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.

# Biometrics: Are YOU the Key to Security?

In the United States, storage and retrieval of digital information is relatively commonplace. Our schools teach children as young as age four how to manipulate a mouse and keyboard. Even some families whose income falls below the national poverty level have a personal computer in their home. We play games, keep in touch, purchase items and to work, all from a computer. International Data Corp (IDC) reported worldwide sales of PCs of 31.4 million computers in the first quarter of 2002 (Lateline News). Considering the ea...

Copyright SANS Institute
Author Retains Full Rights

AD
Take control of vulnerability threats Now!
Request a Free Trial
Secunia Stay Secure

# Biometrics: Are YOU the Key to Security?

**Patricia A. Wittich**
**GSEC v.1.4b**

© SANS Institute 2003, Author retains full rights

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

The computer's role in our daily life has grown over the decades. PCs have evolved from large single-user systems to multi-user networks spanning national and international territory. Computers have become powerful, flexible and affordable, accommodating a wide range of uses and users.

In the United States, storage and retrieval of digital information is relatively commonplace. Our schools teach children as young as age four how to manipulate a mouse and keyboard. Even some families whose income falls below the national poverty level have a personal computer in their home. We play games, keep in touch, purchase items and to work, all from a computer. International Data Corp (IDC) reported worldwide sales of PCs of 31.4 million computers in the first quarter of 2002 (Lateline News). Considering the ease of use, early training, the common practice of digitizing information, and the sheer numbers of computers, it is no wonder that cyber crime is steadily increasing. Cyber crime is sometimes hard to detect and even more difficult to prosecute. The more sophisticated the defenses, the more sophisticated the criminal. How do we fight this trend? Leaders in information technology are touting the prospect of biometrics as a safeguard against some information attacks, especially since 9/11. This paper will discuss the concepts behind the emerging biometrics craze along with its efficiency, cost, privacy issues, and success versus failure rate.

**Emergence of Biometrics**

Biometrics is not a new concept; it is the oldest form of identification. As early as the 14th century, the Chinese were reportedly using fingerprint-like methods as a form of identifying their children (NCSC, fingerprint). During the late 19th century, police authorities throughout the world used a method of bodily measurements called Bertillonage. This method was time consuming, and in 1903 when two Fort Leavenworth prisoner's measurements produced identical results within a given tolerance, Bertillonage lost its popularity and usefulness to fingerprinting (NCSC, body).

The term "biometrics" is derived from the Greek words bio and metric, meaning life and to measure, respectively. Biometrics can be defined as the science of identifying or verifying individuals based on unique physiological or behavioral characteristics. Examples of human traits used for biometric recognition include fingerprints, hand geometry, speech, face, retina, iris, and handwritten signature (Heath, history).

There are three basic, independent but related concepts to security:

1. Identification – who you are,
2. Authentication – proving who you are, and
3. Authorization – what you are allowed to do.

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

Biometrics is used to perform either identification or authentication, the latter being the most common application. In identifying, a sample is presented to the biometric system during enrollment. The system then attempts to determine if a biometric record exists for the sample by comparing it with a database of samples in the hope of finding a match to determine the identity. This is most commonly associated with fingerprint analysis in crimes. In authenticating, the biometric system attempts to verify an individual's identity by capturing a new sample and comparing it to a stored template. If the two samples match, the system confirms that individual is who they claim to be. The main difference is that identification compares a sample against a database of many and verification compares a sample against a database of one. Both methods involve a four-stage process: capture, extraction, comparison, and result (match/non-match) (Podio, Introduction).

The computer industry began using biometrics over ten years ago. However, as with the first computers, biometric systems were massive. Typically created for a specific function, they lacked the adaptability required to integrate into a variety of environments. This resulted in costly solutions that few were able or willing to incorporate. However, over time, as technology advanced and networking and device standards were created, biometric solutions evolved to be widely recognized as viable options to security solutions (Heath, role). Fraud, security breaches, and human administrative error are helping drive the expansion of biometric technology. The following are just a few examples of why biometrics has become a frontrunner in the attempt to find a solution of positive identification and verification.

According to the 2002 Computer Crime and Security Survey conducted by Computer Security Institute (CSI), along with the assistance of the FBI's Computer Intrusion Squad, ninety percent of the survey's respondents identified computer security violations within the last twelve months, with eighty percent reporting financial losses due to those attacks. Just over half of the eighty percent could quantify their losses, totaling a whopping $455,848,000. Over $286 million of the reported loss was attributed to theft of proprietary information and financial fraud. Although proprietary theft and financial fraud occur less often than other security breaches, they are more detrimental to a business causing much more damage (Power, pg 4-5).

The banking industry has reported false acceptance rates at ATMs to the tune of $2.98 billion per year and it has been projected that by the year 2006, financial institutions will lose $8 billion due to identity theft (Rusch). Public assistance recipients are registering under more than one name and/or at more than one location costing taxpayers an estimated $25 billion annually. A staggering number of prison escapees walk right out the front door, posing as someone else. Likewise, once released from incarceration, effectively monitoring more than 3.8 million parolees and probationers has become difficult without the ability

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

to positively identify the people (Page, Facing). Then there are the events of September 11, 2001 that has renewed the fear of terrorism worldwide.

**Efficiency**

Biometric based authentication applications include workstation, network, domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. There are three types of authentication:

- Something you know (most common is a password or pin)
- Something you have (tokens such as a smart card), and
- Something you are (biometric)

Since biometrics is based on the premise that the characteristic measured is unique, a biometric is considered by some to be the most appropriate authentication tool. While a password can be forgotten, an ATM card can be lost or stolen, you will never leave behind a finger (short of amputation) or an eye or conveniently misplace your voice box. And although not impossible, a biometric is difficult to forge (Liu & Silverman).

If biometrics is used for authentication, a password is not necessary. This is appealing to many businesses as well as individuals. Passwords can be laborious, expensive, easy to forget, and ineffective against hackers. In order for a password to be truly effective, it should be at least eight characters in length and chosen at random. Having a person choose an eight-character password is not difficult; but having them choose randomly is very difficult. Any individual successful in selecting a "difficult" password then has the dilemma of remembering it. If that is not enough, just imagine how many passwords the average IT person employs. According to the 2002 NTA Monitor Password Survey as reported by Graham Hayday, the average intensive IT user maintains over twenty passwords, with some managing up to seventy passwords. In order to cope, the user either chooses simple, easy to remember passwords or writes the passwords down. Neither of these options is acceptable from a security standpoint.

The majority of people rely upon the memorability of a password. Therefore, they often select common words, which can make passwords a company's biggest vulnerability. Take for instance a health care company that hired a security firm to find vulnerabilities in their system. Using "John the Ripper" software, the security company was able to decipher 30 percent of the passwords for nearly 10,000 accounts in one hour. Since well-chosen passwords could take years to crack using the ripper software, it is evident that simple passwords are a major weakness in their security (Lemos).

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

Although poor passwords may not make it easier to break into a network, it sure makes an intruder's efforts worthwhile. Once passwords have been discovered, an intruder can wander the network as a valid user, gathering information at will. Since most organizations still rely only on passwords for employee authentication, many are left exposed.

Another advantage of biometrics versus passwords is that the more complicated a password is, the more difficult it is to remember. This results in spending IT time and money to unlock or change passwords to user accounts (Lemos). "Fortune 500 companies currently spend upwards of $400 per year per person to reset forgotten, lost or stolen passwords" (Biometric Digest).

Guessing or cracking a password is not the only threat from a hacker. As security systems are strengthened, a hacker will exploit security's most vulnerable aspect – people. Social engineering is becoming more popular among intruders. A hacker may gather personal information through casual conversation, impersonating staff and asking for a password, or posing as a repairman to gain physical access. As networks and applications become more secure, it is thought that social engineering will become a more popular tool to gain unauthorized access (Turunen).

Social engineering exploits people's trust. Pentasafe Security Technologies did a study that revealed four out of five workers would disclose their password to someone in the company if asked. Another study by Pentasafe revealed that almost 67% of another company polled, when asked, revealed their password to the pollster – someone they did not know (Lemos, Giving away the keys).

With statistics such as these, it's no wonder that some businesses would like to have all network services accessible with each user requiring one password for authentication. Administrators would then need to compel users to pick strong, random passwords and change them regularly. This would eliminate the problem of remembering several passwords and which password goes to what application. The drawback, however, is that now the culprit need acquire only one password to access everything. Therefore, many companies have opted for two-layer authentication with a chip card or biometrics as the second layer of defense (Lemos, Picture this).

Besides addressing the fear of confidential data being compromised by unauthorized users, biometrics can aid in reducing administrative costs. By using biometric technology to secure physical access or to capture an employee's time at work, additional savings can be realized. Biometric timeclock systems would eliminate the overhead expense of processing time cards, dealing with lost or damaged cards, and it would eradicate the "buddy-punching" problem (Page, What's Ahead?). Kronos, Inc., a time management company, now offers labor management solutions and time and attendance/payroll solutions that utilize biometric technology. Aramark believes that using a biometric time clock

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

will pay for itself within two years, since it will ensure accurate payroll records as well as address the aforementioned attributes (Recognition Systems). Using a biometric reader at entrance points can eliminate the demand for security guards and save time for those required to sign in upon arrival (Liu & Silverman). Similarly, it would make a reliable audit trail available real time.

Biometric solutions have also been incorporated into many new computer notebooks and laptops. This is attractive to those who maintain confidential information in a portable computer. If the device is stolen, the data remains confidential since another user cannot access the contents of the hard drive.

Not to forget the growing use of m-commerce – business transactions using mobile devices. There has been a recognized need to secure these transactions, and biometrics is being introduced as a solution.

**Privacy**

Although there seems to be many positive attributes of biometrics, there is one concern above all others that has many individuals hesitant to readily accept biometrics – privacy. Many are apprehensive at the idea of personal information being collected and maintained in a database that can be shared with other companies and agencies. Since the concept of biometrics is uniqueness, the legitimate fear that someone can link incongruent database records that undeniably belong to one individual and use that information to monitor and to continue to build a personal profile without the individual's consent or knowledge justifies the apprehension. Other fears include the intrusive techniques used to authenticate individuals, the association of criminality with gathering personal characteristics such as fingerprinting, the potential for bodily harm from a terrorist extracting your identity based characteristic to gain access to your privileges.

According to Precise Biometrics' Mr. Obrink, however, we need not fear that a finger or hand will be cut off by someone wanting to gain access since "all biometric systems require a 'live' finger" (ebusinessforum, biohazards). Roberta Bragg, a security consultant, supports Mr. Obrink's opinion with the assurances from biometric scientists that within minutes of removing the blood supply from a finger, the unique "whorls and dips" lose the ability to be read accurately by input scanners.

In an attempt to alleviate the fear of "Big Brother", biometric developers are offering alternatives such as smart cards that can be used in conjunction with biometric readers that will not collect personal information and store it in a central repository. Instead, the encrypted template would be stored on the smart card possessed by the user. The biometric sensor would encrypt the submitted sample and compare it to the template stored on the card. If the two match, the individual will be authenticated and granted access. This will be an added layer

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

to security, but it would also the possibility of 'I forgot my…' would remain (ebusinessforum, biohazards).

Kronos, however, uses a different approach to privacy. They do not offer a smart card, but instead rely upon a technology developed by Bioscrypt, Inc. Instead of replicating and storing the actual image, Bioscrypt uses a patented recognition algorithm that utilizes the ridge pattern of the finger to convert the image into a mathematical representation (Kronos). Below is an illustration of how the image is converted to a digital representation.

Figure 1 courtesy of http://www.666soon.com/atm.htm

1. Customer places finger in pressure-sensitive pad.
2. Computer digitizes the pattern using a special algorithm.
3. The pattern is transformed into a 1,024-character record.

The 1,024-character record is the biometric template that is stored in the database. Each time the sensor is activated, it will convert the submitted sample to a digitized record and then compare that sample to the database for authentication.

In an attempt to reduce fraud, increase security, and gain approval from privacy advocates, biometrics will need to continue to find methods of encrypting biometric images that can serve to authenticate, as well as identify, without leaving an absolute surrogate of an enrollee's personal traits.

**Success/failure**

The issue of privacy is not the only obstacle that biometric solutions providers must overcome. There are "what-if" questions such as:

- What if I am a double amputee and the company uses some form of fingerprinting or hand scanning?
- What if I develop cataracts and the company uses a form of iris or retinal scanning?
- What if I have weakly defined fingerprints (elderly, temporarily damaged from burn or other injury, heavily calloused, etc.)?

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

These are questions that are being addressed. Although the amputee question would need to be solved by the company adopting a particular biometric method, the other questions have been answered through real-world testing. Take for example the premise that a "fake" finger cannot fool a fingerprint sensor. Tsutomu Matsumoto, a Japanese cryptographer, successfully fooled eleven different commercially available fingerprint readers eighty percent of the time by creating fake gelatin fingers using two different methods. The first experiment used readily available, inexpensive items to create a plastic mold using a live finger, which was then filled with a liquid gelatin. After the gelatin had hardened, it was removed from the mold and could be placed inconspicuously on the fingertip of another individual to gain access past the fingerprint reader. Once inside, the gelatin fingerprint can be consumed, eliminating the evidence. Although this method was simpler to create, Matsumoto experimented again using a "lifted" fingerprint from a piece of glass. After a little ingenuity and a series of steps, Matsumoto was again successful in creating a "gummy" finger that was able to fool the biometric readers eighty percent of the time (Schneider).

Although the sensors were not identified, knowing that eleven different manufacturers fell prey to artificial fingers is enough to make anyone skeptical of the security abilities that biometrics claim to possess. However, according to Rofin Australia Pty. Ltd., although no assurance can be made that anything is 100% failsafe, there are scanners available that include "liveness" detectors. These detectors have sensors that monitor blood flow or temperature, or measure an electrical attribute such as the "capacitive difference between the ridges and valleys of the fingerprint". Utilizing a more sophisticated detection technology does make these sensors more expensive. The lower-end "liveness" detectors generally measure moisture or test for 3D image and are somewhat easier to spoof (Rofin).

Another shortcoming of the biometric field is standardization. Although standardization is in the works, the industry currently lacks standardized guidelines that would allow interoperability of hardware. Also, once standardized, those companies already invested in biometric solutions may find their systems incompatible with future applications. There are companies that are utilizing architectures that support USB, serial bus, and parallel bus ports, as well as providing greater options for plug-and-play as the industry progresses toward standardization. Standards are emerging to provide a common software interface to allow sharing of biometric templates and to permit effective comparison and evaluation of different biometric technologies. The BioAPI standard release defines a common method for interfacing with a given biometric application. BioAPI is an open-system standard developed by a consortium of more than 60 vendors and government agencies (Liu & Silverman).

While not considered a failure, the invasiveness and complexity of some methods of scanning impede biometrics' rapid acceptance. But as environments demand additional security or alternatives to assist in streamlining business

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

practices, biometrics is becoming the answer. The more they are tested, the more the bugs are worked out and user issues are addressed. As with many technologies, biometrics is still evolving, responding to user concerns and business demands (Liu & Silverman).

A biometric approach that is not as well-known as fingerprinting or iris scanning may be one answer to many of the negative perceptions. BioPassword, a biometric application from Net Nanny Software International, Inc. uses unique typing pattern technology to authenticate a user. It does not replace the user id and password model, but builds upon it. A user is authenticated by the typing technique – strike, timing, strength and force. Ideally, the user's password typing technique is compared to a template on file to determine if the person typing the password is the same person for whom the password was created. If a correct password where entered for an individual but not the same technique template, access would be denied. Theoretically, this would make password cracking obsolete. According to Roberta Bragg's testing, installation was simple, it was not difficult to use, nor was it considered intrusive, and the product proved reliable. This type of biometric, however, does not eliminate the possibility of forgetting a password, nor does it address the issue of hand injury, which would affect a person's typing technique. The administrator would have the ability to allow the injured individual to reset their template. Providing that you have an additional administrator account setup for emergencies, you can accommodate any chances of injury, forgotten passwords, or untimely absence of the administrator. As with other technology, Net Nanny is working to refine the 'what ifs', such as answering a series of questions to allow an administrator access in case of lock-out. (Bragg)

As early as 1991, biometrics was successful in its intended application. The Cook County Sheriff's office of Chicago, Illinois put retinal scanning into effect to eradicate identity swapping. Within the first six months of 1991, they foiled 40 attempts to switch identities (Brakeman).

Many industries that require high security and regulations such the FBI, INS, DOD, banking and health industries have been using biometric solutions successfully. Many more biometric techniques are being tested (ebusinessforum, log on). As biometric use and demand increases, the technology will improve to meet those demands and despite some of the faults of biometrics, they have proven successful in increased security and efficiency.

## Conclusion

Biometrics can only guarantee that the individual is the same person they claimed to be when they obtained their biometric-based identity. Therefore, a potential disadvantage in choosing a biometric solution arises if a false identity is acquired previously. Hence, biometrics would reinforce instead of challenge that identity. Despite this problem, biometrics holds great promise for authentication.

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

Just be sure that any biometric devices you use are secure without compromising privacy, and private without compromising security.

The technologies behind some methods of biometrics are more reliable than others and they will all improve – decreasing false positives and false negatives. Determining which biometric application would best suit your needs requires consideration of several items. You should compare the accuracy (false negatives, false positives), user acceptance, cost, and intended use (network or computer authentication, physical access to buildings). Similarly, you must determine if your goal is to verify or identify the user. Verification is the ability to find and compare the offered template with that of the named user where as identification is finding an unknown user by comparing the offered template with an entire database. Using these assessment guidelines, decide which biometric best fits your needs. Finally, you should allow ample time to test your chosen product in your environment.

No application is infallible, nor is it able to address every concern of an individual or organization. If this were so, there would be no need for the Defense in Depth theory. In considering your line of defense, you must understand your organization's systems, goals, and methods. Information security requires an organization's commitment of financial, technical and human resources to a company-wide program designed to evolve and adapt to new dangers (Power, pg. 3).

A biometric solution may be used in lieu of current security applications, but preferably as an enhancement. Organizations need to become proactive and not reactive to security concerns – attempting to find a last minute cure-all will never work. And finally, although biometrics can identify and verify to grant established authorization, no system can determine what that individual intends to do with that authorization.

Remember Defense in Depth – establish a security policy and adhere to it. Implement network security technologies in a layered approach and audit the network on a recurring basis. Ongoing monitoring, analyzing, and comparing to established security policies and business requirements will help detect irregularities, vulnerabilities and help determine the enforcement, adherence, updating and modification of the security policy as well as business practices. Biometrics may be your added line of defense – Will YOU be your security key?

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

## References


Bragg, Roberta. "Biometric Security Products." Microsoft Certified Professional Magazine Online. April 2002. URL: http://www.mcpmag.com/features/print.asp?EditorialsID=270 (10 Dec. 2003).

Brakeman, Lynne. "Retinal Scans always get their man." URL: http://www.666soon.com/retinal.htm (23 Oct. 2002).

"Business Europe: Biometrics market begins to open up." EbusinessForum. 03 May 2002. URL: http://www.ebusinessforum.com/index.asp?layout=printer_friendly&doc_id=5647 (10 Oct. 2002).

"Did you know…" Biometric Digest. August 2001. URL: http://www.biodigest.com/BiometricDigest/BackIssues/200108.pdf

"Global First Quarter PC Sales Still Slow." LatelineNews. 20 Apr. 2002. URL: http://latelinenews.com/ll/english/1205968.shtml (6 Dec. 2002).

"HandReaders Biometrically Track Employee Time." Recognition Systems. Press Release 31 Jul. 2002. URL: http://www.recogsys.com/news/pressreleases/2002/020731.htm (7 Jan. 2003).

Hayday, Graham. "IT users in password hell." Silicon.com. 11 Dec. 2002. URL: http://news.zdnet.co.uk/story/0,,t295-s2127377,00.html (7 Jan. 2003).

Heath, David. "An Overview of Biometrics Support in NetWare Through NMAS." 28 Jun. 2001. URL: http://developer.novell.com/research/appnotes/2001/july/01/apv.htm (6 Dec. 2002).

"Kronos Unveils Biometric Fingerprint Option for Kronos 4500 Badge Terminal." Kronos. Press Release 13 May 2002. URL: http://www.kronos.com/discover/pr/touchID.htm (7 Jan. 2003).

Lemos, Robert. "Passwords are the weakest link." CNET News. 22 May 2002. URL: http://news.zdnet.co.uk/story/0,,t269-s2110687,00.html (7 Jan. 2003).

Liu, Simon, & Silverman, Mark. "A Practical Guide to Biometric Security Technology." IT Professional. 2001. URL: http://www.computer.org/itpro/homepage/jan_feb01/security3.htm (15 Oct. 2002).

National Center for State Courts. "Biometrics and the Courts: Bertillonage." Court Technology Laboratory. 2002. URL: http://ctl.ncsc.dni.us/biomet%20web/BMBody.html (12 Dec. 2002).

National Center for State Courts. "Biometrics and the Courts: Fingerprint." Court Technology Laboratory. 2002. URL: http://ctl.ncsc.dni.us/biomet%20web/BMFingerprint.html (12 Dec. 2002).

Page, Douglas. "Biometrics: Facing Down the Identity Crisis." High Technology Careers. URL: http://www.hightechcareers.com/doc198/biometrics198.html (10 Oct. 2002).


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

Page, Douglas. "Biometrics: What's Ahead?" High Technology Careers. URL: http://www.hightechcareers.com/doc198/ahead198.html (10 Oct. 2002).

Podio, Fernando L. "Biometrics – Technologies for Highly Secure Personal Authentication." National Institute of Standards and Technology Bulletin. URL: http://www.itl.nist.gov/lab/bulletns/bltnmay01.htm (10 Oct. 2002).

Power, Richard. "2002 CSI/FBI Computer Crime and Security Survey." Computer Security Issues & Trends Vol. VII, No. 1. Spring 2002 (2002): 3-5

Rusch, Jonathan J. "Identity theft: Fact and fiction." CNET News. 18 Sep. 2002. URL: http://news.com.com/2010-1075-958328.html?tag=rn (23 Oct. 2003).

Schneider, Bruce. "Fun with Fingerprint Readers." Crypto-Gram Newsletter May 15, 2002. URL: http://www.counterpane.com/crypto-gram-0205.html#5 (23 Oct. 2002).

Turunen, Pia. "Hack attack, how you might be a target." CNN. 12 Apr. 2002. URL:http://www.cnn.com/2002/Tech/ptech/04/12/hack.dangers/index.html (23 Oct. 2002).

© SANS Institute 2003, Author retains full rights.

Last Updated: June 19th, 2013

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| **Digital Forensics & Incident Response Summit 2013** | **Austin, TXUS** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS London Summer 2013** | **London, GB** | **Jul 09, 2013 - Jul 16, 2013** | **Live Event** |
| **SANS Rocky Mountain 2013** | **Denver, COUS** | **Jul 14, 2013 - Jul 20, 2013** | **Live Event** |
| **SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification** | **Washington, DCUS** | **Jul 22, 2013 - Jul 26, 2013** | **Live Event** |
| **SANS Mumbai 2013** | **Mumbai, IN** | **Jul 22, 2013 - Jul 27, 2013** | **Live Event** |
| **SANS San Francisco 2013** | **San Francisco, CAUS** | **Jul 29, 2013 - Aug 03, 2013** | **Live Event** |
| **SANS Boston 2013** | **Boston, MAUS** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **SANS SEC 560: Network Penetration Testing @ Bangalore 2013** | **Bangalore, IN** | **Aug 05, 2013 - Aug 10, 2013** | **Live Event** |
| **Critical Security Controls Summit** | **Washington, DCUS** | **Aug 12, 2013 - Aug 18, 2013** | **Live Event** |
| **Industrial Control Systems Security Training - DC** | **Washington, DCUS** | **Aug 12, 2013 - Aug 16, 2013** | **Live Event** |
| **SANS Virginia Beach 2013** | **Virginia Beach, VAUS** | **Aug 19, 2013 - Aug 30, 2013** | **Live Event** |
| **SANS Thailand 2013** | **Bangkok, TH** | **Aug 19, 2013 - Aug 31, 2013** | **Live Event** |
| **SANS Melbourne 2013** | **Melbourne, AU** | **Sep 02, 2013 - Sep 07, 2013** | **Live Event** |
| **SANS Capital City 2013** | **Washington, DCUS** | **Sep 03, 2013 - Sep 08, 2013** | **Live Event** |
| **Network Security 2013** | **Las Vegas, NVUS** | **Sep 14, 2013 - Sep 23, 2013** | **Live Event** |
| **SANS Canberra 2013** | **OnlineAU** | **Jul 01, 2013 - Jul 13, 2013** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |