Interested in learning more about security?

SANS Institute InfoSec Reading Room

Formulating a National Cryptography Policy: Relevant Issues, Considerations and Implications for Sin

This paper provides insight into the relevant issues, considerations and implications necessary for formulating an effective National Cryptography Policy, taking into account the protection of privacy, intellectual property, business and financial information, as well as the needs for law enforcement and national security. An analysis of Singapore's present Cryptography Policy is also discussed, with due deference to the OECD Guidelines on Cryptography and determines its adequacy in lieu of the issues, considerations a...

FORMULATING A NATIONAL CRYPTOGRAPHY POLICY: RELEVANT ISSUES, CONSIDERATIONS AND IMPLICATIONS FOR SINGAPORE.

Francis Chong Heng Goh (GSEC Practical Version 1.3)
11 Feb 2002

ABSTRACT

This paper provides an insight into the relevant issues, considerations and implications necessary for formulating an effective National Cryptography Policy that would be able to balance a number of varied interests by taking into account the protection of privacy, intellectual property, business and financial information, as well as the needs for law enforcement and national security. An analysis of Singapore's present Cryptography Policy is also carried out with due deference to the OECD Guidelines on Cryptography and determines its adequacy in lieu of the issues, considerations and implications covered and makes recommendations for any necessary improvements.

INTRODUCTION

In the early part of the 1990's, the market for secure encryption of messages formed a relatively insignificant niche segment in the computer industry. However, with the proliferation of networking technology and the consequent rise of the Internet (ie the network of interconnected networks) and subsequently e-commerce, this niche segment has started to gain increasing importance for the economic and social development of information economies like Singapore for example.

The explosive worldwide growth of open networks has raised a legitimate concern with respect to the adequacy of security and privacy measures for information and communications systems and for the data that is transmitted and stored on those systems. The developing information infrastructure is a melting pot for all kinds of computer-related crime, including fraud and privacy infringement, and electronic business will not advance until effective security measures are adopted and trusted by users and consumers alike. In particular, information has become an increasingly coveted resource in the Internet Age. Hence, effective protection of information resources determines the success and failure of businesses as well as ensuring the national security of countries (ie through the protection of critical information infrastructures and resources). Today, this protection can only be guaranteed by the use of powerful cryptographic methods whose efficiency is increasingly greater than ever.

However, the widespread use of cryptography raises other important issues, and cryptography policy should, therefore, balance a number of varied interests. In addition to its role in the operation of electronic commerce, cryptography has widespread implications for the protection of privacy, intellectual property, business and financial information, as well as law enforcement and national security.

POLICY ISSUES FOR CRYPTOGRAPHY

Cryptography usage, at *prima facie*, allows for the anonymous dissemination of information and to ensure that the documents are not tampered with or altered after release. It also ensures the confidentiality of personal records, such as medical information, personal financial data, and electronic mail where in a networked environment, such sensitive information is increasingly at risk of being stolen or misused.

However, in the wake of the terrorist attacks in New York City and Washington D.C. since September 11, 2001, there is intense debate on how a well-crafted Cryptography Policy could have averted the disaster through restrictions on the use and availability of strong encryption products, government regulation of cryptographic methods and techniques, lawful access and forced disclosure of encryption keys etc. The policy issues and implications of having government controls on cryptography though the use of key escrows/key recovery schemes, lawful access and forced disclosure of encryption keys and the role of import/export and domestic controls etc in the name of national security and law enforcement are thus examined in this light.

A. Key Recovery and Key Escrow Schemes[1]

Key Escrow/Key Recovery was a concept first mooted by the United States Government in 1993. In this scheme, users would be allowed to use strong encryption with the caveat that trusted third parties such as government agencies or specially authorized company (licensed by the government) would hold the keys and provide them to the relevant government agency when requested. With this intent in mind, key escrow was first introduced in the US in the form of the Clipper chip in 1993.

1. Rationale For Key Escrows (Pros)

Law Enforcement Reason

From the standpoint of law enforcement, the capability to conduct court authorized electronic surveillance should be built into any technology. This includes powerful encryption software as it remains as a powerful tool for law enforcement. Today's law enforcement requires the ability to decrypt communications and to read the decrypted contents as a safeguard against cyber terrorism, money laundering, drug dealing and other criminal activities. However, the use of strong cryptographic methods is also helping criminals deter police surveillance instead. Hence, one proposal was the setting up of key escrows whereby users of powerful encryption software turn over their keys to trusted third parties so that law enforcement officials can gain access to them with a lawful court order.

2. Rationale Against Key Escrows (Cons)[2]

Economic Cost Reasons

[1] Dan Fromkin, "Deciphering encryption"
[2] Abelson, Hal. "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption",

Encryption software companies have reiterated that overly strict regulations will make it difficult for them to compete globally for the computer security technology market share. Besides, key escrow schemes tend to weaken encryption, resulting in customers having little confidence in online commerce and communications, hence hampering secure e-commerce efforts.

Software Manufacturers have also feedback that having to build a "key recovery" option into software would be expensive and unpopular with customers as well. Businesses appreciate having the "key recovery" option for encrypted data stored by employees on company computers. In the event that the employee resigns or upon the employee's sudden death without his handing over the necessary decryption keys to the encrypted data, companies will have access to the data without disrupting business operations. Nonetheless, they have no interest whatsoever in weakening the security of transmitted data through key escrows.

Risk and Implementation Cost Reasons

The major reason for involving a third party in the management of keys for confidentiality is to allow the third party to make the keys available to others, other than between the two communicating parties, for example, to law enforcement. However, any involvement of a third party in confidential communication increases its vulnerability, providing a single point of failure. Inevitably, any key escrow scheme will introduce additional ways to break into a cryptographic system with accompanying risks of insider abuse and trusted third parties themselves being subjected to attacks. These new vulnerabilities are complex and need to be understood as substantial liability and privacy questions are implied.

Furthermore, the costs associated with putting in place key escrow schemes can be very high. Important cost factors would be the specific requirements for licensing and serving a warrant on such trusted third parties, for example, key delivery response time, session key storage time, authentication of requesting government agencies, secure transfer of recovered keys, internal user security safeguards and disaster recovery etc. Furthermore, making key escrow schemes scalable (i.e. making it work in a multi-million user environment) will contribute to the high design costs too. The technical challenges, risks and complexity would determine to a large extent the effectiveness of putting in place a key escrow scheme.

Finally, key recovery or key escrow schemes if in place should never involve the archival of digital signature keys as such keys are used to formulate binding commitments for non-repudiation of transactions. Non-repudiation requires distinct keys for all signers, even when two or more individuals are authorized to send a given message; without that, the ability to audit transactions is destroyed. Neither should government surveillance require the recovery of signature keys either. Yet, some key recovery schemes are designed to archive authentication and signature keys along with confidentiality keys. Such schemes destroy the absolute non-repudiation property that makes binding commitments possible. Thus, since there is no legitimate need for authentication or digital signature key recovery as such, only confidentiality key recovery schemes should be permitted.

B. Lawful Access and Forced Disclosure of Encryption Keys[3]

A new approach being considered by many governments is to demand "lawful access" to encryption keys or plain text. Under this approach individuals would be required to disclose keys to law enforcement agencies or face criminal penalties for obstructing law enforcement investigations.

However, such approaches raise issues involving the right against self-incrimination, which is highly respected in many countries worldwide. The privilege against self- incrimination forbids a government official from compelling a person to testify against himself. It has a long history originating from Roman and Canon law and was subsequently adopted by the Common law. This is because the Common Law does not allow the burden of proof to be reversed for the suspect to provide the requested evidence to prove his/her innocence instead.

Another important issue is the penalizing of individuals who may not have access to the keys issued in their name. In many circumstances, an individual may not be in possession of a key, either because it is lost, revoked or never possessed in the first place. Under laws and pending bills of lawful access and forced disclosure, the users could face jail for being unable to provide the keys.

To date, only Singapore and Malaysia have enacted laws that would require users to disclose their keys or face criminal penalties. In both of those countries, police have the power to fine and imprison users who do not provide the keys or the plaintext of files or communications to police.

C. Role of Export Controls[4]

Export controls used to be the strongest tools used by governments worldwide to limit the development of encryption products in the name of national security. Even so, it reduces the availability of encryption in common programs such as operating systems, electronic mail and word processors. As a result, the restrictions make it difficult to develop international standards for encryption and interoperability of different programs. Countries must therefore develop their own local programs, which do not interoperate well with other programs developed independently in other countries. They may also not be as secure because of a lack of peer review. At the same time, as markets are smaller due to export controls, companies and individuals become less interested in developing such programs because of smaller potential market profits, hence hampering the development and growth of encryption software as an inevitable result.

On hindsight, the Internet has significantly changed the effectiveness of export controls too. Strong, unbreakable encryption programs can now be delivered in seconds to anywhere in the world with a network connection. It has been increasingly difficult for countries to limit dissemination, and once a program is released, it is nearly impossible to stop its spread,

[3] EPIC, International Survey of Cryptography Policy, 2000

[4] Hoofman, Lance. "Cryptography: Policy and Trends."

especially if it is in one of the many countries around the world with no export controls. In the United States, export controls were originally used as a justification to limit the availability of encryption on domestic Internet sites and thus serve as indirect domestic controls on encryption too.

Many countries have now relaxed their export controls on encryption products, especially software. The United States Government implemented an encryption policy change and announced in January 2000[5] the latest policy update where it now allows companies to export most encryption products. It is likely that other countries will follow suit too.

D. Role of Domestic Controls on Cryptography and Human Rights[6]

Government regulation of techniques such as encryption that help to protect individual privacy tend to run contrary to the spirit of international laws and norms that recognize privacy and the freedom to communicate in confidence as fundamental human rights. Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights, as well as other international agreements, and national laws, emphasize the importance of privacy protection as an important human freedom and birthright. Only a few countries around the world restrict the domestic use of encryption by their citizens. Amongst the countries that do so, most have strong authoritarian governments. The examples are former republics of the Soviet Union, or are located in Asia, or the Middle East like Belarus, Burma, China, Kazakhstan, Pakistan, Russia, Tunisia, and Vietnam.

CONSIDERATIONS FOR CRYPTOGRAPHY POLICY

A. OECD Guidelines on Cryptography:[7]

The principles for cryptography policy drawn up by OECD are primarily aimed at governments in terms of the policy recommendations, but with the anticipation that they will be widely read and followed by both the private and public sectors. The guidelines are as follows:

1. *Trust in Cryptographic Methods*

Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

2. *Choice of Cryptographic Methods*

Users should have a right to choose any cryptographic method, subject to applicable law

3. *Market Driven Development of Cryptographic Method*

[5] US Dept of Commerce, Federal Register, "BXA Issues Revised Encryption Export Regulations",
[6] EPIC, International Survey of Cryptography Policy, 2000

[7] Organization for Economic Cooperation and Development (OECD) Guidelines for Cryptographic Policy

Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

4. *Standards for Cryptographic Methods*

Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the national and international level.

5. *Protection of Privacy and Personal Data*

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national cryptography policies and in the implementation and use of cryptographic methods.

6. *Lawful Access*

National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data. These policies must respect the other principles contained in the guidelines to the greatest extent possible.

7. *Liability*

Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic services or hold or access cryptographic keys should be clearly stated.

8. *International Cooperation*

Governments should cooperate to coordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

SINGAPORE'S PRESENT CRYPTOGRAPHY POLICY[8]

A. Export/Import controls

The import restrictions that used to require a license from the Trade Development Board have been abolished since 21 January 2000.

There are no explicit cryptography export restrictions either. However, according to the Trade Development Board of Singapore:

"For exports of cryptographic products, TDB requires a permit in the same way as other products. However, no separate application form is needed. For re-exports of

[8] Bert-Jaap Koop, Crypto Law Survey.

cryptographic products from other countries, they will be subject to the agreement or laws of the originating country."

Singapore remains as a major supplier of encryption products to Myanmar

B. Key Escrow/ Key Recovery Schemes

There is currently no mandatory key escrow or key recovery scheme that is enforced by the government. However, companies are encouraged to use confidentiality key recovery schemes themselves to recover encrypted data whenever necessary, so as to minimize possible disruptions to business operations.

C. Singapore' s Domestic Laws and Regulations

There are no domestic restrictions on the use of cryptographic hardware or software, but according to the Singapore Trade Development Board: [9]

"Hardware equipment that will be connected directly to the telecommunications infrastructure will require approval from the Infocomm Development Authority of Singapore". This is to ensure compliance and non-interference with telecommunications requirements."

However, there remains a decryption order for offences under the Computer Misuse Act, as amended in 1998 and in force since 27 February 1999. Article 15 of this Act entitles the police (or other people authorised by the Commissioner of Police), with consent of the Public Prosecutor, at any time to have access to decryption information, code or technology for the purpose of investigating any offence under the Act (or any other offence disclosed by means of this power). Also, they are entitled to require users or people otherwise concerned with the operation of any computer that is likely related to an offence under the Act to provide reasonable technical or other assistance. Moreover, they are entitled to require any person in possession of decryption information to grant access to such decryption information necessary to decrypt data required for the purpose of investigating any such offence. Obstructing the lawful exercise of these powers or failing to comply with an assistance or decryption request is punishable with a maximum fine of S$10,000 or three years' imprisonment.

ANALYSIS OF PRESENT CRYPTOGRAPHIC POLICY

A. Lifting of Export/Import Controls

In lieu of the implications for controls and OECD Guidelines Article 3 and 4 discussed previously, the removal of import and export controls for cryptography products in Singapore is a step in the right direction. This takes into consideration the fact that software programs can easily be delivered from one part of the world to another by a click of a button using the Internet, for instance in the form of zipped enclosures in e-mails. Monitoring and stopping the electronic transfer of encryption programs on the Internet would have been near impossible and hence, it is plausible to remove export and import controls imposed on cryptographic products as the

[9] EPIC, International Survey of Cryptography Policy, 2000

efficacy of such measures is questionable, difficult to monitor and easily circumvented. Furthermore, having such controls in place would have been detrimental to the development and growth of the software encryption market especially since Singapore is a city state with an already small market size. Implementing export or import controls would have discouraged software companies from moving into and investing in Singapore for the development of computer security related products. On the contrary, the lifting of export and import restrictions will instead boost confidence amongst companies to conduct e-commerce in Singapore and support Singapore's vision to be an e-commerce hub.

B. Absence of Mandatory Key Escrow/ Key Recovery Schemes

In light of the highly complex issues pertinent to putting in place a mandatory key escrow or key recovery scheme and OECD Guidelines Article 1, 2, 5 and 7, Singapore has adopted the cautious but thoughtful approach by not making key recovery mandatory for law enforcement purposes. Instead, Singapore encourages private enterprises to voluntarily adopt confidentiality key recovery to suit their own business needs especially since most companies will have little demand for key recovery of session key during real time communications. The reason is that if real time communications is unsuccessful, then it is simply tried again until the communication succeeds. Hence, session key recovery is redundant and extremely wasteful in resources. Digital signature key recovery is discouraged in Singapore as it compromises the non-repudiation element in digital signatures.

This approach is in line with worldwide trends, for instance in the European Union and in US, key escrow proposals are currently being reexamined and debated in the light that it undermines basic human rights to privacy and that it may introduce backdoors to the security of encryption methods, and thus hamper the progress of secure e-commerce. Instead, countries are mostly opting for a voluntary program of cooperation with security services as a better alternative.

C. Implications of Singapore's Domestic Laws and Regulations through Lawful Access and Forced Disclosure of Encryption Keys

As noted in the previous discussion on "Lawful Access and Forced Disclosure of Encryption Keys", Singapore and Malaysia may to date be the only two countries in the world with laws that require users to comply with decryption orders and to provide technical assistance to law enforcement agencies as spelt out in the Singapore Computer Misuse Act 1999. Individuals that disobey will inevitably face criminal penalties for obstructing law enforcement investigations.

On one hand, this "Lawful Access and Forced Disclosure" measure was enacted with the general good and safety of the public in mind so that law enforcement will have the necessary police powers to decrypt sensitive but crucial information to solve their cases. This becomes necessary too in the light that Singapore has no mandatory key recovery or key escrow measures in place for law enforcement to rely upon. Hence, a decryption order supporting lawful access may be the only useful tool in the law enforcement arsenal that will allow law enforcement agencies to carry out their jobs. This is also in line with Article 6 of the OECD Guidelines.

On the other hand, such measures run contrary to the right against self-incrimination that is highly regarded in most democracies and explicitly provided for in the United States Constitution Fifth Amendment on Rights of Persons. This is based on the premise that the burden of proof should not be reversed for the suspect so that no person shall be compelled in any criminal case to testify against himself and therefore accords the suspect with the most basic of human rights against potential abuses by law enforcers.

Presently, "Lawful Access and Forced Disclosure" measures remain a gray area in the legal aspects of encryption policy. Singapore has always had the reputation of having a authoritative government that knows what is best for its citizens and as a result such measures are generally favored in the light of serving public good rather than as an incursion towards depriving a suspect of his human right against self-incrimination. Regardless, this legal measure may need to be examined as and when new issues come about.

RECOMMENDATION

In conclusion**,** Singapore's present National Cryptography Policy adequately addresses the salient issues that most countries have when formulating their cryptography policy. It takes on a cautious stand on most gray areas in cryptography policy like the use of mandatory key escrows, lawful access and forced disclosure of encryption keys, human rights and privacy issues as well as on the issue of implementing domestic controls. Singapore's adoption of a laissez-faire approach in its National Cryptography Policy by creating as little restrictions or controls as possible is a sound one as this will help secure consumer confidence and spur companies to conduct e-commerce in Singapore with confidence. Market forces will be left to determine the type of cryptographic method employed in accordance with Article 2 of the OECD guidelines. In this manner, Singapore has fulfilled Article 14 of the OECD guidelines whereby governments should remove or avoid creating trade obstacles in the name of cryptography policies. Nevertheless, as cryptography is a fast developing field, its associated issues may change rapidly too. As such, Singapore should keep an eye on the latest developments and trends in the world and refine its policies as and when it is justified to do so.

References

1. Singleton, Solvieg. "Encryption for the 21st Century, A Future without Government-Prescribed Key Recovery". November 19,1998. www.cato.org/pubs/pas/pa325.pdf

2. Koop, Bert-Jaap. "Crypto-Law Survey" Version 19.0, July 2001. http://cwis.kub.nl/~frw/people/koops/lawsurvy.htm

3. IDA Press Release, "LIFTING OF IMPORT CONTROL ON CRYPTOGRAPHIC PRODUCTS", January 19 2000. http://www.ida.gov.sg/Website/IDAContent.nsf/dd1521f1e79ecf3bc825682f0045a340/b862cb2072335c19c825686b003b85a9?OpenDocument

4. Smith, Adam. “Debunking the DOJ on Encryption”, January 2001 http://www.senseofsecurity.com/doj.asp

5. OECD Document C(97)62 Annex 2, “Guidelines for Cryptography Policy”, March 12, 1997. http://www.oecdwash.org/NEWS/PRESS/1998X/crypto2.htm

6. OECD Secretariat Team, “REPORT ON BACKGROUND AND ISSUES OF CRYPTOGRAPHY POLICY”, December 19 1997. http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-43-nodirectorate-no-24-10241-29,FF.html

7. Fromkin, Dan and Branson, Amy.“Deciphering Encryption” May 8 2001. http://netsecurity.about.com/gi/dynamic/offsite.htm?site=http%3A%2F%2Fwww.washingtonpost.com%2Fwp-srv%2Fpolitics%2Fspecial%2Fencryption%2Fencryption.htm

8. Madsen, Wayne and Banisar, David. Electronic Privacy Information Center (EPIC), “Cryptography and Liberty 2000”, An International Survey of Encryption Policy. 2000 http://www2.epic.org/reports/crypto2000/overview.html

9. Hoofman, Lance. Under Contract DE-ACO5-840R21400, US Dept of Energy “Cryptography: Policy and Trends.” January 30 1994. ftp://ftp.cpsr.org/cpsr/privacy/crypto/hoffman_crypto_policy_report_jan_94.txt

10. US Dept of Commerce, Federal Register, “BXA Issues Revised Encryption Export Regulations”, October 18, 2000 http://www.bxa.doc.gov/Encryption/pdfs/EncryptionRuleOct2K.pdf

11. Abelson, Hal. Report by Ad Hoc Group of Cryptographers and Computer Scientists. “The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption”, Revised Edition 1998. http://www.cdt.org/crypto/risks98/

12. General Assembly of the United Nations. “Universal Declaration of Human Rights”1948 –1998. http://www.un.org/Overview/rights.html

13. Office of the High Commission of Human Rights. “International Covenant of Civil and Political Rights” 23rd March 1976 http://www.unhchr.ch/html/menu3/b/a_ccpr.htm

14. Akdeniz, Yaman. “No Chance for Key Recovery: Encryption and International Principles of Political and Human Rights.” Blackstone Press 1998. http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html

15. Sergienko, Greg. *“Self Incrimination and Cryptographic Keys”*, 2 RICH. J.L. & TECH. 1 (1996). http://www.richmond.edu/~jolt/v2i1/sergienko.html

Last Updated: October 17th, 2017

Upcoming SANS Training

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

SANS San Diego 2017	San Diego, CAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WAUS	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, AE	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Milan November 2017	Milan, IT	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Amsterdam 2017	Amsterdam, NL	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Miami 2017	Miami, FLUS	Nov 06, 2017 - Nov 11, 2017	Live Event
SANS Paris November 2017	Paris, FR	Nov 13, 2017 - Nov 18, 2017	Live Event
Pen Test Hackfest Summit & Training 2017	Bethesda, MDUS	Nov 13, 2017 - Nov 20, 2017	Live Event
SANS Sydney 2017	Sydney, AU	Nov 13, 2017 - Nov 25, 2017	Live Event
GridEx IV 2017	Online,	Nov 15, 2017 - Nov 16, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CAUS	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, GB	Nov 27, 2017 - Dec 02, 2017	Live Event
SIEM & Tactical Analytics Summit & Training	Scottsdale, AZUS	Nov 28, 2017 - Dec 05, 2017	Live Event
SANS Khobar 2017	Khobar, SA	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TXUS	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, DE	Dec 04, 2017 - Dec 09, 2017	Live Event
European Security Awareness Summit & Training 2017	London, GB	Dec 04, 2017 - Dec 07, 2017	Live Event
SANS Bangalore 2017	Bangalore, IN	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Frankfurt 2017	Frankfurt, DE	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DCUS	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Security East 2018	New Orleans, LAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS SEC460: Enterprise Threat Beta	San Diego, CAUS	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, NL	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SEC599: Defeat Advanced Adversaries	San Francisco, CAUS	Jan 15, 2018 - Jan 20, 2018	Live Event
SANS Berlin 2017	OnlineDE	Oct 23, 2017 - Oct 28, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced