GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Janik, Michael J.
GSEC Practical Assignment Version 1.2f
Title: A Government Encryption Standard

The technology of encryption goes back thousands of years, with traces of it evident in Egyptian times. However, encryption has come a long way in the past few decades. Once a technology reserved for the military, espionage, and plotlines for movies, it has now entered the world of e-commerce and everyday business practices.

As with any technology that benefits law-abiding citizens and organizations, encryption also has the capability to benefit criminals and terrorists alike. Many don't know of the silent war that has been waged over the past few decades concerning encryption and encryption standards. In today's world, with the explosion of e-commerce and business through computers, encryption isn't just a byline for movies, it is a crucial part to the overall integrity of business operations. Because of this new need, it is essential to have a government regulated encryption standard to assist law enforcement and intelligence communities in their duties.

There are many arguments against the development of a perceived "Big Brother" approach. The United States was built around the premise of individual rights with government assistance versus individual rights with government control. This paper aims at dispelling those arguments. The next four sections will show the importance of having a government-regulated encryption standard in place.

The first section is aimed at giving a general overview and history of encryption. This section will be followed by two sections which explain the importance of a standard. The last section will cover some Constitutionality issues and other arguments that have been raised concerning encryption standards.

Encryption Overview

Throughout history, encryption has played an increasing role of importance in events. Traces of the technology itself can be seen in ancient Egypt. "Khan dates the recorded history of cryptology to about 1900 BC and an inscription carved in the tomb of the Egyptian nobleman Khnumhotep II, in which the writing is in places deliberately transformed by the use of some unusual hieroglyphs in place of the more ordinary ones." [1] It has also been seen in the times of Caesar. The encryption utilized by Caesar and in Egyptian times was very simplistic and could easily be broken. More recently, encryption played a pivotal role in World War II. It is difficult to imagine how the war would have turned out had the Allies never been able to break the German codes such as the Enigma or if the Axis powers had been able to compromise the Navajo coderunners that the Allies used.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

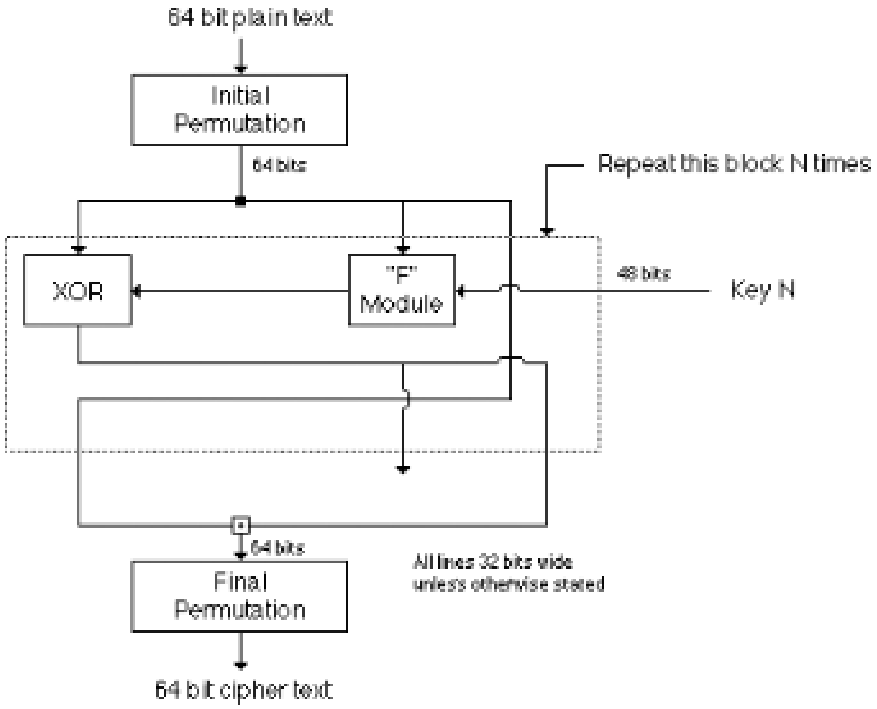
Many people don't know exactly how encryption itself works. In many cases the average user may not even realize that they are running an encrypted system. There are two main Encryption systems; asymmetric and symmetric.

> "Asymmetric key-based algorithms. This method uses one key to encrypt the data and a different key to decrypt the same data. You have heard of this technique; it is sometimes called public key/private key encryption, or something to that effect.
> Symmetric key – based algorithms, or block-and-stream ciphers. Using these cipher types, your data is separated into chunks, and those chunks are encrypted and decrypted based on a specific key." [2]

In other words, asymmetric key-based algorithms rely on two keys for the encryption/decryption process. The public key that is available to anyone is utilized to encrypt the data. Once the data are encrypted only the private key will be able to decrypt the data. As a result a user can publish their public key to anyone they choose while keeping the private key safe. This system operates much in the same way as a mailbox. Anyone can put letters into the mailbox but they can't see any of the other letters inside. Only the postal employee (with the "private" key) can open up the mailbox and retrieve what's inside. Symmetric key-based algorithms are less secure in that the same key is used to encrypt and decrypt the data. Regarding the mailbox example, its contents are open to anyone who has access to it.

Obviously, asymmetric key-based algorithms are the preferred and more secure of the two systems. The following diagram depicts how the algorithm for Data Encryption Standard (DES) works.

"The Algorithm



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

DES Block Diagram

Fundamentally DES performs only two operations on its input, bit shifting, and bit substitution. The key controls exactly how this process works. By doing these operations repeatedly and in a non-linear manner you end up with a result which can not be used to retrieve the original without the key. Those familiar with chaos theory should see a great deal of similarity to what DES does. By applying relatively simple operations repeatedly a system can achieve a state of near total randomness.

DES works on 64 bits of data at a time. Each 64 bits of data is iterated on from 1 to 16 times (16 is the DES standard). For each iteration a 48 bit subset of the 56 bit key is fed into the encryption block represented by the dashed rectangle above. Decryption is the inverse of the encryption process. The "F" module shown in the diagram is the heart of DES. It actually consists of several different transforms and non-linear substitutions. "[3]

The important issue to remember with encryption is that like any other security measure, it can be compromised given enough time and resources. "The trick here is to find mathematical problems of sufficient complexity to ensure it would take an inordinate amount of time – not to mention effort – to use the public key to figure out the private one".[4] The goal is to make compromising an encryption algorithm a task not worth considering. Another important issue is with technology: the world is constantly finding ways to make a better mousetrap. The three number shifting utilized by Caesar would be ridiculous to use in today's world even though it was sufficient at the time. The issue of whether or not an encryption algorithm can eventually be compromised is not the same as the issue of whether or not there should be a standard.

Overview of Encryption Standard

Before getting into the importance of an encryption standard it is imperative to have an understanding of what an encryption standard attempts to accomplish. It is much as it sounds, a standard algorithm for encryption. The government's goal is two-fold. First, the government proposes one encryption algorithm that will be used by everyone. In this case, the algorithm is the result of strenuous contests between different participants. The U.S. government is not stringent with its own plan for an encryption standard. It is willing to work with industry to achieve a compromise. "FBI are engaged in continuing discussions with industry in a number of different fora. These ongoing, productive discussions seek to find creative solutions, in addition to key recovery, to the dual needs for strong encryption to protect privacy and plaintext recovery to protect public safety and business needs." [5]

The second aspect of the goal is to have a key-recovery system in place for the standard. "To protect the confidentiality of the key, it will be "split," and the components will be held by two Federal escrow agents --- National Institute of Standards and Technology (NIST) and the Treasury Department's Automated Systems Division --- one at each. Both

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

components are needed to reconstruct the key. The standard authorizes keeping each chip's private key secret --- unless there is legal authorization to do otherwise. Key registration will occur during manufacturing at a secure commercial facility, and escrow officers from the two agencies will be present during the chip-programming process."[3] It is clear that with this approach in place it would be very difficult for someone to abuse their power and access both "halves" of a key.

To use an analogy of how the key-recovery system would work, imagine a world in which everyone kept all their secrets in their own little lockbox. Each lockbox would have its own key that the person could duplicate. Picture a criminal with his or her robbery plans locked in their lockbox. Although the local police could obtain a warrant to search the box, the problem becomes how to gain access to the contents. Under this scenario, the police have no information about the key other than they know that one is needed to open the box. Law officials must search and attempt to craft a key for each lockbox they wish to search; a daunting task when one imagines how many warrants are issued for searches daily.

Now imagine that everyone has these lockboxes but for each key, there's a registry that can be accessed to find the characteristics of the key. For integrity and confidentiality, half the plans for the key are kept in one location (agency/organization) while the other half are kept in another location (agency/organization). As a result, when a law enforcement agency obtains a warrant for search, it is a matter of obtaining these two plans and building their own lockbox key.

Though the above is a very elementary example, it does explain the purpose of an encryption standard. Much in the same way that the police can wiretap someone's phone, they should have the ability to monitor someone's computer transactions if they receive the proper authority to do so.

