Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Cryptography: What is secure?

As we moved into the information society, cryptography has become increasingly used to provide security. What is secure today can be broken tomorrow or be broken by "something" or "somehow". This rule could just be the only rule that never changes in the ever-changing game of security. It is thus important for security personals to know more than just applying cryptography blindly. This paper looks at how security is achieved by discussing basic substitution and transposition operations, to get an appreciation of secur...

Copyright SANS Institute
Author Retains Full Rights

AD

Title: Cryptography: What is secure?
Name: Willy Jiang
Assignment: GSEC Assignment v1.4b

Abstract

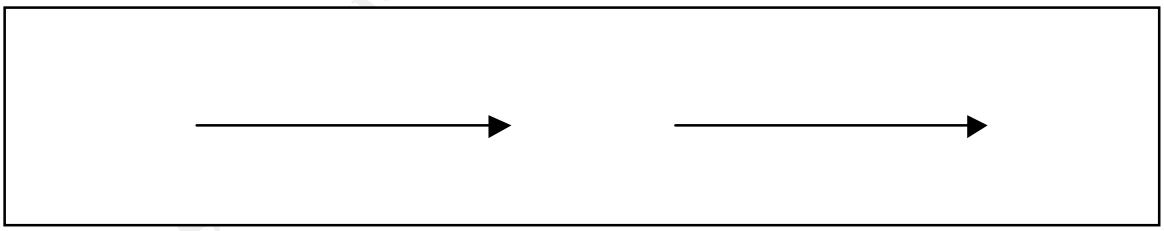
As we moved into the information society, cryptography has become increasingly used to provide security. What is secure today can be broken tomorrow or be broken by "something" or "somehow". This rule could just be the only rule that never changes in the ever-changing game of security. It is thus important for security personals to know more than just applying cryptography blindly.

This paper looks at how security is achieved by discussing basic substitution and transposition operations, to get an appreciation of security in cryptography and recommend basic approach to implement cryptography. It is beneficial for readers to have some knowledge on cryptography to follow certain discussions of the paper.

Cryptography And Security

A widely simplified meaning to many people is that cryptography is encryption.

Plaintext, or cleartext is the information or message itself and encryption is the process of coding the information in such a way that its meaning is hidden. Decryption is the reverse process of encryption. Encryption and decryption usually make use of a Key, and the coding method is in such a way that decryption can only be performed knowing the proper key as shown in the following diagram. [1]



Today's cryptography is more than encryption and decryption. From encrypting files to full scale E-commerce business online, cryptography has developed to provide: [2]

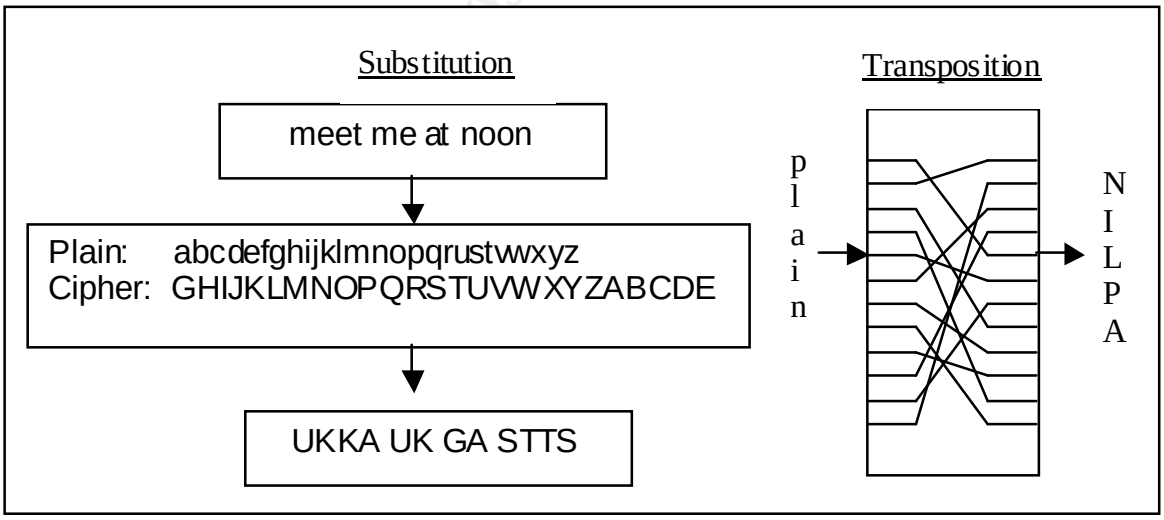
- Confidentiality: The prevention of unauthorized disclosure of information.
- Integrity: The prevention of erroneous modification of information.
- Availability: The prevention of unauthorized withholding of information or resources.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Authentication: The process of verifying that users are who they claim to be when logging onto a system.
- Authorization: The process of allowing only authorized users access to sensitive information.
- Privacy ensures that the only the sender and intended recipient of an encrypted message can read the contents of the message that are transmitted from one place to another and cannot be understood by any intermediate parties that may have intercepted the data stream.
- Non-repudiation provides a method to guarantee that a party to a transaction cannot falsely claim that they did not participate in that transaction.

Substitution and Transposition Operations

The fundamental function of cryptography is to keep information between participants in a way that prevent others from reading it. This basic function is provided by the underlying cryptosystems, also known as the ciphers. And the two basic operations are shown as follows:



The substitution operation is associated with the principle of confusion, can be understood as replacing the letters. Whereas the transposition or permutation operation is associated with the principle of diffusion: meaning rearranging the order of the letters. [3]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

A simple substitution cipher used the substitution method as shown above is commonly refer to as caesar cipher. Each letter is mapped or translated with another alphabet (without duplication), the arrangement is in alphabetical order and the letters are shifted with fixed distance. In the above example, the fixed distance (Key) is 6. Since there are 26 alphabets, there are 25 possible Keys could be used.

Instead of arranging the order of letters alphabetical order, the letters can be shuffled arbitrarily, so there are 26 possibilities for the selection of the 1st letter, and for each of the 26 possibilities, there are 25 possibilities for the selection for the 2nd letter, and then 24 possibilities for the 3rd and so on. This then resulted in a total of $4x10^{26}$ combinations and possible Keys.

Other variants is possible; for example specifying "WILLY" as part of the Key, the other part of the key specify the padding of the remaining letters, as shown in the example on the left.

Plain:	abcdefghijklmnopqrustwxyz
Cipher:	WILYABCDEFGHJKMNOPQRSTUVWXZ
Plaintext:	attack
Ciphertext:	WTTWLG

Notice that there are no space in the ciphertext, this is can help to make difficult the task of the attacker. Similarly, creation of spacing can also confuse the attacker. However, when the ciphertext are converted back to plaintext, the earlier is easier to recognize. Besides, operations may not be restricted to using English alphabets; representations may be pictures or other languages. Simply, the idea is to replace the representations of language (letters) with some form of code.

Substitution would be like creating unlimited amount of representations that would take forever (as long as it should takes) for an attacker to try each and everyone of them while Transposition would be shuffling the information bits to unrecognizable pattern that restrict the attacker to piece back the information. And the Key would be the information to the means of the operations.

A simple transposition process would be writing the plaintext in rows and read off the column. In this example, the Key is Willy; it specifies the Key is 5 columns (5 letters in Willy) and the order of ciphertext follows the sequence according to the order of appearance of its letters.

Plaintext:	attack the town tonight
Ciphertext:	TTWITHNGAETHAKONCTOT

W I L L Y
4 1 2 3 5
attac
kthet
ownto
night

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

There are ways to complicate the transposition process, eg; texts are rearranged in top-to-bottom order, the "spiral" pattern or down, up-across, right, down-across fashion.

The above examples illustrate a simple monoalphabetic cipher which operates on either substitution or transposition function. Monoaphabetic cipher has an obvious weakness and that is that modifying the plaintext proportionally (letter with letter) exhibits obvious regularities and that posts risks of revealing its original form.

The attacker's approach is known as frequency analysis. In every language, some letters are used more often than others on average or some combination of 2 or 3 letters appearing more often in a normal sentence. The attacker gathers statistical information of the occurrences of each letters and uses this information to aid his guesswork when trying to break the cipher.

E	12.7
T	9.1
A	8.2
O	7.5
I	7.0
N	6.9
S	6.3
H	6.1
R	6.0
D	4.2
L	4.0
C	2.8
U	2.8
M	2.4
W	2.4
F	2.2
G	2.0
Y	2.0
P	1.9
B	1.5
V	1.0
K	0.2
J	0.2
X	0.1
Q	0.1
Z	0.1

Say, using the frequency statistics for English letters as shown on the left. And say that for a given ciphertext the attacker get holds of has frequency statistic on the right. [4]

The attacker may guess that for each cipher-letter O might corresponds to plain-letter E, T, A

The attacker may also deduce further with the frequency statistic for double or triple letters or other common patterns in the language.

The frequency statistics also gives a fairly good fingerprint of the language, that the attacker can deduce the language of the ciphertext given its frequency distribution. [5]

This explanation is being simplistic and suggests that the work of the attacker requires a lot of work and luck. In reality, it is very easy to crack monoalphabets ciphers using frequency analysis given a reasonable large ciphertext to analyze.

O	9.9
G	9.3
B	8.6
I	7.9
C	7.6
Y	7.2
W	7.1
A	6.7
V	6.6
F	6.2
S	4.3
U	4.3
J	3.3
D	3.1
L	2.5
M	2.6
P	2.2
Z	2.1
K	1.8
E	1.4
X	1.2
R	1.0
T	0.7
H	0.3
Q	0.1
N	0.1

Weakness in Monoalphabetic cipher is obvious and the cipher can be improvised in several ways as follows: [6]

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Uses several substitutes for each letter (homophonic substitution)
- Replace every 2 letters or 3 letters by something else that stands for that combination of 2 or 3 letters (polygraphic substitution)
- Replace common combinations of letters or words or phase by their own substitutes (nomenclators and codes)

The effect of using multiple cipher alphabets can be design to even out the frequency distribution and thus making the attacker's job harder with more guessing work. The ciphers can be improved further to change from one secret alphabet to another as the message is being encrypted instead of using same set of substitutes all the time, (polyalphebatic substitution). It is also found that when a substitution operation is followed by a transposition operation, a much harder cipher is obtained than combining substitution ciphers or combining transposition ciphers. Substitution-transposition ciphers can also chained together to form product cipher.

Such Substitution-transposition ciphers can be designed that it exhibits: [7]

- Avalanche effect where changing one input bits results in changes of approximate half the outputs bits
- Completeness effect where each output bit is a complex function of all the input bits.

And the transposition operation has the following effect

- Generate a scrambled order letters in the alphabet for use as a substitution alphabet
- Forms part of the operations where letters are divided into parts then the parts are put back together in a different order, belonging to different letters.

As cryptographers try to make the job of attacker seem impossible with complex ciphers and unlimited possibilities number of Keys, cryptanalyst tends to choose the method of brute force or exhaustive key search the least and comes out with different ways trying to break the ciphers. For example:

- Examine the structure of ciphers and look for weakness that might result in leaking of information
- Look for weak keys that show certain regularities in the cipher encryption process.
- Trying sufficient amount of plaintext and compare with the respective ciphertext to look for regularity and gather bits of information of the key
- Testing two related plaintexts as they are encrypted under the same key. Attacker then analysis the difference in the ciphertext and assign possibilities to each of the possible keys, and eventually identify the most probable key.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The illustrations above using very simplified ciphers attempts to give readers an idea of how might cipher are improvised to give variation in security strength and illustrate what are the attackers approaches so that reader can get an appreciation of the kind security is provided by cryptography.

The development of cryptography has come a long way while the cryptographers come up with clever ciphers; cryptanalysts attempt to break these codes and these two disciplines constantly trying to keep ahead of each other. Resulted in cryptosystems getting more complex and diversify to meet different cryptographic needs available publicly and commercially today.

Security In Cryptosystem

These complex ciphers provide security based on difficult mathematical questions with the assumption "If lots of smart people cannot solved the problem, then the problem probably cannot be solved (soon)." [8]

Kerckhoff's Principle suggests that the security of cipher should rely on the secrecy of the Key only. Assuming that the attacker knows the cryptographic algorithm used. [9] Thus making the key difficult to guess and have to try every possible key in turn until the correct key is found. The strength of security therefore is measured against the time which is the time required to try every possible keys.

This makes the security strength difficult to measure since different Key length will give different security strength. As suggested by the table [10] below, the security strength for 56-bits key length is between 10 hours to 2000 years. Furthermore, it is not necessary means that the longer the key length will guarantee higher security.

Key length (bits)	Time (1 microsecond/test)	Time (1 microsecond/106 test)
24	8.4 sec	8.4 microsecond
32	35.8 mins	2.15 millisecond
40	6.4 days	550 millisecond
48	4.46 years	2.35 hours
56	Approx 2000 years	10.0 hours
64	Approx 50000 years	107 days
128	5×10^{24} years	5×10^{18} years

DES utilizes of 56-bits Key and therefore having 2^{56} (approx 7.2×10^{16}) possible keys has been broken 22 hours. [11] Thus it may be considered that it is no longer secure to use 56 bits key length. Key length of 128 bits is typically used today as baseline to achieve minimum security. The table above should not be taken as absolute values as the computational power of computer is increased, more keys can be tried in a shorter time. The cryptographers have anticipated such and the keys can be increase to 256 or 512 bits has been suggested.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Limiting the strength to only the secrecy of the key would be too simplistic. As mention earlier, attackers usually look for weakness in the cipher's structure or characteristics. As a result, cryptographers have improved the structures of the ciphers used today. However, cryptanalysts have also developed more advance cryptanalysis technique.

As of this moment, cryptographers still has the better off to cryptanalysts and keeping ahead. NIST (National Institute of Standards and technology) has officially announced Rijndael on 26 November 2001 as the AES (Advanced Encryption Standard) to replace DES for Federal Information Processing Standard. [12]

Security personals should be aware that security means

- The monetary cost of decrypting the data exceeds the perceived value of the data.
- The amount of time required to decrypt the data exceeded the amount of time for which the data must remain secure. The period, which is defined by the time required for exhaustive key, search to break the cipher.
- The amount of data encrypted with a single Key is less than that of what cryptanalyst could decrypt through a cryptanalytic attack.

It appears that Security (cryptography) has an abstract definition. The discussions so far shows that cryptography can provide security provided that the attacker has not found any way to break it practically. The practicality of cryptography probably means that cryptography comes with an expiry date. Although the expiry is claimed to be unreachable, examples has shown these claims can be proven otherwise.

Security Implementation

Implementing cryptography seems straightforward enough, few decision to make like using 3DES with 128 bits Key, SHA1 for Hash function, the rest is systems' configurations and nothing would probable go wrong. Implementing SSL (Secure Socket Layer) would just be required to purchase digital certificates and installing onto the server, and everything is taken care of, e-commerce is ready and as long as user uses "https". This should not be the case. Security is make simple for, but should not be taken for granted. From some aspect, it is worthwhile knowing that (but not limiting to):

- DES was the first block cipher that has been widely used in the public sector. No easy attack has been discovered although research efforts have put into over many years. 3DES has been deployed instead as a common practice usually in an encrypt-decrypt-encrypt sequence with three different, unrelated keys. Since DES is not a group, encrypting the

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

data three times has increased the security strength of the algorithm. It is remarkable that there are yet any cryptanalytical techniques that would completely break DES in a structural way other than exhaustive search. DES has weak Keys and sub keys, even though it may not cause any worry as the probability of generating one of these key is $16/2^{56}$ [13], it still shows known weakness in the crypto-algorithm that can be taken advantage of.

- Next-to-be Rijndael show the shift of reliance for DES/3DES suggest Rijndael is replaceable as well
- Some reasons to choose Rijndael is because it only uses Boolean operations, table lookups, and fixed shifts/rotations, which are the easiest defend against most attacks, and showing an adequate security margin against contemporary attacks like differential and linear cryptanalysis among other timing and power attacks. Besides, it has high efficiency and low memory requirements. [14]
- Mode of operations in the cryptosystems, example: cipher block chaining (CBC) mode is preferred to electronic code book (ECB) mode, because the latter is easier for attackers to 'obtain' information about the plaintext from the repeated cipher blocks and rearrange the cipher blocks to alter the meaning of the information. The earlier is also susceptible to such risk but it is harder for attacker.
- Buffer overflow attacking techniques to compromise systems offering cryptography service, vulnerability in browser to install fake CA certificates suggests that proper tools are needed to use in conjecture with crypto-services
- A specific security assessment on 512-bit RSA key shows that one can factor the Key in eight months and spending $1,000,000. Hence, it is believed that 512-keys is not secure except for short-term uses. It is recommended that 768 bits key should be used for personal, 1024 bits for corporate and 2048 bits for valuable keys like root-key pair. Changing keys regularly, say every two years for a user's key can also attain higher security level. [15]

In June 2002, DBS Bank in Singapore was alerted about an unauthorized fund transfer via Internet banking using SSL. The investigations revealed that DBS's system had not been hacked into, but there were a total of 21 customers whose accounts had been affected, with amounts ranging from $200 to $4,999 transferred into a single account. [16] The local newspaper later revealed that the attacker collected the necessary information for his job when the victims send their PC to service at repair shop. Needless to say, the attacker was linked to the repairman.

In this example, it is clear that security can be compromised even when cryptography is implemented, proper tools are used when accessing the crypto-service. The paper like to emphases that there are areas which cryptography cannot protect from, such as informants, unauthorized access, human error.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Basic Approach

There are many ways to implement cryptography and one point about this paper is that cryptography alone cannot provide absolute. Implementation guides are widely available but such guides often only include what they can offer and did not mention what they did not cover. Security personal still have the job of securing the implementation as a whole. It is important to have a clear knowledge of the "what to protect", "what are the threats", and with these, I have recommended 6 steps approach would be as follows:

1. Identify what to protect
2. Determine what you are trying to protect from
3. Determine scope of protection
4. Determine scope of related-protection needed
5. Implement measures
6. Review the process continuously and make improvements

Looking back at example of DBS's Internet banking using SSL again, the 1st 3 points can be summarized easily. The protection will be the messages sent over Internet between 2 parties and ensuring the 2 parties are who they claim to be. Protecting from attacker intercepting the communication will not understand the message and masquerading as one of the party involved. SSL is implemented to authenticate the parties involved, encrypted the messages, ensuring integrity of the messages communicated and provides non-repudiation as well.

Point 4 may include, deciding the relevant cryptographic security strength, the security requirement for computers including OS, software patches, virus issues, placement of physical computers, storage of computer's passwords and who has access to them. Risks of contemporary attacks like buffer overflows, DOS attacks. A complete secure implementation would take care of all possible risks, which may be difficult in practical. However, it is better to know and write down the extent of protection so that they can be planned for in future. Security personal may also include risks not protected by the tools listed.

The rational for the above 4 points is to give the security personals a clear understanding of the security coverage in the implementation. And to decide what is needed to implement, any applications that require continuous patching and to determine appropriately the security level achieved.

Implementation phase would be rolling out the selected tools. In the event of computers not in control of the administrator, policy may be published for owners of the remote computers. Like in the case of the DBS's above, users are reminded to clear the browser's cache after logging off, which are implemented now on DBS web site.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Point 6 is critical as implementation needs to be reviewed continuously correcting any weakness found or to extend the protection scope.

It is important that security personal is equipped with reasonable knowledge of what is to be protected and what are the likely threats, otherwise he will not be able to exercise sound judgment to scope the security.

Conclusions

Since there is no way to prove that a system is secure, what is considered as secure system is an un-compromised system to-date. Even though, security personal must clearly aware of what and how is been protected by the systems. The paper illustrates the appreciation of security and suggests basic approach in implementing it, but most importantly security personal must not be misguided to a false sense of security.

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Citation

[1] Charlie Kaufman, Radia Perlman, Mike Speciner. Network Security: Private Communication in a Public World. 41.

[2] Benjamin, Lail. Broadband Network & Device Security. Brandon A Nordin. 18 - 21

[3] Andreas, Steffen. Secure Network Communictaion. 16 Nov 2002. URL: http://www.strongsec.com/zhw/KSy_Crypto.pdf

[4] Introduction To Codes, Ciphers & Codebreaking. 16 Nov 2002. URL: http://www.vectorsite.net/ttcode.html. 9-10

[5] Introduction To Codes, Ciphers & Codebreaking. 16 Nov 2002. URL: http://www.vectorsite.net/ttcode.html. 11-12

[6] John, Savard. A cryptographic Compendium. 16 Nov 2002 URL: http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm

[7] Lawrie, Brown. Cryptography and Computer Security. 16 Nov 2002. URL: http://www.cs.adfa.edu.au/teaching/studinfo/ccs3/lectures/index.html

[8] Oliver, Pell. Cryptology. 14 Oct 2002 URL:http://www.ridex.co.uk/cryptology/

[9] Erkay, Savas. Data Secrurity & Cryptography. 19 Nov 2002 URL: http://islab.oregonstate.edu/koc/ece575/notes/L1.pdf

[10] Lawrie, Brown. Cryptography and Computer Security. 19 Nov 2002. URL: http://www.cs.adfa.edu.au/teaching/studinfo/ccs3/lectures/index.html

[11] RSA laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1. 16 Oct 2002. URL: http://www.rsasecurity.com/rsalabs/faq/index.html.

[12] Charlie Kaufman, Radia Perlman, Mike Speciner. Network Security: Private Communication in a Public World. Practise Hall PTR. 81-82.

[13] Charlie Kaufman, Radia Perlman, Mike Speciner. Network Security: Private Communication in a Public World. Practise Hall PTR. 74.

[14] Report on the Development of the Advanced Encryption Standard (AES) 19 Nov 2002. URL: http://csrc.nist.gov/encryption/aes/round2/r2report.pdf.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[15] Oliver, Pell. Cryptology. 14 Oct 2002 URL: http://www.ridex.co.uk/cryptology/. 22.

[16] ELSIE FOH. DBS to ensure safety, hacker incident not taken lightly. 24 Nov 2002. URL: http://www.sensecurity.org/dbs.htm

Further Readings

1. Cryptology by Oliver Pell
http://www.ridex.co.uk/cryptology/

2. RSA laboratories' Frequently Asked Questions About Today's Cryptography, Version 4.1
http://www.rsasecurity.com/rsalabs/faq/index.html

3. An Introduction to Cryptography And Digital Signature by Ian Curry
http://www.entrust.com/resources/whitepapers.htm

4. Report on the Development of the Advanced Encryption Standard (AES)
http://csrc.nist.gov/encryption/aes/round2/r2report.pdf

5. Advanced Encryption Standard (AES) Questions and Answers
http://www.nist.gov/public_affairs/releases/aesq&a.htm

6. SANS Security Essential IV: Encryption and Exploits

7. Network Security: Private Communication in a Public World by Charlie Kaufman, Radia Perlman, Mike Speciner

8. Broadband Network & Device Security by Benjamin M. Lail

9. A cryptographic Compendium
http://home.ecn.ab.ca/~jsavard/crypto/jscrypt.htm

10. Cryptography and Computer Security
http://www.cs.adfa.edu.au/teaching/studinfo/ccs3/lectures/index.html

11. Introduction To Codes, Ciphers & Codebreaking.
http://www.vectorsite.net/ttcode.html

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: May 24th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced