



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.

Wireless Application Protocol 2.0 Security

This paper will focus on WAP 2.0, how it differs from previous versions of WAP and how these differences impact on security. It will assume the reader has previous knowledge of WAP 1.x, which has already been detailed in earlier SANS documents (for example, [SANS-A], [SANS-B], [SANS-C] and [SANS-D]), and will begin by summarizing current WAP 1.x security mechanisms.

Copyright SANS Institute
Author Retains Full Rights

AD

Veriato

Unmatched visibility into the computer
activity of employees and contractors



Try Now

Wireless Application Protocol 2.0 Security

Tamzin C Jeffs

November 2001

© SANS Institute 2001, Author retains full rights

SANS GEAC Security Essentials Certification (GSEC) Practical Assignment

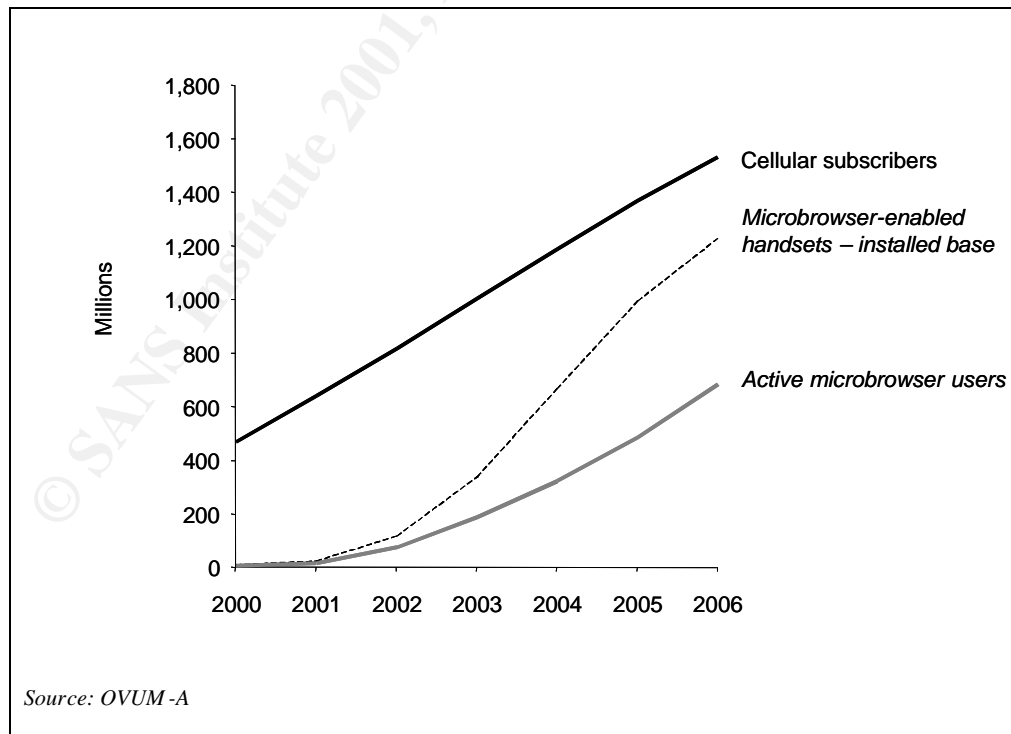
Introduction

During recent years the Internet and wireless voice communications have undergone wide and rapid acceptance. The Internet has proved to be an easy and efficient way of delivering services to millions of wired users. Mobile phones are equally efficient at providing remote services. It was then only a question of time before these two technologies would begin to converge, to bring the convenience of the Internet to the wireless community.

The mobile phone market has grown ten-fold from 1994 to 1999, from 26 million units to 278 million units. Personal computers doubled in the same period. There are now more mobile phones sold annually than PCs and TVs combined [GOLD-A]. The communications industry is fast recognising that the future of e-commerce lies in networked computing from the mobile phone.

Current projections indicate that there will be 1.5 billion mobile subscribers by 2006, 684 million of which will use microbrowser¹-enabled services. This compares with 500 million desktop or laptop Internet users. By 2006, 82% of the installed base will be microbrowser-enabled, but not all will be used [OVUM-A]. See the figure below for the forecasted trends from now to 2006.

Figure 1. Forecast for cellular subscribers, microbrowser-enabled handsets and active microbrowser users (2000 to 2006)



¹ Software that allows the user to access the Internet from a mobile device.

The major problem with converging these technologies is the difference in device structure and network properties. Internet access is generally obtained via a desktop or laptop and this will be replaced by a smaller wireless device. This has limited display capabilities, limited input facilities, limited memory and CPU, plus limited battery power. In addition the wireless network, compared to the wired network, has lower bandwidth that can cause poor performance, high latency and less connection stability.

In order to address these issues, the WAP Forum² has introduced a standardised way to provide communication between the wired and wireless worlds. The phenomenal growth in wireless web phones, personal digital assistants and other handheld devices, together with strong demand for mobile Internet services, have provided the momentum behind Wireless Application Protocol ('WAP').

WAP is optimised for small devices and is based on the Internet client/server architecture. Essentially, it is the mobile equivalent of traditional Internet protocols, but with adaptations to the bounds of the wireless network and the wireless device. It is bearer-independent and supports the major operating systems used in handheld devices (including Epoc, JavaOS, PalmOS and Windows CE).

The WAP Forum released WAP 1.1 in June 1999 and WAP 1.2 was ratified in December 1999. The next generation WAP, WAP 2.0 (also known as WAP-NG), was released for public review on 1 August 2001. WAP 2.0 continues the standard's convergence with Internet technology and is based on the Internet Engineering Task Force ('IETF') standard of TCP/IP and the World Wide Web Consortium's ('W3C') recommendation of XHTML³. It also improves the user experience through additional features, such as Data Synchronization (Sync ML), Multimedia Messaging Service, Persistent Storage Interface, Provisioning, Pictograms and an evolved version of WAP Push [WAPF-A].

This paper will focus on WAP 2.0, how it differs from previous versions of WAP and how these differences impact on security. It will assume the reader has previous knowledge of WAP 1.x, which has already been detailed in earlier SANS documents (for example, [SANS-A], [SANS-B], [SANS-C] and [SANS-D]), and will begin by summarising current WAP 1.x security mechanisms.

² The WAP Forum is an industry association of wireless device manufacturers, service providers and software companies. It was founded in 1997 by three mobile phone manufacturers (Ericsson, Motorola and Nokia), together with the US software company Phone.com (formerly Unwired Planet).

³ eXtensible HyperText Markup Language ('XHTML').

WAP 1.1 security

The main security initiative in WAP 1.1 is the Wireless Transport Layer Security protocol ('WTLS'). WTLS provides similar functionality to that of the Internet's transport layer security v1.0 protocol ('TLS'), the IETF's standard for securing Internet browsing, and this, in turn, is based on Secure Sockets Layer ('SSL') v3.0 Internet protocol.

However, compared to traditional TLS/SSL, WTLS provides faster algorithm processing (by minimising protocol overheads), enables more data compression and provides the added functionality of datagram support⁴, optimised handshake⁵ and dynamic key refreshing.

WTLS provides a robust, efficient basis for secure transactions and supports data integrity, authentication and privacy services between communicating applications [WAPF-D]. A summary of each security service and the corresponding WTLS security mechanism is outlined in the table below.

Security requirement	Security mechanism
Confidentiality/privacy	■ Secret key cryptography using bulk ciphers, such as RC5_CBC, DES_CBC, 3DES_CBC, IDEA
Authentication/authorisation and non-repudiation	■ Public key cryptography using key exchange suites, such as RSA, Diffie-Hellman, Elliptic Curve Diffie-Hellman
Integrity	■ MACs - HMAC based (for example SHA-1, MD5) or XOR based (for example SHA-1)

⁴ TLS/SSL cannot operate over UDP, whereas WTLS can.

⁵ For optimised handshakes, in contrast to the full handshake, the server obtains the client certificate from a certificate distribution service or from its own source, without requesting it over the air from the client.

WAP 1.2 security

To address the lack of both non-repudiation services and real end-user authentication in WAP 1.1, the WAP Forum introduced two new initiatives in WAP 1.2:

- the WMLScript Crypto Library – provides application layer security by the use of WMLScript applets to enable cryptographic signing of WML content. These applets run on the client and are stored within a WMLScript Crypto library; and
- the WAP Identity Module ('WIM') - 'a tamper-resistant⁶ device which is used in performing WTLS and application level security functions, and especially, to store and process information needed for user identification and authentication' [WAPF-B].

These two initiatives are supported by a wireless Public Key Infrastructure ('PKI'), which provides the functions that store and process information needed for user identification and authentication [WAPF-B].

WAP 2.0 security

A much publicised criticism of WAP 1.x, and a primary cause of reluctance to adopt the protocol, is the lack of end-to-end security or end-to-end authentication. This is due to the presence of a WAP gateway, which effectively acts as a bridge between the mobile and IP networks. The gateway is the single point of translation between the WAP and standard Internet protocols (WTLS and TLS/SSL) and markup languages (WML⁷/WMLScript⁸ and HTML⁹/JavaScript). As part of the translation process, data is momentarily present in plaintext and it is this 'gap' in security that can, potentially, pose a serious security risk.

In an attempt to reduce this risk, gateway operators claim to take precautions to ensure plaintext is never written to disk, decryption and re-encryption takes place in the volatile, internal memory and is erased as quickly as possible, the gateway is physically secured and administrative access to the gateway is limited. However, the residual risk may still be too unacceptable for services that require secure transactions, such as banking and brokerage.

Alternatively, vendors with strenuous security requirements could host their own gateway. This would be within the vendor's own network environment and

⁶ Tamper-resistant means that certain physical hardware protection is used, which makes it unfeasible to extract or modify information in the module (volatile, non-volatile memory and other parts) [WAPF-B]

⁷ Wireless Markup Language ('WML').

⁸ Wireless Markup Language Script ('WMLScript').

⁹ Hyper Text Markup Language ('HTML').

would be under their control and security measures. Data, encrypted by WTLS, would pass directly between the client and the vendor's gateway and would then pass through the vendor's network to their web server. This would, effectively, provide a form of end-to-end security. However, in practice this is a very large overhead for vendors. Also, the majority of WAP phones are sold with the mobile operator's gateway setting pre-loaded. It can be complicated and frustrating exercise to change that setting and some operators prevent users from accessing any gateway other than their own.

WAP 2.0 addresses the lack of end-to-end security by introducing support and services for Internet protocols (including TCP/IP¹⁰, TLS and HTTP¹¹) into the WAP environment. Internet protocols can, therefore, be used directly between the client and wireless network and this eliminates the need for protocol translation at the WAP gateway. In doing so, this effectively provides transport level end-to-end security.

WAP 2.0 architecture

In the previous versions of the WAP specification, a new set of protocols, collectively known as WAP 1.x stack, were created to facilitate the transfer of data along low-bandwidth mobile networks to constrained devices. With the emergence of high-speed wireless networks (for example, 2.5G and 3G) and improvements in device technology, appropriate IP connectivity can now be achieved between the device and wireless network. WAP 2.0 takes advantage of this by introducing Internet protocols directly into the WAP environment.

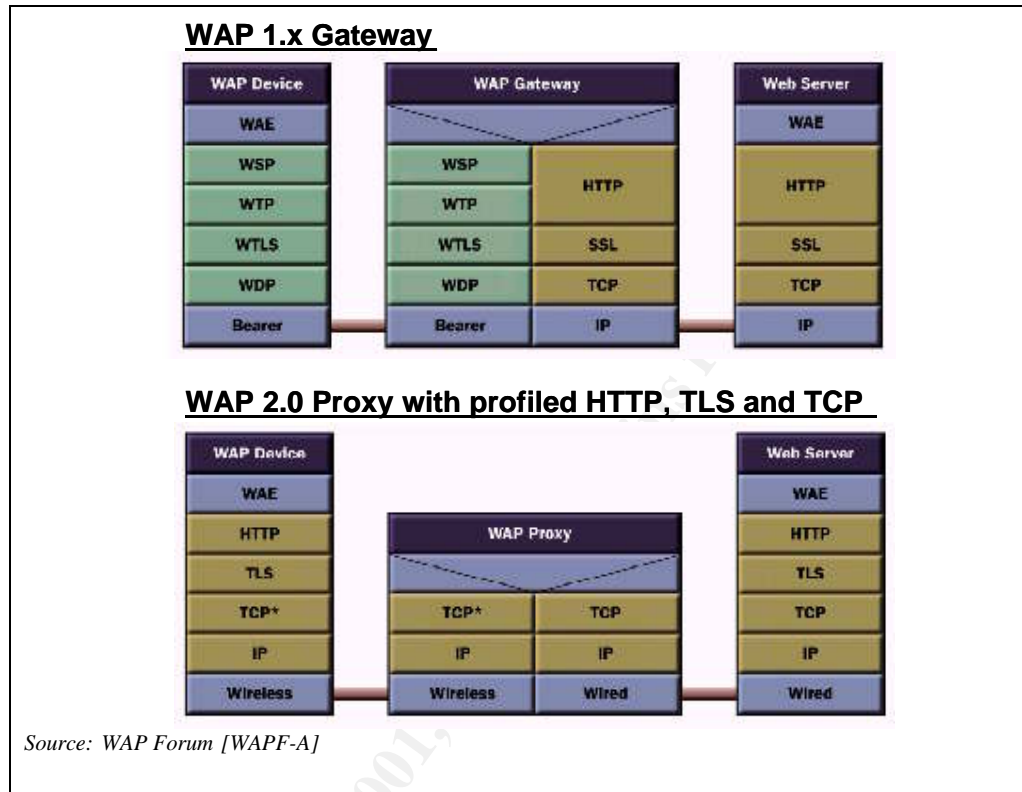
The previous WAP 1.x stack and proposed WAP 2.0 stacks are detailed in figure 2 overleaf.

Note the use of a WAP 'proxy', to replace the gateway in WAP 2.0. This is not used for translation, merely as a conduit to optimise the communications process and perhaps offer mobile service enhancements, such as location-based services. A proxy is also required to enable 'push' capabilities.

¹⁰ Transmission Control Protocol/Internet Protocol ('TCP/IP').

¹¹ HyperText Transfer Protocol ('HTTP').

Figure 2. WAP 1.x stack versus WAP 2.0 stack



The WAP 2.0 stack essentially replaces the four layers beneath the Wireless Application Environment ('WAE') of the WAP 1.x stack as follows (see figure 3 overleaf):

HTTP

- replaces the wireless session protocol ('WSP') and wireless transaction protocol ('WTP'); and
- supports HTTP request/response transactions, response message body compression and the establishment of secure tunnels.

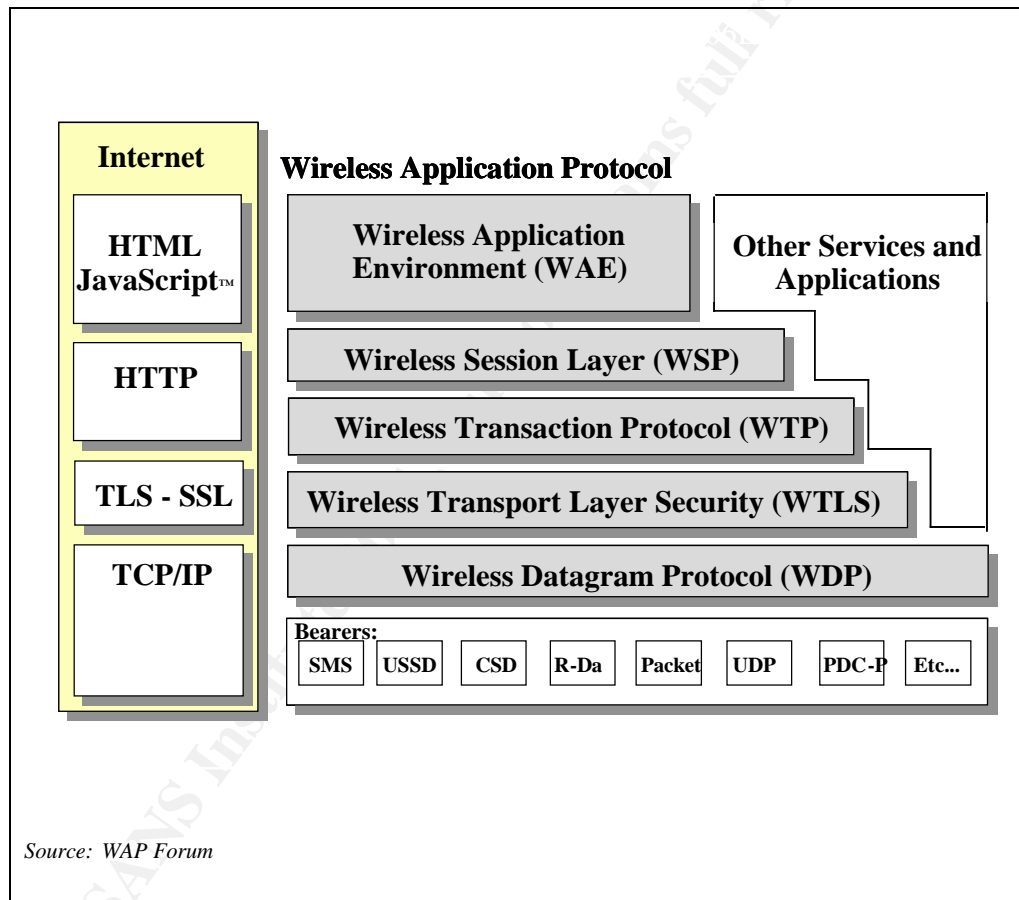
TLS/SSL

- replaces wireless transport layer security ('WTLS'); and
- supports secure transactions with cipher suites, certificate formats, signing algorithms and the use of session resume.

TCP

- replaces wireless datagram protocol ('WDP'); and
- provides connection-oriented services.

Figure 3. Internet and WAP protocol stacks



It is important to note that HTTP, TLS and TCP protocols are not identical to the Internet versions as they are 'wireless profiled'. This means they have been optimised for wireless environments and can interoperate with the standard implementations in the Internet [WAPF-C].

The 'profiled' TLS specification use similar security mechanisms/algorithms to those listed previously for WTLS:

- MACs to carry out message integrity checks (supports the common MAC algorithms SHA-1 and MD5)
- public key cryptographic authentication of the client and server (be it origin or proxy), either through the use of certificates or anonymously (supports the use of RSA, Diffie-Hellman and Elliptic Curve Cryptography algorithms); and
- message confidentiality is protected by secret key cryptography (using DES, triple DES, RC5 and IDEA algorithms).

The WAE, nominally viewed as the 'WAP browser', has evolved in WAP 2.0 to embrace developing standards for Internet browser markup language [WAPF-A]. WAP 1.x uses the lightweight markup language WML (which is a subset of XML¹² and is similar to the Internet's HTML, but optimised for use in handheld mobile devices). WAP 2.0 introduces WML2, which is based on the basic profile of XHTML, developed by the W3C to replace and enhance the HTML language commonly used today. This will eventually enable developers to write applications for both PC and WAP clients using a common subset of language elements and development tools.

Conclusion

WAP 2.0 continues to support the original WAP 1.x stack and, by encompassing both stacks, provides backwards compatibility. Although this has the advantage of enabling connectivity over a broader range of networks and wireless bearers, the wireless environment is now exposed to security issues related to the Internet protocols as well as those related to WAP 1.x and the WAP 1.x architecture.

Some of the weaknesses in WTLS are also present in the current TLS/SSL used over the Internet, and will therefore also apply to the 'profiled' TLS used by WAP 2.0. These include: no obligation to exchange certificates; no obligation to verify certificates and authenticate owners; and the permitting of anonymous Diffie-Hellman mode (where exchanges are not supported by public key certificates) and may allow man-in-the-middle attacks (where an attacker is able to substitute his own public key for the requested public key).

Therefore, some of the old security issues will still remain in WAP 2.0. However, WAP 2.0 does address arguably the largest barrier to WAP's use and acceptance, the 'gap' in security caused by protocol translation at the gateway. There will, no doubt, also be the introduction of new security threats and issues to the wireless environment as it continues its convergence with the Internet.

¹² Extensible Markup Language ('XML').

References

- IMBA-A Durham-Vichr, Deborah & Getgen, Kimberly (2001), 'WAP 2.0 – Securing the Internet Without Wires', IBM, August 2001.
URL: <http://www-106.ibm.com/developerworks/wireless/library/wi-sectrends/>
- GOLD-A Kramer, R & Simpson, B (1999) – 'Wireless Wave II – The Data Wave Unplugged', Goldman Sachs Investment Research, 10 November 1999.
URL: <http://www.gs.com>
- OVUM-A MacKenzie, M & O'Loughlin, MA (2000) – 'WAP Market Strategies', Press White Paper, Ovum, May 2000. URL: <http://www.ovum.com>
- SANS-A Laquina, S (2000), 'Wireless Application Protocol', SANS Information Security Reading Room, 4 September 2000.
URL: <http://www.sans.org/infosecFAQ/wireless/WAP2.htm>
- SANS-B Schramm, J (2000), 'Security Issues in WAP and I-Mode', SANS Information Security Reading Room, 2 December 2000.
URL: <http://www.sans.org/infosecFAQ/wireless/WAP4.htm>
- SANS-C Cutts, M (2000), 'Secure Wireless Application Protocol (WAP) on the Enterprise, Ready or Not?', SANS Information Security Reading Room, 5 September 2000.
URL: http://www.sans.org/infosecFAQ/wireless/WAP_enterprise.htm
- SANS-D Combs, J (2000), 'Security Models for M-Commerce', SANS Information Security Reading Room, 20 December 2000.
URL: <http://www.sans.org/infosecFAQ/wireless/models.htm>
- WAPF-A WAP Forum (2001), 'Wireless Application Protocol WAP 2.0 Technical White Paper', August 2001. URL: <http://www.wapforum.org>
- WAPF-B WAP Forum (2001), 'Wireless Application Protocol Architecture Specification', WAP-210-WAPArch-20010712-a, 12 July 2001.
URL: <http://www.wapforum.org>
- WAPF-C WAP Forum (2001), 'Wireless Application Protocol Wireless Profiled TCP', WAP-225-TCP-20010331-a, 31 March 2001.
URL: <http://www.wapforum.org>
- WAPF-D WAP Forum (2001), 'Wireless Application Protocol Wireless Transport Layer Security', WAP-261-WTLS-20010406-a, 6 April 2001.
URL: <http://www.wapforum.org>
- WAPF-E WAP Forum (2000), 'WAP Identity Module Specification', WAP-198-WIM, 18 February 2000. URL: <http://www.wapforum.org>



Upcoming SANS Training

[Click Here for a full list of all Upcoming SANS Events by Location](#)

SANS Houston 2017	Houston, TXUS	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DCUS	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Milan 2017	Milan, IT	Jun 12, 2017 - Jun 17, 2017	Live Event
SEC555: SIEM-Tactical Analytics	San Diego, CAUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017	Denver, COUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NCUS	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, NL	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MNUS	Jun 19, 2017 - Jun 24, 2017	Live Event
DFIR Summit & Training 2017	Austin, TXUS	Jun 22, 2017 - Jun 29, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, AU	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, FR	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MDUS	Jun 26, 2017 - Jul 01, 2017	Live Event
SEC564:Red Team Ops	San Diego, CAUS	Jun 29, 2017 - Jun 30, 2017	Live Event
SANS London July 2017	London, GB	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, JP	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, SG	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CAUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS ICS & Energy-Houston 2017	Houston, TXUS	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, DE	Jul 10, 2017 - Jul 15, 2017	Live Event
SANSFIRE 2017	Washington, DCUS	Jul 22, 2017 - Jul 29, 2017	Live Event
Security Awareness Summit & Training 2017	Nashville, TNUS	Jul 31, 2017 - Aug 09, 2017	Live Event
SANS San Antonio 2017	San Antonio, TXUS	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, CZ	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Hyderabad 2017	Hyderabad, IN	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MAUS	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UTUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NYUS	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VAUS	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, ILUS	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Adelaide 2017	Adelaide, AU	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS San Francisco Summer 2017	OnlineCAUS	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced