Global Information Assurance Certification Paper

Incorporating Biometric Security into an Everyday Military Work Environment

Russell B. Farkouh

May 12, 2004

SANS GIAC GSEC Practical

Version 1.4b, Option 1

INTRODUCTION

Within day-to-day operations of the US Military, there are many places where biometrics can be implemented to yield convenience, increased security, an audit trail for forensic examination and in some systems a reduced Total Cost of Ownership (TCO). Areas where the Privacy Act of 1974 is a driving force and where security will be enhanced, as well as medical, dental, forensic, dining, payroll, training, communications and military computing services will all be greatly impacted. This is in addition to non-Privacy Act functions such as logical access and physical access to facilities. Moreover, incorporation not only includes the biometric devices themselves, but an enterprise architecture that involves databases, Public Key Infrastructure (PKI) and networking protocols. Migration to and incorporation of biometrics will significantly improve operational readiness and result in lowering the TCO while increasing security.

ABOUT BIOMETRICS

Biometrics can take several forms and is still very much an emerging technology. The term Biometric comes from the Greek words for 'bio' (life) and 'metric' (to measure) [1]. Biometrics is used for the authentication of an individual. It is important to remember that the two components of authentication are identification and verification. Identification is determining who a person is. Verification is determining if a person is who they say they are and the granting of privileges based on that determination. In biometrics, verification is the collection of a measured characteristic and making an exact match with a previously recorded data template of the same characteristic in a database (or on a token with the template placed on it). Current means of using biometrics include iris and retinal scanning, facial recognition, voice recognition, fingerprint, hand geometry, body scanning, vascular patterns, and facial recognition. Other technologies involve keyboard usage pattern and signature (handwriting) matching. The device can take several readings of the subject and create an electronic template, which is stored in a database. This template is what will be used for comparison to the live reading when access is required. Some systems allow for the template to be pro-active in updating of the template- this allows for the changes that aging or other events can present to a person's appearance. With fingerprint or hand geometry for example, individuals who perform heavy work with their hands (such as construction, landscaping, carpentry, etc.) are susceptible to cuts and skin changes, which will impact the reading a biometric device would take.

Biometrics actually dates back to the fourteenth century when Chinese merchants would take palm and footprints to distinguish babies from one another. In the 1890's an anthropologist and police desk clerk named Alphonse Bertillon developed a series of body measurements as a means of identifying convicted criminals. The system was used until proven to be too prone to error. By far, the most common biometric technique is fingerprinting, which has its current origins with in 1901 Richard Edwin Henry of Scotland Yard. Mr. Henry modeled his fingerprinting on the Chinese system used centuries before. Fingerprints fall into three major classifications- loop (65 percent of fingerprints), whorl (30 percent of fingerprints), and arch (5 percent of fingerprints). The loop resembles a balloon at an approximate 45-degree angle, the whorl is a circular pattern similar to a hurricane and the arch is an arch with a series of lines running horizontally underneath. The print itself is comprised of ridges, the elevated portion of the fingerprint, and the furrow, which are the lower portions. It is not the ridges and furrows which make a finger print unique, but the ridge endings, splits, split and join, and dots of the fingerprint. This is what is called 'minutiae', which is comprised of ridge endings, bifurcations, ridge dots and enclosures. A representation of the fingerprint is converted into a digital representation, this occurs before the data is even sent from the acquisition device to the receiving or storage device [2]. Many biometric templates for other measures (voice or facial recognition, hand geometry) are created and stored in the same manner with a digital representation of the physical reading.

It is possible to obtain a false rejection (Type I error) or a false acceptance (Type II error) when reading a biometric sample. The Crossover Error Rate (CER) is the point at which these two rates intersect. The lower the CER is, the higher the accuracy of the apparatus. Another type of error is Failure to Enroll (FTE) where the template is unable to be taken from the individual attempting to lodge a template in the system. For instance, some demographic categories are unable to furnish fingerprints due to the shallow depths of the ridges in their fingerprints. Notwithstanding the difficulties that biometrics faces, it has proven to be a highly reliable and cost-effective means of securing both logical and physical assets.

THE REQUIRED INFRASTRUCTURE

The Common Access Card (CAC) that all Department of Defense (DoD) personnel are presently required to carry contains a 32 KB Integrated Computer Chip (ICC) with three digital certificates, one for digital signature, one for identity, and one for encryption. A digital representation of the card holder's fingerprint is already placed on the card at the time of issuance. It is also placed into the Defense Eligibility Enrollment Reporting System (DEERS), which is the DoD database for human resources and personnel. DoD is in the testing phase of a 64KB ICC on the next generation of cards. It would be possible to place a digital template of the cardholder's biometric on the card within the new allotment of space. That will enable biometrics to be implemented in a timelier manner within

the Military community. Also being experimented with presently are 'contact-less' CAC cards, which can be read by a scanner or card reader rather than having to place the card into a reader. Contactless CACs not only expedite usage, but will also permit people with disabilities to use the biometric devices and gain access. A biometric template would be placed onto the card and then the 'live reading' takes place for comparison. Another extension of this would be to add the dimension of 'something you know' for a third factor of authentication. Comparison of the biometric template on the card, the live biometric reading for comparison and the entering of a PIN number would enhance security to an even higher state.

Presently, the largest rollout of an enterprise biometric smartcard solution is a pilot project occurring in South Korea, Japan, and Europe; but not in the United States according to Kenneth C. Scheflen who briefed the Biometric Symposium 2004 in Washington DC. Mr. Scheflen, the director of the Defense Manpower Data Center, said the pieces are not all there yet for an enterprise biometric solution. Vendors products are still closed to interoperability, he said, and the algorithms used for fingerprint comparison remain proprietary. So far, there are about 650,000 military users and contractors registered in the Defense Biometric Identification System (DBIDS) at European sites, Japan, Kuwait, and the Naval Postgraduate School at Monterey, Calif. Although DoD continues to push vendors toward an interoperable smart card business model, it has managed to badge individuals without DoD credentials in the largest biometric access program in the department according to Mr. Scheflen[3]. The non-credentialed individuals are local nationals- non-military, support personnel located in Korea.

Databases will be a critical piece of the enterprise biometric architecture and their reliability will be crucial. The driving force behind the military's use of biometrics is the DOD Biometrics Enterprise Solution, which aims to store biometric credentials in a central repository for use with whatever biometric authentication systems are employed by DOD anywhere in the world .A warfighter's fingerprints would be collected once, for example, and he or she could then use a fingerprint reader at any military installation. The same would go for iris, face, voice or handprint biometrics. Biometric templates would be downloaded from DOD's central repository to local storage at the user level so warfighters wouldn't have to enter their biometrics into the local system every time they arrive at a new location. The question is how to get those templates from the central repository when needed and how to do it in a timely and cost-effective way [4]. The DoD biometric database is located at the DoD Biometrics Fusion Center in Bridgeport, West Virginia. While some biometric implementation has taken place and templates are being made from samples, retroactive template collection would have to be made from service members already on duty. Biometric data is being collected from new members entering the military either at their enlistment stations or at their Basic Military Training stations. Similar arrangements would also need to be made for DoD civilian and contractor personnel in areas where biometrics is yet to be implemented. The architecture must be able to provide

the template to the biometric device reading the scan from the individual in a narrow timeframe, otherwise the person requesting access could lose patience and abandon the access attempt. This can potentially defeat the purpose of the device; the goal is not to prevent access, but to ensure those legitimately requiring access are granted it in a timely and secure manner.

The database must function quickly and the network must be able to support high speed, secure communications between the device and the database. Speed is a wonderful feature, but security is paramount. Databases must be hardened and physical access policies strictly enforced. One of the primary concerns among the user population is privacy and the thought that they are 'giving away' their personal information. While most people are willing to give personal information in the name of security, most question the ability of Government to safeguard that data. These users must be truthfully educated about the security measures implemented to ease these legitimate fears and to encourage the expansion of biometric technology.

Not only must the database be hardened, cryptography must be employed to protect the data while it is in transmission between the database and the devices. A Symmetric Key algorithm would be the more advantageous method since it would address the concerns of operational speed and data protection. While sensitive in nature and requiring protection, biometric data does not necessitate the elevated security requirements of classified data. Employment of PKI would hamper the attempts of those who desire to access and destroy or replicate biometric templates for masquerade purposes. Again, it eases the concerns of acceptance within the user community and promotes the advancement of biometrics within the security field.

Network redundancy and updating is also a key element of this architecture. One of the 'lessons learned' in the aftermath of the September 11, 2001 tragedy was that many companies had either no back-up computing facilities or had the back-up facilities within the same geographic or even physical location. Losing a database in this architecture will result in a complete denial of service to all users- a very attractive prospect to an intruder or attacker. At least one back-up database should be established in a separate power and water grid to prevent a loss of data in the event of an emergency, network failure, or attack from an intruder. Currently, the financial industry is under a Federal Government mandate to create such database redundancy. The primary database should replicate its data to the backup databases frequently to ensure that the most up-to-date biometric templates, user profiles and related data remain available.

Should a full-scale enterprise biometric solution not be possible or desired, use of biometrics in a simpler two-factor authentication solution may still be possible. Using a fingerprint template embedded on the CAC to compare to a live sample

from the service member would be feasible and less costly. The Navy has experimented with such a system, which will be discussed later in this paper.

POTENTIAL USES FOR BIOMETRICS

Scanning military personnel when they are wearing chemical warfare attire is by far one of the greatest biometric challenges to the military community. The DoD Biometric Management Office (BMO) has successfully tested iris-scanning technology with service members in chemical warfare attire; which is configured such that no part of the body is exposed. The iris scan can read iris patterns through the eye lens of a gas mask and provide the same reliability and security of other biometric devices. Since the CAC has the digital representation of a fingerprint of the holder placed on the ICC at the time of issue, fingerprint technology would be the most logical biometric to use initially. A National Institute of Standards and Technology report last year on biometric technologies found that the print from one index finger can provide a 90 percent probability of verification with a 1 percent probability of false acceptance for verification. It also concluded that the use of prints from more than one finger increased system accuracy [5]. Recently, one vendor has developed and deployed an innovative fingerprint technology that can overcome the difficulties, which a chemical warfare suit will pose. The vendor, Ultrascan, has incorporated ultrasound technology into the capture of the fingerprint. Ultrasound has been use by medical practitioners for many years to examine the unborn fetuses of expectant mothers, and to examine patients with abdominal ailments. The two key benefits to DoD with this technology are (1) that the device can now capture fingerprints from certain demographic groups where fingerprint capture had previously been very difficult; and (2) the ultrasound can read the print through the latex gloves which are a part of the chemical warfare suits. Through use of these technologies, the key challenge to deploying biometrics within DoD may have been overcome.

Within the Military community, there are several functional areas where biometrics can provide operational efficiency, increased security, audit trails and non-repudiation. Deploying biometrics to offices such as the Accounting and Finance, Training, and Personnel will ensure that compliance with the Privacy Act is adhered to- only the authorized staff member and the actual service member will be able to view the personal information. In the case of Finance where monetary disbursements are involved, the ability to have an irrefutable audit trail to trace questionable transactions and prove definitive involvement can prove invaluable to investigative efforts. With identity theft becoming a more prevalent issue within society, the financial industry has been using biometrics to combat fraud. Fingerprint scans are now conducted at ATMs in Australia, iris

scanning has been used in Japanese ATMs, and Chase Manhattan Bank has tested Voice Recognition in telephone transactions. [6]

A military dining facility is another place where biometrics could prove useful. On occasion service members do not have their meal cards, are in a Temporary Duty (TDY) status on a different installation or may be in the process of in-processing onto a new duty installation and have difficulty proving their meal entitlement. Not only will a fingerprint scan prove useful in resolving these issues, it will expedite dining hall operations during peak usage periods. Rather than having to search for a meal card and a CAC, now service members could simply place their fingerprint on the scanner and be approved within seconds. The same holds true for members receiving Basic Allowance for Subsistence (BAS), those members can have the cost of the meal deducted electronically from their payroll account. Once the approval process is completed, usually within seconds, members can dine and return to their regular duties in a more expeditious manner. Efforts are underway to utilize the CAC to accomplish the debiting from service members pay for meals; biometrics will expedite a process already in development and possibly eliminate fraud.

Similarly, access to the Commissary, Post Exchange, and other installation facilities can be expedited. Presently, a Herndon, Virginia firm named Biopay uses biometrics in the commercial sector. Customers who have previously established a fingerprint template and credit card information with the firm simply place their fingerprint on the reader at the point of purchase and the money for the transaction is automatically debited from the customers account; its as though biometrics were applied to the principle of the popular EZPass and Smart Tag currently used on interstate roadways. EZPass and Smart Tag are unique magnetic devices that are place on the inner windshield of a car and permit motorists to pass through toll lanes on roadways without having to stop to pay the toll; they continue driving and the toll amount is automatically deducted from their prepaid account. The biggest biometric challenge in the commercial sector has been acceptance within the population of customers, but this is a challenge with any biometric system and is one that can be overcome with strong security implementation and effective consumer education. Transactions are completed much faster and non-repudiation is assured, plus fraud is significantly reduced.

Military medical applications are another area in which biometrics could have a significant impact. With medical records now automated and HIPAA compliance a major issue facing the medical community, biometrics could provide the same authentication, audit trail and non-repudiation benefits discussed previously. Use of biometrics would enable a service member to go to any medical facility, including facilities that do not have that person's medical record on file. The service member could be authenticated based on his/her biometric instead of

requiring him/her to produce a Military ID; his/her entitlement to health care could then be verified by locating the biometrically authenticated person's name in the database of eligible service members. Used in this way, biometrics could ensure that a service member would receive treatment even if he/she were unconscious or otherwise incapacitated. The portability of medical records, including current and previous treatments, and authentication of a person could make the difference between life and death. Additionally, this technology can be leveraged and be extended to current theaters of operation such as Southwest Asia for forensic identification of service members who are injured or killed. Again, in a combat theater a simple fingerprint scan (or other biometric measure) can immediately access a member's medical records as medical treatment is being administered. One manufacturer has deployed a biometric device in a methadone rehabilitation clinic in Buffalo, New York. In that case, the client of the clinic places their fingerprint onto the device and the appropriate medicine and dosage is dispensed for the recipient automatically. Not only is authentication, the key function, now assured and records of dispensing available- but also the incidents of misdiagnosis or incorrect dosage have become virtually nil. The patient receiving the treatment does not have to bring personal identification; he/she can simply present them self at the clinic for treatment. Moreover, this device eliminates the possibility of patients receiving treatments to which they are not entitled. This same device has been deployed in the state of Ohio for automated prescriptions. In this configuration, the physicians writing the prescription use the fingerprint scanner to authenticate themselves to the on-line service. Once the authentication is complete, the physician can now enter a prescription on-line for the patient to pick up at their local pharmacy. Again, enhanced security and auditing potential are now added to a system previously lacking both and the incidents of mis-prescribed or incorrectly filled prescriptions have decreased dramatically. While identification and credentials may be forged, a biometric cannot. The end result is that lives can potentially be saved, efficiency increased, records automated, and costs reduced.

Some within the military community have entertained thoughts of introducing biometrics to tactical weapons or field communications systems. Vendors have offered a USB key ring token with a fingerprint reader on it as a means of accomplishing tactical biometrics. This is an inherently dangerous prospect and one that should have all aspects carefully considered prior to implementation. While it will be advantageous to enable systems in such a way as to only allow US personnel (or allied personnel) to utilize a system and prevent the enemy from seizing and using the asset; it could come at the risk of those same friendly forces not being able to offer a biometric sample in the heat of combat to engage the weapon system. Unfortunately, the living conditions experienced in the field can make fingers and handprints difficult to read from dirt, fluids and debris. Should hostilities be experienced and warfighters injured through battle, the very body parts necessary to prove identity may now be damaged too severely to

offer an accurate read to the biometric scanner. The inability to offer a valid scan will prevent personnel from accessing the very systems they need to fight the enemy and survive the heat of battle. A weapon or system does US personnel no good if they cannot use it at the key moments it is designed for.

Record access, record updating, audit trail and counter terrorism interests are only one portion of the overall benefit that the Military can realize from biometric implementation. Physical and logical accesses are also key benefits of biometrics. Physical access can not only be controlled to facilities within the post, but onto the entire installation itself.

Physical access is one of the primary benefits of this technology. While security personnel are still staffing entry points at peak usage hours, the volume of security personnel has been sharply reduced in some locations where biometrics has been introduced for access to a base. This has resulted in financial benefits and the ability to shift security personnel to other areas. The Ultrascan device described previously has been utilized in the colder outdoor climates of Northern Canada, so severe cold weather thus far has not proven to be a factor. The commercial aviation industry has utilized biometric devices at major airports such as Chicago O'Hare (the worlds busiest airport) and Charlotte/Douglas International. In each case biometrics was employed to restrict access, Chicago used it in an outdoor environment to speed cargo deliveries. Israel's Ben Gurion Airport uses hand geometry to speed along passengers and Iceland's Keflavik Airport uses facial recognition for surveillance applications [7]. Biometrics can be used as part of an access control system to restrict access to a room, a building, a collection of buildings or an entire installation.

Similarly, biometrics can be used to control logical access. This would be access to systems and assets based on user permissions and need-to-know. This is the same principle that computer operating systems have when granting user permissions to files, folders, and systems within a domain or a network. Biometrics can overcome the prevailing challenges that systems face, with passwords and PIN numbers being targeted or easily guessable and or CAC being lost, misplaced, or damaged. This will be of particular benefit in the areas of communications, intelligence, and computing. Savings can be realized from the implementation of biometrics in that PINs and passwords that are forgotten or lost no longer would need to be reset; which eliminates one burden on help desk personnel and thus reduce the staffing of those positions. The economic benefit from this alone could be substantial over time. When factoring in the costs of lost productivity and the economic gain from increased security, the decision to implement becomes clearer. Biometric implementation will be a significant step in the efforts to ensure that only those individuals with the proper permissions and 'need to know' are granted access to sensitive and classified information.

WHAT THE SERVICES ARE DOING TODAY

The US Air Force has successfully deployed biometrics to Aviano Air Base, Italy and to Scott Air Force Base, Illinois to control base access [8]. In the case of Scott AFB, the biometric device was placed at a main access point nearby a commuter rail station that has peak usage at morning rush hour. Personnel can now access the base faster and security forces have been able to be repositioned rather than support this entry point that has been automated. While they have experimented with biometrics to assist in target acquisition and sensory systems [9], the greatest Air Force biometric activity has been in evaluating fingerprint recognition and handprint geometry for physical access purposes. The US Navy has conducted tests involving 'contact-less CACs' and biometrics for physical access. Essentially, the fingerprint or hand geometry template is placed on a second ICC chip on a CAC. The holder will scan or wave the card in front of a reader and then place the finger (or hand if applicable) onto the reader to compare for a match [10]. Additionally, the Navy is experimenting with voice recognition biometrics as a means of providing safe and reliable authentication in unique situations [11]. Use of this technology also involves the introduction of noise-suppression technology. Since the Navy has the unique benefit of ships being a self contained warfighting center, it has experimented with introducing biometrics to weapons, communication, and command and control systems aboard seagoing vessels. Whereas the Army and Air Force have land-based operations and enabling these systems will pose serious tactical challenges for usefulness and security, the Navy is exempt from the difficulties in large part. The one challenge the Navy has encountered involves inconsistent Operating Systems on its computers, whereas most off-the-ship systems are Windows compatible. The Navy still employs many legacy systems and is working with Johns Hopkins University on applying biometrics to legacy systems.

The DoD is currently using Automated Fingerprint Identification Systems (AFIS) in its counter-terrorism efforts. A fingerprint template is collected at the time of detainment from a suspected terrorist and sent to a repository via a Wide Area Network (WAN) in an encrypted format for security. Should sites in other parts of the world need this template, it is dispatched from the central repository to the requesting site in encrypted form. Presently the US Army is accepting requirements from its proponents to employ biometrics in the area of counter-terrorism. Federal Government agencies conducting counter-terrorism activities and operating in Southwest Asia have enjoyed great success in their efforts through the implementation and employment of biometrics as a means of identifying known terrorists. These agencies have literally implemented identity

management where there has been no such effort ever before. The results have been impressive and substantial- many individuals with known ties to those who desire to harm US interests have been taken into custody and questioned for intelligence purposes. The echo effect from the information collected has been of great value in the ongoing war on terror. During the war with Iraq in 2003, one challenge posed was from enemy combatants masquerading as US service members; biometrics will instantly identify someone as a legitimate US combatant or the absence of a database profile will indicate an imposter. Since the war on terror is an endeavor that will remain a primary mission of the US military for years to come, identity management and biometrics will also follow as a key mechanism in performing and succeeding in that valuable effort.

CONCLUSION

Overall military operations will be impacted tremendously with the adaptation of present day, commercially available, biometric systems. PIN's may be forgotten or socially engineered; CAC's are susceptible to loss or identity theft; the biometric is completely unique to the each individual. Each person's finger has a different pattern from the others, each iris and retina not only unique to the individual but differ from each other on the same person. No two irises and retinas are alike, even on the same person. Using biometrics as a primary, secondary or even third factor of authentication can prove to be an invaluable tool. Individuals previously able to defeat security systems will now have the insurmountable task of having to impersonate the biometric of an authorized person in order to achieve the same access. Used in concert with a CAC and a PIN will make systems even more secure than with simply one factor authentication. Integrity, authentication, auditing capabilities and non-repudiation will be enabled to systems previously susceptible to common intrusion tactics. Areas that traditionally are susceptible to privacy issues and poor operational security, such as Accounting and Finance or the medical community can now be automated and the tenants of information assurance implemented. Access can be strictly regulated and policies better enforced. The medical community would now be empowered to have patient records appear on a monitor both accurately and immediately. Personnel that are in transit can now be assured that they may receive the same meal and healthcare entitlements they would receive ordinarily in a garrison situation. Commercial aspects of military life may now be automated to increase readiness and reduce overall operational costs. Fraud may now be reduced significantly due to the uniqueness of each individual's biometric signature. Counter terrorism efforts can be greatly enhanced to a high level and have the worldwide reach to match that of those who wish to harm US interests. Manpower requirements could be reduced or repositioned to more critical needs - thus raising productivity, time saved, and significant financial benefits could be realized. Most importantly, lives will be saved.

REFERENCES

1. "An Overview Of Biometrics." National Center for State Courts and State Justice Institute E-Court Conference. 9-11 Dec. 2002. 12 May 2004. <http://ctl.ncsc.dni.us/biomet%20web/BMOverview.html>.

2. Chirillo, John and Scott Blaul. *Implementing Biometric Security*. Indianapolis: Wiley, 2003.

3. Menke, Susan M. "DoD tries out biometric smart cards overseas." Newsbytes News Network, 22 Mar 2004. 12 May 2004. <http://security.ittoolbox.com/news/dispnews.asp?i=111796>

4. Robinson, Brian. "Who Goes There?" FCW.com. 30 Jun. 2003. 12 May 2004. <http://www.fcw.com/fcw/articles/2003/0630/cov-bio3-06-30-03.asp>

5. Walker, Richard W. "Security: Biometrics Gains A Foothold." Government Computer News. 5 May 2003. 12 May 2004. <http://www.gcn.com/22_10/biometrics/21976-1.html>

6. O'Sullivan, Orla. "Biometrics comes to life." ABA Banking Journal. Jan. 1997. 12 May 2004. <http://www.banking.com/aba/cover_0197.htm>

7. "Evaluating Biometrics for Airport Security An Overview." 04 Oct. 2001. 12 May 2004. <http://www.biometricscatalog.org/asbwg/Files/Evaluating_Technology_Program_Plan.pdf>

8. "U.S. Air Force Selects IR Recognition Systems HandReaders to Lend a Hand Securing Their Bases." Technology Marketing Corporation. 03 Mar. 2004. 12 May 2004. <http://www.tmcnet.com/usubmit/2004/Mar/1024753.htm>

9. Tirpak, John A, and Adam J. Hebert. "AFA 2003 National Convention, Toward a New Style of Warfare." Air Force Magazine. Nov. 2003. 12 May 2004. <http://www.afa.org/magazine/nov2003/1103warfare.pdf>

10. Conway, Robert. Capt. USNR, Fleet Liaison Officer, DON eBusiness Operations Office. "Access Approved: Biometrics and Smart Cards Open Doors to Improved Efficiency." Fall 2003. 12 May 2004. <http://www.chips.navy.mil/archives/03_fall/PDF/chipsfall03.pdf>

11. Guerrino, Dave. Navy Biometrics Program Overview Biometric Consortium Conference. 24 Sep. 2002. 12 May 2004. <http://www.biometrics.org/html/bc2002_sept_program/BMO_Guerrino_902.pdf>

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event