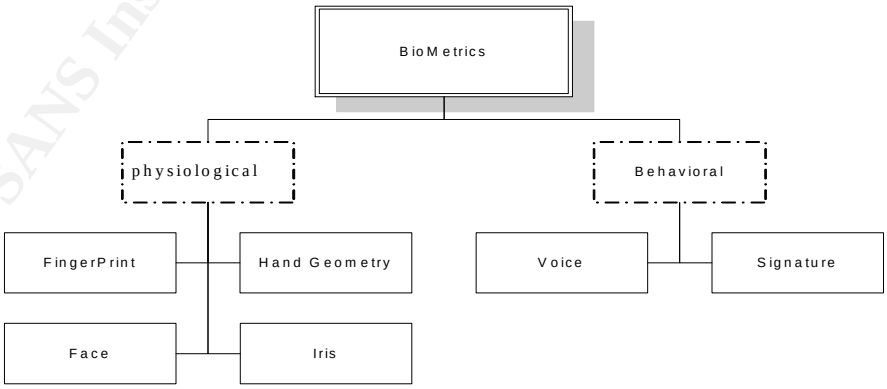
Global Information Assurance Certification Paper

Fingerprint Authentication: A Synopsis
Syed Hussain
v.1.4b
GSEC
July 15th 2004

Abstract

"A biometric factor is something physiologically unique about an individual, such as a fingerprint, facial image, iris, voice pattern, and handwriting. When an individual wants logical or physical access (depending on the implementation), a sample is taken of the authenticatee's biometric data, for example, a fingerprint. Then, the authenticator, using a previously enrolled version of the same biometric template can match the sample against the stored template to verify the individual's identity"[1].
"Biometrics are not secret, as everyone leaves fingerprints everywhere they go, faces and eyes can be photographed, voices can be recorded, and handwriting samples can be obtained. The security of the fingerprint authentication system therefore relies on the integrity and authenticity of the biometric information"[1], therefore careful evaluation must be done for the selection of the fingerprint authentication and Good practices should be followed during the implementation, enrollment and administration of the fingerprint authentication system.
The purpose of this paper is to give a good understanding of fingerprint authentication and to present a set of criteria to be considered while evaluating, implementing and administrating a fingerprint based biometric authentication system.

"Bio Metrics is divided into two factors physiological and behavioral"[2] as shown below in the chart.
"The deployment of fingerprint-based biometric solutions is being driven by technology advances that have achieved high levels of reliability, reductions in sensor costs and size, and an increased need for security. Industry revenues for 2003 were forecast at $185million".[3]



1. **Ref: http**://pkiforum.org/pdfs/biometricsweb.pdf
2. **Ref:** http://www.biometricsinfo.org/biometrics.htm
3. **Ref: www.**frostandsullivan.com

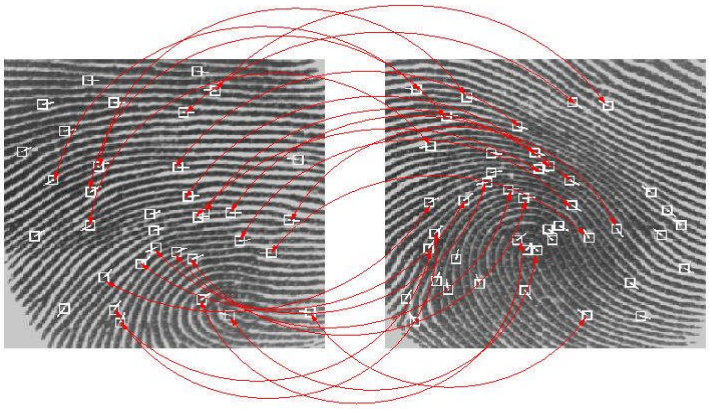
Fingerprint

Fingerprints have been accepted as the most common form of biometrics authentication today.

The strong point about using fingerprint biometrics are that giving fingerprints is more widely accepted, convenient and reliable than other forms of physical identification, especially when using technology. In fact, it is considered that fingerprint identification is the least intrusive of all biometric technologies when privacy is the concern.

