Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Defense in Depth For Private Wireless Communications Networks: A Case Study

Private wireless communications networks utilized by emergency services agencies are vital components of the nation's critical infrastructure. Reliable communications are essential for our nation's "first responders," and successful attacks on these networks could interrupt mission critical operations, compromise restricted information, and contribute indirectly to loss of lives. While the threats of physical attack on infrastructure and interception of wireless communications are long established in the emergency serv...

Copyright SANS Institute
Author Retains Full Rights

AD

Defense in Depth
For
Private Wireless Communications Networks:
A Case Study

Walt Anderson
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b
Option 2: Case Study in Information Security

8/10/03

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

1. Introduction:

Private wireless communications networks utilized by emergency services agencies are vital components of the nation's critical infrastructure. Reliable communications are essential for our nation's "first responders," and successful attacks on these networks could interrupt mission critical operations, compromise restricted information, and contribute indirectly to loss of lives. While the threats of physical attack on infrastructure and interception of wireless communications are long established in the emergency services environment, the threat of electronic attack upon the system infrastructure is a newly emerging and challenging issue. Evolutions in system infrastructure technology, combined with new patterns of system usage, maintenance, and interconnection with external networks, are exposing private wireless communications networks to many of the same threats faced by the enterprise Information Technology world: imagine the next NIMBDA as inhibiting radio communications between police officers and firemen at the scene of a plane crash.

This paper will describe the steps taken by a manufacturer and integrator of private wireless communications systems to enhance the security of its radio network solution. A defense in depth approach improves the value of this vendor's offering and better enables emergency services agencies to defend their communications networks from the threats posed by electronic attacks. This paper examines the threats and vulnerabilities of private wireless communications infrastructures, discusses the selection and prioritization of security countermeasures, and describes the security enforcing equipment and security management services that are now being introduced.

Note: this paper is intended for illustrative purposes only; it shall not be interpreted to make any claims regarding the features, functions, characteristics, terms, conditions, or performance of any specific manufacturer's products or services.

2. The "Before" State

This section will describe the historical security posture of radio networks and the traditional security focus of their owners and operators. It will also describe evolutions in system technology and system usage that may combine to expose radio networks to electronic attack, and will conclude by summarizing the potential threats, vulnerabilities, and resulting risks to these radio networks.

2.1. Background

Private radio networks have traditionally been "closed" systems, dedicated exclusively to voice communications. Network infrastructures were based on custom hardware elements running embedded software, and infrastructure

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

elements were connected together via proprietary protocols and circuit-switched links. Remote access to system equipment was minimal, and maintenance activities that could be performed remotely were also limited. Connectivity with external networks was limited to proprietary protocols and well-defined, special purpose links. For most practical purposes, a communications system infrastructure could be described as a closed network of black boxes.

Because radio communications are considered “mission critical” to the emergency services sector, private radio network infrastructures have been engineered for maximum availability and uptime. Power failures, equipment failures, accidents, natural disasters, and deliberate physical attack have been the primary threats of concern. Correspondingly, radio network call-processing elements have been designed for redundancy and automated fail-over. Tower sites have mature specifications for handling lightning strikes and power failures. Systems utilize overlapping coverage, alternate paths and redundant links, and are capable of graceful fallback to reduced modes of operation in the event of equipment failure. Infrastructure management systems have evolved to quickly identify equipment failures, alerts, and alarms. In addition, many systems utilize extensive physical sensors for tracking temperature and humidity, fire alarms, door & window alarms at remote sites, and so on. Handheld radios are also quite rugged: they comply to mature specifications for impact resistance, extreme operating temperatures, resistance to smoke, wind, rain, and blowing sand, water immersion, and more. His radio is a first responder’s lifeline, and with respect to physical threats, these systems are some of the most reliable communications networks in the world.

While system availability is now understood as a dimension of security, “security” for private radio networks has traditionally focused almost exclusively on confidentiality of wireless voice transmissions. Wireless eavesdropping by criminals, terrorists, and adversarial governments has been the “security” threat. Powerful encryption for wireless voice transmissions has been commercially available for several decades, but until the early 1990’s--when digital voice processing and digital transmission technologies were introduced to this environment--encryption was expensive and largely synonymous with reduced audio quality and reduced range. Correspondingly, utilization of encryption was reserved for a minority of emergency services users, such as federal law enforcement agencies. Nevertheless, encryption and key management are mature technologies in the private radio network environment. For example, encryption methodologies and algorithms are included in the Association of Public Safety Communications Officers (APCO) Project 25 and Terrestrial Trunked Radio (TETRA) standards for digital radio systems, and several vendors supply cryptographic implementations that are certified as compliant to the National Institute of Standards, Federal Information Processing Standard FIPS-140-1 as well.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Private wireless communications systems have historically been owned and operated by well-defined organizations. Many state, local, and federal law enforcement and emergency services agencies independently owned private radio systems, and have staffed an internal communications department chartered with maintaining and operating the radio system. The expertise of the "radio shop" department has largely focused on radio system specific technologies such as radio frequency (RF) transmission and propagation characteristics, tuning, power levels, and antenna related concerns. Radio shop technicians are experts at provisioning and maintaining radio system equipment. They have not, until very recently, been exposed to IP-based networking, nor have they any experience in handling the threats posed by malicious software and electronic attack.

2.2. Evolution of Vulnerability:

There are three significant and intertwined evolutions that have combined to increase the potential vulnerability of private radio networks to electronic attack. First, systems are becoming larger and are shared by multiple organizations. Second, connectivity between the radio networks and external networks is rapidly expanding. And finally, the underlying technology of communications infrastructures has migrated from closed, proprietary elements and protocols to commercial computing platforms and IP based networking. This section will briefly elaborate on each of these evolutions and conclude by describing the primary vulnerabilities that private radio networks now possess.

