Global Information Assurance Certification Paper

Secure Messaging
Ron Hilton
November 7, 2000

Introduction:

Standard email is not considered to be secure. Email is typically transported across networks in clear text, may or may not get to its intended destination and the recipient is not assured that the actual sender was, in fact, the purported sender of the message. As a result, the confidentiality and integrity of important messages is questionable. This paper will review the components of secure messaging and survey the characteristics of several secure messaging products currently offered.

Secure Messaging Standards:

In order to address secure messaging issues, several different mail protocols have been developed. These can be broadly be classified as Internet mail, X.400, and proprietary protocols. Two examples include:

- S/MIME - defined by RSA stands for Secure Multipart Internet Mail Extensions. S/MIME can be used to add cryptographic services to "standard" email. S/MIME has many of the same security features of the X.400 protocol.
- X.400 - a standard defined by the International Telecommunications Union (ITU) and the International Standards Organization (ISO). Used for mission critical applications such as finance and the military. Implemented throughout the world and provided by many telecommunications companies.

These solutions generally do not inter-operate well with each other. Users desiring to communicate securely with each other must use the same solution.

Components of Secure Messaging:

A review of the X.400 and S/MIME specifications offers some insight into several "best practices" for secure messaging. These specifications provide a wide range of functionality that can be applied to encrypted (or non-encrypted) mail systems in order to provide a minimum set of requirements. Many of these features have been implemented by various standard Internet mail agents. It is important to note that the four elements of a secure cryptosystems: confidentiality, integrity, authentication and non-repudiation, have been integrated into this feature set.

Several of the features adopted by the aforementioned standards include:

- Content confidentiality - the use of a secure cryptosystem to encrypt the message.
- Content integrity - used to validate that the message has not been tampered with. Typically the recipient regenerates the has from the message received and compares it to the hash that was sent.
- End-to-end delivery confirmation - the user may request delivery/non-delivery notifications. In addition, the user may elect to be notified when the message was read. If a message is deleted, forwarded or expires before it is read, a non-delivery notification may be issued.
- Non-repudiation of origin – a mechanism which allows the recipient to verify that the message was sent by the person represented as the sender.
- Non-repudiation of delivery - the user can request delivery notifications. The system may also provide non-delivery notifications. In addition, the user can elect to be notified when the message was read. If a message is deleted, forwarded or expires before it is read, a non-delivery notification is issued.

In addition to these features, the U.S. government has promoted the notion of a key escrow, which is effectively a master key to open all messages in question. Corporations have also expressed interest in this feature for keys that they manage. The master key would be used for purposes of investigations when a law or policy was suspected to have been violated.

Secure Messaging Product Overview

Currently several vendors are providing offerings that are identified as "secure" email. To varying degrees they offer the security features identified above. In some cases their implementations may not scale to an organization's security needs. The products surveyed include ZixIt ZixMail, Sigaba SigabaSecure, and ZipLip ZipLip Plus.

Ciphers Used by these Products:

The following products use a combination of the Blowfish and Triple-DES algorithms for encrypting messages.

The Data Encryption Standard (DES) is a symmetric cryptosystem using a 64-bit block algorithm and a 56-bit key. When used for communications, the sender and receiver of the message must know the key used to encrypt and decrypt the data. Triple-DES is based on the DES algorithm and considered to be a secure symmetric key system. In general, the message is encrypted three times with multiple keys.

Blowfish is symmetric 64-bit block cipher. The keys have variable lengths (32 to 448-bits) and the algorithm is supposed to be faster than DES.

Survey Says!

ZixMail

Of the three products surveyed, ZixMail is the closest to a standard PKI product. It offers public/private keys, certificate authorities, and digital signature capability. ZixMail does not support the a key signature authority.

- Features
  - Centralized certificate authority (ZixIt Worldwide Signature Server) including activation and revocation
  - Triple-DES with 3 independent keys for encrypting/decrypting the message
  - 1024 bit public/private keys for message signing (specific implementation of Triple-DES and public/private keys may be found at http://www.zixmail.com/zixmail.pdf)
  - Private key is encrypted onto your disk based upon a user defined pass phrase
  - Digital signature capability
  - Certified time stamp for message status - certification is based upon a combination of the time stamp, the message hash, the status of sender/recipient keys, a super root certificate and a signature by the ZixIt Worldwide Signature Server
  - Certified delivery receipt and tracking
  - Corporate licensees may keep copies of their domain's encryption keys to be integrated into their mail systems
  - No master key

ZixMail also provides the ability to send "secure" mail to individuals who do not have ZixMail certificates. The product used is named SecureDelivery. The ZixIt Support Center has indicated that details of the SecureDelivery hashing algorithm has not been released. The mail process is similar to ZipLip (below) and will not be surveyed here.