Every human beings fingerprint is unique. Each fingerprint has a unique characteristic and pattern that is made up of lines and spaces. The lines are called ridges while the spaces between the ridges are called valleys. These patterns of ridges and valleys are used to match the fingerprint for verification and authentication. This unique fingerprint trait is termed “minutiae” and comparisons are made based on these traits.

“As Dan M. Bowers explains in Access Control and Personal Identification Systems: There are about one billion possible minutiae combinations on a fingerprint; since there are about 5 billion people inhabiting the Earth, and each has ten fingers, this means that statistically it is likely that fifty people on Earth share a fingerprint”.[4]



5

4. Ref: http://www.biometricaccess.com/products/wp_finge.htm

5. Ref: http://biometrics.cse.msu.edu/fingerprint.html

Fingerprint matching techniques

Fingerprint matching techniques can be placed into two categories: minutiae-based and correlation based.

Minutiae-based: "Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. However, there are some difficulties when using this approach. It is difficult to extract the minutiae points accurately when the fingerprint is of low quality. Also this method does not take into account the global pattern of ridges and furrows." [5]

Correlation based Method: "The correlation-based method looks at the entire pattern of ridges and valleys in the fingerprint. The location of the whorls, loops, and arches and the direction that they flow in are extracted and stored."[6] But it is able to overcome some of the difficulties of the minutiae-based approach. However, it has some of its own shortcomings. "Correlation-based techniques require the precise location of a registration point and are affected by image translation and rotation" [5]

Finger print authentication technology

Finger print authentication technology is divided into two processes Identification and Verification

Identification Process

In Identification process, an individual presents a sample to the biometric system during enrolment. The biometric system then attempts to compare the sample with the database which has samples stored in it. This is one-to-many form of comparison. The identification process is further divided into positive identification and negative identification.

Positive identification: In a positive identification system users do not enter a pin number along with their fingerprint, "but simply place their finger on the capture device and their finger print is identified by matching the fingerprints in the database." [7]

Negative identification: In these systems searching the databases is done in the same fashion, comparing one template against many, but these systems are designed to ensure that a person is not present in the database.

6. Ref: http://www.giac.org/practical/GSEC/Lisa_Kuster_GSEC.pdf

7. Ref:http://www.biometricgroup.com/reports/public/reports/identification_verification.html

Verification Process

Verification is a one-to-one comparison in which the biometric system attempts to verify an individual's identity. In this case, a new biometric sample is captured and compared with the previously stored template. If the two samples match, the biometric system confirms that the applicant is who he/she claims to be.

The same four-stage process — captures, extraction, comparison, and match/non-match — applies equally to identification, recognition and verification.

Identification involves matching a sample against a database of many, whereas verification involves matching a sample against a database of one. [8]

Finger Print Identification Techniques

Fingerprint identification techniques fall into two major categories Fingerprint recognition systems and Automated Fingerprint Identification Systems (AFIS).
Fingerprint recognition is considered the best choice for most applications because of its accuracy, speed, reliability, non-intrusive interfaces, and cost-effectiveness.

Fingerprint Recognition Systems

There are four steps in the fingerprint recognition system

- Image Acquisition
- Location and Determination of the fingerprints characteristics
- Template creation
- Template matching

Image acquisition

The first step in fingerprint recognition is known as “image acquisition”. Once the individual places his finger on the scanner numerous images of the centre of the fingerprint are captured as they contain many of the unique features. All of the captured images are then converted into black and white images.[9]

8. Ref: http://www.findbiometrics.com/Pages/guide4.html

9. Ref: http://technologyexecutivesclub.com/biometricsfingerprints.htm

Location and determination of the fingerprints characteristics

The fingerprint is comprises of “ridges” and “valleys” which form the basis for loops, arches, and swirls that are easily visible to the human eye. The ridges and valleys contain different kinds of breaks and discontinuities. These are called minutiae, and it is from these minutiae that the unique features are located and determined. There are two types of minutiae: (1) Ridge endings (the location where the ridge actually ends); and (2) Bifurcations (the location where a single ridge splits and becomes two ridges).[9]

Template Creation

Templates are generated by algorithms which locate and encode distinctive features from an identifiable physiological or behavioural characteristic such as a fingerprint image. Algorithms are used to create template each vendor has a proprietary algorithms and in many cases they represent key components of a vendor's intellectual property. Templates vary widely from sample to sample, such that in theory only a vendor algorithm can determine whether two templates match.

Each minutia has unique features based on these, location, position, type and quality a template is created. Fingerprint recognition technology consists of many vendors and each vendor has his own set of algorithms for template creation and matching.[9]

Template Matching

In this final step the system will either attempt to verify or identify the user, by comparing the enrolment template against the verification template.

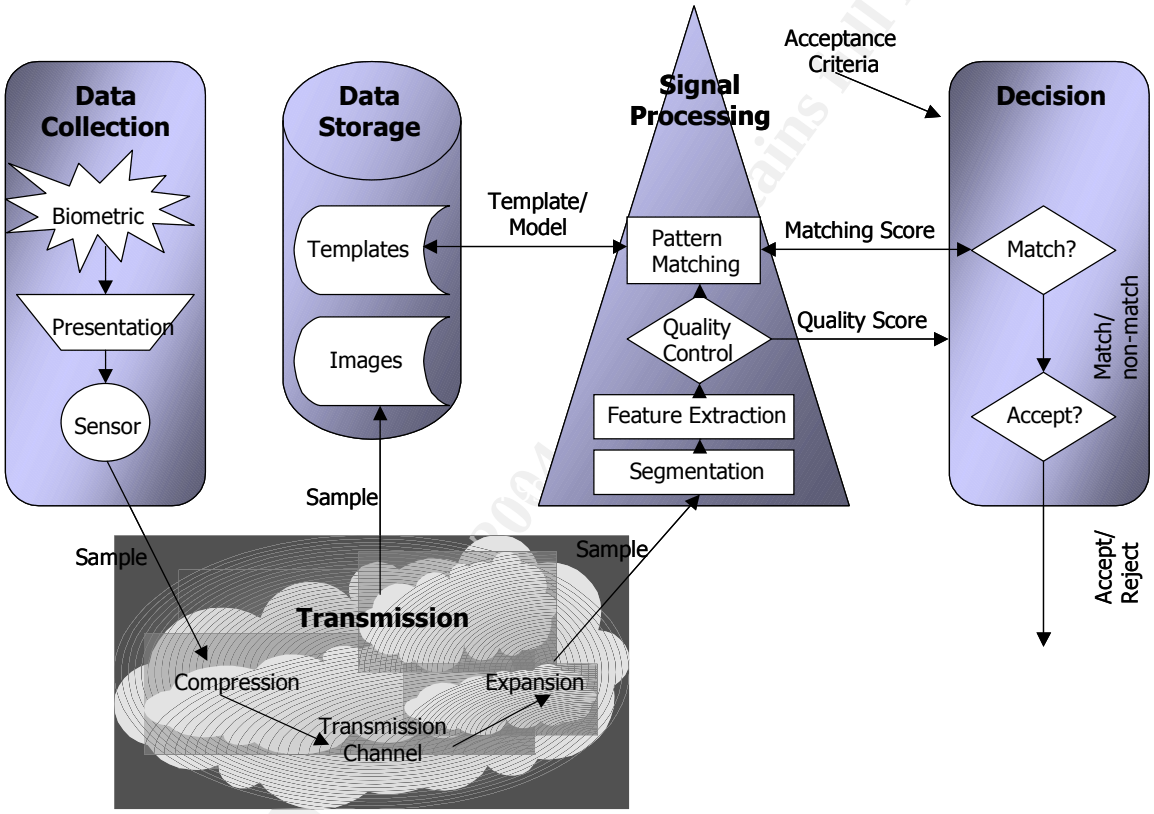
There are three main technologies available today for the capture of fingerprint images:
(1) Optical technology-this is the oldest and most popular form used for image capture. Essentially, a camera (located in the fingerprint recognition device) takes raw images of the fingerprint.
(2) Silicon technology-a silicon chip is used, and the capacitive characteristics of the fingerprint are captured into images.
(3) Ultrasound technology-Basically, an ultrasound image of the fingerprint is captured. [9]

“The Ultrasound technology has proved to work better than the other two, because it can penetrate through different types of fingerprint dirt and residue”. [9]

9. Ref: http://technologyexecutivesclub.com/biometricsfingerprints.htm

Automated Fingerprint Identification System

An AFIS includes all of the hardware, associated software and interconnecting infrastructure to enable the end to end biometric process. If the biometric process is an integral part of a larger system, then this definition extends to any part of the larger system that holds relevant user data, such as directories and transaction logs for example. In addition, in such a system the process extends to the point after which authentication is complete and no longer required for the larger system to function.
Fingerprints can be captured in different ways. Current techniques include optical, ultrasound, or technologies based on semiconductor chips.



10

10. Ref: http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf

Evaluation Criteria for the implementation of finger print authentication

Finger print technology has certainly matured and is capable of providing real benefits when intelligently applied to a given situation, but as in all good application designs, it is the business process requirements which should drive the design and the specific type of biometric chosen, i.e., fingerprints, iris codes, hand geometry etc. The evaluation process should be structured as a valuable learning experience, and benchmarking competitive systems will remove most of the risks prior to making a final decision A successful implementation should follow these key steps:

- Identify the business and operational requirements clearly, together with any current problems and the effect they are having on the situation.
- Develop and agree on a suitable business process which has the potential to significantly improve on the current situation, given the current state of technology.
- Quantify the operational logistics such as number of people, time profile / distribution of transactions, type of entry point, target transaction time, environmental considerations, availability and profile of system operators and so on.
- Analyse the existing situation and processes in order to identify legacy requirements and system interaction - it may be necessary to retain or assure compatibility with certain existing processes.
- Design a system architecture which accounts for all of the above whilst remaining open for future development and enhancement.
- Design an operating methodology and user interface which satisfies the above requirements in an intuitive and attractive manner.
- Choose the appropriate front end technology accordingly (i.e., fingerprint/ fingerprint and smart card etc.) ensuring that the biometric methodology is the most suitable for this application.
- Thoroughly test and document the system in house before demonstrating the system to the client and agreeing and documenting any design changes.
- Develop and schedule an operator training programme.
- Install and commission the system having surveyed the site and noted relevant conditions and with due consideration to existing systems.
- Hand over the system after ensuring that administrators have a comprehensive understanding of the functionality and that all operating data is present and correct.
- In defining the specification required, we should concern ourselves with perceived ease of use, acceptable transaction time, contingency measures for errors, where the biometric template should be stored, enrolment procedures and logistics and general compatibility and connectivity issues.[2]

2. Ref: http://www.biometricsinfo.org/biometrics.htm

Good Practices

We will consider the good practices relating to fingerprint system implementation in six categories:

- Selection of a Biometric authentication system
- Enrolment process
- Technical requirements
- User-related
- Operational
- System Administration

Selection of a Biometric authentication system

Installing a Biometric system is not only a major financial commitment; it involves redesigning the user process for authentication and all that is implied by such administrative changes. The following guidelines can be the basis of user due diligence.

Using formal evaluation methods already in place, a short list of the three top technical scores should be selected for benchmarking. A proven ability to deliver similar fingerprint authentication systems is the most important criteria for selecting a short list of vendors.

The benchmark process is an opportunity to ask many different types of questions and observe first hand how a system works. The objective tests, however, are threefold: a. Accuracy of the system. b. Throughput of the system. c. Functionality and operating simplicity of the system.

- One-to-many search/match
  - Accuracy
  - Throughput

- One-to-one search/match
  - Accuracy
  - Throughput

- Overall assessment of vendor's current technology
- Road Map for future developments of the product
- Ease of administration
- Ease of use for the end user during identification and enrollment
- Security/privacy requirements need to be addressed for the storage of biometric/user data, both locally and centrally.