2.2.1. The Evolution Towards Larger System Size And Multiple Ownership

Because operating and maintaining a private wireless communications network is an expensive undertaking, publicly funded agencies have been driven to leverage investments in communications infrastructures across multiple organizations. Radio systems can now be shared by dozens, even hundreds, of end user agencies and cover huge—statewide and larger--geographic areas. A system supporting one metro area can be shared by the city government, local police and fire departments, public works agencies, ambulance services, and educational institutions; it will also interoperate with the state police, port and border control authorities, the local FBI office, US customs service, and any number of other agencies. This means that what was once the province of a single "radio shop" can now be serviced and supported by a diversity of organizations.

There are multiple implications of this trend. Different organizations naturally have differing levels of training and expertise, have different responsibilities and chains of authority, and have differing security policies. The sheer volume and turnover of employees, and sometimes competitive politics among organizations, further aggravates the situation. It becomes difficult to establish clear authority for security and security policies, which in turn makes it easier for mistakes to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

happen and further opens the door to social engineering and insider attack. For example, just knowing who all the technicians and operators are, let alone ensuring that proper security mechanisms and policies are applied, can be problematic. And it is worth noting that a CompTIA study identified human error as a major underlying factor in 63% of security breaches.[1]

2.2.2. The Evolution Towards Expanding Connectivity

Greater connectivity between private radio networks and external networks is driven by technological capability, the desire to improve the efficiency and accuracy of emergency services missions, and the need to de-centralize command & control. Enabled by advances in digital wireless communications technology, the newest form of connectivity is "integrated data:" just as we are now able to send text messages in addition to voice calls with our digital cell phones, emergency services organizations are able to transmit data on their private wireless networks. Police officers can now download mug shots and check license plates using the same network that was once used only for voice. Firemen can receive maps and structural plans of buildings. Utilities workers can report meter readings. Naturally, these capabilities require access to an array of databases. And these databases are owned and maintained by the enterprise-side IT departments of their home agencies.

Another significant and expanding form of network connectivity is Computer Aided Dispatch (CAD). A modern dispatching center is a multi-function command center. A dispatch operator may simultaneously field a 9-1-1 emergency telephone call, dispatch a squad car by radio, and pull up a digital map and supporting data. The operator's CAD terminal is the aggregation point for all of these activities: it is an element of the private radio network, and it is also connected to the telephone network and several databases, which may in turn reside on one or more external networks.

Network management requirements are also driving increased connectivity with external networks. Radio system managers are the persons responsible for ensuring that the equipment is up and running, for provisioning new radios and network equipment, and for collecting system usage and subscriber billing information. Formerly centralized in one "radio shop," now each agency may have some number of system managers. These system managers work from network management terminals that are elements of and/or interact with interfaces and applications inside the private radio network. At the same time, each system operator may need access to enterprise side applications, and the radio system may need to forward events and alarms to a "manager of managers" located on the enterprise side.

---

[1] Leydon, http://www.theregister.co.uk/content/55/29827.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Therefore, while a private radio network is not Internet facing, it can be connected to multiple enterprise networks for multiple purposes. These external networks are owned and maintained by a diversity of organizations, some of them are quite large, e.g. citywide and statewide IT networks, and many of them will contain Internet facing resources. Understanding who has what access to which radio system resources becomes a challenge and increases the vulnerability to insider attack. The vulnerability to secondary infection also becomes quite real: a virus or worm that infiltrates one of these external networks could in turn propagate into the radio network. And in the case of integrated data, an added complication is the vulnerability to a wireless-originated attack upon the radio network infrastructure or upon connected customer networks.

2.2.3. The Evolution Towards Commercial Technologies And Protocols

In order to accommodate needs for increased size, scalability, performance and functionality, radio network elements have evolved to utilize commercial computing platforms, protocols, and links. Private wireless communications infrastructures now consist of heterogeneous arrays of computing platforms built upon Windows, Unix, and Linux operating systems. Infrastructure links can utilize commercial switches and routers. Communications between radio network elements utilize IP protocols, and network interfaces for CAD, integrated data, and network management also utilize standard ports and protocols. And radio networks also support powerful remote access capabilities for monitoring and maintenance.

A significant implication is that vulnerabilities in these underlying platforms can now jeopardize the availability of the radio communications network. In this context, a vulnerability is a bug or weakness in a piece of software that, if exploited, can enable an attacker to gain access to or privileges on a target system. As vulnerabilities are discovered, hackers develop malicious software programs (viruses, worms, etc) to exploit them, and spread these programs throughout the Internet—often in a ready to use "toolkit" format that makes them simple to use by "script kiddies," an industry term for hackers who indiscriminately wield ready-made attack tools against any available targets. The number of known vulnerabilities continues to grow:

Vulnerabilities Reported to CERT/CC, 2000-2003[2]

Year	2000	2001	2002	2003*
Vulnerabilities	1,090	2,437	4,129	1,993

*Note that 2003 numbers are through the 1st and 2nd quarters alone.

[2] CERT/CC, http://www.cert.org/stats/cert_stats.html#vulnerabilities

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Radio networks are now vulnerable to these exploits due to their expanded connectivity. The "SQL_Slammer" or "Sapphire" worm is a disturbingly relevant example of a malicious software threat: it exploited a buffer overflow vulnerability in Microsoft's SQL Server, was self-propagating, and it spread worldwide to over 75,000 systems, infecting 90% of these within the first 10 minutes of its release.[3] Among its many impacts, it reduced operations in a 9-1-1 Public Safety dispatching center in Seattle, WA to pencil and paper for several hours.[4]

Another implication arises from how modern communications infrastructures are serviced. Because today's radio network may consist of a heterogeneous array of computing platforms, one of the most versatile tools for servicing such networks is a personal computer. Networks support local and remote computer access, including modem dialup for this purpose. While an operational necessity, this also means that radio networks are potentially vulnerable to unauthorized computer access and to secondary infection by a virus or worm carried by a service person's laptop. Recalling the complexities of multiple ownership, IT attacks can now be carried out unwittingly and even inadvertently: a hapless technician, with a laptop that has unknowingly been infected with a virus or worm, can accidentally infect a communications network during the course of a routine service operation.