SigabaSecure

SigabaSecure is a key management authority. Sigaba does not use individual public/private keys for encrypting email. Sigaba performs user authentication based upon their email address and a password, but can also use other forms of credentials that the user may have, such as a digital certificate.

- Features
  - Certificate authority only

- Uses Blowfish with 128 bit keys to generate a unique key for each message
- PKI used to communicate keys to message sender and receiver through an SSL session (for more information please see the SigabaSecure whitepaper, figure 2.0).
- Authentication to receive keys is generally based upon the user's email address and a password
- PKI not used to encrypt mail messages
- Users do not own public/private keys
- Only the keys are stored, encrypted message is forwarded immediately to recipient
- Receipt confirmation provided
- Ability to "shred" unread messages
- Ability to control when a message is available for review
- No master key

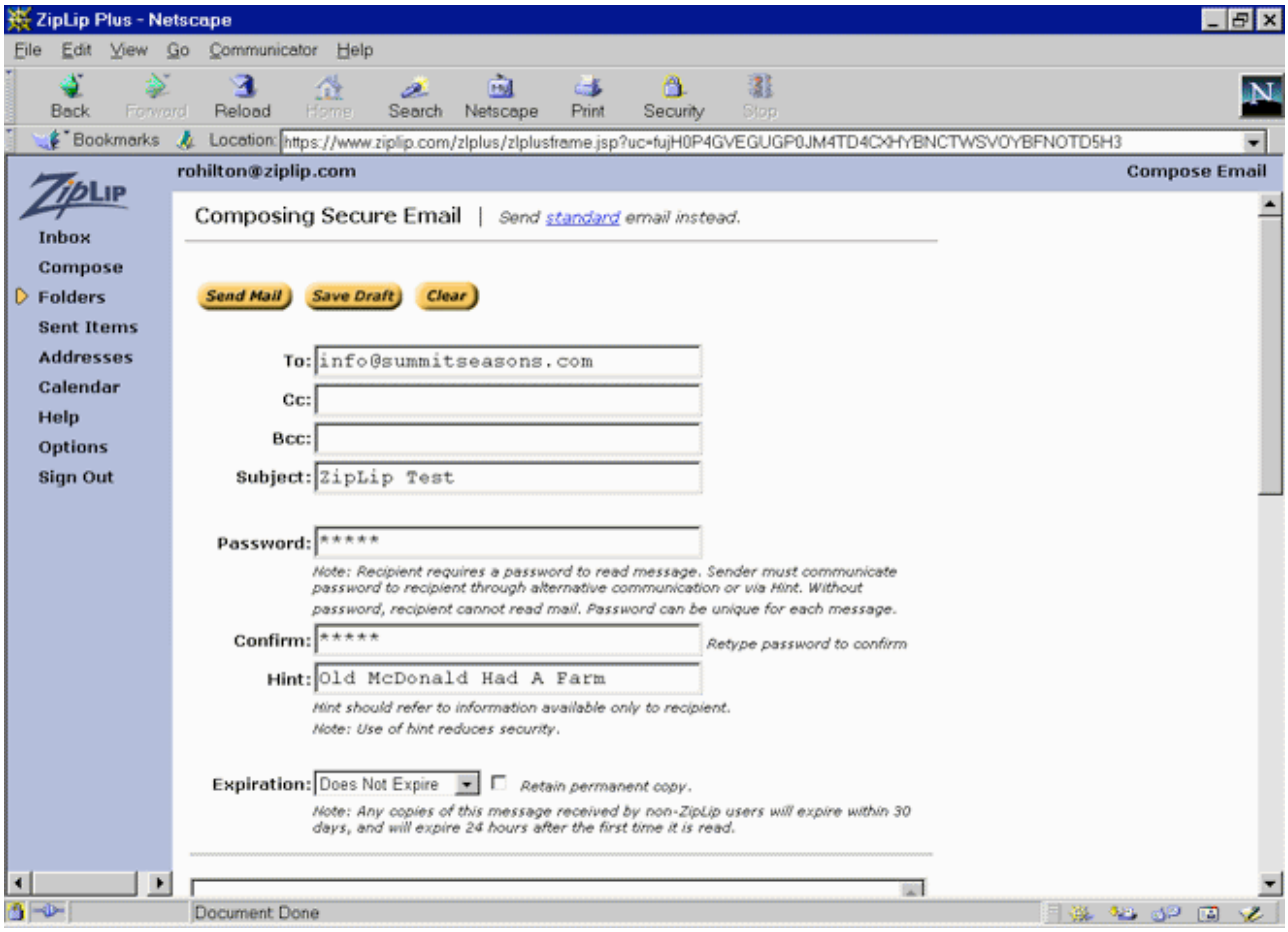
ZipLip

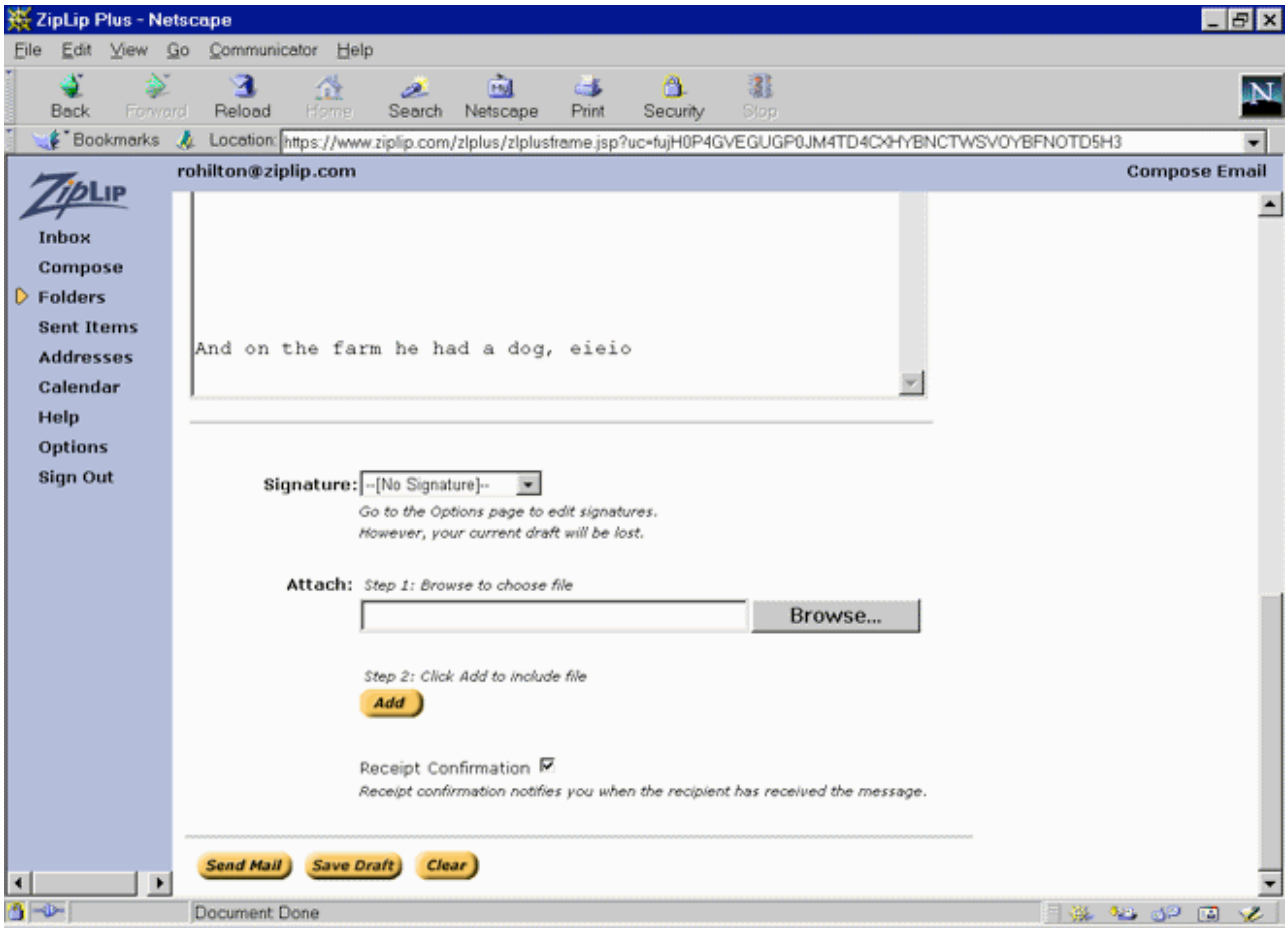
ZipLip is a web based mail system. The mail session between ZipLip and you is encrypted in an SSL session. You are authenticated to ZipLip with a user name and password. To send a secure email you must create a password which must be communicated to the recipient (out of band). The recipient must provide the password in order to receive the decrypted message.

- Features
  - A web based email system
  - Uses SSL to authenticate and pass email to the ZipLip mail server
  - Your mail is encrypted at ZipLip and stored on a ZipLip server
  - Users Blowfish and Triple-DES encryption
  - Access to the mail message is password protected
  - Receipt confirmation is generated
  - No master key

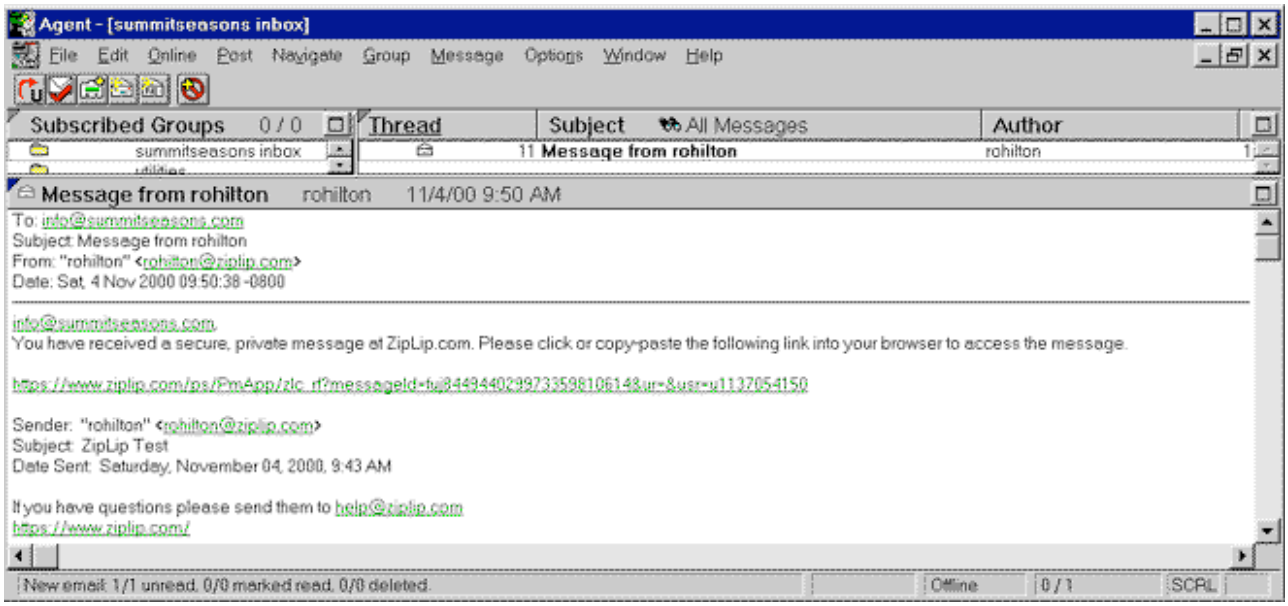
I have provided the following screen shots of the ZipLip process. While following this process, please remember the components of a secure messaging system identified above.

1) The sender creates the "secure" mail message and enters a message password. Sender must communicate the password to the recipient separately.

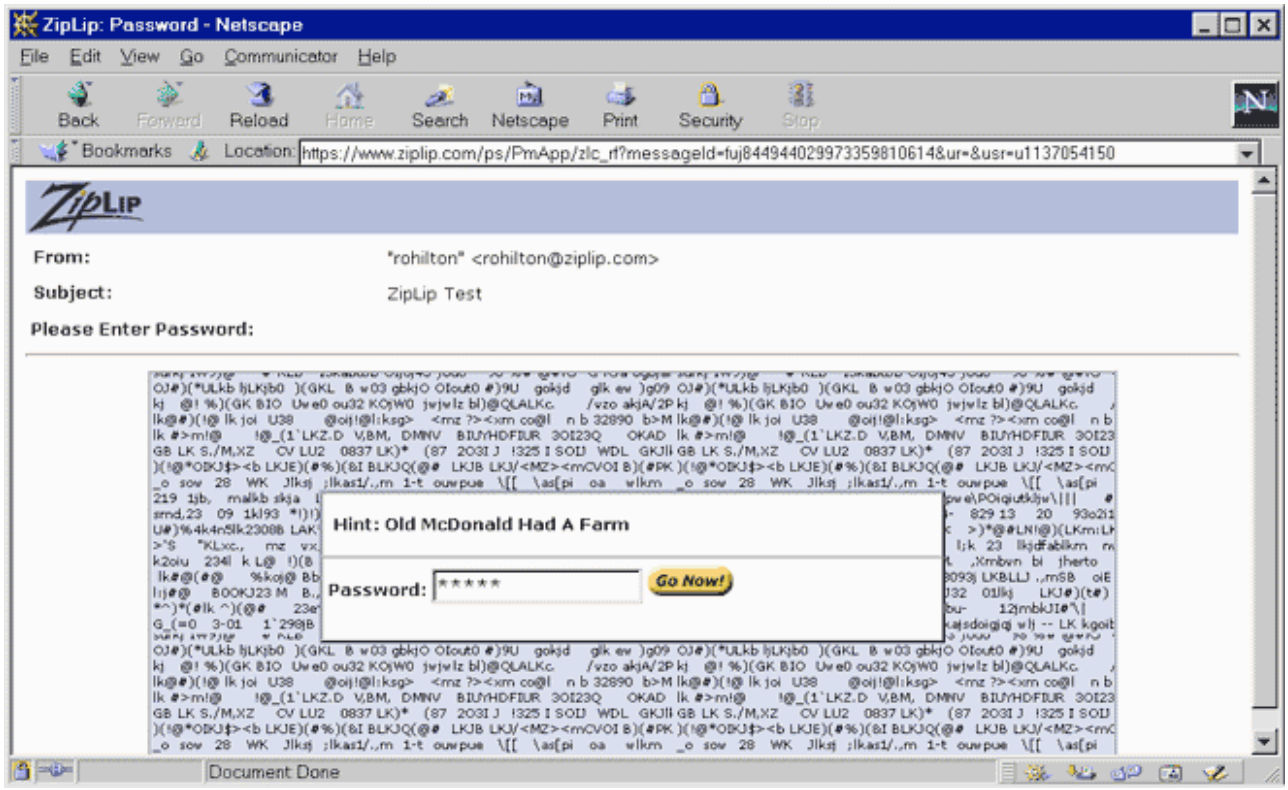




2) Recipient receives a standard email notification with a link to the ZipLip message.



3) Recipient must enter the password provided by the sender. Notice the nice hint that the sender can provide.



Conclusion:

In summary, understand the criticality of the data that you plan to send through your secure messaging system. Once you understand the criticality of the data, you will be better able to determine the level of risk that you are willing to accept and identify the product that conforms to that risk.

All of these products rely on some form of a pass phrase. If the user does not create a secure pass phrase, the security of the product will not protect your data from compromise.

References:

Secure Messaging

MCI Worldcom, "X.400 Email Without the Problems", http://www.legalcommunications.com/x400.html

Alvestrand, Harald T., "Secure E-mail", http://www.alvestrand.no/domen/speeches/nordunet95/, (11/3/95)

Doeherty, Gavin, "X.400 Electronic Mail", http://ntrg.cs.tcd.ie/4ba2/x400/opinions.html

Ramsdell, B, "S/MIME Version 3 Message Specifications", http://www.imc.org/ietf-smime/, (6/99)

Encryption Algorithms

"The Blowfish Encryption Algorithm", http://www.counterpane.com/blowfish.html

"RSA Laboratories Frequently Asked Questions About Today's Cryptography, Version 4.1", http://www.rsasecurity.com/rsalabs/faq/

Products

"ZixMail Help", http://www.zixmail.com/help.html, (9/22/00)

"ZixMail Technical Overview", http://www.zixmail.com/zixmail.pdf, (9/6/00)

"ZixMail Frequently Asked Questions", http://www.zixmail.com/faq.html, (9/22/00)

"ZilT Signature Manager Help", http://www.zixmail.com/sigmanager.html

"Sigaba Frequently Asked Questions", http://www.sigaba.com/corporate/products_FAQ.html

"SigabaSecure - A Technical Whitepaper", http://www.sigaba.com/corporate/sigaba_whitepaper_1.0.pdf

"ZipLip: FAQ", https://www.ziplip.com/zlplus/static_help_FAQ.htm

"ZipLip Technical FAQ", https://www.ziplip.com/zlplus/tech_faq.htm

"ZipLip: Help", https://www.ziplip.com/zlplus/static_help_security.htm

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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 Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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 Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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
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