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.

Information Security Primer

This document discusses fundamental security concepts and architectures applicable to TCP/IP networks. This document is a primer and is meant to convey a broad abstract of security in a networking environment. In instances where specific vendor products are mentioned, the reader should not interpret them as recommendations by me, the author. They are strictly for example purposes. As with any other network technology, one product does not fit all environments.

Copyright SANS Institute

Author Retains Full Rights

AD

INFORMATION SECURITY PRIMER

Written by:

Craig E. Lindner, CISSP

SANS GSEC Practical Assignment
Version 1.2e

© SANS Institute 2001, author retains full rights

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

SECURITY 2
Introduction *2*
Concept of Security *3*
Why Security? 3
Vulnerabilities 4
Attacks 6
Social Engineering 7
Virus/Trojan Horses 7
Denial of Service 8
IP Spoofing 8
Worm 9
Replay Attack 9
Theft of Information 10
Information Security Architecture *10*
Security Policy and Security Standards 10
Security Technologies 11
Security Architecture 12
Security Components 12
Fire Walls 13
Proxy Server 13
Encryption Standards 14
IPsec 16
Certificate Authorities/Digital Certificates 18
Authentication Mechanisms 19
Remote Access 20
Intrusion Detection Systems 21
GLOSSARY OF SECURITY TERMS 22
APPENDIX A: WELL KNOWN PORT NUMBERS 25
BIBLIOGRAPHY 27

© SANS Institute 2001, Author retains full rights

SECURITY

INTRODUCTION

This document discusses fundamental security concepts and architectures applicable to TCP/IP networks. This document is a primer and is meant to convey a broad abstract of security in a networking environment. In instances where specific vendor products are mentioned, the reader should not interpret them as recommendations by me, the author. They are strictly for example purposes. As with any other network technology, one product does not fit all environments.

I hope this document is helpful and proves to be a valuable education aid. Most of the information contained within has been accumulated during security projects I have executed over the past couple of years. Additional information has been gathered from various books, seminars, and Internet sites (see Bibliography).

Be forewarned, information security is a complicated, fast moving field of technology. Therefore, as a speaker at a recent security conference stated before beginning his presentation, "I reserve the right to be out-of-date or simply wrong". Feel free to contact me if you have any questions or concerns about what you find in this document. If I am wrong about something, please let me know.

© SANS Institute 2001, Author retains full rights.

CONCEPT OF SECURITY

The networks of today often include several different operating systems, a variety of web-based and client/server applications, and other components from a potpourri of vendors. These heterogeneous networks introduce a high level of complexity when it comes to management and security issues. This complexity makes it impossible to effectively secure an entire networking environment with a single component such as a firewall.

A total information security solution includes policy and procedure, access control, user authentication, encryption, and content security. By focusing a security solution on an individual component, such as access control or an encryption method, one risks leaving holes in the security shield that can be exploited by a hacker. Approaching security as a concept and not as individual components is the best way to develop and implement secured network environments.

Why Security?

The best way to answer this question is with some statistics. The 2001 Computer Security Institute[1] "Computer Crime and Security Survey" revealed the following facts. Based on responses from 538 security practitioners:

- 85% of respondents detected computer security breaches within the last 12 months.
- 64% acknowledged a financial loss due to computer breaches.
- 35% were willing and/or able to quantify a financial loss due to computer crime. Total losses reported equaled $377,828,700.
- 34 organizations reported $151,230,100 in losses from theft of proprietary information.
- 21 organizations reported $92,935,500 in losses from financial fraud.
- Internet privilege abuse by employees was reported by 91% of respondents.
- 70% reported their Internet connection as a frequent point of attack.
- 31% reported their internal systems as a frequent point of attack.
- 40% of respondents detected system penetration from the outside.
- Computer viruses were detected by 94% of respondents.
- Denial-of-service attacks were detected by 31% of respondents.

[1] www.gocsi.com/prelea_000321.htm (Computer Security Institute/FBI Computer Crime and Security Survey)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Do not overlook the importance of physical security controls. Safeware®[2], a company that provides insurance coverage for computer owners, reports that 403,000 laptop and desktop units with a value of $567,000,000 were stolen in 2000.

The business requirements of many companies dictate the need to provide direct and intermittent connectivity to the local area networks and private networks of remote corporate divisions, business/trading partners, and customer. In the past, the popular way of providing this connectivity was across a private, leased network connection such as frame relay. Unfortunately, this dedicated connectivity can be very expensive. Spurred by the desire to reduce network costs, many companies have begun to leverage the Internet as a ubiquitous, low-cost transport mechanism between themselves and the remote entities.

The desire to leverage the Internet and similar IP-based VPN bearer networks is one of the influential forces behind the recent popularity of network security solutions. The standards for privacy and integrity on these VPN bearer networks vary anywhere from hostile to harmless for routine low-value data traffic. These security variances may be acceptable for routine traffic, but not so for high-value sensitive traffic.

Let me take the time to point out that private leased-line facilities are vulnerable to some of the same security threats as the IP-based bearer networks. However, the lack of ubiquitous access to private line implementations makes protection of these networks easier to implement and sustain. Throughout the remainder of this document, I will focus on securing networks from the Internet and other un-trusted IP-based bearer networks.

Vulnerabilities

If the Internet or other un-trusted network is utilized as the data transport mechanism, one can expect various attacks to be mounted from the underlying infrastructure. The attacks are not necessarily aimed at the network, but at the resources attached to the network and the information contained within. These attacks can be of various forms and impact corporate information resources in a variety of ways.

The typical points of network vulnerabilities are weak administrative and user passwords, modem connections, system back doors, poor user adherence to security policy, and poorly configured firewalls and Web hosts.

For example, a 1997 survey compiled by Compaq[3] in the financial district of London shows just how poorly users choose their passwords. In order of preference, respondents said they used:

- 82% a sexual position
- 30% an abusive name for the boss
- 16% their partner's name or nickname

[2] www.safeware.com/99lossstatisticschart.htm (Safeware® The Insurance Agency, Inc.)
[3] ICSA Library page – Surveys and Estimates

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- 15% their favorite holiday destination
- 13% sports team or player
- 8% whatever they saw first on their desk

Based on my experiences in the past four years, password selection has not improved much. Weak passwords are not the only ports of entry for an attack. Bugs in operating systems and applications provide penetration points for hackers. This means that attacks can be expected regardless of the security resources implemented for protection. Even with leading-edge security features in place, one can only hope to minimize the threats that network connectivity poses to informational resources. Paranoid? Some industry experts think you ought to be.

Cheswick and Bellovin[4] present a humorous axiom regarding program bugs and firewalls to point out that a paranoid stance is necessary for many network sites. The axiom is as follows:

Axiom 1 (Murphy) *All programs are buggy.*

Theorem 1 (Law of Large Programs) *Large programs are even bigger than their size would indicate.*

Proof: By inspection

Corollary 1.1 *A security-relevant program has security bugs.*

Theorem 2 *If you do not run a program, it does not matter whether or not it is buggy.*

Proof: As in all logical systems, (false => true) = true

Corollary 2.1 *If you do not run a program, it does not matter if it has a security hole.*

Theorem 3 *Exposed machines should run as few programs as possible; the ones that are run should be as small as possible*

Proof: Follow directly from Corollaries 1.1 and 2.1

Corollary 3.1 (Fundamental Theorem of Firewalls) *Most hosts cannot meet our requirements: they run too many programs that are too large. Therefore, the only solution is to isolate them behind a firewall if you wish to run any programs at all.*

The axiom leads to the conclusion that ***firewalls must be configured as minimally as possible, to minimize the risk of penetration***.

Many operating systems and applications contain programming holes that can be security risks. Take the popular web-server application Microsoft IIS for example. In addition to the recent Code Red Worm threat, over 190 different vulnerabilities associated with IIS have been reported in the past year.[5] All of the popular operating systems (UNIX, LINUX, and Windows NT) have documented security vulnerabilities. A list of known operating system vulnerabilities can be found on at the following web sites:

http://xforce.iss.net

http://www.cert.org/nav/index_red.html

[4] Firewalls and Internet Security - Repelling the Wily Hacker. William R. Cheswick and Steven M. Bellovin. Copyright © 1994 by AT&T Bell Laboratories, Inc.
[5] http://xforce.iss.net/

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Attacks

The corruption or compromise of data is accomplished in a variety of ways. Corporate data can be damaged, destroyed, and/or stolen when not properly protected. A security breach that corrupts or compromises data can have a significant monetary impact on a company. Theft of corporate secrets can give a competitor an edge that can ruin a business. Fraudulent financial transactions can result in major monetary losses. Rebuilding destroyed data files will take time and money not to mention the business lost while restoring the information. The statistics presented earlier clearly show the potential monetary losses that can be incurred by an organization due to unauthorized access.

Although not a comprehensive list, the following describes many of the attacks that today's information systems are subjected too. It should be kept in mind that these attacks do not always originate from outside of the trusted environment. Currently, more than 70% of unauthorized network activity originates from internal sources.

- Social Engineering
- Viruses/Trojan Horses
- Denial of Service (DoS)
- IP Spoofing
- Worm
- Replay Attack
- Theft of Information

© SANS Institute 2001, Author retains full rights.

Social Engineering

Social engineering is an technique used by attackers to gain system access or information by exploiting the basic human instinct to be helpful. In most cases, social engineering exploits are successful because the targeted enterprise lacks an awareness program to educate employees of their security-related duties and responsibilities. A classic social engineering exploit involves an aggressor (Bob) phoning a target (Sue) and posing as a network support technician. Bob informs Sue that he has been working on a system problem and needs her username/password to verify the 'problem' has been resolved. Having received no security awareness training and always willing to be of assistance, Sue provides her username/password to Bob.

Virus/Trojan Horses

A virus is malicious code that can plant itself into operating systems and programs and modify them. A Trojan-horse is a virus that has been hidden inside of legitimate software. The software is downloaded to a server or workstation and when activated, the malicious code does its thing.

Firewalls provide very little in the way of virus protection. Most viruses are cleverly hidden within binary code making detection difficult. As a second line of defense, a virus detection program such Network Associate's McAfee should be installed on every desktop within the protected network. A process should be put in place to ensure the anti-virus software kept updated.

A list of viruses and hoax viruses can be found on the Web at:

http://vil.mcafee.com/default.asp?

http://vil.mcafee.com/hoax.asp

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Denial of Service

An attack that targets resources within the network with the intention of reserving resource and keeping legitimate users from gaining access. An example of denial of service (DOS) is a *SYN* attack. When a TCP/IP-based workstation initiates a request for server services it transmits a *SYN* packet to the server. Upon receipt of the *SYN* packet, the server reserves resources for the anticipated session and responds back to the workstation for further identification.

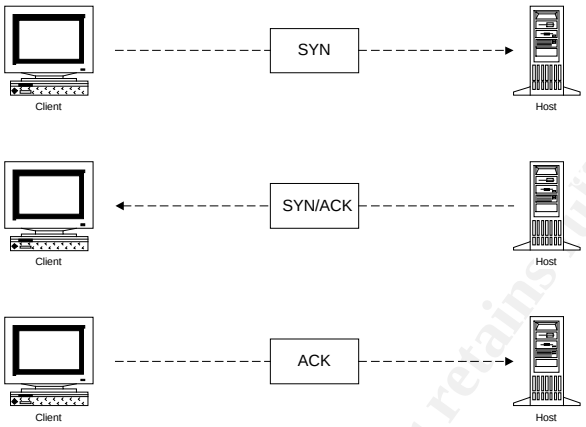

Figure 1. TCP/IP Session Establishment

During a *SYN* attack, an enemy workstation will generate a deluge of session requests using bogus IP addresses. The target server begins reserving resources for each request while waiting for the completion of the TCP/IP handshake process. The expected reply from the enemy workstation never comes. Meanwhile, the server has reserved its resources for the fraudulent requests and must deny legitimate users.

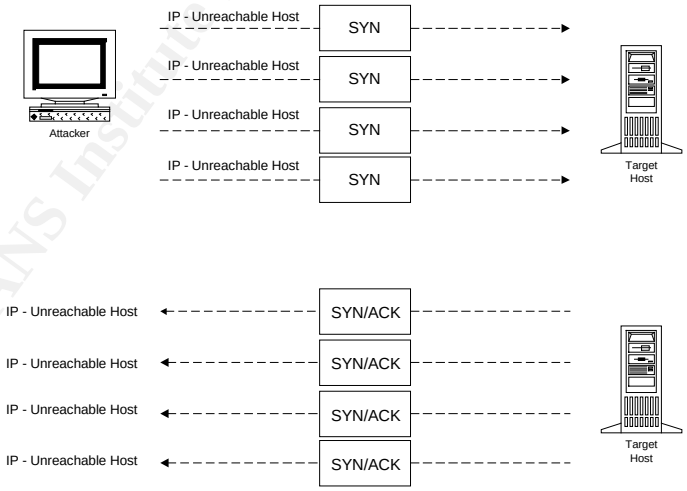

Figure 2. SYN Flood

IP Spoofing

IP spoofing is accomplished when an outside hacker uses a discovered IP address to gain access to the trusted environment. A hacker can obtain a valid IP address in a variety of ways including snooping and social engineering. Configuring a

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

firewall to identify addresses that are expected to be on the Internet verses the Intranet can foil spoofing. Do not pass traffic between internal (trusted) resources through a firewall that is protecting the network from an un-trusted environment.

Worm

Worm is industry nomenclature for a self-contained program that will replicate itself across a network, infecting each server and workstation it can access. The following is a portion of an article written by Major Dale Long[6], USAF, and concerns the 1988 release of a worm into the Internet by MIT student Robert Morris. The spread of the Morris worm resulted in a wide spread denial-of-service (DoS) situation as computers across the Internet crashed or went dormant due to the worm's consumption of resources.

> *This is the way the world ends: At 8:00 p.m., a 22-year old college student launches an autonomous, semi-intelligent agent onto the Internet. The agent's job is to traverse the Internet and visit as many places as possible and return a log of its travels. Part prank, part self-study project on intelligent agents, the worm ventures forth.*
>
> *Unfortunately, there's a math error in the program that causes it to reproduce itself 14 times faster than intended. The now cancerous worm multiplies exponentially, its copies occupying memory, filling disk drives and eating CPU clock cycles like a horde of virtual locusts. In a few hours, 6000 computer systems are crippled, affecting all finance, business, education, government and military systems. The rest of the network must be shut down to stop the infection's spread. Everything that depends on networked information comes to a halt while teams repair the carnage.*
>
> *What happens next? Does the high-octane world economy collapse when its drive to buy and sell 24 hours a day loses the electronic mechanisms that support it? Do terrorists or rogue nations take advantage of the loss of some military command and control systems to launch sneak attacks? Do cyberbandits strip-mine what's left of the Internet?*
>
> *Fortunately, on November 2, 1988, when Robert Tappan Morris launched his infamous Internet Worm from an MIT computer, none of those things occurred. Of course, we were a lot less dependent on networks and the Internet than we are now. And Morris' worm wasn't an attack by thieves or terrorists. It was just a program designed by a college student to traverse the network through loopholes in Unix and idiosyncrasies in sendmail to scan address lists and guess at passwords.*
>
> *However, if that's what a relatively innocent prank can do, what would happen if someone launched a focused, full-scale attack on our entire information infrastructure?*

Replay Attack

[6] original article found at www.chips.navy.mil/chip/archives/97_jan/file6.htm - link is no longer active

A replay attack occurs when a hacker intercepts a communication between two parties and replays the message. For instance, a hacker might intercept a credit card transaction between a consumer and a Web site. The hacker then replays the transaction multiple times resulting in multiple debits to the consumers credit account.

Theft of Information

Theft of information can be accomplished several ways. A simple way is accomplished by eavesdropping on the network with a sniffer device and recording traffic that is being transported in clear-text. Other methods include hacking network servers and removing files or acting as the 'man in the middle' and intercepting file transfers destined for a legitimate user.

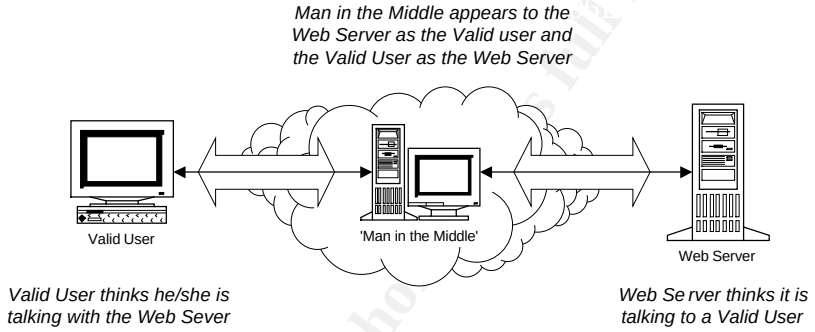

Figure 3. Man in the Middle

INFORMATION SECURITY ARCHITECTURE

Security Policy and Security Standards

The first step in development of an information security architecture is to establish a high-level security policy. A security policy establishes the rules or protocol under which the entire organization or company will be required to operate. The protocol established in an organization's security policy must be incorporated into the daily habits of every employee. The policy is backed up by an ISO 17799-based standards or procedures document that specifies the access control requirements for information and other assets throughout the company.

Formal security policies and security standards documents should be tailored specifically for each networking environment. The documents must be distributed to every employee throughout the organization and be an integral part of an ongoing security education and awareness program. A typical security policy will include the following:

- Purpose of the security policy document
- Scope of the security policy
- Primary points of contact and responsibilities
- Change logs or history of the policy documentation
- Policy compliance

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

A typical security standards document will include the following:

- Information, Host, and Network Marking Requirements
- Host Security Control Requirements
- Network Security Control Requirements
- Monitoring and Alert Management
- Internet and Intranet Access
- Authorization and Access Controls
- Data Backup and Restoration
- Encryption Technology
- Move/Add/Change Management
- Auditing Functions
- Physical Security
- Accountability and Responsibility

Information System Security Policies and Procedures: A Practitioners' Reference and The Complete Manual of Policies and Procedures for Data Security, both written by Tom R. Peltier, are excellent resources for the development of Information Security policies and procedures.

Security Technologies

As much as possible, the security technologies implemented must be transparent to the user base. The best way to insure non-conformance to any policy or procedure is to upset the normal operating procedures of the user. The security technology should be as transparent as possible to higher level (re: OSI Model) services and their protocols, and to the underlying bearer facilities. The technology should provide little or no administrative overhead to users and support an adequate level of authentication between users and core services.

Basic areas to focus on during the development of security requirements are as follows:

- Verify that data traversing the network arrives at its proper destination.
- Guarantee that the data received is the data that was sent without any additions or deletions.
- Restrict and control access to network resources. Resources include routers, gateways, terminals, servers, and modems.
- Protect data from being seen, changed, or removed by any unauthorized person, device, or application during transmission.
- Insure packet ownership (non-repudiation).
- Put auditing and reporting mechanisms in place to record any intrusions or breaches of the security architecture.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Install real-time intrusion detection and response systems to stop an intrusion or attempted intrusion before damage occurs.
- Establish a business continuity plan that will compensate for failed or breached security elements.
- Implement a security architecture that is based on open standards and is scalable with the rest of the network.

Security Architecture

Prior to developing security architecture, a risk analysis must be performed. The purpose of the analysis is to define a balance between the available technologies, the costs of those technologies, perceived threats, and the true value of the information being protected. To the point, one must establish a value for the resources being protected, then establish a cost justifiable security architecture.

The architecture development process can be broken down into the following steps:

- Map out the flow of information assets across the enterprise (network, system, storage, and print resources).
- Review the enterprise and identify areas where the confidentiality, integrity, and/or availability of an information asset could be threatened by aggressors.
- Establish a value for each information asset targeted for protection.
- Identify security controls (hardware, software, procedures) that would mitigate the threat presented to each information asset.
- Establish a cost for each of the security controls identified and compare against the information asset value.
- Use results of the analysis to determine cost-effective security controls to deploy in the architecture.
- Determine how the security controls will be monitored and managed.
- Identify mechanisms that will provide intrusion and audit capabilities for the enterprise.

Security Components

There are many hardware and software components that make up a comprehensive security architecture. These components or sub-systems will vary in size, capacity, processing power, and traffic throughput. The categories of security sub-systems and the core technologies are:

- Firewalls
- Encryption Standards
- Certificate Authorities
- Authentication Mechanisms

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Remote Access Services
- Intrusion Detection/Response
- Logging/Audit

Fire Walls

A firewall is a device or system that enforces an access control policy between two networks. In principle, the firewall provides two basic services: (1) blocks undesirable traffic and (2) permits desirable traffic. A firewall provides a single point of entry into your corporate network from an un-trusted network (i.e. the Internet). It is at this 'choke point' that the access control policy and auditing capability are enforced.

A firewall is not a universal remedy for network security. Firewalls are not very effective at screening for viruses and cannot protect the network against attacks that do not go through it. Industry statistics show that a majority of security breaches originate from internal sources unseen by the firewall. Firewalls will not protect the network from vulnerabilities introduced by a lapse in security-consciousness by the user community.

Firewalls on the market today take many shapes and forms. The simplest ones enforce security policy at the lower layers of the OSI Model by keying on source and destination addresses, and IP packet types. More complex firewalls are software-based applications that enforce security policy at higher layers of the OSI Model. Other complex implementations are hardware appliances with serial and LAN interfaces and pre-loaded software. Vendors such as Cisco and Nortel/Bay Networks have combined high-end software-based firewall applications with their full-functional routers. Although this line of thinking runs counter to the earlier recommendation that *firewalls must be configured as minimally as possible, to minimize the risk of penetration.*

It is important to note that most firewall vendors implement a mixture of proprietary and 'open' security architectures. It is recommended that extensive lab testing and evaluation be performed prior to committing to a specific product.

Proxy Server

A proxy server is an application that acts as the middle-man between an un-trusted resource and a resource located within the trusted network. A proxy server performs several functions: (1) eliminates direct contact between a trusted resource and an un-trusted user (2) hides the identities of resources within the protected network and (3) provides additional authentication and auditing capabilities.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

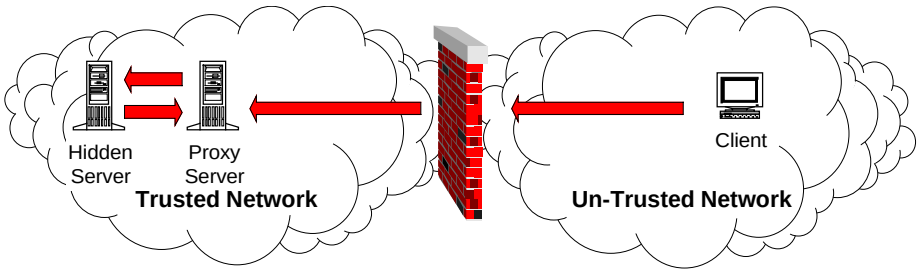

Figure 4. Proxy Server

Encryption Standards

As shown in the list below, there are many different standards in use today for encryption. Encryption can be accomplished client to server, client to client, server to server, bulk encryption, network layer encryption, or application layer encryption. Encryption methods can be divided into two basic types: Secret Key and Public Key.

Secret Key Encryption Methods:

- Data Encryption Standard (DES) – Submitted in 1974 by IBM and adopted by the National Institute of Standards (NIST) in 1976, DES is a form of data encryption system known as a block cipher. DES uses a 56-bit key and encrypts and decrypts data in fixed block lengths of 64-bits. Over the past several years, a number of methods have been discovered that decreased the time it took to break the DES key. Combine these methods with the increase in compute power, and it became obvious that a 56-bit key was not adequate to protect sensitive information. In 1997, NIST discarded its endorsement of DES and began work on a replacement method called Advanced Encryption Standard (AES).
- Triple DES – Using three 64-bit keys (overall key length is 192-bit), data is encrypted three times to make it more difficult to decipher. Triple DES is available in a number of modes including DES-EEE3 where encryption is accomplished using three different keys; DES-EDS3 where the three DES operations are in an encrypt-decrypt-encrypt sequence with three different keys; and DES-EEE2 where the first and third encryption operations use the same key. It should be noted that if all three keys, the first and second keys, or the second and third keys are the same then the encryption is essentially the same as DES. NIST has endorsed Triple DES as a temporary encryption standard until AES is finalized.
- IDEA – Similar in overall structure to DES, IDEA performs three different operations (instead of one for DES) during each round of encryption. In addition, IDEA uses a 128-key to guard against brute-force attacks.

Public Key Encryption Methods:

- Secure Socket Layer (SSL) – developed by Netscape as a method to provide encryption for the web-based services. Besides encryption, SSL provides several features including authentication and repudiation of servers and clients, and data integrity via message authentication codes. SSL is very effective at protecting against 'man-in-the-middle' attacks and replay attacks. SSL rides on top of TCP and is not supported by UDP.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- RSA – Named after its inventors Rivest, Shamir, and Adleman, RSA is the best-known public key cryptosystem. Public key systems use a two-key approach, a public key and a private key. Each user places an encryption key in a public directory, while keeping its decryption key (private key) a secret. To send a message to someone, you simply obtain the targets public key and, combined with your private key, encrypt the message.
- SKIPJACK – A conventional cipher block encryption method that uses a 674-bit block size, 80-bit key size, and implements a key escrow system. The transmission contains an encrypted header that contains a session key. Government agencies with access to the header-encryption keys are able to decrypt the transmission. SKIPJACK is used in the Clipper, Capstone, Keystone, Regent, and Krypton encryption chips.

© SANS Institute 2001, Author retains full rights.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Pretty Good Privacy (PGP): Created by Philip Zimmerman and published in 1991 as freeware, PGP is easily installed computer program that encrypts and decrypts data to safeguard its transportation (confidentiality) and verify its authenticity (integrity). PGP uses the RSA public-key encryption system and also employs the IDEA encryption method. At start up, PGP generates two unique keys. One key is kept secret and is stored on your computer, the other is given to your colleagues and/or posted on a public key server.

IPsec

IP Security Protocol (RFC 1825) is an IETF-ratified security architecture (authentication and encryption) for IP-based communication. IPsec is an option for the current version of IP (IPv4), but support will be standard with the release of IPv6.

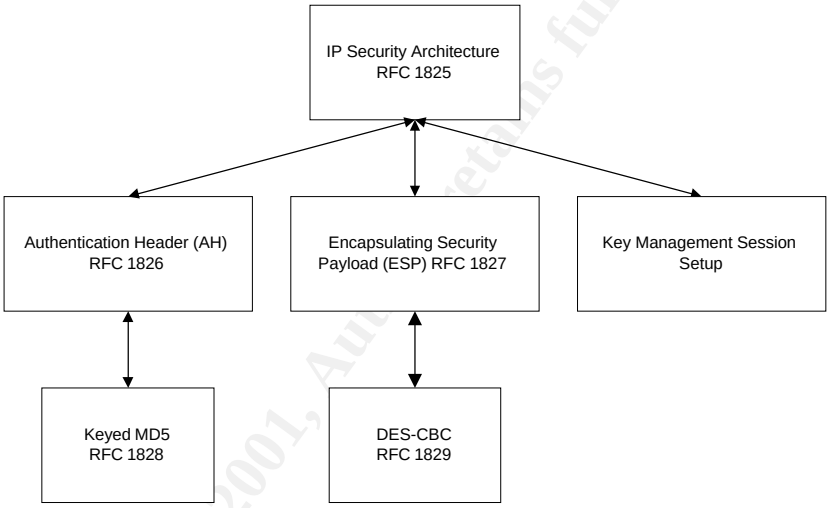

Figure 5. IPsec Structure

As indicated in the diagram above, the RFC 1825 references two additional RFCs, Authentication Header (RFC 1825) and Encapsulation Security Payload (RFC 1827). Authentication Header (AH) is a special header attached to an IP packet used to authenticate the packet sender. The message authentication code (MAC) found in the AH is computed on the sender side, appended to the packet, and is verified on the receiver side. In instances where digital signature algorithms are used, non-repudiation services may be provided.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The format for the AH header[7] is as follows:

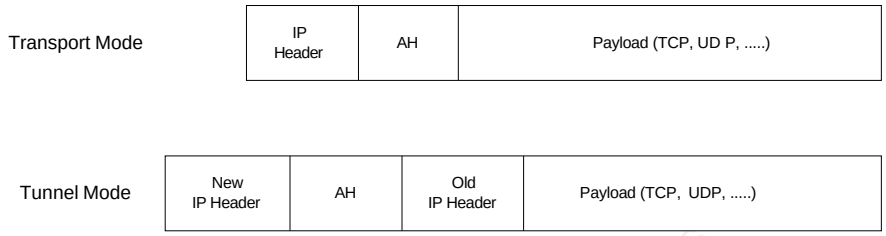

Figure 6. AH Format

Encapsulating Security Payload (ESP) provides for encapsulation of the IP packet. The IP packet can be encapsulated in its entirety (Tunnel Mode) or just the upper layer protocol data (Transport Mode). In the event the entire packet is encapsulated, a new IP header is created in order to route the packet through the network. The new IP header is in clear-text.