Importance of an Encryption Standard

In the argument for an encryption standard, it isn't a question of law enforcement being able to function with or without a standard in place but rather a question of whether law enforcement officials can operate effectively without an encryption standard. This concern was emphasized by Louis Freeh in a Congressional Statement before the Senate Select Committee on Intelligence concerning Threats to U.S. National Security. In his opening statements, Mr. Freeh states the following:

> "The overriding concern now facing law enforcement is how rapidly the threats from terrorists and criminals are changing, particularly in terms of technology, and the resulting challenge to law enforcement's ability to keep pace with those who wish to do harm to our nation and our nation's citizens. This is why the encryption issue is one of the most important issues confronting law enforcement and potentially has catastrophic implications for our ability to combat every threat to national security that I am about to address in my statement here today. Law enforcement

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

> remains in unanimous agreement that the widespread use of robust non-recovery encryption ultimately will devastate our ability to fight crime and terrorism. Uncrackable encryption is now and will continue, with ever increasing regularity, allow drug lords, terrorists and even violent gangs to communicate about their criminal intentions with impunity and to maintain electronically stored evidence of their crimes impervious to lawful search and seizure. Other than some type of key-recoverable system, there is currently no viable technical solution to this problem for law enforcement." [6]

Freeh continues to emphasize that this isn't just a threat in the foreseeable future but rather a threat that is here now:

> "This is not a problem that will begin sometime in the future with theoretical implications. In many important investigations effective law enforcement is being frustrated by criminals and terrorists using non-recoverable encryption. For example:
>
> - Convicted spy Aldrich Ames was told by his Soviet handlers to encrypt computer file information that was to be passed to them.
> - Ramzi Yousef and other international terrorists were plotting to blow up 11 U.S.-owned commercial airliners in the far east. Yousef's laptop computer, which was seized in Manila, contained encrypted files concerning this terrorist plot.
> - A major international drug trafficking subject recently used a telephone encryption device to frustrate court-approved electronic surveillance." [6]

One of the main supports for the use of an encryption standard is its value as an evidence gathering tool. Evidence is the make-or-break of all cases. To prove someone guilty, evidence must be present. Before computers, wiretaps and surveillance have proven to be crucial in most criminal cases. Title III of the Omnibus Crime Control and Safe Streets Act designated the use of wiretapping only if probable cause showed that a communications device was being used in conjunction with the crime. An encryption standard isn't a matter of the government having complete control over its citizens. If the United States were the "Big Brother" that many in our society believe, the debate over encryption would not even exist. What is at stake is the effectiveness of the law enforcement community. Building cases is an uphill battle. The defendant has his or her constitutional rights protecting them at every turn. An encryption standard compliments what wiretapping and surveillance accomplish. It provides the law enforcement community with a way to do a nearly impossible job. For all purposes an encryption standard provides a facet for law enforcement to perform their wiretapping and surveillance. An encryption standard needs to be taken for what it is, a tool to assist law enforcement in wiretapping and surveillance. The guidelines for the use of an encryption standard are already spelled out in Title III.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Another reason for having an encryption standard is the trend of criminals to use advanced technology. As stated by Freeh, "Many traditional and non-traditional adversaries today are technologically sophisticated and have modified their intelligence methodologies to use advanced technologies to commit espionage. In telecommunications, even some smaller intelligence adversaries now use equipment the FBI is unable to monitor."[6] In the last two years (96-98) "the FBI has also seen the number of computer-related cases utilizing encryption and/or password protection increase from two (2) percent to seven (7) percent…" [6] Criminals will use whatever means necessary to hide their actions. Freeh's findings already show the difficult task of law enforcement. The Honorable John D. Dingell, who is by no means a full supporter, states that an encryption standard may not be the only solution but it is the best solution at the present. Dingell states, "Removing all government controls over encryption is tantamount to sending our troops to war without necessary arms or protective gear… The American public has no assurance that a technology lab will be effective in providing law enforcement with the tools necessary to protect them. Without possessing a key to encrypted messages, the only way to unlock the door is through brute force. A brute force attack on today's encryption products requires both enormous computing power and a good deal of time. Law enforcement authorities possess neither luxury when confronted with an imminent, real-time threat to public safety. A technology lab will not change that reality. Some producers of encryption products have offered informally to provide the lab with technical assistance and perhaps some amount of private funding. But we have no specific commitment with regard to either offer, nor can we be sure that any such contribution would be sufficient to achieve the lab's purpose. The industry has specifically rejected the notion of providing source code for its encryption products to the lab, which is arguably the best hope for giving law enforcement a leg up on cracking these codes without a key."[7]

