Global Information Assurance Certification Paper

Wai Lee
March 1, 2004
GSEC Practical Assignment v1.4b

WLAN Technologies – Physical Layer Security
(Radio Wave)

Abstract

Wireless Local Area Network (WLAN) has been proliferated for the past few years. It's almost become a commodity as a television set to every household. You do not need to be a computer genius to install a WLAN at home or at work. The top issue with WLAN is security. I found that there are many excellent GSEC practical papers on authentication and encryption, but very little, or almost none on the transmission media, radio wave. I am kind of puzzled by this finding. Why such little effect be done on wireless transmission for improving overall network security. Is it because of higher degree of difficulty to accomplish as compare to others? Is it because of much higher cost? Is it true that the cost to benefit ratio is much lower than the others? Or is it technically not feasible? All these questions stimulate my motivation and curiosity into this wireless transmission technology. In order to propose methods of improving security to the wireless transmission layer, a throughout understanding of the technology is a must. The objective of this paper is to provide a good understanding of various components and concepts for wireless transmission, layer 1 of the OSI model. I will limit the scope to 802.11b and 802.11g only. Concepts of electromagnetic wave, antennas, radiation patterns and modulation techniques will be examined. I will also discuss WLAN deployment methods with emphasis in security.

Radio Frequency

Our atmosphere is filled with electromagnetic waves beside the air we breathe on. With proper tools and equipment, we can pick up these electromagnetic waves or radio wave and may be able to extract some meaningful or usefully contents from them (Electromagnetic wave and radio wave are used interchangeably hereafter). Radio and television are examples of using radio wave as the transport media. Radio provides audio – sound; whereas, television provides audio and video – sound and picture. Radio and television provide unidirectional information flow. Cellular phones and WLAN provide bi-directional or interactive information flow.

Radio waves are differentiated by their frequencies. The unit of frequency is measured in cycles per second or hertz (Hz). FM radio operates from 88 megahertz to 108 megahertz. The UHF television frequencies are from 470 megahertz to 890 megahertz [1]. For 802.11b and 802.11g, the frequency range is from 2.4 gigahertz to 2.4835 gigahertz. There are 11 channels available in the United States from this frequency range.

The relationship between frequency (f), wavelength (λ) and velocity (v) is denoted by the equation $v = f \times \lambda$.

For 802.11b or 802.11g at a frequency of 2.4 gigahertz and travels at the speed of light, the wavelength is approximately equal to 12.5 centimeter (cm) or 5 inches.

Electromagnetic Wave

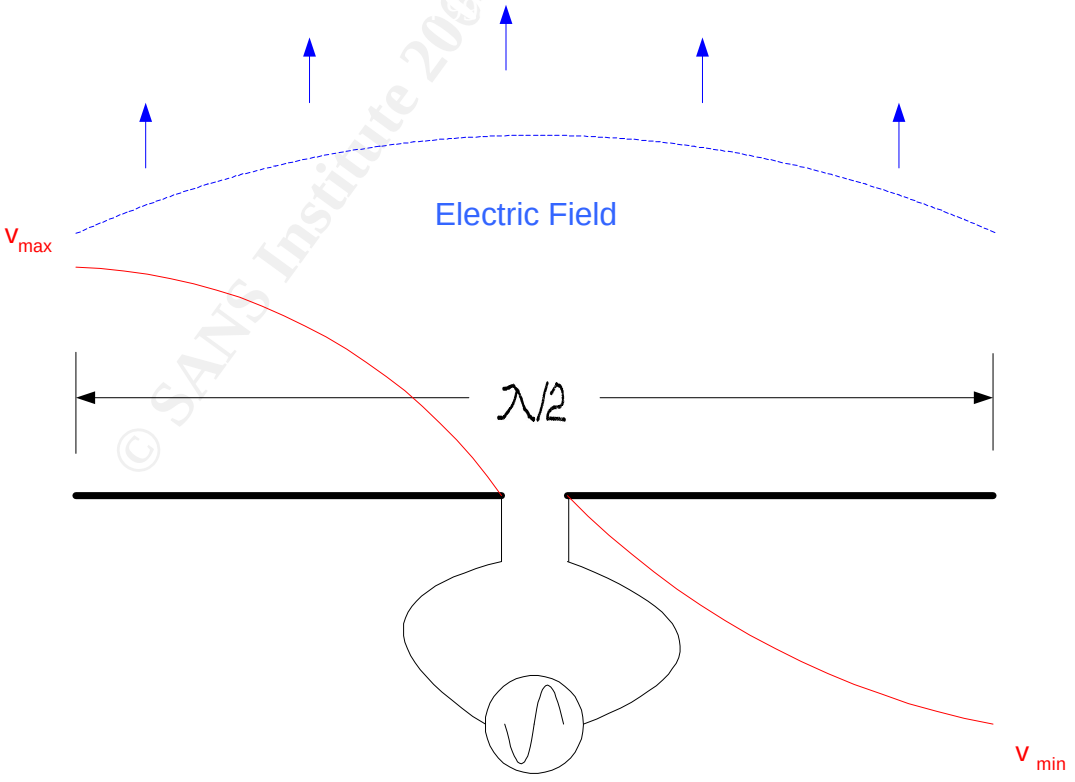
Let us investigate how electromagnet field is formed and how it is propagated away from the antenna into air. There are three basic components for radio transmission. They are transmitter, antenna and receiver. At the transmitting end, a transmitter sends electrical signals to an antenna, and the antenna converts the electrical signals to their corresponding electromagnetic wave and sends them to the air. At the receiving end, an antenna intercepts the electromagnetic waves in the air, converts them into electrical signals and sends them to the receiver for process.

When a sinusoidal voltage of frequency f is applied to dipole antenna of length l, the antenna exhibits a reactive field and radiating field. The reactive field is also called the near field because it is near to the source – the antenna. The radiating field is called the far field because it is far away from the antenna. The boundary between the near field and the far field can be approximately represented by $\lambda/(2\pi)$ [2],[4] . The reactive field becomes negligible at distances of 3 to 10 λ. It is the far field carries the energy generated

from the source in the form of electromagnetic wave and propagates into the air. The amount of electromagnetic energy radiated into the air depends on the current magnitude, frequency and the length of the antenna.

A dipole antenna is chosen for analysis in this case. Resonant frequency for a dipole antenna is about λ/2 [2]. Refer to figure 1, when we feed a voltage with a frequency of wavelength λ to a dipole antenna with physical length of λ/2, at some point of time, voltage will reach its maximum level between the end points. Then it will diminish to zero and will increase again in the opposite direction until it reaches it maximum level. The cycle repeats again at a frequency of 1/λ. At any discrete time interval, an electric field will be formed in associated with the applied alternating current. Strength of the electric field is proportional to the magnitude of the applied current at that particular time interval. Current will be at its maximum when the voltage across the antenna is at its maximum. Electric field diminishes to zero when the current is at zero. The electric field generated at time interval t1 will be pushed away from the antenna by the electric field generated at time interval at t1+Δt, or t2. The electric field generated at time t2 will be pushed away from the antenna at time interval t2+Δt, or t3. As this process keeps going, a continuous electrical field will be formed and will propagate into the air space. At a distance greater than one λ, this field is in the form of spherical waves. At larger distances, the field is in the form of traveling plane waves [2].

Figure 1. Dipole Antenna



For every electric field, there is an accompany magnetic field and is perpendicular to the electric field. The electric field and the magnetic field combine and form an electromagnetic field. This electromagnetic field travels in the direction perpendicular to both the electric field and the magnetic field. A series of these electromagnet fields is called electromagnetic wave.

The shape of the electromagnetic wave depends on the type of antenna. A quarter wavelength dipole antenna has a horizon (Azimuth) and elevation radiation patterns as shown in figure 2. There is nothing below the Y-axis on the elevation plot because of the effect of the ground plane. In this case, the elevation plot represents the electric field and the Azimuth plot represents the magnetic field. Since the electric field is perpendicular to the earth, it is vertical polarized. If we rotate the antenna 90 degrees, the electric field will be parallel to the earth, and the electric field will exhibit horizontal polarization.

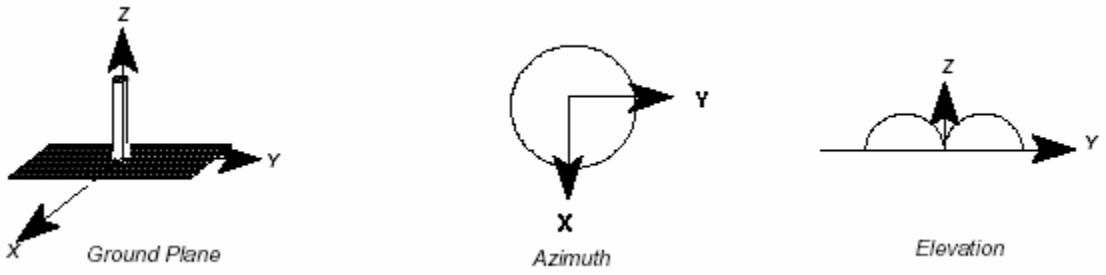


Figure 2 [3]

Notice that the electric field is radiating at 360 degrees away from the antenna. This is called an Omni-directional radiation pattern.

Another common antenna type is Yagi. Referring to figure 3, it consists of a dipole element where signal will be fed, several shorter front elements called directors, and a longer back element called reflector. The Yagi antenna has radiated wave mostly in the front. The radiation pattern resembles a slant rain-drop with the heavy end away from the antenna. Since the radiated wave concentrates in a certain direction, it is called a directional antenna.

There is non-existent, theoretical antenna called isotropic radiator. It radiates equally well in all directions with 100 percent efficiency. It is used as a reference point for antenna gain, and is expressed as dBi.

A quarter wavelength dipole antenna is also used as a reference point for antenna gain, and is expressed as dBd. One dBd is equal to 2.14 dBi.

An antenna radiation pattern represents a 3-dimensional region where the radio wave. Unit of measurement for signal strength used in 802.11 is dBm. 0dbm denotes 1 milliwatt or 1mW. 10dBm denotes 10mw, and 100dBm denotes 100mw. If we do the mathematic in the other direction, we can establish the relationship between –dBm and signal strength in mW as shown in table 1. Most of the NIC can transmit at a maximum of 100 mW, and can receive at a signal strength of no lower than –96dBm. The formula for calculating the power in decibel (dB) with reference to 1 milliwatt is:

$$P_{dBm} = 10 \log (\text{Power in milliwatts} / 1 \text{ milliwatt})$$

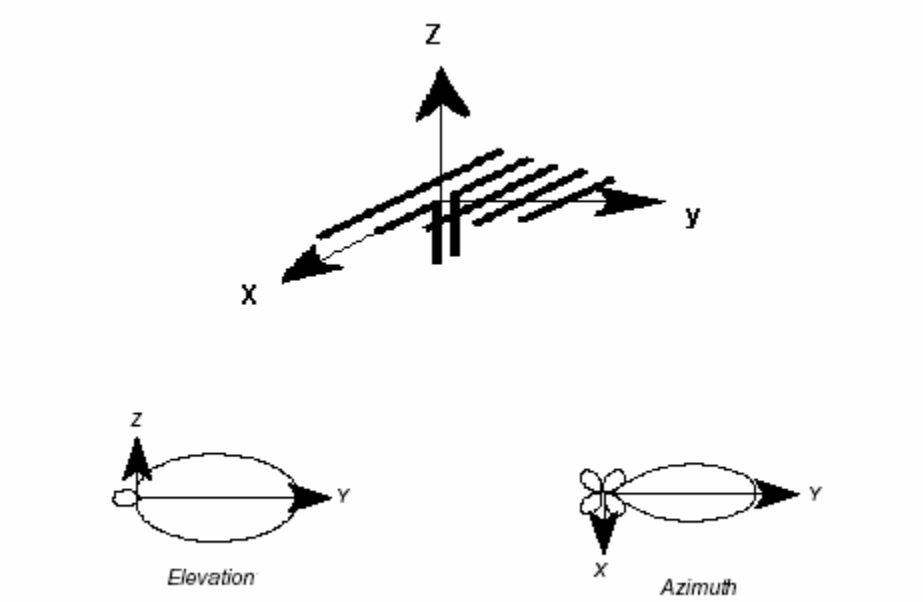


Figure 3 – Yagi Antenna [3]

-0dBm	1 milliwatt
-10dBm	0.1 milliwatt
-20dBm	0.01 milliwatt
-30dBm	0.001 milliwatt
-40dBm	0.0001 milliwatt
-50dBm	0.00001 milliwatt
-60dBm	0.000001 milliwatt
-70dBm	0.0000001 milliwatt
-80dBm	0.00000001 milliwatt
-90dbm	0.000000001 milliwatt
-96dBm	0.0000000002511 milliwatt

Table 1

Conventional Land Local Area Network

In a wired local area network environment, a category 5 or category 6 cable is used to connect a computer to the network. Each cable has 8 conductors, but only 4 conductors are used to transmit and receive data. In an Ethernet environment, a computer can operate on half duplex mode or full duplex mode. Half duplex mode means a computer can either transmit or receive at one time; whereas, full duplex mode means a computer can transmit and receive at the same time. Voltage or current running on the cable is used to carry information from one computer to another computer. The speed of electronics running in the wire is close to the speed of light. Sometimes it is not feasible or not economical to run cables from one location to another location. In this scenario, radio wave technology is one of the options.

Wireless Local Area Network

A key component of the wireless local area network is an access point (AP). An AP for 802.11b and/or 802.11g has a transmitter, a receiver and an antenna. Transmitter and receiver are also referred to as transceiver. An AP usually has two interfaces. One layer-two Ethernet interface for connection to the conventional wired LAN segment, and one layer-one radio frequency interface. This layer one interface replaces the function of a category 5 cables.

If a desk top computer or lap-top computer is equipped with WLAN, it has a built-in wireless adapter or a PCMCIA wireless LAN module.

At the sending end, electronic data is converted to binary electrical format and transmit to the air via an antenna in the form of electromagnetic wave. At the receiving end,

electromagnetic energy is received by the antenna and is converted to electrical signal. This electrical signal is then translated to binary data for processing.

When deploying a WLAN, a physical site survey is a must. Radio coverage from an AP in a confined office area is much smaller and different than that of in an open garage type environment.

Physical site survey includes the following:

- Dimension of the area to be covered - Remember 300 feet may not be the maximum distance between the AP and the client PC.
- Materials of the boundary – Check if there are any concrete wall or wall-to-ceiling metallic panel in the way. Those will block radio waves.
- Large size of furniture – Radio wave tends to go around object which is smaller than it wavelength. If the size of the object is much larger than the wavelength, the radio wave will be absorbed or bounced off or both by the object.
- Location for AP – Check all areas that offer easy access to the LAN and have least obstacles to all possible remote wireless client access points. These are the possible locations for the AP. Usually AP will be mounted in the ceiling for better coverage.
- Other 802.11 WLANs – Make sure there is no other unplanned WLAN operating in the same area.
- Other possible interference sources – Check for other electronic devices operating in the nearby frequency range. Relocate or remove those interference sources.

After the physical site survey, you should have a possible location or locations for your AP. You need to select the type of antenna for your AP. It will be based on the geographic location of the AP in relation to the area to be covered. If the AP is in the middle, an omni-directional antenna may be used. If the AP is at a corner, a directional antenna may be considered.

Finally, an on site radio survey should be conducted to determine the following:

- Mounting point of the AP antenna
- Power output of the AP
- Type of the antenna for the AP
- Orientation of the AP antenna
- Gain of the AP antenna

From the radio survey, you should create a radio coverage map for the site. Pay close attention to the signal strength at the perimeter. The signal strength at the perimeter should be kept to a minimum such that no excessive signal will leak out. If too much signal is found at the perimeter, you can trim it down by lower the power output of the AP, antenna gain, or change the orientation of the antenna. If you are on the upper floor of a high-rise building, you need to consider the distance of buildings next to yours when calculating the signal strength by the windows or by the outside walls. Keep this in mind,

power level drops approximately in half as the distance doubles; concrete wall can block, absorb or reflect radio waves. It is also important to consider the vertical space as far as the horizontal space when you are in the middle floor of a multi-story building if the floor structure is not concrete.

A WLAN client may experience an interesting situation where he has a very strong receiving signal at one location but has very little or none just a few feet away. To understand why this could happen, we need to learn some of the behaviors of radio waves. Radio waves follow the laws of physics. Radio waves reflect, refract and diffract when traveling in air. Reflection occurs when radio waves encounter an object and bounce off. The dimension of the object should be multiple factor of the wavelength. In the WLAN environment, the length of the object must be at least one foot – about 2 x the wavelength (5 inches). Refraction occurs when radio waves travel from one medium to another medium and change its direction. For example, when radio waves travel through a glass of window or a thin office panel. Diffraction occurs when radio waves bend or go around an object in its path as it travel. The size of the object must be smaller than the wavelength. As radio waves reflect, refract or diffract, it will lose some of the energy due to absorption by the objects it encounter. Depending on the nature of the object, some objects absorb little energy while other objects absorb a lot or even all energy. The degree of absorption is proportional to the thickness, the size, and material compositions of the object. If the dimension and the thickness of the object are each greater than several wavelengths, it will absorb a lot of the radio waves' energy. This explains why radio waves can penetrate thin office partition panels but not thick boxes filled with papers. To answer the question in the beginning of this paragraph, the second location for the wireless client may be behind a metal file cabinet or where signal cancellation occurred due to reflection.

Now, we know how to control the radio power strength in the air by controlling power output of the transmitter, radiation pattern and antenna gain. And we also know the characteristics of radio waves, techniques for physical site survey and radio coverage survey. With all of these knowledge, we can minimize the risk of intrusion by consider the following:

- Keep the signal strength to a minimum near the perimeter by manipulating the transmit power, antenna gain and radiation pattern – This sometimes can hide your AP from being detected by "wardriving", and some low budget hacker who can not afford more expensive equipment.
- Make use of walls as shields to radio signal for being leak out – Exterior walls of a building or perimeter concrete walls on the ground can block radio waves; however, they also reflect radio waves. A throughout radio survey should be taken if radio coverage is required.
- Lower the receiver sensitivity of the AP such that it will not pick up enough radio signal from regular computers outside the coverage area – This will prevent your AP from communicating with unwanted parties outside the planned coverage area.

- Block transmit and receive paths from and to the AP in the direction where there is no planned users – This will narrow the area to be protected. Sometimes this is very difficult to achieve because the difficulty and cost involved in adjusting the radiation pattern.

Transmission Technology

Modulation and spread spectrum technologies are the key components that make WLAN possible. There are basically two types of modulation technique which are amplitude modulation and frequency modulation. There are also two spread spectrum systems which are direct sequence spread spectrum (DSSS) and frequency hopping spread spectrum (FHSS). Frequency modulation includes binary phase shift keying (BPSK), quadrature phase shift keying (QPSK), complementary code keying (CCK). Amplitude modulation only uses multi-level quadrature amplitude modulation (QAM). Orthogonal frequency division multiplexing (OFDM) is a technique which makes use of AM, FM and spread spectrum technologies.

Among the two technologies, spread spectrum has inherent security. Since DSSS is widely used by 802.11b than FHSS. We will examine DSSS.

In a DSSS system, a pseudo-noise (PN) code, at a higher speed than the signal, is used to modulate the information signal. In the Cisco 802.11b system, BPSK is used for 1 mbps, QPSK is used for 2 mbps, and CCK is used for 5 and 11 mbps data rate {page 2-18 of [9]}. The effect of this modulation technique is to spread the bandwidth of the original signal. The multiplication factor depends on the rate of the PN code - it is called the chip rate. The higher the chip rate, the wider the bandwidth. In the frequency domain, this makes the signal appears as noise. Then, the PN modulated signal is multiplied with the radio frequency carrier before it is transmitted in the air. At the receiver, A reverse process using the same PN code is required to recover the original signal.

Some of the characteristics of DSSS are low probability of intercept and anti-jam [13].

Some of the benefits of using PN codes are lower interference, high signal to noise ratio and privacy [11].

In 802.11b using DSSS, PN code is fixed and known to everyone. Therefore the inherent security feature offered by PN codes is not used. One of the reasons is to sacrifice security for error correction automation. However, DSSS is already more immune to interference and noise, and provides higher signal to noise ratio. Therefore error correction automation is not necessary.

An algorithm similar to the Private Key Infrastructure (PKI) with Diffie Hellman should be developed for selecting the PN code for the AP and the wireless clients. Imagine this

scenario, an 802.11b AP operating on channel one (2.412Ghz) is communicating with a client. After establishing a radio connection with the client, the AP sends a request to the client for identification. The client will send an encrypted user name with password to the AP. The AP will pass the encrypted user name and password to an authentication control server (ACS). It could be a Cisco TACACS, a RADIUS server or a Kerberos server. If the user name and/or password are/is not invalid, the ACS will acknowledge the AP. The AP will then disconnect the session. If the authentication is valid, the AP will start a Diffie Hellman alike algorithm with the client. A secret key will be generated at the AP and the client via an unsecured radio channel. Both the AP and the client will use the same secret key to generate the PN code for use in DSSS. The AP should renegotiate the secret key for the PN code at a predefined time interval.

If an algorithm as described in the previous paragraph exists, an intruder would not be even able to decipher the PN code, and as a result it will not be able to communicate with the AP. This mechanism will fortify the security on the physical layer. Of course it may take a developer a considerable period of time to develop an algorithm like this.

CONCLUSION

Wireless network security builds on all seven layers of the OSI model. Physical layer is the first layer of the seven layers. It is the first layer of defense. A strong first layer is very crucial to network security. The first layer is analogous to the gate of a fortress. Once the gate is open, everything inside the fortress is vulnerable to the attackers. Controlling this gate is not an easy task. You need to know when to open for your friends and when to close it to keep your enemies out. Protecting the first layer, the radio wave, in the wireless world is very different from the wired network. In the wired network, your can restrict physical access to the switches and the routers and the 802.3 Ethernet jacks from strangers. In the wireless network, however, signals are in the free air space. Anyone with a 802.11b or 802.11g transceiver can pick up the signals. It is also very difficult or even impossible to elect a physical barrier to enclose the radio signals.

Through my research in preparing this paper, I have built a solid understanding of the physical layer for wireless local area network. I hope this paper can provide basic information and references resources to those who would like to explore the wireless local area network security arena.

REFERENCES

[1] URL: http://www.csgnetwork.com/tvfreqtable.html

[2] Ron Schmitt, Sensor Research and Development Corp. EDN March 2, 2000
URL: http://www.reed-electronics.com/ednmag/article/CA82250?text=understanding+electromagnetic+fields+and+antenna+radiation&stt=000

[3] URL: http://www.tscm.com/radiapat.pdf

[4] URL: http://www.tmeg.com/tutorials/antennas/antennas.htm

[5] URL: http://www.gigaant.com/antennabasics/basicknowhow/whatantenna.asp

[6] URL: http://www.umich.edu/~navyrotc/NS202/EnergyFundamentals.ppt

[7] URL: http://hyperphysics.phy-astr.gsu.edu/hbase/waves/emwavecon.html#c1

[8] URL: http://www.qsl.net/n9zia/wireless/dsss.html

[9] Aironet Wireless LAN Fundamentals, Volume 1, Version 3.1, Cisco System Inc., 2003.

[10] URL: http://www.astronantennas.com/radiation_patterns.html

[11] URL: http://www.commsdesign.com/showArticle.jhtml?articleID=16501183

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor