GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

United States National Security Threat Reduction: The Use of Biometrics in the War Against Terrorism

Nicole Niebur
GIAC Security Essentials Certification (GSEC)
Practical Ass. Version 1.4b
September 20,2004

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Table of Contents

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Introduction (A Senario)

On September 11, 2001 at 5:45:06 Eastern Standard Time, video monitors at Portland Airport capture video frames of Mohamad Atta and Abdulaziz Al-Omari passing through airport security.

http://www.solcomhouse.com/terror.htm(19)

© SANS Institute 2005 Author retains full rights.

Moments later, the FBI Center for Biometric Analysis alerts airport security, federal agents link the individuals to the National Security watch list of known terrorists. Airport security agents take immediate action and arrest the terrorists. The terrorist plot is thwarted and the U.S. Government learns of what the World would have called “9/11” or “The September 11, 2001 Terrorist Attacks on the United States of America”.

Unfortunately, automated biometrics and an analysis center were not in place. In reality, the terrorists passed through airport security, got on planes carrying 24,000 gallons of fuel and flew them into World Trade Center One, World Trade Center Two, The Pentagon, and a field in Pennsilvania (with the intention of hitting The Capitol).

http://www.normer.com/2001/sept11th/planeintotower.jpg
Frank J. Denicola / New York Times (5)

© SANS Institute 2005 Author retains full rights.

http://www.sdnet.org/personal/events/terrorism/abn.jpg (17)

The attack was the largest attack on mainland United States since 1814 (War of 1812), where nearly 3,000 people lost their lives.

Looking back on September 11, 2001 we have determined what mistakes have occurred and the corrective actions that should take place to prevent or at least minimize the likelyhood of a event similar to the terrorist attack of 2001. The truth remains, prior implementation of biometrics along with an analysis center in major airports could have prevented the atrocities of 9/11.

Abstract

The objective of this paper is to inform the reader about biometric technologies and focus on the use of these technologies to combat terrorism. This paper will converse the issues that biometrics have encountered in the past and the future that it holds. The body of the paper discusses biometric uses in the war against terrorism, specifically focusing on the different technologies including: facial recognition, hand geometry, iris scanning, retina scanning, signatures recognition and speech recognition. The advantages and disadvantages of each technology and the significant changes in each system post September 11, 2001 will be discussed. The different technologies of biometrics and how products incorporate them to use in different industries will be addressed. Finally, the use of biometrics in response to terrorism after September 11, 2001 will conclude the paper.

© SANS Institute 2005 Author retains full rights.

Biometrics

Biometrics is the study of behavorial or physiological characteristics of a person (18). Examples of behavorial biometrics include voice recognition, signature recognition and keystroke recognition. Examples of physiological characterisitics of biometrics include fingerprinting, hand geometry, iris recognition, retinal scanning and facial recognition. The biometric system performs in two different ways. There is verification biometrics and identification biometrics. These two different measurements are used within biometric identification systems. In a verification process the person has to claim who they "say" they are (4). The systems that run the verification process contain intelligence about the person being identified. This identification is a one to one relationship. The information the person provides the system is compared to information that is in a template already in the system. If the system matches the information provided by the person who uses the product then they are authorized. Identification is the process in which the person must establish his or her own identity (4). This is a one to many relationship. One must provide the system with a sample of information which is compared with the information in the database that contains the "sample" data.

Biometrics, unfortunately, has some faults....

There are two different methods of inaccuracy that biometric systems frequently encounter. There is a False Acceptance Rate (FAR) and False Rejection Rate (FRR).

> "These two terms refer to the imprecision that biometric systems may potentially comprise.The probability that a biometric system will incorrectly identify an individual or will fail to detect an imposter. When a system's FAR is too high, the threshold for the FAR is set too low." (Department of Defense and Federal Biometrics System Protection Profile For Robustness Environments (6)).

The False Rejection Rate (FRR) also refers to the inacurracy that systems may have and the opportunity for error.

> "The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. When a system's FRR is too high, the threshold for the FRR is set too high." (Department of Defense and Federal Biometrics System Protection Profile For Robustness Environments (6)).

These two methods are important when considering implementing a biometric device because organizations require high levels of user acceptance which requires these systems to be refined.

The Past, Present, and Future of Biometrics

In the past, biometrics use was limited. Not only was there little use of biometrics but the technology to develop and support biometrics systems was not

© SANS Institute 2005 Author retains full rights.

available. There was, however, the use of personal characteristics to identify oneself such as fingerprints and footprints. For example, drivers licenses are a form of "old" biometric usage because a picture is used for identification purposes in different circumstances. Biometrics in the past was defined by something we know and something we had. Something we know is our Social Security number, mother's maiden name, and personal identification number (PIN) to something we had such as our drivers licenses, ATM machines and keys to unlock cars or unlock doors (20).

The present usage of biometrics is limited. While biometrics is limited in its use, the CIA, FBI, military installations, and other high security buildings that require high levels of clearance employ this technology to provide a layer of security that other technologies can not provide. Error rates as menitiond earlier: the False Acceptance Rate and the False Rejection Rate are a major problem today. The future of biometrics will help reduce the amount of error rates that we are seeing. Error rates are important when deciding what type of device to purchase for a specific application. These two deciding factors will help a company get the best device possible that is applicable for their environment (16).

The future of biometrics is uncertain. Like any other technology that is first introduced it will evolve if the economical means, profitable means, and user means are backing it. Indivduals will have some influence to where this technology leads. Some interesting ideas about the future of biometrics are listed below:

1. Widespread adoption is 5 years away.
2. Biometrics is on the verge of profitability.
3. Biometrics will bring a new era of security, convenience and user friendliness in the future.
4. Biometrics will become faster, cheaper, and more accurate.
5. Biometrics will not fullfill promises for years to come.
6. Biometrics will definiely take away your privacy. (The Past and Present Future of Biometrics (20))

The above ideas are predictable when following any major benchmarking technology. If these ideas materalize, biometrics will become one of the major technologies used for homeland security.

Biometric Issues

There are two main issues facing the use of Biometrics in the workplace. Legal issues and privacy issues. The legal issues consist of the following six areas of discussion: the public sector, the personal documentation, the law enforcement sector, the private sector, contractual issues, and finally legal issues in the workplace.

© SANS Institute 2005 Author retains full rights.

The public sector is the first area of discussion aiming at biometrics becoming a mandatory implementation when interpreting old and new laws (12). This means that whenever there is a new law brought into place biometrics will have to be implemented to protect that law.

The second area is personal documentation. Personal documentation is important because after September 11, 2001, there were two laws that were put into place that are highly significant mandates. The first law is the USA Patriot Act. This law was developed on October 26, 2001. The law was passed with a vote of 98 to 1 in the Senate. This vote was swayed this way when the event of September 11 occurred after Daschle in the magazine *TIME* made the comment,

> "We're not Democrates here, we're not Republicans, We are Americans" (6).

This Act was developed as a biometric technology standard to detect multiple enrolees in non-immigrant-visa-issuance. Focus of system development is on the a) utilization of biometric technology and b) tamper-resistant documents readable at ports of entry (12).

The second law is the Enhanced Border Security and Visa Entry Reform Act of 2002. In this law, non-US citizens will be issued entry documents that utilize biometrics as a form of identification (12).

The third area of discussion is in the area of the law enforcement sector with a focus on immigration and asylum. This area focuses on taking fingerprints or DNA verification from individuals in criminal investigations or individuals with the intent of seeking a safe haven in the United States (12). This information is then put into a database for later retrieval.

The fourth area is the private sector, which focuses on the legality of digital signatures. This technology has become more prominent in today's society. It binds an electronic document with the signature of intent (12).

The next area focuses on the contractual issues. Contractual issues focus on deciding who is liable for the functionality of the biometric systems or the biometric characteristics of a system (12). This is significant because if the device does not fulfill its function as intended then somebody could be considered liable.

The final sector deals with legal issues in the work place. Organizations will have to take special measures when implementing biometrics such as consent forms because biometrics could leak into the area of personal privacy (12).

The second issue is the Privacy of individuals. There are four different types of privacy:

© SANS Institute 2005 Author retains full rights.

1. Informational privacy

2. Bodily privacy

3. Privacy of communication

4. Territorial privacy

Informational privacy involves rules for the handling of personal data (13). Bodily privacy is the protection of the physical self against procedures (13). Privacy of communication is the security and privacy of mail or telephone calls (13). The final type of privacy is territorial privacy, which involves setting limits to people into domestic and other environments (13).

Biometrics can be looked at in different ways depending on the views of the individual. People may view biometrics in two very different ways. Biometrics can be privacy enhancing, meaning that you have more privacy than you had before. Biometrics can also become a threat to your personal privacy. Studies show that biometrics uses stronger authentication methods when compared to password or pin numbers (13). On the reverse side, biometrics can be used against individuals. There are issues when biometric characteristics change or when someone has compromised the system. If an individual's biometrics is stolen it is hard to retrieve because biometrics is usually permanent to an individual. Currently pin numbers and passwords are easily changed or stolen.

Types of Biometrics

Facial Recognition

There are a couple of different technologies associated with facial recognition. There is the biometric system for the size of a face known as facial retrieval and there is the biometric system for face recognition which uses a camera to capture the image of the face, and the geometry of the facial features, such as distance between the eyes and nose (8). These two technologies are both common ways to analyze a person's face. Some advantages of facial recognition is its ease of use and speed of operation.

A disadvantage to this technology is that it can be hard on an individual. If one is wearing a hat or sunglasses it is not as accurate as when one is not wearing them. Facial recognition has become more and more popular since September 11, 2001. Numerous airports have investigated this technology (22). It is being installed in, or considered for, airports in Boston, Fresno, and elsewhere. However, doubts have been cast as to the effectiveness of these systems in real life applications (22). This is the fastest growing biometric technology since 9/11 (22). There are more companies implementing this product because it can pick a "so called" terrorist out of a crowd. The problem

© SANS Institute 2005 Author retains full rights.

with this technology is that the "so called" terrorists' pictures must be entered into the system prior to the scan. This involves having a photograph of every terrorist in the world. This is impratical and can cause inaccuracy of the application. New technologies are aiming for one to one matching which could eliminate the false negatives and be more effective.

Hand Geometry

Hand geometry developed in the late 80s (around 1986). Hand geometry is the image of lines on the hand. It takes a picture of the hand and examines up to 90 characteristics including 3D shape, length and width of fingers (22). An advantage to this type of technology is that it is very easy to use. The data is also very small in size. The operation is intuitive, meaning it is self explanatory for the end user to use. Hand geometry is also known for being integrated with card readers.

The disadvantages to this technology vary. This technology can run into some problems because one's physical characteristics of the hand change over time and the actual scanning is slow. The accuracy of the hand geometry model is actually proven to be more accurate than the fingerprint verification because of the larger area of scanning surface. One example of the technology used today is by Recognition Systems which dominates the market for Hand Geometry Systems. It uses a technology called HandKey II which stores a 9 byte template of your hand. This technology has been used in the Atlanta Olympics, SFO International Airports, and at the University of Georgia (2).

Fingerprint Authentication

Fingerprint authentication is one of the oldest technologies used in biometrics (16). Fingerprints are currently being used for personal identification. This method is used to identify murderers in crime scenes and to locate missing children. The newer age technology is called finger scanning. This method scans a persons fingers and studies the unique characteristics of that person. The advantage to this technology is that it is fast and user friendly.

A disadvantage to this technology is that it carries a negative connotation. Many people feel that they are doing wrong when they need to get their fingerprints taken. It feels to them like they are being treated like a criminal. This technology can also face problems if the quality of the fingerprint is not adequate. In Newsweek, Brandon Mayfield was fasly accused of having his fingerprint found on a plastic bag which belonged to a terrorist which matched their database of the Madrid Bomber. In actuality, the Spanish gave the FBI a poor digital copy which confused even its best analysts (10). Fingerprint authentication can also be seen in offices for password authentication in computer use.

After Septemeber 11 the changes in fingerprint technologies have increased. People's attitudes have changed. People are familiar with the

© SANS Institute 2005 Author retains full rights.

technology and are confident in the reliability of the basic ink fingerprints that have been used for decades. Another aspect that people enjoy about this technology is the fact that it is one of the most inexpensive biometric systems to implement. Finger reader installations has dropped to as low as $149.00 US per work station (11).

Growth of the finger scanner use has led to technologies such as readers built into smart cards, keyboards, and the mouse. One such technology is called the Touchsmart. The Touchsmart is a mouse with a reader inserted on it (2). It comes in two different models: one has a fingerprint sensor interface, the other has a fingerprint sensor coupled with a smart card interface (2).

Both of these technologies have power management with sleep and suspend modes. There is a ergonomic feature built in so it can fit any user. It comes attached to a 6 foot USB cable so it can plug it into the back of the computer. There are red, green, and amber LEDS so it can adjust where the finger is hitting (2). Another technology using the popular fingerprint scanning biometric is the Defcon Authenticator(14). This device recognizes fingerprints which are available in PC cards and USB versions. This technology is designed for mobile users.

Retina Scanning\Iris Scanning

Retina scanning and Iris scanning are both two different types of biometrics used today featuring the eye as a authentication device. Retina scanning entails the scanning of the blood vessels on the retina at the back of the eye (11). Some advantages to this device include the accuracy of the device, the retina is ever lasting, and there is low interference. The disadvantages to this technology include the high cost associated with purchasing one of these products, the potential for possible retina damage, and it is intrusive to the customer. Iris scanning also involves the scanning of the eye. This device however, captures the image of your iris and stores it in its database for further use. This technology is accurate and unique to an individual. It is very expensive and could also cause eye damage.

Retina scanning has not changed much since September 11, 2001. There are two main factors that could influence this:

1. The required process for capturing the biometric-placing one's eye against or in very near proximity to a reader (Sean O'Connnor, Biometrics and Identification after 9/11 (11)).
2. The cost of retina scanning is still relatively high, particularly when compared with the falling prices of some competing biometric technologies (Sean O'Connor, Biometrics and Identification after 9/11 (11)).

© SANS Institute 2005 Author retains full rights.

Since Spetember 11 iris scanning has become more and more popular. It is one of the most dependable biometric on the market today. This technology is also software driven in some circumstances and can utilize the software in a computer or in a digital camera to provide the needed functionality(11).

Signature Authentication

Signature authentication is when a user signs their signature to a signature tablet with a stylus. A stylus is used on a screens that measure speed, stroke, and pressure. These elements are then analyzed and stored for later use. This is used because it is socially accepted by others, it is very accurate, fast, and the data that is required is very small. The only issue you run into with this technology is that it requires user effort. This technology is called behavoral biometrics which I mentioned earlier. It relies on the way we do certain things. One technology that people are familiar with is the signature pads that we use at retail store or with the UPS. This technology is not assiciated with signature biometrics. Signature authentication is useful because it relies on your signature which is one of the few characteristics that utilizes a specific attribute unique to an individual. It is also second nature to us. We are able to leverage our talent that was learned years ago for biometrics. Another authentication method similar to this technology is keyboard dynamics. Keyboard dynamics analyze the speed, rhythm, and pressure with which we type (22). Both these technologies are used frequently however, it is questionable whether they are true biometric technologies.

National Security and the Use of Biometrics

With a supporting analysis system, biometrics can help overcome human inefficiencies in identifying potential terrorists and by protecting resources and assets, ultimately improving national security. Terrorists have utilized or attacked the banking systems, airports, airplanes, public locations, corporate buildings, military facilities, transportations systems of the United States. We must accept the fact that our own systems can be utilized against us. We must also understand that protections must be put in place to reduce the threats faced by terrorism in order to reduce the risk of attack. Biometrics can provide a protective layer in a wide range of systems including: borders, sea ports, airports, airplanes, public locations, corporate buildings, military facilities, classified information, major gatherings (World Series, Super Bowl, Olympics), food supplies, transportation of materials, nuclear facilities, and banking systems.

The United States Government has implemented several biometric measures to protect the citizens of the United States. One of these measures is the protection of US borders. Prior to September 11, 2001, the US Government passed 19 individuals through US borders without detecting them as known terrorists. However, after 9/11 these individuals were discovered to be the terrorists of 9/11. Clearly after 9/11 the Department of Homeland Security

© SANS Institute 2005 Author retains full rights.

needed to implement some type of system that would help identify valid entry into US territories and prevent known terrorist entry.

> "The Secretary of Homeland Security announced that US-VISIT would have the capability to collect biometrics, initially digital "fingerscans" and photographs, at air and sea ports by the end of 2003 (Homland Security (7)).

With the implementation of biometrics in border protections, terrorist will have a more difficult time achieving identity theft as well as falsifying or disguising “who” they are.

Public locations and major gatherings are another concern for terrorist attack due to the number of people present and the visibility an attack would provide terrorist due to media coverage. One of the measures taken is facial recognition which is the most common biometric method the US Government has utilized to attempt to detect terrorist. Case in point, during the Super Bowl XXXV, facial recognition was used to monitor every person entering the stadium for potential terrorism.

> Viisage Technology CEO Thomas Colatosti stated “that during the monitoring at the Super Bowl that the system "matched" 19 faces (none known to be terrorist) however, the system did pickup petty criminals, proving that the system worked.” (Viisage Technology, Snooper Bowl (3))

Biometric facial recognition provides a weapon against terrorists by using existing CCTV. If the CCTV systems are linked back to a central monitoring post, images can be analyzed for matches. In the United States there are many CCTV systems that could potentially be "linked" to provide a incredible network of surveillance and detection of facial pattern matches. Known terrorists would have a difficult time operating on US soil. US video surveillance systems include ATMs, Banking buildings, many gas stations, toll booths, shopping centers and other locations – it is likely if one were to leave their home they would be captured by a CCTV system.

> “Our discoveries in Afghanistan confirmed our worst fears…We have found diagrams of American nuclear power plants…” (President Bush, The White House (21))

The statements by the President of the United States confirmed, to the public, that terrorists are seeking the destruction or intrusion of sensitive facilities that could have devastating effects against society. Facility protection is an important aspect of biometrics. Corporations, military installations, nuclear facilities, and classified information storage can utilize biometrics to provide key security controls to protect the national security of the United States. An example of this technology used today is hand geometry readers located at Hydro-Quebec’s Gentilly-2 nuclear generating station.

© SANS Institute 2005 Author retains full rights.

> "Hydro-Quebec's Gentilly-2 nuclear generating station is enforcing security, physically restricting non-qualified, non-trained personnel from hazardous zones, and implementing a log of personnel and visitors' coming and going with HandKey hand geometry readers." (Applying Biometrics to Door Access (1))

Biometrics provides a proven technology for identifying airport personnel to protect sensitive areas of internal personnel access. However, there is a more difficult area that biometrics can provide support for but the technology is not completely proven. The use of biometrics to identity terrorist is more difficult because the system would have to know which faces belonged to terrorists. Face recognition systems have a higher false positive rate than other biometric identification systems (such as an Iris scan). Terrorists may bypass detection by wearing a mask, hat, and glasses. They may also use other methods to disguise personal features. Biometrics could also be used on airplanes to prevent non-authenticated individuals from flying planes by implementing some type of aircraft controls that require the proper "hand" accessing the controls. This control alone could have prevented the 9/11 terrorst attack from using planes as missiles and flying them into buildings.

The protection of food supplies and the transportation of materials within the United States is an important aspect to national security. The use of biometrics can help protect these resources by preventing non-authorized individuals from transporting dangerous materials and from accessing food supplies.

> "On March 1, the U.S. Federal Motor Carrier Safety Administration (FMCSA) and partners announced the success of the final Hazardous Materials Safety and Security Field Operational Test. The test team includes government agencies; private sector organizations such as the Commercial Vehicle Safety Alliance; suppliers and shippers such as ExxonMobil, BP Chemical, and Roadway Express; and truck and engine manufacturers such as Caterpillar, Cummins, Detroit Diesel, Freightliner Trucks, and International Truck and Engine.
>
> The test is demonstrating the effectiveness of technologies called Intelligent Trucking Systems. The initiative is intended to facilitate a government plan to deter the hijacking of commercial trucks by terrorists.
>
> The test uses smart cards in conjunction with fingerprint scanners to validate the identity of drivers and monitor truck startups, pickups, and drop-offs. The smart cards contain driver-specific information and biometric fingerprint templates that are integrated with a global log-in system designed to alert dispatchers if an unauthorized person attempts to operate a truck. In addition, through GPS technology, remote control of truck ignition and braking systems by dispatchers in the event of an alert is being tested." (International Biometric Industry Association (8))

© SANS Institute 2005 Author retains full rights.

A critical asset that is utilized by terrorists is the banking system of the world. One of the key fronts on the war on terror is tracking down funding and finances of terrorist organizations. Many key terrorists were tracked down and captured by reviewing banking records. The implementation of biometrics in banking systems would put up another barrier of security for known terrorists, making it difficult to open accounts or conduct other financial transactions. The use of biometrics in the banking industry also provides several other critically important security measures that combat fraud. Fraud in the banking systems is astronomically increasing and banks are starting to use biometrics to protect them and their customers from identity theft scams and general financial fraud. According to PC World,

> "Indeed, a growing number of financial services firms are strongly considering the use of biometrics technology sooner rather than later because of heightened security concerns sparked by the September 11 terrorist attacks and skyrocketing fraud rates."
> (Lucas Mearian, Banks eye Biometrics for ATM's (9))

Conclusion

Biometrics is only one layer of protection needed to help mitigate risks presented by terrorism. There are numerous security measures that must be implemented in order to fight terrorism. The threat reduction initiatives being undertaken by the United States, including fighting terrorism offensively (military actions), and defensely (protection provided by technologies such as biometrics), must coexist to provide a comprehensive method to combat this enemy. Biometrics compliments other security measures and improves efficiencies of human intelligence systems. Facial recognition alone cannot combat terrorism. However, facial recognition devices with a database of known terrorist faces could be implemented to combat terrorism. A combination of facial recogniton, hand geometry, fingerprint authentication, retina scanning, iris scanning devices, and signature authentication devices can enable a society to equip themselves with identification weaponry to combat terrorism.

Biometrics pre 9/11 was a limited use technology. Post September 11, biometrics played key roles in providing security at major gatherings such as the Olympics and the Super Bowl. After September 1, 2003 the United States had a supporting analysis center that biometrics could utilize post December 1 2003. As stated by U.S.News & World Report,

> "the new database, and the mulitagency Terrorist Screening Center created to run it, were to be "operational" December 1,2003.(15)"

The use of biometrics to combat terrorism will take us closer to preventing catastrophic events such as September 11 2001.

References

1. *Applying Biometrics to Door Access.* August 2004 URL:

© SANS Institute 2005 Author retains full rights.

http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,84627,00.html

2. *Biometric Fingerprint Technology.* July 2004 URL: http://64.233.167.104/search?q=cache:VMhQqsIZteAJ:www.sanmina-sci.com/Fujitsu/biometric.html+Biometric+Fingerprint+Technology&hl=en&start=4

3. Chachere Vickie. "Snooper Bowl?" ABCNews.com. Febuary 2004. URL: http://abcnews.go.com/sections/scitech/DailyNews/superbowl_biometrics_010213.html

4. *Department of Defense and Federal Biometrics System Protection Profile For Robustness Environments.* September 2004 URL: http://www.biometricscatalog.org/2003GBW/downloads/PP_BSPP-MR_V0.02.pdf

5. Frank J. Denidola. *New York Times*. September 2004 URL: http://www.normer.com/2001/sept11th/planeintotower.jpg

6. Gibbs Nancy and John F. Dickerson. "Inside The Mind of George W. Bush". *TIME* September 2004: 26-36.

7. *HomeLand Security*. September 2004. URL: http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0444.xml

8. *International Biometric Industry Association.* Biometrics Advocacy Report. September 2004 URL: http://www.ibia.org/newslett040305.htm

© SANS Institute 2005 Author retains full rights.

9. Lucas Merian. *Banks Eye Biometrics for ATM's.* Increasing Security Concerns and Fraud Renew Interest in Alternative Password Methods. January 2002 URL: http://www.pcworld.com/news/article/0,aid,79424,tk,dn011402X,00.asp

10. Murr Andrew. "The Wrong Man". *Newsweek* June 2004: 30-31.

11. O'Connor Sean. *Biometrics and Identification after 9/11*. September 2004, URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=299950

12. *Privacy Issues and Biometrics.* September 2004 URL: http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=405

13. *Privacy Issues and Biometrics.* September 2004 URL: http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&subMenu=4&displayPage=406

14. Review: *Targus Defcon Authentication.* August 2004 URL: http://abcnews.go.com/sections/scitech/TechTV/techtv_fingerID020425.html

15. Samantha Levine. "Spinning Terror's Rolodex". *U.S.News & World Report* February 2 2004: 31-32.

16. *Security*. September 30. URL: http://www.securitymagazine.com/CDA/ArticleInformation/features/BNP__Features__Item/0,5411,77209,00.html

17. "September 11, 2001 Picture" No Date. Online Image. August 2004. http://www.sdnet.org/personal/events/terrorism/abn.jpg

© SANS Institute 2005 Author retains full rights.

18. *Simple Technology Inc.* September 2004, URL:

http://www.simpletechnology.com/misc/biomain.htm

19. *Solcomhous.* September3 2004. URL:

http://www.solcomhouse.com/terror.htm

20. The Past and Present Future of Biometrics. September 2004, URL:

http://www.biometricscatalog.org/biometrics/history_docs/futureofbiometrics.pdf

21. *The WhiteHouse*. January 2002. URL:

http://www.whitehouse.gov/news/releases/2002/01/20020129-11.html

22. Wondernet-Biometric Signature Authentication. July 2004. URL:

http://www.wondernet.co.il/html/

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005 Author retains full rights.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor