Global Information Assurance Certification Paper

Satellite Security: The Weakest Link?

Maryse Medawar
Date: January 22, 2003

GSEC Practical Assignment
Version: 1.4b

Abstract

Whenever the vulnerabilities of information security are discussed, the issue seldom involves the area of satellite communication. This disregard proves to be a critical mistake according to a report recently published by the GAO, the U.S General Accounting Office. This paper discusses the points raised by the GAO, while extending the discussion to include additional concerns raised throughout the industry about securing satellite communication. These additional points include elements involved in satellite communication, security techniques employed in the industry, the issue of security and latency, the international regulations inherent to the use of satellites, and lastly the market trends of the satellite industry.

A network will only be as strong as its weakest link. This means that satellite communication needs to be treated more scrupulously because the current situation allows for immense vulnerabilities. This gap in the security chain could lead to detrimental consequences and should therefore be remedied as swiftly as possible. Efforts are being made throughout the industry, however more focus is necessary for effective solutions to be implemented.

GAO Investigation

In essence, the GAO report concluded the following:

> Satellites are not specifically identified as part of our nation's critical infrastructure protection approach, which relies heavily on public-private partnerships to secure our critical infrastructures. As a result, a national forum to gather and share information about industry wide vulnerabilities of the satellite industry does not exist, leaving a national critical infrastructure without focused attention (GAO, p.40).

The GAO identifies the satellite industry as a critical infrastructure because of the many services it has grown to provide. These include communication, navigation, remote sensing, imaging, and weather and meteorological support. Satellites support direct radio communication and provide television broadcast and cable relay services, as well as home reception. They also support applications such as mobile and cellular communication, telemedicine, cargo tracking, point-of-sale transactions, and Internet access. This is also done while providing redundancy and backup capabilities to ground-based communications, as was demonstrated after the events of September 11, 2001, when satellites provided critical communications while ground-based lines were unavailable.

The vulnerabilities mentioned in the GAO excerpt above have something to do with the fact that the satellite infrastructure relies on two providers of different nature: commercial and federal. Commercial satellite service clients include telecommunication companies, television networks, financial institutions, major

retailers, Internet service providers, and governments. Some companies resell leased satellite services to their clients. For example, major telecommunication companies sometimes include satellite services in their product line. Ground equipment manufacturers build and sell the items needed to use satellite services, such as ground station hardware (antennas), data terminals, mobile terminals (truck-mounted units), and consumer electronics (satellite phones). Federal agencies constitute another kind of provider for satellite communication. For example, the U.S. military and intelligence communities have satellites to provide capabilities for reconnaissance, surveillance, early warning of missile launches, weather forecasts, navigation, and communications. In addition, some federal civilian agencies own satellites that are used for communications, scientific studies, and weather forecasting.

The public-private partnerships are necessary when discussing U.S satellite communication because federal agencies rely heavily on the use of commercial satellites, which are sometimes owned by foreign countries. Federal agencies use commercial satellites for services such as communications, data transmission, and remote sensing. For example, the Department of Defense (DOD) typically relies on commercial satellites to fulfill its communications and information transmission requirements for non–mission-critical data and to augment its military satellite capabilities. The National Defense Industrial Association (NDIA) reported in December 1998 that the government's overall use of commercial satellites for communications and remote sensing is expected to grow significantly because of increased communications requirements. According to a DOD official, the department's reliance on commercial satellites is expected to grow through 2020. In addition to the U.S. military, several civilian government agencies also rely on commercial satellite systems. However, the federal government does not dominate the commercial satellite market. According to commercial satellite industry officials, the revenue provided to the satellite industry by the federal government represents only about 10 percent of the commercial satellite market.

However, the importance of commercial satellites for government operations is evident during times of conflict. For example, according to a DOD study, commercial communications satellites were used in 45 percent of all communications between the United States and the Persian Gulf region during Desert Shield/Desert Storm. Further, during operations in Somalia from December 1992 through March 1994, U.S. military and commercial satellite coverage was not available, so Russian commercial satellites were used. DOD currently reports approximately 50 percent reliance on commercial satellites for wideband services.

It is important to point out that federal agencies do secure data links and ground stations when relying on commercial satellites, however some components, involved in the communication, will rely on the security guidelines implemented by the private companies owning the commercial satellites. These guidelines are

based on the customers' requirements and on the companies' business objectives, which means that the level of security is much weaker than with federal satellites and is left without focus. However, before discussing the pitfalls of satellite security, a diagram illustrating the components involved in satellite communication in the next section must be examined, as shown in figure 1.

Satellite Communication – Dissected

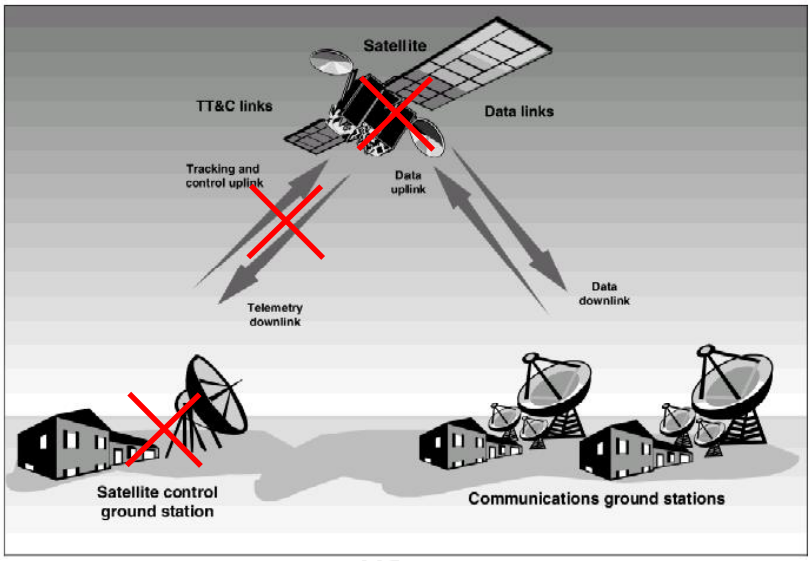

Figure 1 – "Satellite Communication Components" (GAO, p.32)
Crossed out components are not controlled by federal agencies

As shown in the figure above, a satellite system consists of ground stations, tracking and telemetry control links (TT&C links), data links, and satellites. Control stations are responsible for performing tracking and control functions, thereby ensuring that satellites remain in the proper orbits while monitoring their performance. Communications ground stations process imagery, voice, or other data while providing a link to ground-based terrestrial network interconnections.

The TT&C and data links are the links between the two types of ground stations and the satellites, allowing the exchange of commands and status information between control ground stations and satellites. Data links, on the other hand, allow the communication, navigation, and imaging data between communications ground stations and satellites. As shown in figure 1, links are also distinguished by the direction of transmission: uplinks go from Earth to space, and downlinks from space to Earth, while cross-links allow inter-satellite communication. Every satellite has a payload, which contains all the equipment that a satellite needs to perform its function and a bus to carry the payload and any additional equipment into space.

There are four general system designs, which are differentiated by the type of orbit in which the satellites operate: Geostationary Orbit (GEO), Low-earth Orbit,

Medium-earth Orbit (MEO), and Highly Elliptical Orbit (HEO). Each of these has various strengths and weaknesses in its ability to provide particular communications services. LEOs require more satellites, all of which must be in orbit before service can be provided. However, LEOs address latency, the fundamental problem with GEOs. Because of their high altitude, GEOs typically require larger, bulkier antennas and tend to be more bandwidth constricted than LEOs. MEOs are a middle ground between LEOs and GEOs. HEO systems operate differently than LEOs, MEOs or GEOs. As the name implies, the satellites orbit the Earth in an elliptical path rather than the circular paths of LEOs and GEOs. The HEO orbital design maximizes the satellites' time spent over populated areas, thus requiring fewer satellites than LEOs and providing superior line-of-sight in comparison to most LEOs or GEOs.

Security Techniques

A range of security techniques is available for protecting satellite systems: encryption is used on TT&C and data links, robust parts are used on the satellites, and physical and cyber security controls are applied at the ground stations. Techniques to protect satellite links include the use of encryption, high-power Radio frequency (RF) uplinks, spread spectrum communications, and having a digital interface unique to each satellite. Commercial satellite service providers, federal satellite owners and operators, and customers stated that they typically use at least one of these techniques. Usually, only the military uses spread spectrum techniques.

Both TT&C and data links can be protected by encryption. Generally, for TT&C links, the tracking and control uplink is encrypted, while the telemetry downlink is not. For satellite systems transmitting non–national-security information, there is no policy that security is required for the links. Even though satellite service providers and federal satellite owners and operators state that they protect tracking and control uplinks with encryption, it is known that not all commercial providers' tracking and control uplinks are encrypted. Concerning the data links, customers are responsible for determining whether they are encrypted or not. Most commercial satellite systems are designed for "open access," meaning that a transmitted signal is broadcast universally and unprotected.

Also, high-power RF uplinks can be used as a technique to provide security, with a large antenna to send a high-power signal from the ground station to the satellite. To intentionally interfere with a satellite's links, an attacker would need a large antenna with a powerful radio transmitter.

A technique that the military implements, is the use of spread spectrum communication. This technique is a form of wireless communication in which the frequency of the transmitted signal is deliberately varied and spread over a wide frequency band. Because the frequency of the transmitted signal is deliberately

varied, spread spectrum communication can provide security to links because it increases the power required to jam the signals even if they are detected. Spread spectrum communication is primarily used to optimize the efficiency of bandwidth within a frequency range, but it also provides security benefits.

TT&C links can be protected by the use of a unique digital interface between the ground station and the satellite. According to one commercial satellite service provider, most commercial providers use a unique digital interface with each satellite. Tracking and control instructions sent from the ground station to the satellite are encoded and formatted in a way that is not publicly known. Officials from the commercial satellite vendor state that even if an attacker were successful in hacking one satellite, the unique interface could prevent the attacker from taking control of an entire fleet of satellites. In addition, communication with the digital interface to the tracking and control links requires high transmission power, so that an attacker would need a large, powerful antenna.

Security and Latency

When it comes to attempting to implement end-to-end security schemes, latency and security do not mix very well, especially in the case of standards-based IP Security (IPSec). TCP spoofing, used to bring GEO transmissions up to speed, is a satellite-specific measure for generating early packet acknowledgments to fill broadband pipes. Spoofing generally benefits larger data transfers and can be augmented by other latency-reducing measures. Security experts say spoofing and IPSec are incompatible because once a transmission is encrypted, it becomes impossible for an outside entity such as a satellite service provider to see into the packets to perform spoofing.

An alternative to IPSec is application-layer security, like Secure Sockets Layer (SSL), which secures the user, transaction or application, instead of the node, as IPSec does. Application-layer security is compatible with TCP spoofing. The downside to application security is it must be implemented individually in each application and intruders can still snoop out certain information, including the destination of transmission. However, with application security alone, network proxies, like mail and other ports, end up in the clear, providing an entry point for attacks.

Some think it might be possible to perform spoofing on the traffic at the user site before it is encrypted, but that means the traffic will be in the clear until it reaches the spoofing box. Still, others say that even if encryption follows spoofing, it will defeat the process.

International Commercial Satellite Industry

According to "Networking in the 21st Century: The Sky's the Limit", a survey of the leading broadband satellite companies shows that most companies are unwilling to discuss security, and the few that are less discrete, tend to present simplistic solutions. The discretion is understandable from one point of view because of the competitive nature of the market. However, in this case the reluctance seems to stem from the global nature of satellite communication. Since many next-generation satellite systems switch traffic between and among nations, as pointed out previously by the GAO report, global security policy has no continuity. Another major problem is that the bulk of these providers fall under U.S. restrictions on the export of strong encryption, whether that encryption is used to protect customer information or to secure network resources, such as satellite controls, billing or other vital information. Moreover, as pointed out previously, businesses that need low latency alongside end-to-end encryption are apt to run into some significant technology hurdles with high-orbiting geostationary systems.

How can security be guaranteed in a system that spans multiple countries with possible conflicting interests? While most businesses with sensitive traffic will want to secure their own satellite transmissions, they also have an interest in securing the entire security chain, which means that they need their satellite providers to deploy strong link encryption and to protect the integrity of critical network information. But how do satellite providers meet the needs of multiple nations if one nation opposes its national traffic to potentially being subjected to review by another nation? Some view these issues optimistically and naively by hoping that the mix of traffic and networking schemes will discourage intruders. However, this has already been contradicted since hackers have already admitted to hacking into satellites.

The GAO reports that in April 1986, an insider, working alone under the name "Captain Midnight" at a commercial satellite transmission center in central Florida, succeeded in disrupting a cable network's eastern uplink feed to the Galaxy I satellite. Although this event was a minor annoyance, it had the potential for disrupting services to satellite users. In 1995, MED-TV, a Kurdish satellite channel, was intentionally jammed and eventually had its license revoked because its broadcasts promoted terrorism and violence. In 1997, Indonesia intentionally interfered with and denied the services of a commercial satellite belonging to the South Pacific island kingdom of Tonga because of a satellite orbital slot dispute. In one instance, the leader of a Chinese hacking group claimed to have temporarily disabled a Chinese satellite and to have formed a new global hacking organization, known as the "Yellow Pages", to protest Western investment in China. "Many of these companies have computer networks and there are a lot of members in the Yellow Pages who have excellent hacking skills," (Hesseldahl), he said in an interview held by a United Nations representative.

Other experts are considering scrambling, as implemented for video broadcasts. But with chips coming on the market for $2,000 or less, to decode 40-bit Data Encryption Standard (DES) at speeds close to real-time, most security experts remind us that weak encryption is inadequate for sensitive traffic.

Another solution is for satellite companies to try to launch their satellites with strong encryption and then negotiate to whatever encryption level is mutually satisfactory to the nations involved. But winning approval to launch with strong encryption is not as simple as it sounds. The U.S. government, for example, prevented protecting the control information stream used for the Optus system it manufactured for an Australian group, because the launch was to occur in China. While policies seem to have changed since then, some countries would still be questionable. Some suggest that what is likely to happen is for U.S.-based constellations to launch with strong encryption that can be used only within U.S. boundaries; thus broadband satellite providers can encrypt uplinks to the satellite over the United States, but downlinks to another nation will remain in the clear. However, currently the U.S Federal policy regarding the security of commercial satellite systems is still limited because it only pertains to satellites used for national security purposes, only addresses security techniques associated with links, and does not have an enforcement mechanism for ensuring compliance. Also, even if providers find a way to surmount export issues, they still face a very fractured world of multinational security policies, as illustrated in the figures below.

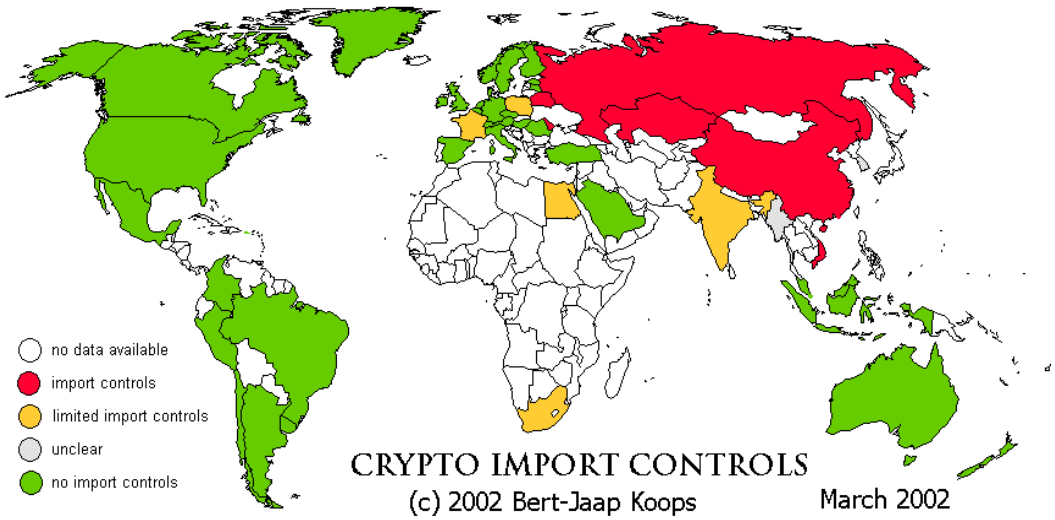

Figure 2 – “Cryptography Import Controls” (Koops)

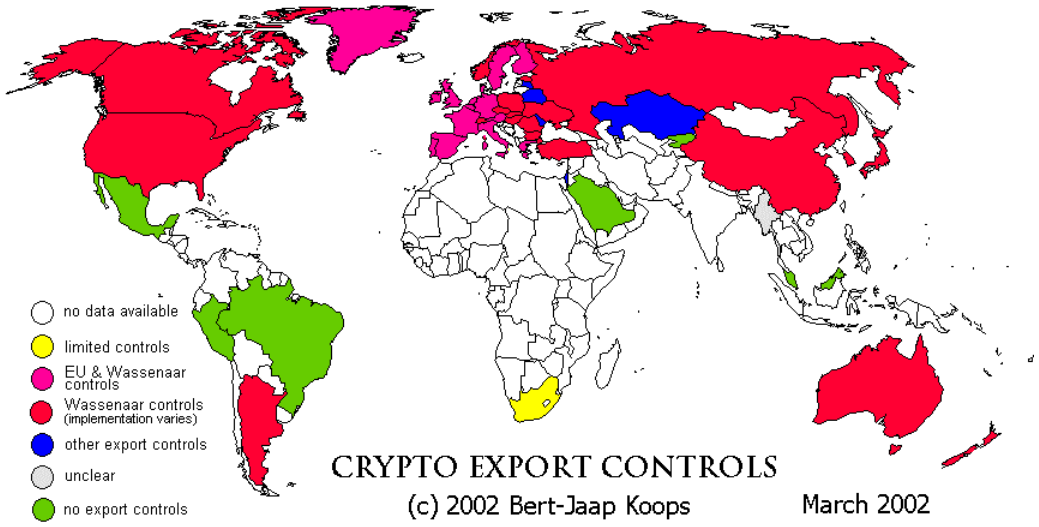

Figure 3 – "Cryptography Export Controls" (Koops)

The Wassenaar Arrangement referred to in figure 3 is an arrangement controlling the export of weapons and of dual-use goods, which means goods that can be used both for a military and for a civil purpose, such as cryptography. Refer to Koops' "Crypto Law Survey" (Koops) for an extensive description of this arrangement.

Market Trends

Before any efforts are made to secure satellite communication, it is important to know whether the market reserves a need for this industry in the future. According to Futron Corporation, a technology management-consulting firm, a ten-year forecast, made in 2001, for satellite demand shows that the business is somewhat volatile but with a solid base and a strong growth potential. Satellites will continue to be required to meet key telecommunications service needs. These needs are not spread uniformly in either time or geography, and each individual market demonstrates distinct patterns of demand. Key findings of the forecast show that in both the short and longer term, there are opportunities as well as issues to be faced. The number of on-orbit geostationary commercial satellites will grow by some 30% from 2001 to 2011. Demand for satellite will grow much more quickly than the number of satellites. The figure below shows the global demand for satellite service for the next nine years.

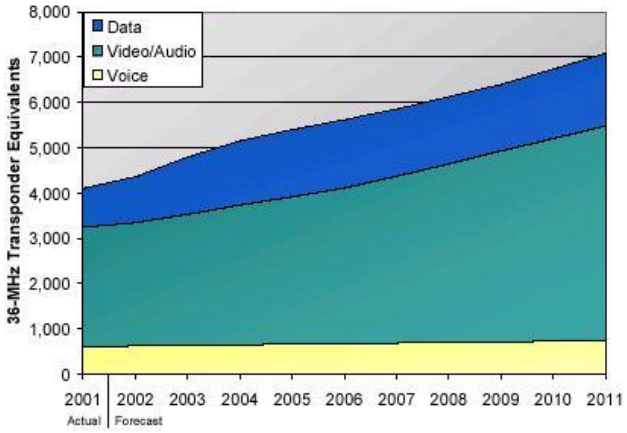

Figure 4 – "Global Demand for Satellite Services" (Futron, p. 3)

Twelve commercial geostationary communications satellites were placed in orbit in the first half of 2002 and at least ten more such satellites are scheduled to launch this year. The obvious market for commercial satellite communication exists in locations with underdeveloped communications infrastructures. The main problem satellite system is solving lies in getting high-bandwidth access to places without a high-bandwidth infrastructure. In some countries, stringing copper or fiber is simply impossible because the empty distances to cover are too great and the available money is too little. "For some applications, landlines will always be superior. But when your reach is diverse and you have last- and first-mile problems, then satellite will be the better choice," (Montgomery), says Edward Fitzpatrick, Hughes Communications' vice president. The second market that most broadband vendors have identified exists in low-population areas. They state that it is unlikely that a satellite system could compete with Digital Subscriber Line (DSL) to the home or fiber to the office, if those services are available. Still, in a low-population area, these services may not be available. Satellites will deliver them, enabling not only high-speed Internet browsing, but all forms of high-speed networking, including such things as videoconferencing, collaborative work sharing, and telemedicine. The industry seems to agree that satellites are here to stay because their advantages are immense. Not only can the signals sent by satellites positioned in geostationary orbit directly reach whole countries and even continents, but they are also optimal for all broadcasting services: TV, radio, data or any other new services. Moreover, new services can be deployed quickly, in that satellite signals are sent directly from the satellite to the end user, while terrestrial networks would need lengthy upgrades of the infrastructure. Also, the versatility of satellite communication systems makes them very suitable for infrastructures that need a quick deployment, such as for emergencies or disaster relief. Satellite technology can also provide specific high-capacity links on demand, for example for journalists transmitting videos of news, sports or other events from any place on the globe. From a cost perspective, the price of a satellite link is independent on the distance between the connected locations. While high-capacity trunks are usually being replaced

by fiber-optic systems, satellites continue to be a key element of thin routes of public networks in countries where the deployment of a terrestrial network would be unrealistic. In this case satellites are the most economical, and often the only solution.

Conclusion

The literature suggests that the industry is concerned about satellite security but undoubtedly a more pronounced effort is necessary to effectively deal with the current uncertainty. As the GAO reported, it is paramount for satellites to be identified as part the nation's critical infrastructure protection approach. Moreover, it is equally important that an international initiative is taken to implement end-to-end security for commercial satellites because the commercial satellite industry is also a critical component of the worldwide and national economy: "the industry generated $85 billion in revenue in 2000" (GAO, p.1). When or if this is done, perhaps we will sleep more peacefully knowing that we have created a robust security chain in the sky. Let us not forget however, that there is always a possibility all this will turn to worthless liquefied plasma in the case of a meteor storm – but as information security experts, let us not think of that for the time being.

References

GAO. “Critical Infrastructure Protection: Commercial Satellite Security Should be More Fully Addressed.” August 2002. URL: http://www.gao.gov/new.items/d02781.pdf (15 January 2003).

Koops, Bert-Jaap. “Crypto Law Survey.” October 2002. URL: http://rechten.kub.nl/koops/cryptolaw/ (19 January 2003).

Koops, Bert-Jaap. “Summary of International Crypto Controls.” October 2002. URL: http://rechten.kub.nl/koops/cryptolaw/cls-sum.htm (19 January 2003).

Futron. “Satellite Steer Into the Future: Course is Strong, If Not Steady.” 12 August 2002. URL: http://www.telecomweb.com/papers/Futron%202002%20Forecast%20White%20Paper1.pdf (19 January 2003).

CompassRose International Publications. “Introduction to Global Satellite Systems.” 1999. URL: http://www.compassroseintl.com/pubs/Intro_to_sats.html (17 January 2003).

Americans for Computer Privacy. “Myths vs Realities.” 2003. URL: http://www.computerprivacy.org/myths/ (17 January 2003).

Hesseldahl Arik. “Hacking for Human Rights.” 14 July 1998 URL: http://www.wired.com/news/politics/0,1283,13693,00.html (17 January 2003).

Hudgins-Bonafield, Christy. “Networking in the 21st Century: The Sky’s the Limit.” 15 March 1998. URL: http://www.networkcomputing.com/905/905f2.html (19 January 2003).

Hudgins-Bonafield, Christy. “The Achilles Heel Of Next-Generation Satellites.” 15 March 1998. URL: http://www.networkcomputing.com/905/905btb.html (17 January 2003).

Montgomery, John. “The Orbiting Internet: Fiber in the Sky.” November 1997. URL: http://www.byte.com/art/9711/sec5/art1.htm#117covb2 (January 19 2003)

Last Updated: September 25th, 2017

Upcoming Training

SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event