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.

Case Study: Implementing a Secure Wireless Network using WPA

Wireless network cards are becoming quite common at my company especially in notebook computers. With this proliferation of wireless network cards have come requests from the users of these computers to access the corporate network using a wireless connection. In 2001 and 2002 I implemented an 802.11b system on a limited scale for my company using Wireless Encryption Protocol (WEP) encryption as the sole security mechanism. Demand for wireless service has steadily increased since then, and in July of 2003 I was asked t...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Case Study: Implementing a Secure Wireless Network using WPA

Randy Hensel
8 October 2003
GSEC Version: 1.4b Option: 2

© SANS Institute 2003, Author retains full rights

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

Table of Contents

Introduction 2
The Network Prior to the WPA Upgrade 2
The Process of Upgrading to WPA 4
- Configuring the Access Point 5
  - IP Addressing 5
  - 802.1x Authentication 5
  - RADIUS Authentication Server 6
  - Other Configuration Settings 7
- Configuring the Network Interface Card 7
- Configuring the Windows 2000 Network Services 7
  - Certificate Services 8
  - Internet Authentication Service (IAS) Client 8
  - Domain Security Group 8
  - Remote Access Policy 9
  - DHCP Server 9
- Configuring 802.1x Authentication Client 10
- Conclusion 10

References 12

© SANS Institute 2003, Author retains full rights

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

Introduction

Wireless network cards are becoming quite common at my company especially in notebook computers. With this proliferation of wireless network cards have come requests from the users of these computers to access the corporate network using a wireless connection. In 2001 and 2002 I implemented an 802.11b system on a limited scale for my company using Wireless Encryption Protocol (WEP) encryption as the sole security mechanism. Demand for wireless service has steadily increased since then, and in July of 2003 I was asked to implement a wireless network on a larger scale. I explained to the management team at my company the many shortcomings of the WEP encryption protocol, and they agreed that any upgrade of our wireless network should also include better security. It was also important to them that any upgrades integrate with our current network infrastructure.

During the past year, the Wi-Fi Protected Access (WPA) components of the upcoming 802.1i standard have been released. My research has indicated that many vendors have begun supporting these components. I was pleased to learn that 802.1x authentication was based on authentication methods that we already were using for our remote users. I chose the Proxim AP-2000 Access Point because Proxim has a strong product line, a good reputation in the market, and because Proxim has been successfully used by a local college Information Services staff who I spoke with while researching this issue.

The Proxim equipment along with the services installed on my Windows 2000 network provided an environment that enabled me to leverage the existing authentication services currently in place. Aside from the Proxim access point and network interface card (NIC), no additional hardware was needed and the configuration of the Windows services was relatively minimal. This enabled me to upgrade our old WEP secured wireless network to an 802.1x secured platform that is impervious to all currently known wireless attacks.

The Network Prior to the WPA Upgrade

When I began this project, our network infrastructure consisted of a single Windows 2000 active directory forest with a single domain. Our internal users use standard Windows domain authentication. Our remote dial-up users dial in through a Shiva LAN Rover and also use Windows domain authentication. Remote VPN users are authenticated by IPSec group authentication on a Cisco VPN 3005 and then on the domain by a Microsoft IAS server. Dynamic Host Configuration Protocol (DHCP) is used to configure IP settings on all workstations whether they access the network locally or through remote access.

My company's wireless network consisted of a single NETGEAR WG602 802.1g wireless access point. Security on the wireless network at the time consisted of a single WEP key. I considered modifying our current wireless infrastructure to

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

improve security by moving the access point to the DMZ on our PIX firewall and requiring our wireless users to connect via a VPN client. While this option would have been effective, I ruled it out because the VPN client adds a level of complexity that many users would have difficulty mastering.

WEP encryption and its vulnerabilities are well documented. Arunesh Mishra and William A. Arbaugh at the University of Maryland have developed two successful attacks against the 802.1x authentication protocol. By sending a disassociate message to the client and then spoofing the client's MAC address, an adversary could launch a successful session-hijacking attack. A successful man-in-the-middle attack can be accomplished by an adversary acting as both an access point for the client and as a client for the access point. This attack is possible because of the 802.1x protocol's inherent trust of the access point. Mishra and Arbaugh state that, "The entire framework is rendered insecure if the higher-layer protocol also performs a one-way authentication (like EAP-MD5)" (Mishra p. 7).

Although 802.1x provides the flexibility to use any Extensible Authentication Protocol (EAP), Mishra and Arbaugh's research shows that not all EAP protocols are ideal for use in a wireless network.

WEP encryption vulnerabilities are also documented in "Intercepting Mobile Communications: The Insecurity of 801.11" (Borisov), and "Unsafe at any key size; An analysis of the WEP encapsulation" (Walker).

Because of the well documented vulnerabilities of WEP encryption, the Institute of Electrical and Electronics Engineers (IEEE) is developing a new standard for wireless security called 802.1i. Some components of the 802.1i standard, called Wi-Fi Protected Access (WPA), are currently available on some wireless equipment. In their white paper titled "Proxim and Wi-Fi Protected Access (WPA)," Proxim describes WPA as,

> … a specification of standards-based, interoperable security enhancements that strongly increase the level of data protection and access control for existing and future wireless LAN systems. Wi-Fi Protected Access is derived from, and will be forward compatible with the upcoming IEEE 802.11i standard (Proxim WPA).

WPA consists of two components, 802.1x authentication and an upgrade to WEP encryption called temporal key integrity protocol (TKIP).

When a wireless client comes within range of an access point configured to use 802.1x authentication, the access point challenges the client. The client responds to the challenge by sending its identity, which the access point passes on to the Remote Authentication Dial-in Users Service (RADIUS) server that supports 802.1x authentication such as Microsoft's IAS or Funk Software's Steel-Belted Radius. The authentication server then requests the client's credentials

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

and the type of credentials that are expected. The client then sends the credentials, which are validated by the authentication server. If the credentials are accepted, the client is successfully authenticated and the access point will then allow data traffic to flow from the client to the protected network.

The 802.1x authentication protocol provides a secure way to authenticate the users and allow them access to the network. Once authenticated, the data needs to be encrypted to thwart attackers who may be sniffing the wireless packets. TKIP is the protocol that provides data encryption. TKIP is essentially WEP without the flaws of weak initialization vectors (IV) and static keys. Proxim describes TKIP as providing,

> … important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC) named Michael, an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism (Proxim WPA p. 1).

Since our network already had the active directory, the Microsoft IAS Server and the DHCP server necessary to implement the advanced authentication protocols specified in 802.1x, I wanted to make every effort to implement our new wireless network security based on these new products and protocols.

The Process of Upgrading to WPA

My first task was to research the available wireless products on the market. Since we owned a NETGEAR WG602 Access Point, I started with NETGEAR. NETGEAR caters to the small office and home market and does not currently support advanced authentication or encryption protocols. While a NETGEAR Support Technician indicated that WPA support would be available for their products in the future, he was unable to provide an estimate of when that would occur. I found the same to be true with DLink. 3Com supports TKIP re-keying, but I could find no mention of 802.1x authentication. Cisco, Buffalo Technology, Linksys and Proxim all support the full WPA specification. After reviewing the wireless products available I chose Proxim because of their strong enterprise capable product line and support of leading edge security protocols. Cisco also has a very strong product line but was ruled out because of their lack of support for 54 Mbs 802.11g protocol.

Having made the decision to use the Proxim products, I purchased a Proxim AP2000 with an 802.11b/g radio, and a Proxim 802.11b/g Gold PC card. Out of the box the Proxim AP-2000 did not support WPA, but it was a simple process to download the latest firmware and install it through TFTP. Since I upgraded the access point firmware, I thought it important to upgrade the software for the network interface card as well. I first went to the Proxim Web site. When I could not find the proper drivers I called technical support. The driver that the technician directed me to was not labeled for the wireless NIC that I had

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

purchased but he assured me that it was the right one. When the driver did not work once installed I called technical support again. Their call center appears to be in India and with a poor connection as well as the language barrier, all they could tell me to do was to uninstall the driver and then reinstall it, which did not solve the problem. After they had me do that about five times I decided to try the driver that came with the card. As it turned out the driver that came with the card worked just fine.

Microsoft and Cisco have developed a new authentication protocol called Protected Extensible Authentication Protocol (PEAP). PEAP itself does not provide the authentication. Instead it creates an encrypted transport level security (TLS) channel which provides security for Extensible Authentication Protocols (EAP) such as EAP-MSCHAPv2 and Extensible Authentication Protocol – Transport Level Security (EAP-TLS). Microsoft supports both the username/password-based authentication protocol EAP-MSCHAPv2 as well as the certificate-based authentication protocol EAP-TLS. I opted to use EAP-MSCHAPv2 because EAP-TLS had the added complexity of needing to maintain a certificate authority (CA) and requires that each client computer be temporarily connected to the wired network to install a user certificate.