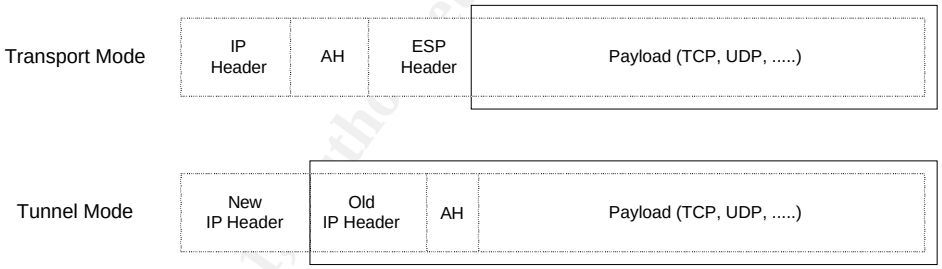

Figure 7. ESP Encapsulation

By no means is IPsec the panacea for authentication and security of IP-based networks. Although somewhat strong in the area of packet authentication via AH and payload encryption via ESP, one must still be concerned with the transmission of host source/destination addresses across un-trusted networks. Encrypting the entire packet using ESP Tunnel Mode may appear to be the answer, but that would require the configuration of static route tables – broadcasting routing tables would defeat the purpose of encrypting addresses. Besides the administrative difficulties of installing and maintaining static tables, the ability to reroute traffic due to a link or equipment failure is limited.

[7] www.ietf.org/rfc/rfc2402.txt

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Certificate Authorities/Digital Certificates

Certificate authorities provide for the issuance and maintenance of digital security certificates. Major certificate authorities include Entrust and VeriSign. The standard for digital certificates is the Public Key Infrastructure (PKI) based on the OSI/ITU X.509 Version 3 certificate. The X.509 standard defines the format for the digital certificate and the certificate revocation list (CRLs). X.509 includes a number of optional features, so compatibility issues should be of concern when mixing vendor implementations.

The authority facets of digital certificates are Certificate Authority and Registration Authority. Presentation layer encryption and digital signatures are used to protect communication between the CA and RAs.

- Certificate Authority - The CA performs the core certificate generation function. It accepts certificate generation and revocation requests, and generates certificates and certificate revocation lists.
- Registration Authority - A RA acts as an administrative front end to the CA. The RA performs local administrator data capture and status reporting, and provides a user friendly front end for non-specialist operational staff. A number of RAs can support a single CA or a CA can provide the registration functions itself.

The functional elements of certificate authority are:

- Certificate Revocation List (CRL)
  - A certificate revocation mechanism that lets the Certificate Authority (CA) publish or transmit lists of invalidated certificates corresponding to communicating entities whose authorization has been withdrawn.
- Certificate Repository
  - A certificate storage and distribution mechanism that allows the CA to manage certificates efficiently.

Work is underway to establish standard APIs between certificate authorities and applications that will resolve deployment problems created by the incompatibility of proprietary code.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The following diagram (courtesy of Dr. Piers McMahon of Platinum Technologies)[8] depicts how a CA will interface with RAs and 'plug & play' applications under the PKIK Model.

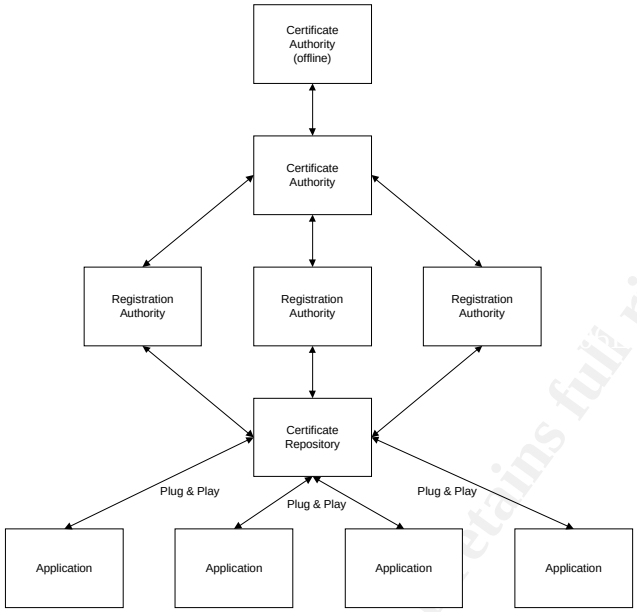

Figure 8. PKIK Model

Authentication Mechanisms

Authentication is the process of proving identity. In the security arena, authentication can be broken down into to distinct pieces: user-to-host authentication and host-to-host authentication. User-to-host authentication is typically accomplished through the use of User-ID and password. Other user-to-host methods include the use of smart cards with one-time use passwords and biometrics. Host-to-host authentication is typically accomplished via network based characteristics such as source address and/or computer name. Needless to say, these network-based authentication methods are extremely weak since addresses and names can easily be spoofed.

Cryptographic techniques are a much stronger method of host-to-host authentication. Cryptographic techniques rely on the use of secret keys or digital signatures as positive identification. Unfortunately, implementation of the crypto techniques can be expensive and one must be concerned about the secret key or the key distribution center (KDC) being compromised.

[8] Dr. Piers McMahon. Platinum Technologies. December 9, 1998, presentation at the 14th Annual ACSA Conference.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Many different types of authentication mechanisms are available. Some of the most popular methods are discussed below.

- Password Authentication Protocol (PAP) – an extremely weak but simple Internet standard authentication method. PAP uses a two-way handshake for authentication purposes. The client sends a user code and password in plain text (bad karma) to the server (or authenticator). The server then looks up a user record based on the login-id. If the user code and password sent by the client matches the user record, access is allowed. If not, access if denied.
- Challenge-Handshake Authentication Protocol (CHAP) – this Internet authentication method uses a three-way handshake and is more secure than PAP. During the logon process, the server sends a unique challenge message to the client. The challenge changes at each logon. The client calculates a response based on a secret algorithm (Internet standard Message Digest 5) and transmits the response back to the server. The server looks up the user name in its records and calculates its own version of the response based on the challenge message and the client's algorithm. If the responses match, access is allowed. If not, access is denied.
- Remote Authentication Dial-In User Service (RADIUS) – client/server security system developed by Livingston Enterprises that protects remote access to the network and network services from unauthorized access. User authentication and network service access information is located on the RADIUS server. The RADIUS client portion (residing on the user workstation) generates authentication requests to the RADIUS server and acts on responses received back for the server.
- Secure Socket Layer (SSL) – Developed by Netscape, SSL provides a method of authentication for both clients and servers through the use of digital certificates and digitally signed challenges. SSLv3 uses X.509 v3 certificates.
- TACACS – Terminal Access Controller Access System – Authentication protocol developed by Cisco Systems and defined in RFC 1492. TACACS runs on a LAN-based server (usually UNIX-based) and acts as a proxy client to the security server for clients. TACACS+ is an upgrade of TACACS.

Remote Access

Remote access services (RAS) provide IP connectivity to the corporate Intranet for remote sites, mobile users, and telecommuters. Although the use of the Internet as a transport mechanism between hosts and remote users has become popular in recent year, many companies still rely 1-800 numbers and Plain Old Telephone (POTs) lines to connect to their remote users.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

RADIUS and TACACS, as discussed earlier are two competing protocols used by remote access services for user authentication. A number of Data-Link Layer protocols are available that support remote IP access. Some offer a limited level of virtual private networking (VPN) capability, others such as PPP do not.

- PPP - Point-to-Point Protocol – a Data-link layer protocol that provides dial-up access over serial lines by encapsulating protocols such as IP, IPX, and NetBEUI in Network Control Protocol packets. PPP was an improvement over Serial Line Internet Protocol (SLIP), allowing the use of CHAP or PAP for user authentication. PPP does not provide VPN capabilities.
- PPTP - Point-to-Point Tunneling Protocol – Data-Link layer protocol developed by the PPTP Forum (made up of Microsoft and various hardware vendors) in 1996 that uses IP encapsulation to tunnel data-grams of common network layer protocols. PPTP provides VPN capabilities, but experts have shown it to be vulnerable to attack.
- L2TP - Layer 2 Tunneling Protocol – Data-Link layer protocol that supercedes PPTP. L2TP tunnels PPP traffic over IP networks and inherits the features of PPP including authentication, PPP Encryption Control Protocol (ECP), and Compression Control Protocols (CCP).[9]

Intrusion Detection Systems

As the use of the Internet as a cost-effective transport mechanism increases, so does the need for a real-time, automated intrusion detection and reporting capability. Firewalls and authentication servers act as 'passive' deterrents to unauthorized access to network and computer assets. However, in the event that a hacker is not deterred, network and compute assets are immediately at risk. In many cases, a breach will not be detected until the damage is done and the hacker is long gone. Real-time intrusion detection and reporting systems are 'proactive' deterrents, constantly scanning the network for suspicious activity and automatically logging and terminating those activities before any damage can be done.

ISS RealSecure™ and Axent NetProwler™ are two popular intrusion detection systems (IDSs) on the market today. Pricing range from $1,495 to $25,000 depending on product selected and the number of nodes supported (25/100/1,000).

[9] www.ietf.org/internet-drafts/draft-ietf-l2tpext-security-04.txt

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

GLOSSARY OF SECURITY TERMS

Application-level Firewall: A firewall system in which service is provided by processes that maintain complete TCP connection state and sequencing. Application level firewalls often re-address traffic so that outgoing traffic appears to have originated form the firewall, thereby protecting the identity of the internal host.

Authentication: The process of determining the identity of a user trying to access a network system or resource.

Authentication Token: A portable device used for authenticating a user. Authentication tokens operate by challenge/response, time-based code sequences, or other techniques.

Authorization: The process of determining what type of activities are permitted within the enterprise.

Application Programmer Interface: (API) A detailed software interface that includes routine declarations, data structures, and tasking structures.

Availability: The assurance that authorized users can access the information necessary to complete their jobs.

Block Cipher Encryption: An encryption system that works on blocks of data. DES is an example of a Block Cipher – DES encrypts 8-byte blocks at a time.

Brute-Force Attack: Typically an attack that uses no insight into the cryptosystem. Usually accomplished by searching the entire keyspace to discover the cryptographic key. Brute force attacks are very CPU intensive.

Challenge/Response: An authentication method where a server sends an unpredictable challenge to a user attempting to log on. The user must compute a response using some form of authentication token.

Certificate Authority: (CA) Trusted entity that has the ability to create and revoke public key certificates.

Cookie: Token that is used to provide a simple source address identification between parties involved in a conversation.

Confidentiality: The protection of information against unauthorized disclosure.

Data Encryption Standard: (DES) A symetric key cryptographic system that has been standardized by NIST.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

DES (Triple): An enhancement to DES that uses two DES keys (112 bits to encrypt, decrypt, then encrypt) in three successive rounds.

DES (3DES): An enhancement to DES that uses three keys (168 bits to encrypt, decrypt, then encrypt) in three successive rounds.

DNS Spoofing: Technique of assuming the DNS name of another system by either corrupting the name service cache of a target system, or by compromising a domain name server for a valid domain.

Dual Homed Gateway: A system that has two or more network interfaces, each connected to a different network segment. In firewall configurations, a dual homed gateway usually acts to block or filter traffic trying to pass between the networks.

Federal Information Processing Standard (FIPS): U.S. federal standards body.

Insider Attack: An attack that originates from within the protected network.

Intrusion Detection: Detection of a break-in or attempted break-in either manually or by automated tools.

Integrity: The protection of information against unauthorized modification or destruction.

IPSec: network layer encryption method for IP packets.

IP Spoofing: An attack whereby a system attempts to impersonate another system by using it IP network address.

IP Splicing/Hijacking: An attack whereby and active, established session is intercepted and co-opted by a hacker. IP Splicing attacks may occur after an authentication has been made, permitting the hacker to assume the role of an already authorized user.

Kerberos: An authentication and key distribution system developed by MIT.

Logging: The process of storing information about events that occur on the firewall or network.

Non-repudiation: The capability that allows the receiver of an electronic message to prove who the sender was. Capability necessary incase the sender later denies sending the message.

Proxy: An agent that acts on behalf of another user. Typical proxies accept a connection from a user, makes a decision as to whether or not the user or client IP address is permitted to use the proxy, does some authentication, and then completes the connection. Main purpose is to eliminate direct contact to protected resource and secure its identity.

Repudiation: Denial by a participant of having participated in all or part of a electronic communication.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

RSA: Rivest, Shamir, Adleman Public Key technology based on factoring large numbers. Patents for crypto technology held by RSA Data Security Inc.

SATAN: Unix-based network scanning tool. Scans networks and resources for vulnerabilities.

Security Control: A countermeasure put in place to prevent, deter, detect, mitigate, or recover from the actions of a threat agent.

Trojan Horse: Software program that appears to do something normal but which, in fact contains a trapdoor or attack program.

Threat: Condition that has the potential to violate the integrity of the network or cause harm to system resources.

Virtual Private Network: A network consisting of a number of host that have implemented protocols to securely exchange information.

Virus: Malicious code that can plant itself into operating systems and programs and modify them.

© SANS Institute 2001, Author retains full rights

APPENDIX A: WELL KNOWN PORT NUMBERS

Keyword	Decimal	Description
	1/tcp	TCP Port Service Multiplexer
	1/udp	TCP Port Service Multiplexer
	2/tcp	Management Utility
	2/udp	Management Utility
	3/tcp	Compression Process
	3/udp	Compression Process
rje	5/tcp	Remote Job Entry
rje	5/udp	Remote Job Entry
echo	7/tcp	Echo
echo	7/udp	Echo
discard	9/tcp	Discard
discard	9/udp	Discard
systat	11/tcp	Active User
systat	11/udp	Active User
msp	18/tcp	Message Send Protocol
msp	18/udp	Message Send Protocol
ftp-data	20/tcp	File Transfer
ftp-data	20/udp	File Transfer
ftp	21/tcp	File Transfer (Control)
ftp	21/udp	File Transfer (Control)
ssh	22/tcp	SSH Remote Login Protocol
ssh	22/udp	SSH Remote Login Protocol
telnet	23/tcp	Telnet
telnet	23/udp	Telnet
smtp	25/tcp	Simple Mail Transfer
smtp	25/udp	Simple Mail Transfer
time	37/tcp	Time
time	37/udp	Time
name	42/tcp	Host Name Server
name	42/udp	Host Name Server
nameserver	42/tcp	Host Name Server
nameserver	42/udp	Host Name Server
nicname	43/tcp	Who Is
nicname	43/udp	Who Is
tacacs	49/tcp	Login Host Protocol (TACACS)
tacacs	49/udp	Login Host Protocol (TACACS)
domain	53/tcp	Domain Name Server
domain	53/udp	Domain Name Server
bootps	67/tcp	Bootstrap Protocol Server
bootps	67/udp	Bootstrap Protocol Server
bootpc	68/tcp	Bootstrap Protocol Client
bootpc	68/udp	Bootstrap Protocol Client
tftp	69/tcp	Trivial File Transfer
tftp	69/udp	Trivial File Transfer
gopher	70/tcp	Gopher
gopher	70/udp	Gopher
finger	79/tcp	Finger

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

finger	79/udp	Finger
www	80/tcp	World Wide Web HTTP
www	80/udp	World Wide Web HTTP
www-http	80/tcp	World Wide Web HTTP
www-http	80/udp	World Wide Web HTTP
kerberos	88/tcp	Kerberos
kerberos	88/udp	Kerberos
hostname	101/tcp	NIC Host Name Server
hostname	101/udp	NIC Host Name Server
rtelnet	107/tcp	Remote Telnet Service
rtelnet	107/udp	Remote Telnet Service
pop3	110/tcp	Post Office Protocol –version 3
pop3	110/udp	Post Office Protocol –version 3
sunrpc	111/tcp	Sun Remote Procedure Call
sunrpc	111/udp	Sun Remote Procedure Call
sftp	115/tcp	Simple File Transfer Protocol
sftp	115/udp	Simple File Transfer Protocol
ntp	123/tcp	Network Time Protocol
ntp	123/udp	Network Time Protocol
snmp	161/tcp	Simple Network Management Protocol
snmp	161/udp	Simple Network Management Protocol
snmptrap	162/tcp	SNMP Trap
snmptrap	162/udp	SNMP Trap
bgp	179/tcp	Border Gateway Protocol
bgp	179/udp	Border Gateway Protocol
ldap	389/tcp	Lightweight Directory Access Protocol
ldap	389/udp	Lightweight Directory Access Protocol
https	433/tcp	SSL Protected HTTP
ssmtp	465/tcp	SSL protected SMTP
snews	563/tcp	SSL protected Usenet news
ssl-ldap	636/tcp	SSL protected LDAP
spop3	995/tcp	SSL protected POP3

© SANS Institute 2001, Author retains full rights.

BIBLIOGRAPHY

Books

[Cheswick and Bellovin, 1994] William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security, Repelling the Wily Hacker*. Addison-Wesley Publishing Company. Copyright ® 1994 by AT&T Bell Laboratories, Inc.

[Oppliger, 1997] Rolf Oppliger. *Internet and Intranet Security*. Artech House (Boston/London).

[Chapman and Zwicky, 1995] D. Brent Chapman and Elizabeth D. Zwicky. *Building Internet Firewalls*. O'Reilly & Associates, Inc.

[McMahon, 1998] Piers McMahon. PKI Discussion. 14th Annual ACSA Conference, Phoenix, Az., December 6-11, 1998.

[Anonymous, 1997] Anonymous. *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network*. Sams.net Publishing. First Edition.

Internet Sites

Carnegie Mellon CERT Coordination Center - http://www.cert.org/nav/index_red.html

Computer Security Institute – http://www.gocsi.com/prelea_000321.htm

International Computer Security Association - http://www.icsa.net/

Cryptography FAQ Index - http://www.faqs.org/faqs/cryptography-faq/

Information Warfare on the Web - http://www.fas.org/irp/wwwinfo.html

IETF –
http://www.ietf.org/rfc/rfc2402.txt
http://www.ietf.org/internet-drafts/draft-ietf-l2tpext-security-04.txt

Safeware – www.safeware.com

ISS xforce - http://xforce.iss.net

NAI McAfee – Virus http://vil.mcafee.com/default.asp? Hoaxes http://vil.mcafee.com/hoax.asp

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 23rd, 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