2.2.4. Summary of Threats and Vulnerabilities

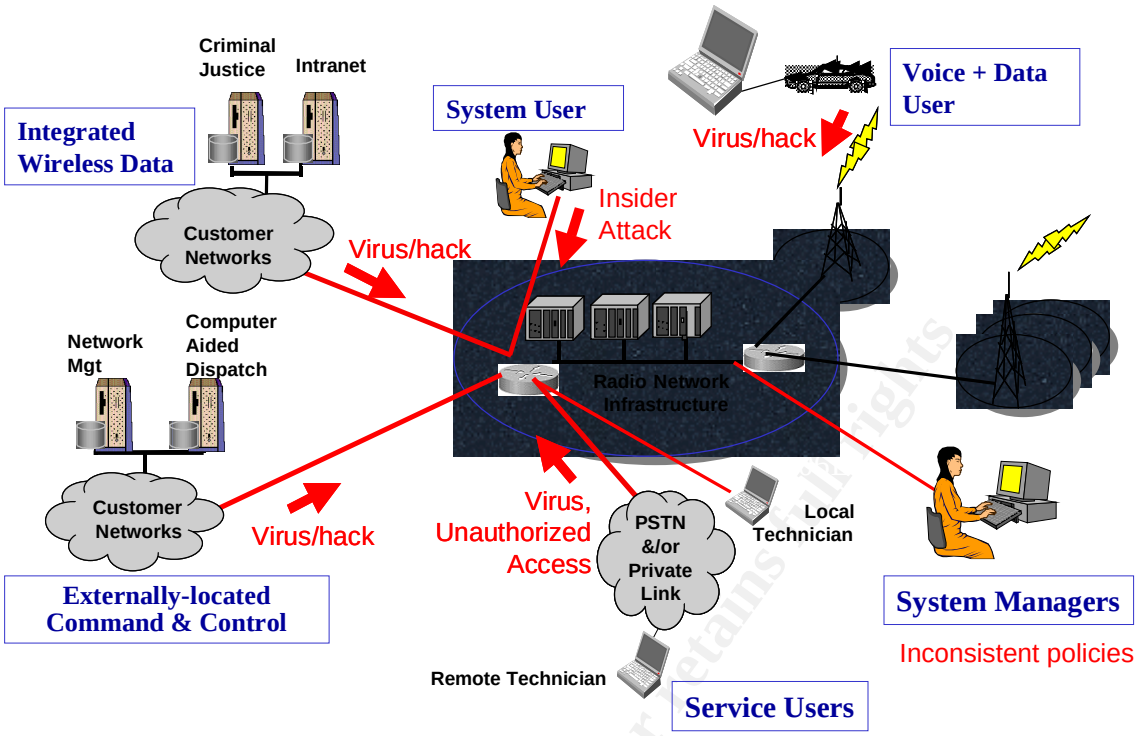
Due to the evolutions towards multiple ownership, expanded connectivity, and adoption of commercial platforms and protocols, radio network infrastructures are now vulnerable to a number of threats, as identified in the figure below:

Figure 1: Threats and Vulnerabilities of Radio Network Infrastructures

[3] Moore, http://www.caida.org/outreach/papers/2003/sapphire/

[4] Wells, http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=webworm27m&date=20030127

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



In order to understand the extent of these threats, it is necessary to examine the environment in which communications systems now operate. A security incident is an adverse event, such as virus infection, that harms, compromises, disrupts, or threatens operations of an information technology network. The number of security incidents is growing at an alarming rate:

Security Incidents reported to CERT/CC, 2000-2003[5]

Year	2000	2001	2002	2003*
Incidents	21,756	52,658	82,094	42,586

*Note that 2003 numbers are through the first quarter alone.

As a result of sharing the same technologies of IT networks and sharing connectivity with IT networks, methods of electronic reconnaissance and attack now apply to radio networks. According to the 2002 FBI study on computer crime, 90% of large corporations and government agencies detected computer security breaches within the last year, and 40% detected system penetration from the outside.[6] And as the multiple ownership environment diffuses responsibility while increasing complexity and connectivity, the threat of insider attack, be it intentional or not, becomes more relevant to radio networks. An

[5] CERT/CC, http://www.cert.org/stats/cert_stats.html#incidents

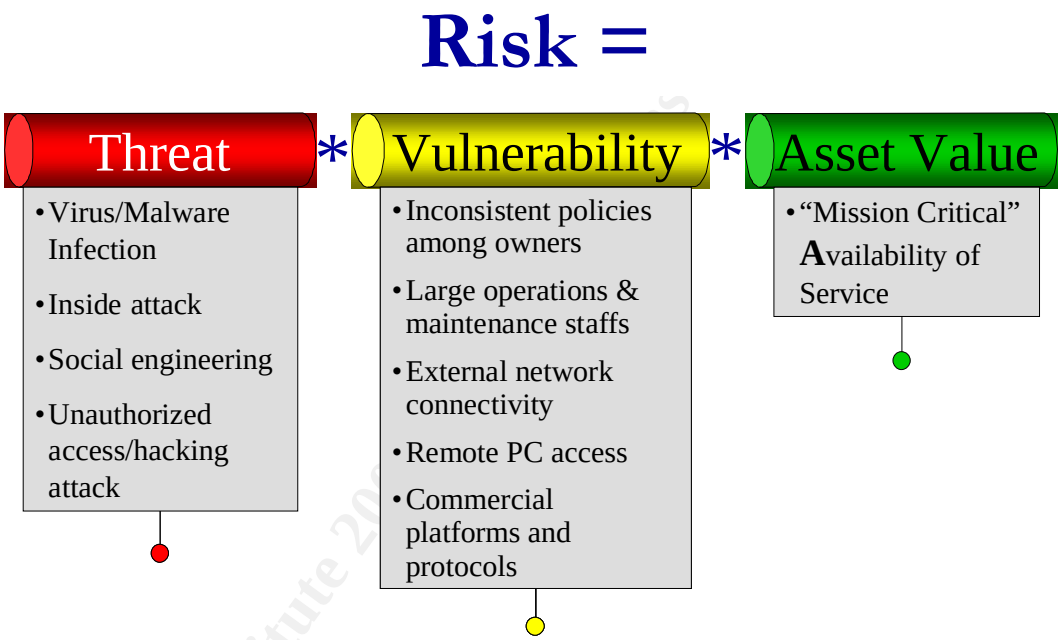
[6] Computer Security Institute

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

insider with physical access to the network, the right skills, and the wrong motives can wreak havoc on a communications system.

As we have seen, both the threats and vulnerabilities faced by radio networks present considerable challenges. Failure to systematically address network security needs in today's hostile environment can lead to massive system failures that jeopardize mission critical operations, compromise restricted information, and contribute indirectly to loss of lives. The risk equation can be expressed as described in Figure 2 below

Figure 2: Risk Equation for Radio Network Infrastructures



The remainder of this paper will focus on describing the steps taken to manage this risk via the application of best security practices to the radio network environment.

3. The "During" State

This section discusses the selection and prioritization of security countermeasures by a vendor of private wireless communications infrastructures. The author's role in this process has been to serve as the vendor's internal strategic marketing champion, with responsibilities including: convincing the organization that the risk is both real and urgent, identifying the business objectives and key elements of a solution strategy, providing requirements to engineering in order to develop that solution, providing guidance to the customer service organizations in order to support the solution, and providing education to

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

the sales force and key customers regarding security needs and the benefits of the vendor's solution.

3.1. Defining the Business Objective

The first key question was, "What is the vendor's role in addressing the risks described above?" As has been described at length, radio networks have historically been closed systems and security has meant encrypting the voice. The evolution of vulnerability has been gradual, and its coalescence into a severe risk is very recent: of the more than a thousand radio networks fielded by vendors over the years, less than a dozen have converted to IP based platforms, and deployment of integrated data and connectivity to multiple customer networks is just beginning. Radio networks have not grown up in the hostile IT environment—they are new to the neighborhood.

Therefore, neither the network vendors nor the end customers have a historical wealth of IT security expertise that can be readily applied to radio networks, nor has a paradigm of "who's responsible for what" been established. Building recognition of the problem, and establishing the boundaries between what is the vendor's responsibility and what is the customer's responsibility was critical.

From the vendor's point of view, it is essential that the brand promise for mission critical solutions be preserved: when serving the emergency services sector, a vendor's solution must, above all else, be perceived as trustworthy. And regardless of who may or may not be legally at fault, the court of public opinion rather than a court of law will determine whether a given vendor's solution is trustworthy: in the event of a high-profile, successful attack, the vendor's brand would be unavoidably associated with vulnerability and failure. Combined with the fact that customer awareness of the problem is low and demand for security solutions must be carefully stimulated, the vendor's primary business objective is one of managing a downside risk. To do so, the vendor must **field a defendable network and assist customers in defending it.**

It was necessary to obtain senior management sponsorship for achieving this business objective, and to from a core, cross-functional team combining strategic marketing, development engineering, and service/support operations to define and pursue a solution strategy.

3.2. General Solution Strategy

In conjunction with the macro analysis described in the evolution of vulnerability section, an internal, hands-on vulnerability assessment was conducted to baseline the security posture of the vendor's radio network platform. Network mapping and port scanning tools and white-hat penetration tests were utilized to identify deficiencies. While specific vulnerabilities cannot be discussed in this paper, it is appropriate to describe the platform as a product of its former, closed-

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

network environment: it relied upon isolation as its primary defense against electronic attack.

For the radio network, a comprehensive defense strategy was required. The defense must address vulnerabilities in external network access, service access, and user/insider access, while at the same time improving system resilience to attack and establishing means for detecting and responding to attacks. A "Defense in Depth" approach was envisioned, such that an array of complementary security enforcing tools, technologies, and procedures would be deployed throughout the network core and along its perimeter.

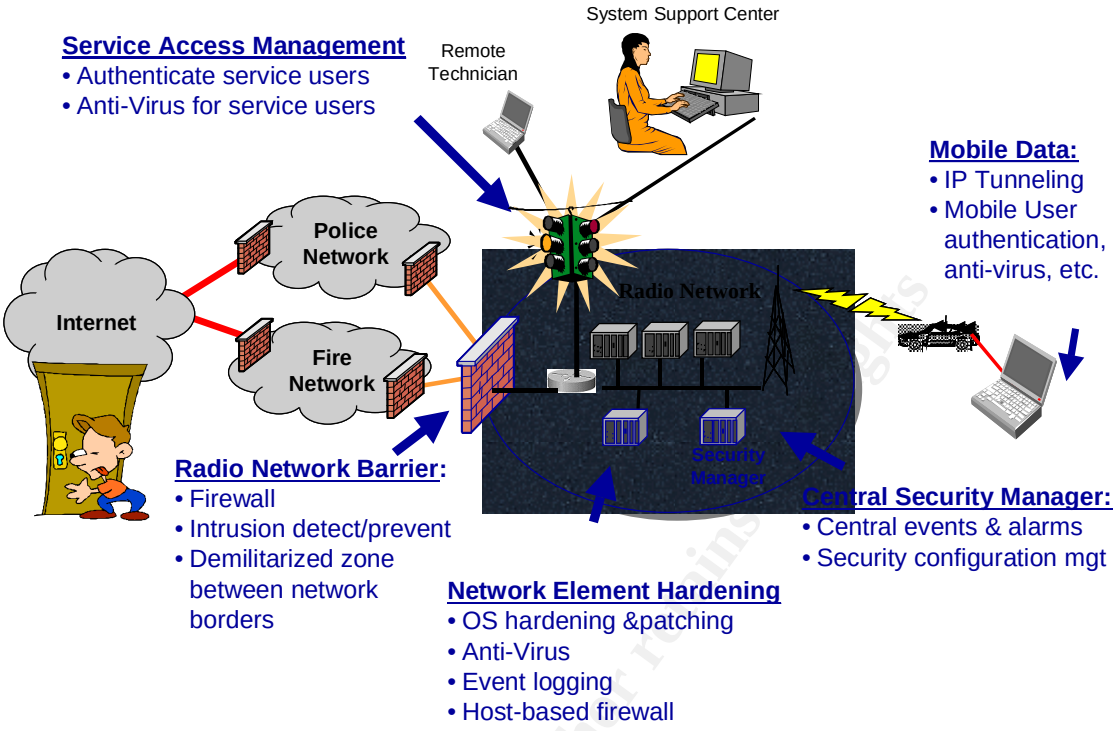
Business realities dictated that it would be impossible to fix everything at once. Therefore a strategy of incremental investment was formulated, with the goal of rolling out security improvements in multiple phases. The initial phase would focus on establishing a hardened network perimeter and creating a baseline ability to detect and respond to attacks. Subsequent phases would continue to harden the interior of the network and improve capabilities in detection and response. All phases would utilize commercial technologies & best practices. And all phases would offer both security enforcing equipment and supporting security management services.

3.3. Specific Requirements: Security Enforcing Equipment

Figure 3 below depicts the elements of the security enforcing equipment and practices to be incorporated into the radio network.

Figure 3: Network Security Countermeasures

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.



3.3.1. Radio Network Barrier

A barrier at the radio network perimeter is necessary to actively restrict external access to known entities and protocols, and to detect potential attacks. Elements of this barrier include:

- CEN border: The vendor must advise each customer to present the Customer Enterprise Network (CEN) to the radio network as it would to any other external network or wireless service provider. CEN egress filtering should be employed to ensure that only the appropriate hosts and applications are allowed to communicate traffic towards the radio network. Ingress filtering and remote user authentication should be employed to ensure that only legitimate applications and users are permitted to access enterprise resources from the outside; these controls are particularly important when the radio network is shared by and connected to multiple customer enterprises.
- DMZ: The vendor and customer must cooperate to create a "Demilitarized Zone" or DMZ between the border routers of external networks and the radio network. Network Address Translation (NAT) should be employed to protect the private address space of the radio network.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Firewall: The vendor expects to supply a firewall capable of both packet filtering and inspection of connection state, to be placed at each geographic point of connection between the radio network and external networks; the radio network is on the protected side of this firewall. The firewall will be configured in a "least permissive" state such that network traffic is permitted only between known sources and destinations, and such that network traffic is restricted to only those specific protocols that are defined in the radio system's interfaces and utilized in the particular network environment.
- Network Intrusion Detection: The vendor expects to supply a network intrusion detection sensor, to be deployed in front of each radio network firewall, in order to detect potential attacks that may attempt to traverse the firewall. Note that IDS sensors often rely upon an attack-signature knowledge base that must be regularly updated, and that configuration of the network intrusion sensor requires explicit knowledge of radio network interface protocols in order able to distinguish between expected and anomalous behavior. It is also worth noting that this sensor is not expected to be as "chatty" as a perhaps more typical, Internet facing IDS sensor would be. Alarms generated by the IDS sensor will indicate unexpected activity occurring INSIDE a customer's network that is attempting to reach the radio network.
- Future barrier capabilities: Note that the radio network does not support web interfaces nor does it support email. If these services are utilized in the future, then the network barrier is expected to be adapted to accommodate proxy server functions and to conduct content filtering at the gateway.

3.3.2. Network Element Hardening:

Several steps in network element hardening are necessary to improve the system's resilience to attack. Steps being taken include:

- OS Hardening. Because commercial operating systems are often deployed in their least secure states, steps must be taken to "harden" the configuration of network elements--without interfering with their required functions. Operating systems are continually evolving, as are best practices in hardening them, so an ongoing process is required. The vendor expects to apply the Center for Internet Security (CIS) guidelines for hardening the network's Windows, Solaris, and Linux based elements and its CISCO IOS based routers and switches.[7]
- OS Patching. Regular software updates are required to deploy security patches to commercial operating systems and applications. The most common software industry response to discovery of new vulnerabilities

[7] Center for Internet Security, http://www.cisecurity.org/

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

is to issue a patch or hot fix. The vendor expects to establish a patch baseline for each element, and provide means to update the radio network with applicable patches on an as needed basis. Note that updates must be pre-tested to ensure that they do not interfere with radio network functions.

- Network Anti-Virus. The vendor expects to deploy commercial anti-virus software on all Windows based elements of the radio network. Note that anti-virus definitions must be updated regularly, and that updates must be pre-tested to ensure that they do not interfere with radio network functions. A mission critical radio system cannot afford the blue screen of death, nor can it afford to have an anti-virus engine mistakenly interpret normal radio network functions as virus behavior.
- Event logging. Operating system features for event logging are expected to be consistently enabled, and means for archiving and collecting logs are to be established.
- Host based firewalls: Several of the network's Solaris based servers are termination points for the computer aided dispatch (CAD) and network management application interfaces. These interfaces use common TCP and UDP ports and services, and these servers also utilize a variety of trust relationships within the network for exchanging data with other network elements. TCP-Wrappers is expected to be utilized as simple and effective means to further control use of these services.

3.3.3. Service Access Management:

Several steps were necessary to better control access the radio network for service purposes. It was necessary to supply protections against accidental infection of the network by service personnel, and against unauthorized access to the network. Steps being taken include:

- Service Access Policy: The vendor found it necessary to advise the customer on the need to update their service user access control policies in a few key areas. Product documentation updates as well as white papers and references to best practices have been provided by the vendor to assist in this process. Some key aspects of the vendor's advice include:
  - Customer security policy must define consistent procedures for service access including means to enable new service accounts, retire old ones, and update passwords and authentication credentials.
  - Customers must equip service technician computers with anti-virus scanning software, establish means for keeping it up to date, and periodically audit service computers to verify compliance and integrity. Customers are advised to consider requiring technician laptops to be dedicated tools used only for servicing the radio

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

network rather than utilized as general-purpose computers. If service laptops are likely to be used as general-purpose computers, then personal firewalls and PC-based intrusion detection tools should also be deployed on them.

  - Customers are also advised to consider deploying file encryption and theft prevention tools on service laptops; these laptops often contain information that is critical to the communications network that should not be left unprotected.

- Radio Network Authentication. For dialup service access, the vendor expects to equip the network with a centralized authentication management scheme such as RADIUS for service account management. Capability for 2-factor authentication mechanisms such as secure tokens will also be supported. When service personnel are on-site and plugging directly into service ports on the networks switches and routers, port authentication is utilized.
- Radio Network Anti-Virus for Service Users. At the customer's option, the vendor-provided anti-virus scheme utilized for fixed radio network elements can be extended to service computers as well, i.e. service laptops can contain an anti-virus scanning client that is home to the radio network's anti-virus server. In this way, service computers can be updated and checked when they access the radio network.
- Port lockdown: Radio networks cover vast, geographic expanses and contain links to many unmanned, remote sites. Fortunately, the radio network is largely static: elements stay put, and network element connectivity is well defined. Therefore, unlike a modern enterprise network replete with removable and transportable laptops, once a radio network is assembled, it is feasible to lockdown the ports on the network's switches and routers to the unique, known MAC addresses of the fixed radio network elements. While admittedly not foolproof, this does make it more difficult for an intruder to insert a new element into the network.
- Physical Security: The vendor and customers have to a great extent already covered their needs for physical security. As part of this project, vendor supplied documentation was updated to ensure that physical security was considered as part of an integrated, defense in depth strategy for the radio network, but new advice on physical security practices was unnecessary.

3.3.4. Central Security Management.

Several steps were necessary to enable customers to maintain radio network security. Steps being taken include:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Customer Security Program Office. The vendor found it necessary to advise end-customers on the need to create a central authority for security management, especially when faced with a multiple-ownership environment. Product documentation updates as well as white papers and references to best practices have been provided by the vendor to assist in this process.

- Central Security Management Server. The radio network is expected to be equipped with a central security management server. This server is home to the anti-virus management, authentication management, firewall management, and intrusion sensor management applications. It enables the customer security administrator to centralize his access to security related events and alarms as well. Event consolidation and correlation tools can also be overlaid to this platform.

3.3.5. Mobile Data Protections

Several steps were necessary to protect the radio network's "integrated data" capability. Steps being taken include:

- IP-IP Tunneling. Mobile data subscribers and applications are securely tunneled through the radio network infrastructure. Radio network elements and resources are not visible to data users, nor can data payload be delivered to radio network elements.

- Customer wireless access policy. Customers are reminded to treat mobile data users (that utilize the radio network) as they should treat any other form of remote access to their enterprise networks. Mobile data computers are members of the customer enterprise IP domain, and customer policies for user authentication, anti-virus, encryption, and so forth must be extended to these computers. Product documentation updates as well as white papers and references to best practices have been provided by the vendor to assist in this process.

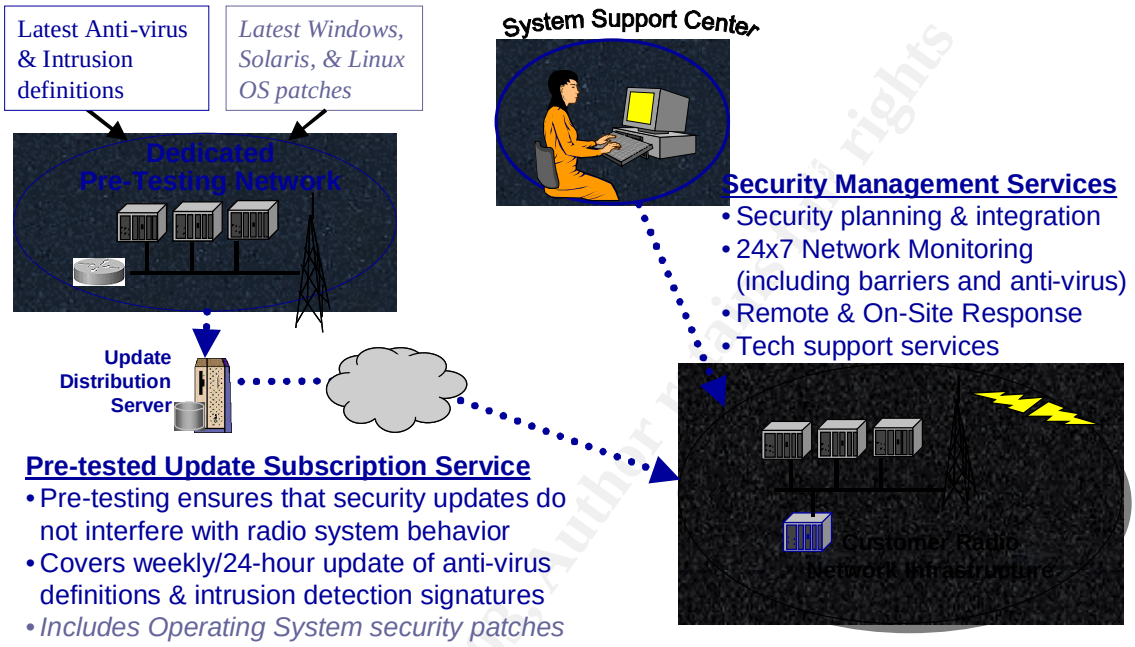
- Credential Forwarding. The radio network can be configured to participate in the customer's mobile user authentication process. When a mobile user attempts to gain wireless access to the customer's enterprise network, the radio network collects his username and password and forwards them the customer's authentication server. If approved, the radio network opens the IP-IP tunnel; otherwise no tunnel is established and the mobile data user is denied access to the CEN.

3.4. Specific Requirements: Security Management Services

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Recalling the second half of the business objective: “assisting customers in defending their mission critical radio networks,” the vendor has found it both necessary and advantageous to offer a portfolio of security management services. Figure 4 below depicts the security management services that may be offered by the radio network vendor.

Figure 4: Security Management Services



3.4.1. Pre-tested Anti-Virus Update Subscription

In this subscription service, the vendor collects, pre-tests, and electronically distributes “pre-tested” anti-virus definition and intrusion detection signature updates to subscribing customers; the customer is responsible for actual installation/activation of the updates. Pre-testing is to be done on a representative radio network platform in order to confirm that definitions do not interfere with normal system operations; when issues are encountered, the vendor modifies the relevant configuration settings and anti-virus scan engine rules to ensure that anti-virus processes do not disrupt radio network functionality. The vendor distributes the updates electronically to subscribing customers; file protection methods including encryption and digital signatures may be employed to ensure file authenticity and integrity. Distribution will normally occur weekly, and the vendor will attempt to expedite a release within 24 hours in high priority situations.

3.4.2. Pre-tested OS Patching Update Service

In this service, the vendor collects, pre-tests, and assists installation of “pre-tested” Windows, Linux, Solaris, and CISCO IOS operating system patches and

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

hot fixes to subscribing customers; the vendor will then assist the customer in installing the updates on the respective radio network elements. Pre-testing is to be done on a representative radio network platform in order to confirm that patches are compatible with radio network element functions, and extensive vendor engineering is necessary to resolve issues. Because installing patches may require scheduled down-time of system elements (which requires careful coordination, as a radio network is mission critical, 24x7x365) and because the testing/resolution process is so resource intensive, patch updates will occur no more frequently than monthly.

3.4.3. Security Monitoring and Management

In this service, the vendor actively monitors the customer's radio network and remotely resolves issues as feasible. Prior to this project, the vendor already offered a 24x7x365 network monitoring service, primarily focused on identifying and resolving networks fault and alarms. That service has been extended to include monitoring of the radio network security enforcing functions. The vendor collects alarms from the anti-virus server, network interface barriers, and authentication management functions. The vendor remotely conducts response & recovery operations and performs as-needed/pro-active maintenance of the anti-virus and service interface barrier elements, including updates to security policy, configuration, and rule bases. Note that this service complements the pre-tested anti-virus update service, as the vendor will remotely pushdown and install the pre-tested updates.

3.4.4. On-Site Emergency Response

In this service, the vendor provides on-customer-site support staff to respond to security incidents. Prior to this project, the vendor already offered on-site response services, primarily focused resolving networks faults and assisting in disaster recovery. That service has been extended to include responding to and recovering from security related incidents such as virus infections.

3.4.5. Security Planning and Integration

In this service, the vendor incorporates and specifically configures the radio network security enforcing elements to accommodate the customer's particular environment. This includes such steps as identifying the number of network barriers needed, designing the customer network to radio network interface and IP plan, configuring the network firewall to match the specific services required by the customer, and tuning the network intrusion detection sensors to minimize false alarms. Prior to this project, the vendor already offered extensive system planning and design services, focused on such topics as RF coverage planning, antenna site design, wide area link design, integration of CAD applications, and so forth; that service has been extended to include the network security design as well.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

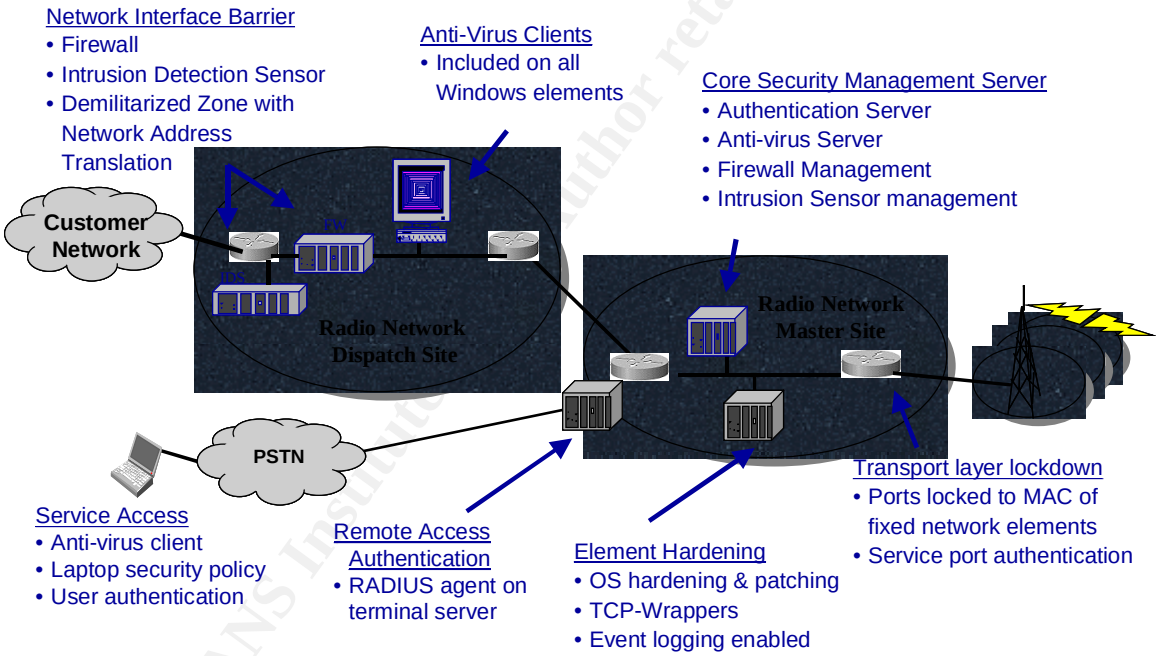
4. After:

This section will describe the summary impact of the security project to the vendor's product line and support organizations. It will also describe how achieving its business objective of fielding a defendable network and enabling its customers to defend their radio networks has created a unique leadership position for the vendor.

4.1. Product Line Impact

A summary view of security enforcing equipment being developed for and integrated into the radio network during the course of this project is provided in figure 5 below:

Figure 5: Security Enforcing Equipment

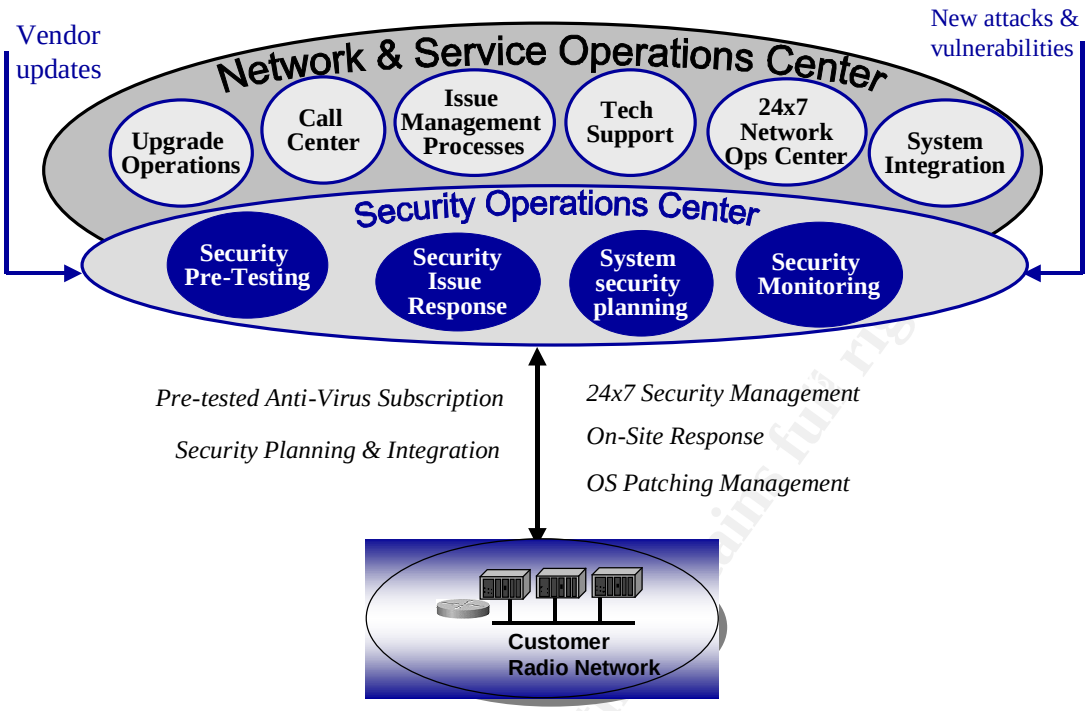


4.2. Impact to Support Services

The impact to the vendor's service and support organization has been quite extensive. The vendor is essentially creating a security operations center overlay to its existing system support center, and is working to update the majority of its existing support functions to incorporate security requirements and security expertise. This is depicted in Figure 6 below:

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Figure 6: Security Impact to System Support Services



4.3. A Leadership Opportunity

Throughout this paper we have described the radio network as containing commercial computing platforms and technologies. And although a radio network utilizes many commercial IT platforms and protocols, it is important to understand that a radio network is most definitely NOT an IT network. It may utilize commercial routers and switches, but they are highly and specifically specialized to enable instant access, multi-cast voice switched by IP. It may utilize Solaris based computing platforms, but these are again highly specialized to create a real-time call processing architecture. And many of the Windows platforms contain custom hardware and software to enable multi-stream digital voice processing and encryption.

It is therefore no simple matter to apply commercial security enforcing technologies and best practices to this environment. Even seemingly straightforward practices in OS hardening can create unintended effects on system performance. Through the ongoing exercise of creating a defendable network and developing security management services, the vendor now

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

possesses a rare and vital combination of expertise: it knows how security mechanisms interoperate with the highly specialized, real-time intensive radio network infrastructure. And this expertise in turn positions the vendor to provide considerable value to its customers: it can provide security consulting and security management services that customers cannot readily provide for themselves and 3rd parties cannot readily duplicate.

Communications networks utilized by emergency services organizations have been classified by the Department of Homeland Security as part of the nation's critical infrastructure. The vendor is achieving its objective of fielding a defendable network, demonstrating its merit as a partner in homeland security, and by so doing is defending its "mission critical" brand promise.

© SANS Institute 2003, Author retains full rights.

Cited references:

Leydon, John, “People are the Biggest Security Risk.” 3/19/2003. http://www.theregister.co.uk/content/55/29827.html (8/9/2003)

CERT/CC Statistics 1988-2003, “Vulnerabilities Reported” http://www.cert.org/stats/cert_stats.html#vulnerabilities

CERT/CC Statistics 1988-2003, “Number of Incidents Reported” http://www.cert.org/stats/cert_stats.html#incidents

Moore, David, Paxson, Vern, Savage, Stefan, Shannon, Colleen, Staniford, and Weaver, Nicholas, “The Spread of the Sapphire/Slammer Worm, http://www.caida.org/outreach/papers/2003/sapphire/

Wells, Robert Marshall, “Dispatchers go low-tech as bug bites computers”, The Seattle Times, Monday, January 27, 2003, http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=webworm27m&date=20030127 (8/9/2003)

Computer Security Institute, “Cyber crime bleed U.S. corporations, survey shows; financial losses from attacks climb for third year in a row” April 7, 2002, http://www.gocsi.com/press/20020407.jhtml;jsessionid=ZZIQTJBILTA2WQSNDBCCKHOCJUMEYJVN?_requestid=693649

Center for Internet Security, “CIS benchmarks and scoring tools”: http://www.cisecurity.org/

Additional references:

Department of Homeland Security, “National Strategy for Physical Protection of Critical Infrastructures and Key Assets,” February 2003: http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf

Department of Homeland Security, “National Strategy to Secure Cyberspace,” February 2003. http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf

Critical Infrastructure Protection Plan, Emergency Law Enforcement Services Sector, February 2001. https://www.pcis.org/getDocument.cfm?urlLibraryDocID=29

“NLECTC Guide for Applying Information Technology in Law Enforcement” April 22, 2003 http://www.nlectc.org/pdffiles/infotechguide.pdf

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**