Configuring the Access Point

There are many configuration options on the Proxim AP2000. All access point configuration was done through the Web interface, and all access point configuration steps came from the AP-2000 user's manual provided on CD with the access point (Proxim Corporation, AP-2000 User's Manual). Detailed below are the configuration steps necessary for configuring 802.1x authentication.

A. IP Addressing

Click Configure > Network > IP Configuration.
IP address type needs to be static because the RADIUS server will be configured with the access point's IP address. I configured the IP address, subnet mask, default gateway, and DNS per my network's configuration.

B. 802.1x Authentication

1. Click Configure > Security > 802.1x.
2. Set 802.1x Security Mode to 802.1x.
3. Select an Encryption Key Length.
4. Enter a Re-keying Interval.

   The re-keying interval determines how often a client's encryption key is changed and can be set to any value between 60 to 65,535 seconds. Re-keying frustrates hacking attempts without taxing system resources.

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

Setting a fairly frequent re-key value (900 seconds or 15 minutes) effectively protects against intrusion without disrupting network activities.

Click “OK” to save the changes.

5. Reboot the access point.

C. RADIUS Authentication server

1. Click Configure > RADIUS > RADIUS Authentication.
2. Disable RADIUS MAC Access Control. I did not use MAC address control although I will likely implement it in the near future.
3. Check the box labeled Enable Primary RADIUS Authentication Server.
4. If you want to configure a back-up RADIUS server, check the box labeled Enable Back-up RADIUS Authentication Server. I currently have only one RADIUS server.
5. Enter the time in seconds that each client session may be active before being automatically re-authenticated in the Authorization Lifetime field. This parameter supports a value between 900 and 43,200 seconds; the default is 900 seconds. Since traffic is expected to be fairly light to start with, I have left the re-authentication value at 900 seconds. As user load increases, the value may need to be increased.
6. Select a server addressing format type (IP Address or Name). If you want to identify RADIUS servers by name, you must configure the AP as a DNS client.
7. Enter the server’s IP address or name in the field provided.
8. Enter the port number which the access point and the server will use to communicate. By default, RADIUS servers communicate on port 1812.
9. Enter the shared secret in the Shared Secret and Confirm Shared Secret fields. This is a password shared by the RADIUS server and the access point. The same password must also be configured on the RADIUS server.
10. Enter the maximum time, in seconds, that the access point should wait for the RADIUS server to respond to a request in the Response Time field. The range is one to 10 seconds; the default is three seconds.
11. Enter the maximum number of times an authentication request may be retransmitted in the Maximum Retransmissions field. The range is one to four; the default is three.
12. If you are configuring a back-up server, repeat steps six through 11 for the back-up server.

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

13. Click OK to save your changes.
14. Reboot the access point for these changes to take effect.

D. Other Configuration Settings
The management interfaces must also be secured or disabled. By default the password to get to the Web and Telnet configuration tools is “public” and the SNMP read/write community name is also “public”.

Passwords are configured by clicking Configure > Management > Passwords.

I also control access to the management interfaces by IP address. This can be done by clicking Configure > Management > IP Access Table. Access can be controlled by the individual IP address or by IP mask. I chose to configure management access for only one workstation.

The SNMP, Telnet and Web management tools can be disabled by clicking Configure > Management > Services. Since I did all configuration via the Web interface and since my company is not using SNMP, I have disabled both Telnet and SNMP. The serial interface is the only management tool that cannot be disabled. Access to the serial port must be controlled by physical security.

It is also very important to secure the access point itself. Physical security is very important because the configuration can be erased by pushing and holding the reset button on the access point for five seconds.

Configuring the Network Interface Card

Detailed below are the steps necessary to configure the PC card on the notebook.

1. Install the Proxim Client Utility on the client computer.
2. Physically install the NIC
3. Open the Client Utility, create a new profile and associate the profile with the Proxim AP-2000.
4. Under the security tab select Externally Managed 802.1x Keys.

Configuring the Windows 2000 Network Services

The next step is to configure the Windows services that will authenticate the wireless clients when the access point makes an authentication request. There are five components that need to be configured on the Windows 2000 network: certificate services, the RADIUS client (Microsoft’s IAS), a domain security group, a remote access policy and the DHCP server.

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

A. Certificate Services

A certificate must be obtained by the IAS server. This certificate could be obtained from pubic certificate authority but for internal use I installed certificate services on one of my domain controllers. Later when I configured remote access policies I was able to choose this certificate to authenticate the IAS server.

B. Internet Authentication Service (IAS) client

The Proxim AP-2000 is configured to authenticate against a Remote Authentication Dial-In User Service (RADIUS) which is a client/server authentication protocol used extensively by Internet service providers (ISPs), and is a very popular method of authenticating dial-up and VPN network users. Microsoft provides RADIUS authentication through its internet authentication service (IAS.) IAS is installed by going to the Control Panel, and then to Add/Remove Windows components. IAS is a subcomponent of networking services. Once installed IAS is launched from a menu item in Administrative Tools. To configure RADIUS authentication open the IAS administration tool and right click on Clients, choose New Client. The client needs three things, a friendly name the IP address of the device initiating the authentication and the shared secret.

1. Give the IAS client a friendly name.
2. Since RADIUS is the only option available for the protocol field on this page just leave that field alone, click Next.
3. Enter the IP address of the device initiating the authentication.
4. The Client-Vendor field should stay at the default (RADIUS Standard).
5. Enter the shared secret and confirm. This is the same shared secret that was entered in the RADIUS tab when configuring the access point.
6. Click Finish to save and close.

C. Domain Security Group

I wanted to control who has permission to connect to the wireless network, so I created a group called Wireless Network and added the users who currently wish to have access to the wireless network. This is done from Microsoft's domain administrative tool Active Directory Users and Computers.

1. Chose the Organizational Unit (OU) Users
2. Right-click and choose New Group.
3. Give the group a name. I chose the name Wireless Network.
4. Click the Domain Local, and Security radio buttons.
5. Click OK to save and close.

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

D. Remote Access Policy

1. Start the IAS management tool from the Administrative Tools menu.
2. Right click Remote Access Policies.
3. To start the remote access policy wizard, click New Remote Access Policy.
4. Give the remote access policy a name. I gave my remote access policy the name Wireless Authentication. Click Next.
5. The next window specifies what conditions you want to place on who is allowed to authenticate. Click Add. I wanted only those who are in the Wireless Network group to be allowed to authenticate. So for Conditions I chose Windows-Groups. This brings up a window where you can add a list of users or groups.
6. Click Add. Select the Wireless Network group that was created in the previous section. Clicking OK twice saves the selection and takes you back to the remote access policy window.
7. Click Next. Here you will have a window with two radio buttons. Your options are to choose to allow or deny access to those who meet the criteria specified in the policy. This policy was created to allow access to users so click the Grant Remote Access Permission radio button. The remote access policy is created, but authentication and encryption still need to be configured.
8. Click Edit Profile. Then click the Authentication tab.
9. On the Authentication tab, select Extensible Authentication Protocol. Next select Protected EAP (PEAP) from the drop down and Microsoft Encrypted Authentication Version 2 (MS-CHAP-V2).
10. Click Configure to configure PEAP authentication. Choose the certificate that was created when Certificate Services was installed. Then choose the EAP type that is being used. For PEAP I chose Secured Password (EAP-MS-CHAP v2).
11. That is all that needs to be configured on the Authentication tab. Click OK to close the Configure EAP window, and click on the Encryption tab.
12. On the Encryption tab we want to ensure that the No Encryption option is not selected. The remote access policy is now complete.

E. DHCP Server

The wireless clients need to have their IP settings configured. I have had a Microsoft DHCP server running for several years so there was no configuration needed on my part to enable DHCP configuration of the client computers. For information on setting up a Microsoft DHCP server see http://www.microsoft.com/windows2000/docs/dhcp.doc. (Microsoft Corporation. “Dynamic Host Configuration Protocol for Windows 2000.”)

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

Configure 802.1x Authentication Client

Since the network interface card passes the 802.1x authentication requests on to the access point, the operating system must initiate the request. In Microsoft operating systems this is a function of the Microsoft 802.1x authentication client. This client is a standard part of Windows XP and is a free download for Windows 2000. See http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp for more information (Microsoft Corporation. "Microsoft 802.1x Authentication Client.")

The 802.1x authentication client adds an authentication tab to the network interface properties dialog box. This tab provides the ability to enable 802.1x authentication. Once enabled, a drop down allows you to choose PEAP or certificate-based authentication. As stated earlier, my environment was configured to use PEAP. If the computer has already been configured as a member of the Windows 2000 domain, and the user is logged into the client computer with a valid domain username and password, when the client comes within range of the access point it attempts to authenticate on the network. Opening the status window of the wireless interface will show the authentication status. If the user is logged on to the computer with the proper credentials, authentication will be completed automatically and the user will be given access to the network.

The Microsoft Windows 2003 product documentation describes what happens when the wireless client comes within range of the access point:

> The wireless client associates with a wireless access point. An IEEE 802.11-based association provides an Open System or Shared Key Authentication before a secure association is created between the client and access point. After the IEEE 802.11-based association is successfully established between the client and access point, the TLS session is negotiated with the access point. After authentication is successfully completed between the wireless client and the server (for example, an IAS server), the TLS session is negotiated between them. The key that is derived during this negotiation is used to encrypt all subsequent communication (PEAP page 1).

At this point the wireless network configuration is complete and ready to use.

Conclusion

Successful attacks against WEP secured networks are well documented and most security experts consider WEP to be very ineffective as a security mechanism. For this reason the IEEE standards body is working on 802.1i, a new standard for securing wireless networks. Because of the immediate lack

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

of adequate wireless security protocols, the IEEE has released the authentication and encryption portions of the 802.1i standard dubbed WPA. By making use of hardware and software that is WPA compliant, I was able to adequately secure my company's network against current known wireless vulnerabilities.

Although using WPA to secure our wireless network has mitigated the vulnerabilities that our WEP-secured network had, there are ways it could be secured further, and there are issues that may prevent some users from being able to use it.

Username/password protocols like the PEAP protocol are very commonly used, but they are also vulnerable to brute force and dictionary attacks and therefore need the support of a strong password policy. Other EAP protocols that use certificate-based or hardware-based authentication are typically more secure. One of the benefits of using 802.1x is that as my company grows and as new authentication protocols are implemented, they can be easily integrated into the wireless network.

Because WPA is only a partial implementation of 802.1i (a protocol that is very new and has not yet been ratified by the IEEE) not all manufacturers have implemented WPA on their products. It is very likely that I will encounter users who have Network Interface Cards that are not WPA compliant. These older wireless cards will have to be upgraded or replaced.

Overall I was very pleased with how well 802.1x authentication integrated with the authentication framework that I already had in place. The standards body has done a good job of specifying a very thorough authentication protocol that will be easy for most organizations to implement. With many hardware and software vendors adding support for it to their products I expect to see 802.1i widely implemented in the very near future.

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

References

Arbaugh, William; Mishra, Arunesh A. “An Initial Security Analysis of the 802.1X Standard.” 6 February 2002. URL: http://www.cs.umd.edu/%7Ewaa/1x.pdf (11 September 2003).

Borisov, Nikta; Goldberg, Ian; Wagner, David. "Intercepting Mobile Communications: The Insecurity of 802.11." 16-21 July 2001. URL: http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf (4 September 2003).

Cisco Systems, Inc. “Cisco Aironet Response to University of Maryland’s Paper, “An Initial Security Analysis of the IEEE 802.1x Standard.”” 2002. URL:http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00800a9e74.html (24 September 2003).

Microsoft Corporation. “Dynamic Host Configuration Protocol for Windows 2000.” 1999. URL: http://www.microsoft.com/windows2000/docs/dhcp.doc (5 October 2003)

Microsoft Corporation. “Microsoft 802.1x Authentication Client.” Microsoft News Bulletins. 10 January 2003. URL: http://www.microsoft.com/windows2000/server/evaluation/news/bulletins/8021xclient.asp (24 September 2003).

Microsoft. “PEAP.” Windows 2003 Product Documentation. URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_ias_protocols_peap.asp (9 September 2003).

Microsoft Corporation. “Using 801.2x Authentication on Computers Running Windows 2000.” KB Article 313664. 15 August 2003. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;313664 (5 September 2003).

Network World Fusion. “Microsoft, Cisco prepare for PEAP Show.” 23 September 02. URL: http://www.nwfusion.com/cgi-bin/mailto/x.cgi (1 September 2003)

Proxim Corporation. “AP-2000 Users Manual.” 2003. Orinoco AP-2000 Software and Documentation CD.

Proxim Corporation. “Proxim and WI-FI Protected Access (WPA).” 2003. URL: http://www.proxim.com/learn/library/whitepapers/WPA_White_Paper.pdf (9 September 2003).

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

Walker, Jesse. "Unsafe at any Key Size: An analysis of the WEP encapsulation. November 2000." URL: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (4 September 2003).

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, 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