Global Information Assurance Certification Paper

How To Keep Your Email Messages Private Through Encryption

By:

Adelina Ortega

GSEC Version 1.4 b

26 November 2002

Table of Contents

Table of Contents.....i
1.0 Abstract.....1
2.0 Introduction.....1
2.1 Email Security.....1
3.0 What Is Encryption?.....2
4.0 How Encryption Works.....3
4.1 Symmetric Encryption.....4
4.2 Asymmetric Encryption.....5
5.0 Using Encryption.....6
6.0 Encryption Tools and Software.....6
6.1 File Encryption.....6
6.2 Email Encryption.....7
6.2.1 Pretty Good Privacy (PGP).....8
6.2.2 HUSHMAIL.....9
7.0 Summary.....10
APPENDIX A: References.....A-1

1.0 Abstract

This paper will discuss the issue of electronic mail security and the use of encryption as a method of keeping messages private and secure. This paper will also discuss possible solutions on encryption as a data security solution and focus on the application of encryption concepts to the individual and business environment.

2.0 Introduction

Electronic mail, also known as email, is quickly becoming one of the most widely used forms of communications for individuals and businesses alike and accounts for the single largest use of the Internet. Whether for business or recreational use, individuals have come to rely on email as an effective and indispensable means of sending and receiving messages and data. Additionally, the ease and low cost of email continues to fuel its growth as a means of communication.

However, there are concerns regarding privacy and security of data – a concern borne out of the fact that the transmission of email messages and data is susceptible to interception and interpretation by unwanted recipients. In other words, without safeguards, an individual has no level of confidence that his or her email will not be intercepted. Consequently, how does one protect the privacy and ensure the security of messages and data transmitted over the Internet?

In the following sections of this paper, the follow points are discussed:

Section 2.1 is an introductory section dealing with email security
Section 3 deals specifically with what encryption is and how it is used
Section 4 discusses how encryption works
Section 5 discusses the use of encryption
Section 6 provides a few examples of several encryption tools and software and provides a summary of each
Section 7 contains a summary
Appendix A contains references used to prepare this document

2.1 Email Security

Email has become an important communication tool within the business community because the Internet has made it relatively easy to use; it is universally accepted and it serves as a low cost, efficient and effective means of sharing information. According to UC Berkeley's Education Department, the increasing reliance on email is evidenced by the fact that "today's users send about 15 messages a day and receive about 20 a day on average. This volume

is expected to grow by 60% and 80% respectively by 2002."[1] Consequently, the increased usage and importance of email and the Internet, has raised the awareness of and need for electronic security.

For example, many Web-based business are concerned for their customers' privacy because their electronic commerce Web sites collect a great deal of personal and financial information about each customer. Additionally, these Web sites regularly issue user ID's and confirm passwords via email. This creates potential risks to customer credit ratings and bank accounts and to the Web-based company in the form of potential losses and reduced customer satisfaction.

Consequently, the use of protected electronic correspondence is very important to a Web-based business. However, this risk is not isolated to electronic commerce businesses only.

Any company sending proprietary and/or sensitive information via email has concerns for protecting trade secrets; business plans, engineering designs, customer correspondence, etc. This applies to most companies; therefore electronic security is a current and growing concern for the entire business community. Other reasons may include obligations to data protection laws that require the protection of personal, sensitive, or professional customer information. Fortunately, encryption methods have been developed to protect the security of email.

3.0 What Is Encryption?

Encryption is a way of scrambling and encoding data transmission to reduce the risk that it is read by any unauthorized party, even if the email is intercepted during transmission. Specifically, it is a process by which the original message is translated into unreadable text before transmission. Therefore, any unintended recipient during transmission will not be sensible. The intended recipient then retranslates, or decrypts, the email through the use of a key. This process makes the email fairly secure during transmission provided the sender and recipient are the only individuals with the key, and the key is such that it is not easily deciphered.

A drawback to encryption is that it can be time consuming and complicated to code and decode messages. Fortunately, faster computers have revolutionized encryption because text can be encoded and decoded at higher speeds, and

[1] "How Much Information?" UC Berkeley. 2000, URL:http://www.sims.berkeley.edu/research/projects/how-much-info/internet/emaildetails.html (18 November 2002)

many common software packages have encryption program plug-ins available, further streamlining the process.

In concept, encryption is quite simple. Data is encoded to make the data unintelligible to those except intended recipients. In practice, this can be quite complex. It is accomplished through cryptography, or the sending of messages in a secret form, so that only those authorized to receive the message will be able to read it.

Cryptographers encode messages by applying a mathematical function to plain text that converts it to encrypted cipher. Probably the most difficult part of encryption is how to ensure that senders and recipients can decipher the message, and, more importantly, those that are unauthorized do not have access to view the message. Encryption programs and judicious distribution of them can facilitate secure communications.

A key is a data string, which is combined with source data and an algorithm to produce output (cipher text) that is unreadable until decrypted. An algorithm is a complex mathematical function, and the key and the source data are inputs to the algorithm.

It was not that long ago when only governments and diplomats used encryption to secure sensitive information. Today, the Internet has grown into a vast network throughout the world consisting of individual computers and computer networks that are all interconnected by many paths.

Since the Internet is a public network and can be accessed by anyone, it is impossible to regulate or monitor every computer. With the vast amounts of information moving quickly and effectively across great distances, it is unlikely that the number of Internet transmissions will decrease. Relying on encryption to ensure the safety of data will give businesses confidence to conduct business, send messages securely, and set up secure connections over the Internet. Therefore, encryption security for Internet transmissions continues to be the key to achieving confidence in protecting privacy.

4.0 How Encryption Works

The goal to encryption is to make the data ineligible for everyone else except those specified. This can be accomplished by using cryptography. It is sending messages in a secret form so that only those authorized to receive the message will be able to read it.

The essential concept underlying all automated and computer security applications are cryptography. The two methods of cryptography are symmetric encryption and asymmetric encryption.

4.1 Symmetric Encryption

Symmetric encryption, otherwise known as single key encryption or private key, has five components:

- The plain text is the information to which an algorithm is applied.
- The encryption algorithm is the mathematical formula that outlines the substitutions and transformations to the plain text.
- The secret key is the input to the algorithm that dictates the encrypted outcome.
- The cipher text is the encrypted or scrambled message produced by applying the algorithm to plain text message using the secret key.
- The decryption algorithm is the encryption algorithm in reverse. It uses the cipher text and the secret key to reconstitute the plain text message.

When using this form of encryption, it is essential that the sender and the receiver have a way to exchange secret keys in a secure manner. If another party has the secret key and can derive the algorithm, the communications will not be secure.

There is also the need for a strong encryption algorithm. Otherwise, an unintended recipient may be able to derive the algorithm from intercepted cipher text and plain text. There are two approaches used to derive algorithms: by force and cryptanalysis.

By force uses a computer to create all possible combinations and eventually determine the plain text message. Cryptanalysis focuses on the characteristics of the algorithm and attempts to deduce a specific plain text or the key used. If a correct deduction is made, the cipher text can be decoded to recreate the plain text.

Figure 1 (below) provides an easy overview explaining the symmetric encryption process.

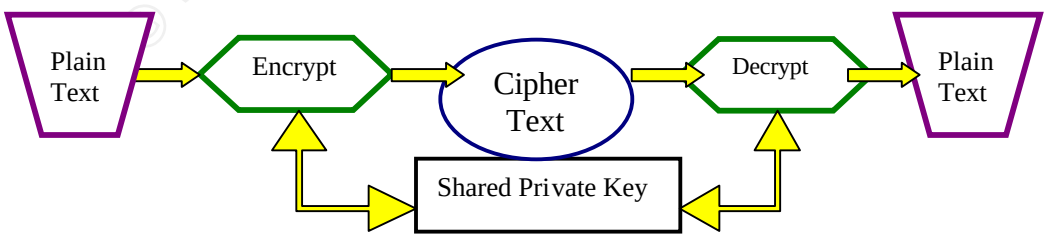


Figure 1: Symmetric encryption process

4.2 Asymmetric Encryption

Asymmetric encryption, otherwise known as public key encryption, has the following major components:

- The plain text is the text message to which an algorithm is applied.
- The encryption algorithm performs mathematical formula that outlines the substitutions and transformations to the plain text.
- The public and private keys are a pair of keys where one is used for encryption and the other for decryption.
- The cipher text is the encrypted, or scrambled, message produced by applying the algorithm to the plain text message-using key.
- The decryption algorithm is the encryption algorithm in reverse. It uses the cipher text and the matching key to reconstitute the plain text message.

Asymmetric encryption is centered on the premise of making the encryption and decryption key different, where the knowledge of one key would not implicate the other. Each encryption/decryption process requires one public key and one private key. Messages encrypted with the public key can only be decrypted with private key and vice versa.

Figure 2 (below) provides an overview explaining the Asymmetric encryption/decryption process.

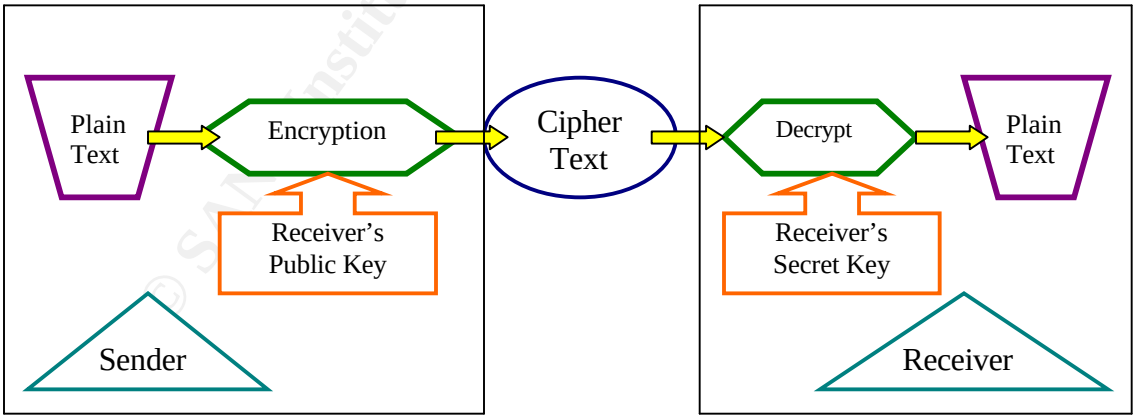


Figure 2: Asymmetric encryption/decryption process

5.0 Using Encryption

The importance of using encryption is apparent once it is understood that unencrypted email and attachments are similar to postcards in the mail. It can be read by anyone. However, encryption is not limited to only protecting email and its attachments. It can be used for a number of different purposes.

First, it can help secure the data transmitted by a computer system; second, messages sent over the Internet can be encrypted to prevent unintended reading; third, recipients can authenticate the identity of the sender by using a digital signature based around encryption; fourth, information on a computer disk can be encrypted to prevent unauthorized access; and fifth, encryption systems can be built into communication equipment, such as telephones or Web browsers, to provide encryption of information in realtime to prevent interception or eavesdropping on communications.

6.0 Encryption Tools and Software

There are hundreds of encryption products available on the market in the form of commercial software and hardware products. Identifying which encryption product is best suited for what purpose can be a challenge.

However, while some products and packages are better than others, it is highly advisable to have a basic system in place rather than no system at all. Secure messaging systems (email encryption), secure transactions (SSL enabled Web browsers), and secure connectivity (VPNs) can be acquired on a very small budget. Cost varies depending on the complexity of the system with many products that are competitively priced and some that are free.

Examples of specific security solutions include:

6.1 File Encryption

1. **FileCrypto** – FileCrypto is a software encryption solution designed by F-Secure Corporation and developed by Datafellows Corporation. This is a long-standing file encryption application that supports strong encryption. The company is headquartered in Helsinki, Finland, with a North American office in San Jose, California. It is a centrally managed solution for protecting files stored in desktops and laptops. FileCrypto stores local data securely and keeps confidential files protected by offering encryption.

2. **ShyFile** – ShyFile was developed by Consens Software. It is 6,144-bit encryption software with an added feature of allowing the recipient to

read the sender's encrypted message without having to download extra software. A user only needs to enter a 32-character key and then either enter the message text directly into the input filed or import a .txt file to encrypt the message. The software is free except for versions of a strong encryption application that allows a user to create self-executable and encrypted packages.

3. **WebCrypt Pro** – WebCrypt Pro is software designed by Moon Light Software. It allows the user to encrypt the text on his or her Web site. Anything between the <body> and </body> tags will be encrypted, while other things like meta tags are not. A free trial is available, but a $20 fee is required to keep the program.

4. **aCrypt+** – aCrypt+ is software designed by Data Rescue. It is a security tool that allows a user to email securely encrypted attachments as self-extracting executable files.

   The recipient does not need any software to decrypt the package, only the sender does. To encrypt a message, the sender drags and drops the file or directory structure intended for the recipient into aCrypt+. The sender then enters a password known by the recipient and drops the self-extracting archive into an email message.

   Other ways to use aCrypt+ include browsing to the file(s) or folder(s) and integrating aCrypt+ with Internet Explorer's "Send To" desktop extension.

6.2 Email Encryption

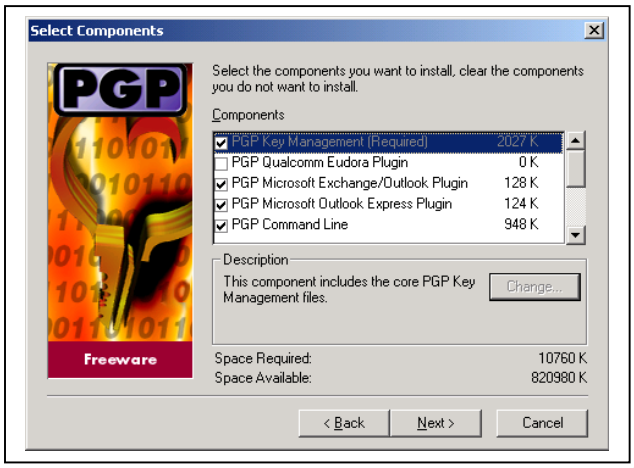
To ensure a moderate level of security in email encryption, certain basic criteria should be met. First, the method of security has been properly examined and tested by experts; second, the encryption methods are publicly known; and third, the software is of high quality.

The various public key encryption software packages on the market range in effectiveness and reliability. However, the single most important factor for ensuring security is the size of the key. The larger the key, the more secure; consequently, more computing power is require to break the code.

For example, an early system called Data Encryption Standard (DES) used a 56-bit key. The number of permutations in a binary 56-bit key is 2 raised to the power of 56, a total of 72 million billion combinations. Today, there are programs that use much larger keys to generate a significantly larger number of permutations, and this makes it much more difficult to break the code or codes.

Pretty Good Privacy, (PGP) and Hushmail are packages that use larger key sizes to protect information.

6.2.1 Pretty Good Privacy (PGP)



6.2.1.1 PGP History

Phil Zimmermann, the original creator of PGP, wrote and released it as freeware on the Internet in 1991. It was considered one of the first tools of its kind and drew considerable interests within the Internet community at the time, especially the U.S. Government. Specifically, the government was concerned about enemies of the state using PGP's strong encryption to hide secrets.

PGP, which uses asymmetric encryption, continues to be an effective secure messaging standard on the Internet.

Unfortunately a company called Network Associates Inc. has dropped this product suite. However, as of August 2002, a new company was formed called PGP Corporation, which purchased Network Associates Inc.'s PGP assets and is planning to release a new version.

The strong user base of PGP is likely to stay the most popular email encryption tool.

6.2.1.2 What is PGP?

PGP is a commercial product for encrypting email messages, attachments, files, hard disks, et cetera. PGP uses several encryption methods that are known to be secure. The source code to PGP is publicly available. It allows programming and encryption experts to examine it and search for back doors and bugs.

PGP has been in use for many years and is highly regarded among the cryptographic community. It is used as a standard today. As it has evolved, PGP has come to use a different set of mathematical algorithms to generate key lengths from 128-bits to 2048-bits or higher. This gives a huge number of possible combinations and several layers of complexity, thereby increasing its secure nature.

When using PGP, it first generates a key pair. There is a public key in which a user can give out to anyone or post it on a Web page. Then, there is a secret key in which a user keeps only on his or her own PC and a back up in a secure place.

Anyone can send a private email message by encrypting it with a public key. Only the recipient can decrypt the message because the recipient has his or her own private key. To keep the private key safe, it is encrypted itself on a user's hard disk. Each time the user uses PGP, he or she enters a pass phrase, a user-created password to render it usable.

To facilitate a secure exchange of information, it is necessary for everyone with PGP to exchange public keys. However, exchanging these keys can be a cumbersome process; consequently, special software was developed called "keyserver" that allows people to upload their public keys. This streamlines the process by allowing anyone with access to the keyserver to retrieve their public key and send encrypted data.

6.2.2 HUSHMAIL

6.2.2.1 Hushmail History

Hushmail is the first product from the company called Hush Communications. They use industry standard algorithms as specified by the OpenPGP standard to ensure the security, privacy, and authenticity of the users' email. A user only needs to know his or her own password, and secure Hushmail server protects any transmission.

6.2.2.2 What is Hushmail?

Hushmail is another way to encrypt messages using the OpenPGP algorithm. It is a free, fully encrypted, end-to-end, Web-based email service. It is a patented technology. This employs a fast and easy process by which the exchange of keys takes place behind the scenes without prompting from the user. When a user wishes to encrypt data and/or decrypt data, a connection is automatically made to a Hush Key Server to retrieve the necessary public and/or private key. This is a very user-friendly secure email solution.

Some shortcomings of Hushmail include the lack of a spell check function and the limitation that encrypted messages can only be sent to other Hushmail users.

Overall, Hushmail is another way of adding encryption to an email. The cost ranges from $2.50 per month to $29.99 per year, and a user can get the flexibility of a Web-based email account combined with the security of 2,048-bit encryption, digital signatures, and support for the OpenPGP standard. Additionally, since the service is Web-based, then the user can access email from any machine with an Internet connection. Though Hushmail is limited to only those having the software, its popularity is growing as more servers come equipped with Hushmail software.

7.0 Summary

Businesses and individuals have come to rely on email as an effective and indispensable means of sending and receiving messages and attachments. Users are becoming more aware of how exposed their plain text emails are, and they are beginning to require the capability to encrypt messages.

The emailing community is becoming better educated in Internet security, including the added security benefits and potential vulnerabilities and shortcomings of security systems.

As outlined in the above text, there are many choices for protection packages. The only problem with the packages on the market is that they are options, not

requirements. Therefore, the security may be only as good as the user's vigilance in using it.

Perhaps primary vendors of email software will include encryption as a standard feature rather than as a plug-in. Integrated solutions, such as standard features and new software products, are likely to make communications increasingly secure. However, encryption software, email security, and the implementation of protection programs still remain the responsibility of the individual and companies.

APPENDIX A: References

[01] Burnett, Steve & Paine, Stephen. RSA Security's Official Guide to Cryptography. California: Osborne/McGraw-Hill, 2001. 311-322.

[02] Adams, Carlisle and Lloyd, Steve. Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations. Indianapolis, IN: New Riders Publishing, 1999. 19-24, 80-86, 210-215.

[03] Nash, Andrew; Duane, William; Joseph, Celia; and Brink, Derek. PKI Implementing and Managing E-Security. California: Osborne/McGraw-Hill, 2001. 4-9, 47-60.

[04] Stallings, William. Cryptography and Network Security: Principles and Practice, 2nd edition. New Jersey: Prentice-Hall, Inc.1999. Chapters 4,5,10.

[05] APC and Paul Mobbs. "Using Encryption and Digital Signature." APC participating with safety briefing no. 4, 2002. URL:http://secdocs.net/manual/lp-sec/scb4.html>, (3 September 2002).

[06] Williams, Gerald. "CrossNodes Briefing: Encryption Products." Earthweb Networking and Communications, 10 September 01, URL: http://networking.earthweb.com/netsecur/article/0,,12084_881471,00.html, (10 September 2002).

[07] "RSA Cryptography Standard." RSA Laboratory. October 1998. URL: http://www.ietf.org/rfc/rfc2437.txt (10 October 2002).

[08] Kay, Russell. "Encryption Pipe Dream." Computerworld. 13 August 01, URL:http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,62959,00.html (10 October 2002).

[09] Fordahl, Matthew. "PGP Gets Email Encryption Rights." Daily News of the Computer User.com. 22 August 02, URL:http://www.computeruser.com/news/02/08/22/news1.html (12 October 2002).

[10] Jesdanun, Anick. "Keeping email encryption alive." The Morning News. 21 April 02, URL:http://www.nwaonline.net/pdfarchive/2002/april/21/4-21-02%20C12.pdf (12 October 2002).

[11] Heath, Jim. "How electronic encryption works and how it will change your business." Viacorp. 22 August 2002, URL:http://www.viacorp.com/crypto.html (12 October 2002).

[12] Hushmail.com "How Hushmail Works." 11 October 02, https://www.hushmail.com/about.php?PHPSESSID=ff21cdab4c6d122c0961fdffcca6faaa&subloc=how

[13] "About FileCrypto." F-Secure, URL: www.f-secure.com/products/filecrypto/ (09 November 2002).

[14] Strom, David. "Hushmail: Secure and easy to use." Security Tips & Newsletters-Search Systems Management.com. 09 July 2002, URL: http://searchsecurity.techtarget.com/tip/1,289483,sid14_gci837606,00.html (09 November 2002)

[15] "About ShyFile." ShyFile, URL: www.shyfile.net/page2.html (16 November 2002).

[16] "About aCrypt+." *aCrypt+,* URL:www.acrypt.com (16 November 2002).

[17] "About WebCrypt Pro." Moonlight Software, URL: www.moonlight-software.com/webcrypt.htm (18 November 2002).

[18] "How much information?" UC Berkeley, 2000, URL: http://www.sims.berkeley.edu/research/projects/how-much-info/internet/emaildetails.html (18 November 2002).

Last Updated: July 26th, 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
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
SANS Adelaide 2017	Adelaide, Australia	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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
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
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event