Arguments against an Encryption Standard

Given the different reasons an encryption standard is needed, it is also important to recognize some of the counter arguments against a standard. The most important argument against an encryption standard is that it is unconstitutional. Most critics holding this position site violations of either the first or fourth amendments. Concerning first amendment violations, critics argue that by mandating what encryption algorithm people may use, the government is in effect mandating or controlling their speech. This interpretation is stated clearly in a law professors' letter regarding SAFE Amendments (SAFE is the Security and Freedom through Encryption Act):

> "The amendment raises profound questions about rights of free speech. The right to speak freely includes not only the right to say what you want, to whom you want. It also includes the right to choose how to speak, and whether to speak at all. The right has no preconditions. In America, at least, you do not need a license to speak; you do not need the government's permission to speak in the language of your choice; and you do not have to organize your speaking in a way that happens to suit the needs of the government. The Constitution no more permits Congress the power to regulate the software within which speech may occur than it give

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

> Congress the power to say what kind of paper a diary may be written upon. These are choices rightly left to the individual.
>
> The amendment would undermine these constitutional rights to free speech. By imposing requirements on cryptographic programs - used by individuals and corporations to protect the privacy and security of their papers and telephone or e-mail conversations - it would in effect be mandating the code software writers may write. Only governmentally approved code could be used to transmit speech the speaker wants to protect; authors and speakers would be required to use this code to say what they wanted to say. This forced speech, we believe, takes the government's power too far. " [8]

It can be effectively argued that freedom of speech is not being violated with an encryption standard. Encryption is a way of conveying a message rather than the actual substance in the message. Proposals by the government explained above require the police to show probable cause to even access the keys. If critics are using this argument against encryption standards, the same argument goes against any kind of evidence gathering and surveillance tactic used today.

Another argument against an encryption standard is that a U.S. citizen's fourth amendment right protects people from unreasonable search and seizure. Critics argue that this right would be violated based on what the scope of evidence gathering through encryption would be.

> "Under the Fourth Amendment, the police can conduct a search after they present probable cause to a judge that a crime is being committed. The amendment does not require that all persons leave a copy of their house keys at the police station before any crime is suspected. Under the constitution, personal privacy is not entrusted to the police or military and then doled back to the public by a balance determined in back rooms.
>
> In any event, the key escrow mechanism does not provide any real insurance that it will prevent government abuse. The key escrow procedures exempt any legal repercussions for their violations with the following disclaimer: "These procedures do not create, and are not intended to create, any substantive rights for individuals intercepted through electronic surveillance, and noncompliance with these procedures shall not provide the basis for any motion to suppress or other objection to the introduction of electronic surveillance evidence lawfully acquired."[9]

This interpretation ties in with first amendment violations in that people's privacy would be violated based on what is deemed to be abuse of power. This argument has nothing to do with the merits of an encryption standard but more to do with surveillance and investigations as a whole. An encryption standard doesn't mandate what evidence will be

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

gathered, it simply is a tool for gathering that evidence. Instead of wasting taxpayer money and time cracking each encryption algorithm, law enforcement would be able to access the keys after they obtain a warrant. Individual rights dealing with privacy and illegal searches and seizures need to be protected whether or not an encryption standard is in place.

Another argument against an encryption standard is that it is faulty. A mandated encryption standard makes it that much easier for that standard to be compromised. This flaw has been proven time and time again as teams have broken different standard encryptions. No matter what safeguards one comes up with to deter a thief, someone is going to eventually compromise that safeguard. As with any technology, there will be faults and eventually the technology or algorithm will be proven obsolete. The same is true with an encryption standard. However, the reason a particular standard will prevail is that there is intense competition among standards. Only the strongest, most unbreakable algorithm will survive. The following is a quote from a Peter Wayner Article concerning the encryption standard competition held in 1999 to decide which encryption standard was to be endorsed by the Government:

> "The competition will grow more intense as the teams prepare for a final conference in March. The National Institute of Standards and Technology will choose the winner next summer. Bruce Schneier, the lead designer of Twofish and the president of Counterpane Systems, a software company based in Minneapolis, said: "This fall the Twofish team is having a one-week retreat. We're going to analyze ciphers. We're going to try to break these things."
>
> None of the finalists have any glaring weaknesses, which means that the teams are also trying to one-up each other by comparing their proposals' efficiency and adaptability."[10]

Finally, many argue that with all the other encryption systems and algorithms that exist, the formal encryption standard would only be utilized by law abiding citizens and corporations while illegitimate individuals and corporations would continue to use other non-breakable encryption systems. Among other things, the worry here is that the U.S. can't control the encryption market forever. As stated by Jeffrey Smith in a Report For Americans for Computer Privacy in 1999, "Encryption algorithms are nothing but sophisticated mathematics…And while the United States may realistically hope to remain the leader in such a field, it cannot realistically expect to monopolize it…If we do lose that U.S. leadership position, what will that mean? It will mean that the national security agencies will be confronting ubiquitous encryption made not by U.S. companies, but by foreign companies. Where then will the national security agencies go for technical help on encryption?" [11] By utilizing an encryption standard, law enforcement is under no illusion of obstacles they may face through criminal or foreign development of

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

encryption algorithms. The United States cannot control all of the development that takes place. By utilizing an encryption standard, law enforcement is taking the best possible approach. It would be better to be able to simply access a key for a portion of the data obtained through a search warrant than having to attempt a brute-force attack on all of the data obtained. Furthermore, foreign intelligence has found that many intelligence adversaries utilize legitimate channels to conduct their business. This is supported through a press release from the Whitehouse Office of the Press Secretary entitled "A National Security Strategy for a New Century". It states, "We must be concerned about efforts by non-state actors, including legitimate organizations, both quasi-governmental and private, and illicit international criminal organizations, to penetrate and subvert government institutions or critical sectors of our economy."[12]

Conclusion

The past three months have tested the United States. There have been many events that have raised questions of government control and involvement. It is important in these times to remember what truly makes this country what it is. Overall, the United States is built on the rights and freedom of the individual. Those rights and freedoms need to be protected at all costs. In preserving these rights and freedoms, law enforcement needs to be given tools to enable it to do its job. At the same time, law enforcement must be kept in check to insure that it is not abusing its use of these tools.

An encryption standard is necessary for law enforcement to do its job. The general movement of the criminal element toward utilizing technology proves that encryption is an area in need of some government control in order to ensure the rights and freedoms of the individual. An encryption standard in place is an element of government control. This control does not infringe on one's Constitutional right as there are still checks to ensure that the tool is not abused. Furthermore, the tool itself will be the most powerful tool at the present time.

Ultimately, an encryption standard may be proven obsolete. Twenty years in the future, technology may have progressed so that it is possible for law enforcement to crack "uncrackable" codes. For the time being, an encryption standard is the best possible tool for law enforcement to do its job in this area.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] George McMurdo, "Pretty Good Encryption", http://jimmy.gmuc.ac.ud/jisew/ewv22n2/

[2] Julie Meloni, "Encryption Tutorial Overview", http://hotwired.lycos.com/webmonkey/programming/php/tutorials/tutorial1.html

[3] Peter Costa, Ryan Nation, "Standards & Specifications: Key Materials on the US Digital Signature Standard", April 29, 1998, http://www.biz.uiowa.edu/class/6k180_park/Student-Reports/rnation/Standards.htm

[4] Will Knight, "Stealth Message: Encryption – A Brief Overview", http://www.stealthmessage.com/s/home/encryption.cfm

[5] "Testimony of Ronald D. Lee Associate Deputy Attorney General", March 4, 1999, http://www.usdoj.gov/criminal/cybercrime/leesti.htm

[6] "Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Threats to U.S. National Security", January 28, 1998, http://www.fbi.gov/congress/congress98/threats.htm

[7] John D. Dingell, "H.R. 695, The Security and Freedom Through Encryption (SAFE) Act", http://www.house.gov/commerce_democrats/comdem/legviews/mv05695.htm

[8] CDT, "Law Professors Letter Regarding SAFE Amendments", September 23, 1997, http://www.cdt.org/crypto/legis_105/SAFE/970923_profs.html

[9] David Banisar, Ken Robinson, "Security and Privacy on the Information Highway: Point/Counterpoint", http://www.educause.edu/pub/er/review/reviewArticles/29536.html

[10] Peter Wayner, "Encryption Teams Circle, Firing Away", September 9, 1999, http://www.nytimes.com/library/tech/99/09/circuits/articles/09next.html

[11] Americans for Computer Privacy, "ACP Seeks Support for SAFE Act in Testimony Before House Subcommittee", May 18, 1999, http://www.computerprivacy.org/news/927051821.shtml

[12] The Whitehouse, "A National Security Strategy for a New Century", December 1999, http://www.dtic.mil/doctrine/jel/other_pubs/nssr99.pdf

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: July 22nd, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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 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
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 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 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 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
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
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor