Interested in learning more about security?

SANS Institute InfoSec Reading Room

Scouts Out! - Protecting the Army's Wireless Networks and its impact on Corporate Wireless Co

When an Army tactical commander begins a campaign, one of the first orders he issues is "Scouts Out.!" This order is given to provide security to the front and flanks of his force by sending security elements (Cavalry Scouts) to guard his flanks and provide early warning to the commander. The U.S. Army recently announced the adoption of two wireless network systems for soldiers called "Land Warrior" and CAISI that provide wireless communication between the individual soldier and his leaders as well as support teams and...

Jim Mussulman
GSEC Practical Assignment v. 1.4b, Option 1

Scouts Out! - Protecting the Army's Wireless Networks and its impact on Corporate Wireless Computing

Abstract

When an Army tactical commander begins a campaign, one of the first orders he issues is "Scouts Out.!" This order is given to provide security to the front and flanks of his force by sending security elements (Cavalry Scouts) to guard his flanks and provide early warning to the commander. The U.S. Army recently announced the adoption of two wireless network systems for soldiers called "Land Warrior" and CAISI that provide wireless communication between the individual soldier and his leaders as well as support teams and their supply depots. The Army has chosen AES because it is a more robust wireless security protocol than is the commonly used WEP. This use of advanced technology on the battlefield is certain to have a positive impact on the use of wireless in the business community, both in the implementation of wireless technology and in the use of advanced methods to secure the network traffic. This paper will discuss the following: the Army's implementation of 802.11 wireless networks and the methods used to secure those networks, the issues with WEP, DES and AES, current issues in corporate wireless security, and a look at Defense in Depth as the best practice to secure the wireless network.

Security Concepts - Force Protection Doctrine

Securing an armed force (force protection) is a concept that has been practiced for thousands of years. Sun Tzu wrote, "It is only the enlightened ruler and the wise general who will use the highest intelligence of the army for purposes of spying and thereby achieve great results." (Giles, 186) Spying is only one method of gaining intelligence about the plans and movements of the enemy in order to secure the force. Tactician General Carl von Clausewitz recommended that the commander incorporate the use of advanced guard and outposts to act as "the eyes of the army" (von Clausewitz, 1182). Fortresses are built for security of the men and their equipment, and to protect them from attack by an enemy when they are not involved in a campaign. When they are involved in a campaign, away from the fort (tress), commanders utilize scouts to protect their flanks from attack.

Security operations tasks for Cavalry units in today's Army doctrine state that they are to:

> …obtain information about the enemy and provide reaction time, maneuver space, and protection to the main body. Security operations are characterized by aggressive reconnaissance to reduce terrain and enemy unknowns, gaining and maintaining contact with the enemy to ensure continuous information, and providing early and accurate reporting of information to the protected force. (U.S. Army Field Manual 17-95, 4-1)

Security tasks, as defined above, refer to protecting the maneuver force in order to provide room to conduct operations. Although this doctrine does not specifically address securing information, the concept of securing the force through continuous flow of intelligence information to the commander is a primary tenet. The commander who knows the disposition of his own and the enemy's forces can better plan both offensive and defensive operations. Another Field Manual defines the use of technology in the conduct of operations.

> "Technology …affects how Army forces conduct (plan, prepare, execute, and continuously assess) full spectrum operations in peace, conflict, and war….. Battle command benefits from the ability of modern microprocessors and telecommunications to collect, process, store, display, and disseminate information faster and with greater precision. Technology improves soldier endurance and protection, thereby increasing the potential for mission accomplishment." (U.S. Army Field Manual 3-0, 1-39).

How does this doctrine of force protection apply to the implementation of new wireless technologies? The capabilities of two new Army wireless networks will protect the data being transmitted and will provide the commander with extended "eyes" from the soldier on the ground to allow continuous updates of the tactical situation, and more accurately plan for future operations by the dissemination of information regarding both the tactical and logistical requirements of the force.

Land Warrior and CAISI

Land Warrior Computer/Radio Subsystem

Land Warrior is a series of innovations and improvements to the Army combat soldier's uniform and equipment which are designed to prepare him for combat in the 21st Century battlefield. The program includes technology upgrades to the M-16 individual weapon, the helmet (with an integrated display), protective clothing enhancements, and a Computer/Radio subsystem (CRS). This CRS subsystem provides the hardware for the wireless network in addition to providing Global Positioning System (GPS) information and radio control capabilities for the soldier.

> The subsystem comes in two flavors: The leader version has two radios and a flat panel display/keyboard, and soldiers have one radio. With the

> equipment, leaders and soldiers can exchange information. Soldiers using their weapon-mounted camera, for example, can send videos to their leaders. (FAS).

When the program contracts were awarded in the late 1990's, Raytheon was the contractor who developed the initial system. Many soldiers who tried the prototypes did not like the weight or the short battery life of the system. The Army reviewed the results and held another competition and a small firm, named Pacific Consultants, was awarded the follow-on contract to refine the system.

> Soldiers say the newest Land Warrior is the best version yet. At 12 pounds, the vest and body armor fit snugly around a soldier's torso. Its Microsoft Windows 2000 software still has bugs but is nearing the project goal of 10 days of use without breaking down. (Iwata)

The revised CRS subsystem relied on securing the data transmissions using the Wired Equivalency Privacy (WEP) protocol. The protocol was found to be easily breached, so the need for data security as a force protection measure was still required.

CAISI

The Army's Combat Service Support Automated Information System Interface (CAISI) project has been under development concurrently with the Land Warrior system. The intent of the CAISI system is to provide wireless data collection and transfer capabilities to logistics support forces. This system is an interface from the mechanic and supply sergeant to the standard Army Logistics systems and their support networks which are housed on rear area mainframe and mini-computers. “It will provide wide area connectivity between the end users and the networks.” (Jackson). During Desert Storm and operations in Bosnia, the Army found that it needed to be able to quickly assess the logistics requirements of its fighting force. For example, when a helicopter needs maintenance or a tank needs a new tread, the parts and manpower requirements for those actions can be passed to the rear area maintenance and supply systems computers quickly using CAISI and wireless 802.11b protocols. When the system interface was conceived in the late 1990's, the plan was to use 128 bit WEP encryption. "The program was held up last year because of security exposures found in IEEE 802.11b networks’ Wired Equivalent Privacy protocol." (Jackson)

WEP vs. DES vs. AES

WEP

Both of the wireless systems described above were originally developed with a reliance on an encryption standard that was thought to be secure. The Wired Equivalency Privacy Protocol is defined by the IEEE 802.11 WiFi standards. It is

intended to provide an wired security equivalent to data being transmitted wirelessly. The standard recognizes that radio waves cannot be controlled in the same manner as a wired network, so the WiFi standard called for an encryption method to provide for privacy and security of the transmissions. The standard calls for both a 64 bit and a 128 bit encryption algorithm, which is based on the RC-4 stream cipher method, "... a variable key-size stream cipher with byte-oriented operations." (RSA, Cryptography FAQ). This implementation of the RC-4 has been proven flawed and inadequate to protect the data being transmitted. In August, 2001 researchers at ATT and Rice University demonstrated that the WEP implementation of the RC-4 was flawed and therefore insecure for use in securing wireless transmissions. (Stubblefield, et.al. 2)

DES

Both the Land Warrior system and the CAISI system can also use the Data Encryption Standard (DES). DES was developed for use in protecting data transmitted by U.S. Government organizations, and the standard was reaffirmed in FIPS Publication 46-2 on December 30, 1993 (although it had been approved and in effect since 1977). (FIPS Pub 46-2). DES uses a 64 bit input block and creates a 56 bit key cipher block to encrypt the data. Although this standard was prescribed by the Federal Government, it was also found to be vulnerable to compromise.

> Unfortunately, over time various shortcut attacks were found that could significantly reduce the amount of time needed to find a DES key by brute force. And as computers became progressively faster and more powerful, it was recognized that a 56-bit key was simply not large enough for high security applications. As a result of these serious flaws, NIST abandoned their official endorsement of DES in 1997 and began work on a replacement, to be called the Advanced Encryption Standard (AES). Despite the growing concerns about its vulnerability, DES is still widely used by financial services and other industries worldwide to protect sensitive on-line applications. (Tropical Software website)

Because the information transmitted over the Army's wireless networks affects the protection of the force, a new algorithm was needed. "Advances in semiconductor technology make the key-length issue more critical. Chip speeds have caught up so that DES keys can be broken with a bit of cleverness and exhaustive search." (Kaufman, et.al. 63.) Enter AES.

AES

The Advanced Encryption Standard is a Federal Information Processing Standard which was selected as a result of submissions to the National Institute of Standards (NIS). It is based on the submission from two Belgian cryptographers and derives its name, *Rijndael*, from their two last names -

Rijmen and Daemen. (Kaufman, et.al. 82.) It was awarded FIPS Standard 197 on December 6, 2001. (Federal Register. 63369). AES' strength is that it uses three different key sizes - 128, 192 and 256 bit. The Fact Sheet from the NIST home page puts the new algorithm in perspective, relative to the DES and the projection for cracking keys used in this new algorithm.

> In the late 1990s, specialized "DES Cracker" machines were built that could recover a DES key after a few hours. In other words, by trying possible key values, the hardware could determine which key was used to encrypt a message.
>
> Assuming that one could build a machine that could recover a DES key in a *second* (i.e., try 2^{55} keys per second), then it would take that machine approximately 149 thousand-billion (149 trillion) years to crack a 128-bit AES key. To put that into perspective, the universe is believed to be less than 20 billion years old. (NIST, #16)

The above presumes that in the future, weaknesses will not be discovered in the Rijndael algorithm, as they were in the WEP and DES standards.

Securing the Army's wireless networks

As was stated above, both of the Army's systems were developed to use either the WEP or the DES encryption standard. Since neither of these standards was found to be really secure, the Army had to find an implementation of the new AES standard to secure their wireless networks. They chose a combination hardware and software implementation developed by Fortress Technologies. The product is called AirFortress and uses a defense in depth concept of a hardware gateway, secure clients software, and strict access control using a database of authorized clients.

> The AirFortress™ provides enterprise strength security for wireless networks through sophisticated encryption, strong authentication and stringent access control. The AirFortress™ combines Layer 2 privacy, a Closed Network Architecture, and Re-Play Protection to ensure the wireless network, mobile devices, and communication are all protected. Unlike traditional VPNs, Fortress' Layer 2 security protocol, wLLS, protects important session data, which otherwise exposed renders WLANs susceptible to analytical attacks. (Fortress, AirFortress™ Wireless Security Solution Features).

One of the reasons this combined technology implementation is so successful is because it acts as a secure gateway to the numerous networks that must be accessed in either of the Army's systems. The client is validated by the hardware and then is seamlessly connected to the server, without having to individually validate to each of the systems inside the gateway. Another feature is the Layer

2 security protocol, which Fortress calls wLLS. It protects the IP addresses and other session data to keep an attacker from learning about the structure of the network. "wLLS supplements encryption security by altering the Media Access Control (MAC) ID number into one that will only be recognized by Fortress Technologies' products." (ISP-Planet). This hardware appears to meet force protection requirements for it not only secures the transmissions from prying eyes, but keeps the transmission client information secure so that other means cannot be used to spoof network clients and gain access to the network. Even its name, Fortress, implies a secure place for the soldier (and his information) to be protected

Current practices in corporate wireless networks

To date, 802.11b Wireless networks have been installed in many corporate and public organizations. Universities have installed campus based wireless LANs to provide student access to the internet and to share information sources on university servers. Amusement parks and other large entertainment venues have installed extensive wireless networks in order to manage resources such as rides, as well as conduct the e-commerce activities of recording and managing foot and drink carts spread throughout the park. Coffee houses, such as Starbucks, are opening their networks to customers who pay a fee for accessing the Internet while sipping their Grande Mocha Latte. Airlines utilize wireless networks at major airports to control ground operations. Auto manufacturers use wireless technologies to provide information flows in a production facility that is hostile to wired topologies.

> Major US retail chain Best Buy has been forced to close down its wireless cash registers after security experts revealed it had been making credit card information available to anyone in the vicinity with the equipment to detect wireless networks. And global supermarket giant WalMart and US pet store PetSmart are under pressure to investigate claims their systems have exactly the same flaws. (Silicon.com. May 2nd 2002)

The cost of the Wireless Access Points (AP's) and wireless network cards has dropped to below $100, so many employee have purchased the hardware and installed them on the corporate network. These installations are knows as rogue wireless LANs, for they are not managed or controlled by the IT department. These rogue access points often circumvent expensive firewalls and other corporate network security devices that were implemented by the IT department to secure corporate data. The Pentagon was recently found to have insecure AP's, even though they were managed by the IT department.

> Chris O'Ferrell, chief technology officer at NetSec Inc. in Herndon, Va., which provides intrusion-detection services to numerous federal agencies and commercial customers, detected the nonsecure wireless LAN at the Defense Information Systems Agency (DISA) on May 10.

> While parked across the street from DISA's headquarters, O'Ferrell was able to view the Service Set Identifier (SSID) numbers of access points and numerous IP addresses. Using a standard 802.11b wireless LAN card attached to his laptop computer and AP detection software from San Diego-based NetStumbler.com, he was able to scan the network in less than half an hour. (Brewin and Verton)

The Pentagon has found other rogue access points and has issued a directive that will ban not only wireless network devices, but other nonsecure wireless technologies such as two way pagers and cell phones. "Pentagon officials fear that the latest generation of wireless devices, including cell phones and two-way pagers, can be used as eavesdropping devices during classified meetings." (Verton).

Even when the access points are controlled and managed by the IT department, the use of easily cracked WEP security has opened unsecured gaps in their network. I was discussing the topic of wireless security with a security consultant and he alleged that he was able to use a laptop running Airsnort software and a wireless NIC to determine the AP's identification names (SSID) and passwords used by a major amusement park to manage their operations. He stated that he did not use the information to break into the network, but only to validate the insecurity of the wireless network.

Many organizations which had installed wireless access points have begun shutting them down because of the lack of security that WEP provides. Others have decided to wait to implement wireless networks until the security issues are solved, or at least tightened up a bit. Alan Coen, in a recent PC Magazine article says, "…the state of wireless these days [is] — one big holding pattern. The optimism of a year ago hasn't evaporated, it's just more cautious. Analysts still give rosy forecasts, but those forecasts are looking farther into the future" (Coen, iBiz 3.) :" For businesses contemplating wireless, "wait and see" may seem to be a reasonable approach. But "plan and see" may be the smarter one. "(Coen, iBiz 6.)

So far, the discussion has involved large corporations with a structured IT department to manage the wireless frontier of its network. What about the thousands of small businesses and corporations that are attracted to the wireless capabilities and the low cost of implementation? These businesses are at just as much risk as the large corporations, maybe even more so. They are lulled into a false sense of security by the advertising and marketing of a "SECURE" (sic) network using WEP.

In a recent test of wireless security in my local metropolitan area, I connected my IPAQ to a wireless NIC, "Mini-stumbler" software from Netstumbler.com and my GPS receiver and went "war-driving". On this 30 mile trip along major interstate highways, I found 45 access points that were within range of my card. Of those

45, only 5 had WEP enabled. Many used the default SSID for the wireless hardware, and others used SSID's that, coupled with the location from the GPS, allowed me to identify the company by their name which was on the side of the building. Many of these were small businesses which had given their name to me in their SSID. Although I did not attempt to connect to any of these networks, this little trip proved to me that wireless technology has been implemented with little thought to security.

What corporate wireless networks, both large and small, need is a fortress to protect their data and business information. The Army has chosen AirFortress to protect their wireless networks, but this technology requires additional, costly hardware and an IT staff to implement and maintain the walls of this wireless fortress. Many corporations and small businesses will probably not implement this technology because of its cost and complexity as well as its use of proprietary software (AirFortress's wLLS, layer 2 security software).

Securing the Fortress - Defense in Depth

What are the best practices to implement in a small or large corporation to maintain data security while using wireless data communications? Is it just a new piece of hardware, a new security algorithm, or the removal of all wireless devices to prevent outsiders from getting to their data? It may be a combination of the above, but any search for a solution should start with a risk analysis to determine the vulnerability of the system and the measures being taken to protect the network and data. From this analysis comes an overall view of the organizations security structure, and this is the starting point for constructing a defense in depth. In effect, the Risk Analysis lays the foundation for the fortress of defense in depth.

Defense in depth is not just one article like a firewall or a fortress appliance, but a series of layers of protection, like the inner walls in a fortress. Each layer has its own vulnerabilities which must be assessed from a "confidentiality, integrity, and availability" (SANS, 1-3) standpoint. The security of corporate data is the key element - the reason for implementation. Security is only as good as the policies that implement and enforce it. A written and widely disseminated policy is the first layer in a defense in depth strategy. All employees should be required to read and certify that they understand the policy and will adhere to it.

Next is the securing of any applications that produce the data or have access to the data. These are secured in the same manner as the next level, the server level, with passwords. Passwords for applications access should be enforced and should be different than the passwords used to access the network servers. The use of strong passwords - ones that cannot easily be guessed (with a dictionary or other attack) should be required by the policy and enforced by the systems administrators. Passwords should be changed frequently and should be

monitored by the system to ensure they are not ones that have been used before.

Securing the servers where the data is stored is the next level. The servers should be protected from both physical access as well as unauthorized network access. Physical security keeps intruders from gaining the ability to steal the hardware in order to get to the data. Servers and other network hardware should be behind locked, limited access doors to maintain security. Security access logs recorded on the servers that list both successful and unsuccessful login attempts provide a method to track and begin to find possible intruders. Another method for Windows NT and 2000 servers is to take away all access rights to the default Administrators account (make Administrator a member of the guest group and create another user with the full administrative rights) and then log all successful and unsuccessful attempts to login as the Administrator. Since the Administrator user no longer has any rights, it is immediately evident that the system is being probed.

The last level in this discussion of defense in depth is the network level. The network must be secured from unauthorized access and protected by a firewall and other intrusion detection systems. Since the majority of attacks come from the Internet, a combination of a firewall and a Network based Intrusion Detection device, or NID, will provide security to the network. The firewall filters data coming out of the network as well as that coming into the network. The implementation of wireless networks makes the network level most important, for the usual security measures in force in a wired environment are not available. The network then becomes the primary attack vector. In those organizations which use an IT managed wireless network access point, the placement of this (AP) device is critical to managing a defense in depth. If the device is placed outside the firewall, then another layer of security must be added. Typically a Virtual Private Network (VPN) solution is used in this instance, so that only validated wireless VPN clients can access the network through the firewall. The problem discussed earlier (of the insertion of an unauthorized or rogue AP's) allows this defense measure to be circumvented and provides wide open access to the network.

All of the defense in depth measures above can be implemented in both large and small companies. The key to the implementation and adherence to any of these measures is the commitment of management to the concept of security. Any policy not supported by management oversight is usually a policy that is not followed. It is like building a fortress using sand instead of cement for the mortar. The structure will look good and will withstand minor attacks, but does not have a strong enough foundation nor structure to withstand repeated and concentrated attacks.

Conclusion

Wireless networking technologies are widely available and are used in all kinds of organizations, from the U.S. Army to small businesses to allow remote access to the network servers and stored data. The IEEE standard for Wired Equivalency Privacy as a part of the 802.11 standard has proven to be a flawed implementation, and so is not widely used. The Army has decided to use the latest standard encryption, AES, for securing its wireless networks. The cost of the hardware and the use of proprietary software in the Army's selected solution will likely not garner its wide acceptance in the corporate wireless community. Although many companies are adopting a wait and see attitude, (waiting until a more secure standard is approved), others will continue to use wireless data communications as a means to connect their employees to the data they must use. Defense in Depth strategy should be used by all companies to protect not only their wireless networks but, more importantly, the data residing inside them. Corporate managers and combat commanders alike must plan for security and must protect their forces and flanks from attack. SCOUTS OUT!

References

Giles, Lionel. SUN TZU ON THE ART OF WAR, Huntsville, AL. Elegant Solutions e-Books. (2001):174-186.

von Clausewitz, Carl. ON WAR. Potsdam, 1832. Republished as an e-Book, 2001.

U. S. Army, Field Manual 17-95 Calvary Operations, Washington, D.C. 1996. Chapter 6, Security Operations.

U.S Army Field Manual 3-0 (100-5) Operations. Department of the Army, Washington D.C. 14 June 2001. Chapter 1, The Technology Dimension.

Federation of American Scientists (FAS),"Land Warrior" http://www.fas.org/man/dod-101/sys/land/land-warrior.htm

Iwata, Edward, "Silicon Valley techies suit up Army with sleeker gear". USA Today, February 6, 2002. http://www.usatoday.com/money/covers/2002-02-07-tech-contractors.htm .

Jackson, William, "Secure Wireless, Army ready to go wireless with combat support." Government Computer News, April 15, 2002 http://www.gcn.com/21_8/tech-report/18361-1.html .

RSA Security Incorporated. (RSA). Bedford, MA. 2002.. http://www.rsasecurity.com/rsalabs/faq/3-6-3.html .

Stubblefield, Ioannidis and Rubin, Using the Fluhrer, Mantin, and Shamir Attack to Break WEP. ATT Labs. August 21, 2001. http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Federal Information Processing Standard (FIPS). Data Encryption Standards (DES). National Bureau of Standards, Gaithersburg, MD. 1993 http://www.itl.nist.gov/fipspubs/fip46-2.htm

Tropical Software. Sammamish, WA. http://www.tropsoft.com/strongenc/des.htm

Kaufman, Charlie; Perlman, Radia; and Speciner, Mike. Network Security PRIVATE Communication in a PUBLIC World. Prentice Hall. Upper Saddle River, NJ. 2002.

Federal Register. Announcing Approval of Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard (AES) Vol. 66, No. 235 . December 6, 2001. Washington, D.C. http://csrc.nist.gov/encryption/aes/frn-fips197.pdf

NIST. Advanced Encryption Standard (AES) Questions and Answers. U.S. Department of Commerce. Washington, D.C. 2002. http://www.nist.gov/public_affairs/releases/aesq&a.htm

Fortress Technologies Inc. Olmar, FL http://www.fortresstech.com/

ISP- Planet. Surround Your Wi-Fi Gear With An AirFortress Fortress Technologies introduces a suite of products that take 802.11 security up a notch. December, 2001. http://www.isp-planet.com/fixed_wireless/equipment/2001/airfortress.html

Brewin, Bob and Verton, Dan DOD IT projects come under fire. Computerworld. May 16, 2002. http://www.computerworld.com/mobiletopics/mobile/story/0,10801,71231,00.html

Verton, Dan. Pentagon to issue wireless disconnect order. Computerworld. August 1, 2002. http://computerworld.com/mobiletopics/mobile/story/0,10801,73150,00.html

Silicon.com. Major stores beam credit card details to the car park. May 2nd 200 http://www.silicon.com/public/door?6004REQEVENT=&REQINT1=53089&REQSTR1=silic

Coen, Alan. Off-Site, Online. PC Magazine, September 17, 2002. p.iBiz 1-6 http://www.pcmag.com/article2/0,4149,485642,00.asp

SANS Courseware. Threat and the Need for Defense in Depth. SANS. Security Essentials Day 2.

Last Updated: October 23rd, 2017

Upcoming SANS Training

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

SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS San Diego 2017	OnlineCAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced