not support the multiple collection, handling, and distribution of the information so it is a logical step to interconnect the control system with the business or administrative information systems. This will most likely mean some sort of pathway to the Internet and the more than 500 million users connected to it.[6]

The Internet has brought many things, but probably nothing is more of a mixed blessing in its impact than statistics. Generating numbers is much easier than producing, and interpreting, quality statistical information. Often the numbers create more of an impression than is warranted by the supporting data. In keeping with the spirit of the Internet here are some numbers to emphasize a point. Consider the 500 million Internet users mentioned above. By some unsubstantiated estimates as many as 1 percent, or 5 million, of them could be classified as some sort of hacker. Of that group assume one percent, or 50,000, are above the novice level. Of that 50,000 assume there is again one percent, or 500, at the pinnacle of the hacker pyramid. Even one percent of that much criminal genius could wreak havoc on a system.

Several estimates put the number of Internet users at 1 billion by 2005. If the hacking community grows at the same rate, the threat should nearly double in the next 3 years. Since the general trend is for sustained growth through the foreseeable future, the problem will only get worse.

The following examples provide a snapshot of what is being published about the threat facing the nation's critical infrastructure:

> -Computer Security Institute Press release, April 2002.
>
> The United States' increasing dependency on information technology to manage and operate our nation's critical infrastructures provides a prime target to would be cyber-terrorists. Now, more than ever, the government and private sector need to work together to share information and be more cognitive of information security so that our nation's critical infrastructures are protected from cyber-terrorists.[7]

> -From an article in InfoWorld, July 2002.
>
> Companies involved in critical infrastructure work, such as power and energy companies, were bigger targets for attackers, with 70 percent of such companies undergoing a severe attack in the six-month period, up from 57 percent facing such a threat in 2001, Riptech said. Overall, public companies were nearly twice as prone to attack as private companies, non-profit groups and government agencies, the study found. [8]

> -And in the following article from Federal Computer Week, July 2002.
>
> There is a 50 percent chance that the next time al Qaeda terrorists strike the United States, their attack will include a cyberattack, Rep. Lamar Smith (R-Texas) warned.
> In closed-door briefings for members of Congress, Smith said officials from federal law enforcement and intelligence-gathering agencies disclosed that al Qaeda operatives have been exploring U.S. Web sites and probing the electronic infrastructure of American companies in search of ways to disable power and water supplies, disrupt phone service and damage other parts of the critical infrastructure.[9]

But not everybody agrees about the nature or seriousness of the reported threat as noted in this excerpt from a San Francisco Chronicle Article of June 2002.

> Despite growing government concern that al Qaeda and its allies may try to use computers to disrupt electrical power grids, transportation systems and emergency communication networks, many experts on terrorism and computer security are skeptical about the overall menace of cyber-terrorism.[10]

One more quote from William Murray in SANS NewsBites, 10 Jul. 2002 may add some perspective on the problem of defining the threat.

> It has been suggested…that post 911 there is a moral equivalence between hackers and terrorists. …However, for security purposes it is useful to distinguish. For hackers, the network is both the target and the means: for terrorists the application is the target and the network merely the means. The hacker attacks targets of opportunity in a target-rich environment; the terrorist attacks targets of choice. The hackers are attacking instances of ubiquitous operating systems and applications where the necessary special knowledge is essentially public. The terrorist is after applications (where the money and the power are); where the necessary special knowledge

> is more narrowly held. The hacker succeeds because targets are numerous and most targets are the same. The terrorist succeeds because his cost of attack, while higher than that of the hacker, is very low when compared to the value to him (martyrdom and eternal fame and happiness?) of his success. There is some limit to what hackers will do. [11]

The outside threats may use the Internet as a common access route, but most commonality ends there.

Given the above, a very common response would be to remove the outside connection and assume the problem goes away. This may be a valid defensive option, but it comes with a price. First of all, it is a short-term fix. Information has value and all indicators point to increased access requirements for business or regulatory needs. Deciding to remove the link implies the information transfer process will be supported some other way. Secondly, the direct connection is not the only avenue for the threat from outside. Less direct connections such as on-demand dial-up can go overlooked and the proverbial "sneaker net" transport of recorded media can introduce malicious code. Obviously the external threat is compounded by direct connection to other networks, but it isn't limited to that connection.

Outside attacks are only 20 percent of the problem, the other 80 percent coming from insiders.[12] Textbook examples of the insider threat illustrate, again, the problem of conventional thinking when assessing threats. The insiders who are going to compromise the system are motivated by different factors than other employees. They don't even need to have access to the system to cause harm. Sometimes just knowledge of the system can be used. There are reports of employees offering to sell systems information on the Internet.

Obviously the problem is real and the threat exists. Fine points of the nature of the threat may remain debatable, but the broad-brush scope should be clear. It is diverse in scope, widespread in origin, unpredictable in nature, and present 24/7. It may not be imminently threatening, but it is formidable.

Fortunately the solution is much more manageable and outlined nicely by Dick Clarke, special advisor to the president on cyberspace security,[13] and reported by M. E. Kabay.[14]

> In any case, it doesn't matter who's causing damage to our information infrastructure. We're never going to be able to tell people in advance on a consistent basis who's going to attack what, when and how - so let's worry about the vulnerabilities, not the threats. …. Do your vulnerability analysis, rank the vulnerabilities, and start solving the problems step by step.

In other words, deal with the vulnerabilities that can be controlled rather than the threats that can't be. Risk is reduced since it is the product of threat and vulnerability.[15] The balance of this paper will deal with some of the vulnerabilities of the GDACS implementation and the issues for the organizations involved.

Vulnerabilities

Discussing the issue in a public forum might be raised as vulnerability by those who subscribe to the notion of "security through obscurity." Here it is a moot point because the information has been published as noted before, is almost certainly available under the Freedom Of Information Act (FOIA), and is being marketed by the contractor who did much of the development work for the government agencies. If it weren't already public information, this would still do little more than provide a false sense of security and provide the added burden of keeping secrets. The safest approach is to assume all vulnerabilities are public knowledge and then deal with them.

The brightest target on most people's radar screens are outside connections to the control system network. Obviously this includes the interconnection with the administrative LAN at each site, but it also includes the modems used for the Automatic Generation Control (AGC) link to BPA, the Columbia Basin Teletype (CBT) system, and the off-site support link.

Initially, no connections were to be allowed between the administrative and control networks. After much discussion, the decision was made to implement a connection. The belief was a connection was inevitable and the best course of action was to provide some standard of protection.

The initial connection to the administrative network will be through a hardware firewall configured to allow specific traffic to be pushed outward from the control network only. On the control system side, this connection will be to a dual-ported machine rather than directly onto the control network backbone. This will address the need to provide information about the operating plant to other users. It must be stressed that a firewall is the minimum protection for this connection, and there are ways of getting past them. The firewall is not a fix-all solution, and other supporting elements will be discussed later.

Without going into details, the nature of the existing AGC signaling protocol, it's implementation, and the physical link make it reasonably secure. There are plans to convert the signaling protocol to ICCP as well as increase the bandwidth of the physical link. In light of these changes, there should be an inter-agency review of the end-to-end connection and how it is handled. Before ICCP is implemented, all parties need to have a good understanding of the security features and limitations it brings with it.

The CBT link presents some concern because it isn't uniformly implemented across all plants. Since most long-term scenarios will dictate the need for automated reporting, a uniform plan should be developed for all sites. This will require coordination with a number of other elements inside and outside the parent agency.

The off-site support link is infrequently used, but it is a potentially serious problem. If not properly configured, it could be used to bypass the firewall and the protection associated with that portal. Although the plan is to physically disconnect it when not

required, it is essential that the modem auto-answer feature be disabled and only dial-out connections be allowed. This will allow the plant to control connections made to their system and reduce the risk from "war-dialers" if the modem isn't physically disconnected between uses.

Responses

Each implementation of the GDACS system will involve variations on the base system to connect to legacy system. When making these connections, it is imperative to maintain a clear definition of the perimeter of protection. This will be an ongoing issue as more digital based systems are installed throughout the plants to replace existing analog equipment and meet new requirements. To support this effort, the network needs to be well documented, clearly showing the location and destination of all connections to the Ethernet backbone.

Because the perimeter protection outlined above is not infallible, there need to be internal checks consistent with best practices. There should be at least one network based Intrusion Detection System (IDS) running inside the hardware firewall and tuned to detect unexpected activity.

Because of performance issues, it may not be feasible to run individual Host based IDS or firewall software on all machines, but it must be run on the machine with the direct connection to the firewall.

Progressing from perimeter protection inward, and following the philosophy of "Defense In Depth," all key machines on the network should be configured for "root kit" detection. In addition, all machines should be configured to maintain system log files and archive them at a central location for review.

The configuration of all machines running the Windows operating system should be reviewed against the latest version of the "SANS Securing Windows 2000 Step By Step Guide"[16] publication as a first step in dealing with the inherent security problems of Windows. This may identify vulnerabilities, which must be accepted because of other issues; the key thing is to identify and document them. The next step would be to implement the Consensus Baseline Security Settings jointly developed by the Center for Internet Security[17], DISA, NSA, NIST[18], SANS, and GSA.

Both of these measures combine the fundamental elements of any good security program and industry best practices. While they involve much more than how to do the initial configuration of the software, they are intended to harden the individual machine against the majority of system compromises.

Because so many manufacturers provide network services such as FTP and HTTP for customer convenience, every device connected to the Ethernet must be reviewed for services it runs. Those that are not essential should be disabled and those that are used should be configured securely.

The configuration of each machine must be documented to allow later verification, restoration, or re-evaluation.

One thing will become very evident at this phase of the security implementation; it is part of a process, not just a one-time effort. Many things recommended are the groundwork for follow-on activities. An example of this is anti-virus software, which must be installed and updated on a regular basis. Since the update is usually downloaded from the Internet there are procedural details that must be worked out. To comply with DOD regulations, these updates must come from specific sites.

Another point brought out is the need for policy to back up the program. This will be the most difficult phase of implementing security for this collection of systems. Because of past business practices and the underlying organization structure, it is going to be much easier to install a reasonably secure system than to maintain it that way.

Historically each site has had considerable freedom in how they operated their individual control systems after they were installed. Since it has worked well for years, there will be no perceived need to change. What has happened that begs for change is the transition from many isolated systems toward a much more widely distributed, and tightly integrated, system. With the prospect of this system being used for remotely controlling plants, this transition will be more deeply embedded. The more tightly integrated it becomes; the more the whole will be impacted by the actions of one element.

Organizationally the challenge is coordinating the efforts of entities under three different chains of command. Even if the three commanders agree to common policy, consistent implementation will not be assured. Past practices will only be changed when the end users believe in the need for change.

A prime example of this can be seen in the organization's Information Management arena. As part of the DOD, the Corps of Engineers is required to comply with DISA regulations. DITSCAP is one such effort and typical for a program implemented by policy. It has met with resistance and confusion as policy is filtered by local interpretation. The measure of full and effective implementation can probably be measured in years.

DITSCAP illustrates a problem of approaching policy as an end in itself. The process itself is informative and has merit, but it is complex, time consuming, and documentation intensive. It has little immediate impact on security. GDACS needs the backing of policy that has immediate, positive impact on system security while addressing the issues of existing regulations.

Policy that changes existing work habits must be backed up by education and enforcement to succeed. In light of past practices and lacking any existing organizational position to champion the case before the various commanders, policy

based security elements are going to be subject to local whim for implementation. One result is that the security of all GDACS systems will be judged by the performance of the weakest link, the first one compromised.

The matter of just how much system security is enough will largely fall out from the command decision on how to deal with this issue.

Challenges

Based on past practices, the types of things subject to compromise if not enforced by policy would be as follows: strong password implementation, physical security, system perimeter, and procedures for audit and review.

Passwords are a nuisance, particularly if they are complex and changed frequently. Strong password implementation would require both non-trivial and routinely changed passwords. One future option that might strengthen the authentication process while reducing the nuisance factor would be some form of smart token technology.

The suitable level of physical security needed in a controlled access facility is always going to be debated. It is included here because it is part of industry best practices and the existing practice is somewhat non-uniform between plants.

Compromise of the system perimeter over time is likely due to the competing demands of funding and operational needs. This might include addition of a new peripheral system, adding a link to a manager's desktop PC, or installing a modem to a control system PC to facilitate anti-virus software updates.

A poor policy implementation will have the greatest ramifications if there is failure to implement audit and review procedures. As noted before, it is one thing to install a secure system, quite another to maintain it in a secure state. In the cyber world, the nature of the threat will change over time. In the operating plant, the need to keep things running will result in temporary changes made to the system, and they may become more permanent than planned. It takes constant vigilance to maintain a given level of security. An audit process would be one mechanism to provide an independent evaluation and report on system status.

Part of the audit process should also include a review of log files generated by the system. These log files capture predefine system events and can reveal unusual activities otherwise unnoticed. This is the level most likely to reveal the activities of the professional hacker that has compromised the system. The probability of it happening is low, but the risk potential is high. In the unlikely event there were indications of criminal intent, the auditors would help preserve forensic information. This is one situation that is probably covered by existing policy.

The audit process would also be a key factor in providing information to the people using and maintaining the system. As noted before, education is essential to the success of policy implementation. Hopefully the audit process would be a positive one rather than an adversarial one. If the people doing the audit are knowledgeable of the system, and not just the audit process, it should be a positive exchange.

Recommended Actions

An audit process needs to be implemented across the system. In order to make it cost effective and maximize the use of specialized expertise, it should be a cooperative effort between the three command elements. The members should be knowledgeable of the control system and involved in developing the audit criteria. They should have reasonable belief their recommendations will be acted upon.

After the audit process is complete, it is critical to take action on any findings. Response is the third element of the security mantra "protect, detect, respond."

The essence of protection is to understand the vulnerabilities and deal with them. The threat vector is constantly changing but it is always directed to the vulnerabilities. The challenge then shifts from second guessing the adversary to understanding the system, making the task difficult instead of impossible. It isn't enough to know some particular component well; it is essential to understand the entire system. The essence of security is a comprehensive understanding of how the system components interact.

Auditing is all about detection. Many tools are available to help track the health of the system, but too often the value is lost because the results are ignored. This is also a lost opportunity to make needed corrections to the security configuration.

Auditing is the comprehensive review of the system and its tools to detect problems, hopefully before damage is done. After the fact it becomes forensics, and for the purpose of this discussion, best left to criminal experts.

The response to some system problems will not change much. The basic system value is the real-time operational response, rather than protection of historical or sensitive information, and manual system operation while restoring the automatic control is well practiced.

The response phase does need to be enhanced if an audit program is implemented. Since the audit phase is designed to detect problems with system security, procedures must be in place to correct those problems or system security will degrade over time. One element of the response plan must be designation of responsibilities and whom to call for expert assistance.

Summary

The paper summarizes the control system, the general nature of the electric utility industry, and some of the collateral issues related to the system implementation. The nature of security threats to critical infrastructure, as reported by the media, was explored. Although the nature of the cyber threat to critical infrastructure facilities is unclear, there is abundant indication it does exist. Rather than following a strategy focused on the ill-defined threat, a strategy of dealing with known vulnerabilities was proposed.

Following the discussion on known vulnerabilities, actions were proposed consistent with the security mantra "protect, detect, respond." The epicenter of an effective security movement must be an organizational response that empowers implementers to do the job and ensures it is done uniformly across the organization.

It is important not to lose site of the difference between protecting the corporate infrastructure and the unique position of GDACS in the realm of critical infrastructure. Developing GDACS required a different organizational approach. Protecting the investment in a changing world may be even more challenging. The real performance test is at the tip of the spear, or how this over-arching guidance is applied to the frontline of defense.

---

[1] Mahar, p.12-19.

[2] Braithwaite, p.48-5.

[3] CIAO.

[4] NIPC.

[5] Crume, p.25.

[6] Computer Industry Almanac, Press Release: 21 Mar. 2002.

[7] Computer Security Institute. Press release: 7 Apr. 2002.

[8]Costello.

[9] Matthews.

[10] Wallace.

[11] Murray.

[12] Office of Public Information. 10 Aug. 2002.

[13] The White House, Press Release: 9 Oct. 2001.

[14] Kabay, 07/01/02.

[15] "SANS Security Essentials II: Network Security,"

[16] Shawgo.

[17] Center for Internet Security.

[18] NIST.

List of References

CIAO. "About CIAO." URL: http://www.ciao.gov/publicaffairs/about.html (18 Sep. 2002)

Arena, Keeli and Ensor, David. "U.S. infrastructure information found on al Qaeda computers." © 2002 Cable News Network. 27 Jun. 2002. URL: http://www.cnn.com/2002/US/06/27/alqaeda.cyber.threat/index.html

Braithwaite, Timothy. "Y2K: LESSONS LEARNED FOR COMPUTER SECURITY." Computer Security Handbook, Fourth Edition. (New York: John Wiley & Sons, Inc., 2002) 48-5

Center for Internet Security. "Center for Internet Security Benchmarks and Scoring Tool for Windows 2000 and Windows NT." URL: http://www.cisecurity.org/bench_win2000.html (18 Sep. 2002)

Computer Industry Almanac, Inc. Press Release: "Internet Users Will Top 1 billion by 2005." 21 Mar. 2002. URL: http://www.c-i-a.com/pr032102.htm (18 Sep. 2002)

Crume, Jeff. "Inside Internet Security: What Hackers Don't Want You To Know." (Reading, MA: Addison-Wesley, 2000) 25

Computer Security Institute. Press release: "Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row." 7 Apr. 2002. URL: http://www.gocsi.com/press/20020407.html (18 Sep. 2002)

Costello, Sam. "Internet attacks up 28 percent in 2002" InfoWorld, 8 Jul 2002, URL: http://www.infoworld.com/articles/hn/xml/02/07/08/020708hnriptech.xml (18 Sep. 2002)

Kabay, M. E. "View From the White House." Network World Security Newsletter, 07/01/02, URL: http://www.nwfusion.com/newsletters/sec/2002/01416242.html (18 Sep. 2002)

Kabay, M. E. "Studies and Surveys of Computer Crime." © 2001, URL: http://www2.norwich.edu/mkabay/methodology/crime_studies.htm (18 Sep. 2002)

Kabay, M. E "Understanding Studies and Surveys of computer Crime." © 2001, URL: http://www2.norwich.edu/mkabay/methodology/crime_stats_methods.htm (18 Sep. 2002)

Lawson, Shannon M. "Information Warfare: An Analysis of the Threat of Cyberterrorism Towards the US Critical Infrastructure." SANS Institute, 19 Feb. 2002 URL: http://rr.sans.org/infowar/us_critical.php (18 Sep. 2002)

Loos, Mark. "Implementing a Local Security Program to Protect National Infrastructure System Companies and Facilities." SANS Institute, 8 Apr. 2002. URL: http://rr.sans.org/infowar/local_sec.php (18 Sep. 2002)

Mahar, James R. “Taking Control on the Columbia: Enhancing Reliability through Automation.” HYDRO REVIEW. March 2002 (2002): 12-19.

Matthews, William. “Al Qaeda cyber alarm sounded.” Federal Computer Week, 25 Jul. 2002. URL: http://www.fcw.com/fcw/articles/2002/0722/web-attack-07-25-02.asp (18 Sep. 2002)

Murray, William. “Are hackers the moral equivalent of terrorists?”
SANS NewsBites Vol. 4 Num. 28, July 10, 2002

NIPC. History. URL: http://www.nipc.gov/about/about3.htm (18 Sep. 2002)

Office of Public Information. “Latest Web Statistics.” 10 Aug. 2002. URL: http://www.intergov.org/public_information/general_information/latest_web_stats.html (18 Sep. 2002)

Perez-Lugones, Kimberly. “Protecting America’s Critical Infrastructure.” SANS Institute, 6 Sep. 2000. URL: http://rr.sans.org/infowar/protecting.php (18 Sep. 2002)

Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey." © 2002, Computer Security Institute URL: http://www.gocsi.com/press/20020407.html (18 Sep. 2002)

Rasmussen, Scott. “Centralized Network Security Management: Combining Defense in Depth with Manageable Security.” SANS Institute, 29 Jan. 2002. URL: http://rr.sans.org/practice/central_netsec.php (18 Sep. 2002)

Stidham, Jonathan. “Can Hackers Turn Your Lights Off? The Vulnerability of the US Power Grid to Electronic Attack.” SANS Institute, 26 Sep. 2001. URL: http://rr.sans.org/hackers/lights.php (18 Sep. 2002)

Swartz, Bruce. “Information System Security Evaluation Team: Security Insurance?” SANS Institute, 27 Jul. 2001. URL: http://rr.sans.org/audit/eval_team.php (18 Sep. 2002)

SANS Institute. “Windows 2000 Gold Standard Security Benchmark Training.” Website. URL: http://www.sans.org/Win2KWorldTour/ (18 Sep. 2002)

Shawgo, Jeff Editor, SANS Securing Windows 2000 Step By Step Guide. A Survival Guide For Windows 2000 Security: A consensus document by security professionals Version 1.5 The SANS Institute. 1 Jul. 2001. URL: http://store.sans.org/store_item.php?item=22 (18 Sep. 2002)

Stevens, W. Richard. TCP/IP Illustrated, Volume 1. (Reading: Addison Wesley Longman, Inc, 1994)

NIST, Computer Security Division. “System Administration Guidance for Windows 2000 Professional.” URL: http://csrc.nist.gov/itsec/guidance_W2Kpro.html (18 Sep. 2002)

Wallace, Bill. “Security analysts dismiss fears of terrorist hackers Electricity, water systems hard to damage online.” San Francisco Chronicle, 30 Jun. 2002. URL: http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2002/06/30/MN152350.DTL (18 Sep. 2002)

The White House, Press Release: “New Counter-Terrorism and CyberSpace Security Positions Announced.” 9 Oct. 2001. URL: http://www.whitehouse.gov/news/releases/2001/10/20011009-4.html (18 Sep. 2002)

The White House. “National Plan For Information Systems Protection.” Released 7 Jan. 2000. URL: http://cryptome.org/cybersec-plan.htm#President (18 Sep. 2002)

Last Updated: September 19th, 2017

Upcoming Training

Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**vLive**
Rocky Mountain Fall 2017	**Denver, CO**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, Denmark**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MD**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Community SANS New York SEC401*	**New York, NY**	**Sep 25, 2017 - Sep 30, 2017**	**Community SANS**
SANS DFIR Prague 2017	**Prague, Czech Republic**	**Oct 02, 2017 - Oct 08, 2017**	**Live Event**
Community SANS Sacramento SEC401	**Sacramento, CA**	**Oct 02, 2017 - Oct 07, 2017**	**Community SANS**
Mentor Session - SEC401	**Minneapolis, MN**	**Oct 03, 2017 - Nov 14, 2017**	**Mentor**
Mentor Session - SEC401	**Arlington, VA**	**Oct 04, 2017 - Nov 15, 2017**	**Mentor**
SANS October Singapore 2017	**Singapore, Singapore**	**Oct 09, 2017 - Oct 28, 2017**	**Live Event**
SANS Phoenix-Mesa 2017	**Mesa, AZ**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS Tysons Corner Fall 2017	**McLean, VA**	**Oct 14, 2017 - Oct 21, 2017**	**Live Event**
CCB Private SEC401 Oct 17	**Brussels, Belgium**	**Oct 16, 2017 - Oct 21, 2017**	
SANS Tokyo Autumn 2017	**Tokyo, Japan**	**Oct 16, 2017 - Oct 28, 2017**	**Live Event**
Community SANS Omaha SEC401	**Omaha, NE**	**Oct 23, 2017 - Oct 28, 2017**	**Community SANS**
SANS vLive - SEC401: Security Essentials Bootcamp Style	**SEC401 - 201710,**	**Oct 23, 2017 - Nov 29, 2017**	**vLive**
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**vLive**
SANS Seattle 2017	**Seattle, WA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS San Diego 2017	**San Diego, CA**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS Gulf Region 2017	**Dubai, United Arab Emirates**	**Nov 04, 2017 - Nov 16, 2017**	**Live Event**
Community SANS Colorado Springs SEC401**	**Colorado Springs, CO**	**Nov 06, 2017 - Nov 11, 2017**	**Community SANS**
SANS Miami 2017	**Miami, FL**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
Community SANS Vancouver SEC401*	**Vancouver, BC**	**Nov 06, 2017 - Nov 11, 2017**	**Community SANS**
SANS Sydney 2017	**Sydney, Australia**	**Nov 13, 2017 - Nov 25, 2017**	**Live Event**
SANS Paris November 2017	**Paris, France**	**Nov 13, 2017 - Nov 18, 2017**	**Live Event**
Community SANS St. Louis SEC401	**St Louis, MO**	**Nov 27, 2017 - Dec 02, 2017**	**Community SANS**
Community SANS Portland SEC401	**Portland, OR**	**Nov 27, 2017 - Dec 02, 2017**	**Community SANS**
SANS San Francisco Winter 2017	**San Francisco, CA**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS London November 2017	**London, United Kingdom**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS Khobar 2017	**Khobar, Saudi Arabia**	**Dec 02, 2017 - Dec 07, 2017**	**Live Event**
SANS Austin Winter 2017	**Austin, TX**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**