Enrolment

"Enrolment is the process of registering a user. The Enrol function accepts a raw image delivered directly from a sensor. The image is processed, enhanced, and compressed to create a fingerprint template. The template is returned, along with image statistics reflecting the quality of the enrolment. Subsequent verifications and identifications compare live-scan images to previously enrolled templates".[11]

- Define enrolment policy
- Establish enrolment template storage size
- Define number of attempts enrolment will be allowed
- If a user cannot contribute a valid template for enrolment, either temporarily or permanently, what work-around measures can be defined?
- Define enrolment time for each individual
- Establish how long will an enrolled template be considered valid, since a user's biometric characteristic(s) change over time?
- Define based on the organization criteria and needs if multiple templates per user will be required

Technical requirement

To come up with the technical requirements careful assessment must be done keeping in mind the cost factor so that it doesn't overshoot the cost of the resources which are to be protected.

- Based on the assessment envision the resources which will be needed to support your overall system.
- Take into consideration the cost of the biometric solution in terms of hardware, software, personnel, training, and impacts on existing procedures before coming up with the requirements.
- Consider interoperability of the biometric system with other existing, non-biometric, systems within the environment.
- "Design a procedure for user data collection, data capture, data transmission, data translation, signal processing, template storage, and user management".[10]

10. Ref: http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf

11. Ref: http://www.bioscrypt.com/products/bioscrypt_core.shtml

User-acceptance

- The user must be considered at each stage of the process of planning implementing and technical configuration. The aim is to have well trained users who have good quality templates and are happy with the system concept and benefits.
- All the users have to be educated to allay their doubts/fears about implementing a biometric authentication system in the environment.
- Clearly define the user benefit and present it in the form of a user awareness program.
- Conduct training to the users on how to properly use the system. The enrolment procedure should be carefully guided and done in a patient manner.
- "Administrators should provide a method for individuals to correct, update, and view information stored in conjunction or association with biometric information". [10]

Operational measures

There are four basic error rates employed in fingerprint authentication systems which have to be considered to configure the Biometric authentication system before it is operational:

- False Acceptance Rate (FAR);
- False Rejection Rate (FRR);
- Equal Error Rate (EER);
- Failure to Enroll Rate (FER).

False Acceptance rate

The FAR represents the probability that a false match occurs, for example, an unauthorized user is erroneously accepted as an authorized user by the system.[12]

False Rejection rate

It is the opposite of FAR, this represents a probability that a false rejection occurs, and for example, an authorized user is erroneously mistaken for an unauthorized user. [12]

Failure to enroll rate

The FER represents the probability that a single fingerprint cannot be enrolled in the system, such as when an individual wants to use his right thumb with the fingerprint authentication system, but for some reason the system determines that his right thumb is not usable for this purpose. [12]

Equal Error Rate

The EER is when the FAR maps to FRR.

12. Ref: http://www.fidelica.com/Documents/Interpret_Finger_Auth_Perf.pdf

Note:

If a system has various security settings at which it can be operated, then the FAR and FRR will vary in accordance with the security setting selected. In general, as the FAR is reduced the system becomes more secure .The FRR is increased. A consequence of a higher FRR is user inconvenience, since successful authentication of an authorized user may require additional access attempts.[12]

After the configuration is done the processing the first biometric sample and extracting the features, we have to store and maintain the newly obtained master template choosing proper discriminating characteristic for the categorization of records in large databases .This can improve identification search tasks later on. There are basically 4 possibilities where to store the template:
On a smart card
On the central database
On a server,
On the authentication terminal.
The storage in an authentication terminal cannot be used for large-scale systems, in the case of large deployments the first two possibilities are applicable.[13]

Before the Biometric authentication is operational the following questions should be taken into consideration.

- Will the biometric system in a particular application be used for positive identification, negative identification, or both?
- If both positive and negative identification are required, will they be required from the same biometric measure, and can two measures be used (e.g. fingerprint and voice, face and voice, etc.)?
- During operational use, will the system automatically flag poor quality biometric input data? How much of the input can be reasonably tolerated to be flagged as poor quality data?
- What are the throughput rate requirements for both enrolment and operational use?
- How many false match errors can be tolerated?
- Will the probability of a false match be low enough to deter fraud?
- How many false non-match errors can be tolerated?
- In the case of a false non-match, will the user be given additional attempts for recognition?
- What will be the tolerable rate of occurrence for false non-matches that require intervention by the administrator?

12. Ref: http://www.fidelica.com/Documents/Interpret_Finger_Auth_Perf.pdf

13. Ref: http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf

System Administration

The System administration process should take into consideration the following:
1. The back-up methods for user authentication in the cases of equipment failure or temporary unavailability of the user's biometric feature
2. Develop an appropriate contingency plan and disaster recovery policy
3. Hardware replacement and response times by the vendor
4. Back-ups for personnel critical to the operation of the system?
5. Defined roles and responsibilities for administrators and backup administrators
6. Training for system administrators and backup administrators
7. Check and confirm biometric capture device have the capability to perform automatic self-diagnostic and calibration tasks (for both enrolment and operational use), or will the system administrator have to attend to this periodically?
8. Configure the system a lockout threshold for excessive invalid access attempts?
9. Monitor the audit information eg... number of new biometric records accepted, the number of biometric records verified, the number of users the system was unable to enroll, the quality measurements for the captured biometric data, the amount of system down time, the kinds of system errors by type, and the average enrolment processing time on a daily, weekly, and monthly basis
10. "Biometric information should be protected at all stages of its lifecycle, including storage, transmission, and matching. To protect biometric information in storage and transmission and matching it is ideal to use encryption, VPN, secure facilities, administrative controls, and data segregation." [14]
11." Biometric data should be stored separately from personal information such as name and designation etc….. .Depending on the manner in which the biometric data is stored, this separation may be logical or physical". [14]

Conclusions

Any organization planning to integrate a Biometric authentication system should be mindful of the following issues:

- All security systems, biometric or otherwise, require time, money, and energy to setup and administer/maintain properly.
- System throughput rates must be carefully addressed, for both enrolment and operational use.
- Remember that the need for enrolment sessions/training for all users is mandatory.
- Despite the fact that studies of user attitudes show a strong preference towards the acceptance of biometric technology, there will always be users who object to the use of it. What policy have you defined to address this?
- Choose your system integrator carefully. Hardware/software integration will prove to be the hardest task.
- Biometric technologies are not very adept at 'plug and play' integration should be considered if it is required.

14. Ref: http://www.bioprivacy.org/

- Expect system integration to require changes in other pieces of hardware and software.
- Examine the track record of the technology vendors closely. Products and vendors are in a continual state of flux. Look for stability of the product and the future roadmap for the product.
- Vendor support and SLA should be carefully examined.

References

1. **"Biometrics PKI Note" May 2001 (15/07/04)**
   http://pkiforum.org/pdfs/biometricsweb.pdf

2. **Biometrics (15/07/04)**
   http://www.biometricsinfo.org/biometrics.htm

3. **frost and sullivan**
   www.frostandsullivan.com **(02/07/04)**

4. **"Fingerprints - The Biometric of Choice"**
   http://www.biometricaccess.com/products/wp_finge.htm **(15/07/04)**

5. Salil Prabhakar, Anil Jain **"Fingerprint Matching"**
   http://biometrics.cse.msu.edu/fingerprint.html (**15/07/04)**

6. Lisa Kuster **GSEC Practical Assignment October 22, 2003,**
   http://www.giac.org/practical/GSEC/Lisa_Kuster_GSEC.pdf (**15/07/04)**

7. **"How Do Identification and Verification Differ?" IBG 2004**
   http://www.biometricgroup.com/reports/public/reports/identification_verification.html
   (15/07/04)

8. **"Identification versus Verification"**
   http://www.findbiometrics.com/Pages/guide4.htm **(15/07/04)**

9. Ravi Das **"The Application of Biometric Technologies: Fingerprint Recognition"**
   http://technologyexecutivesclub.com/biometricsfingerprints.htm **(15/07/04)**

10. A. J. Mansfield, National Physical Laboratory and J. L. Wayman,
    San Jose State University August 2002
    "Best Practices in Testing and Reporting Performance of Biometric Devices"
    http://www.cesg.gov.uk/site/ast/biometrics/media/BestPractice.pdf **(15/07/04)**

11. **"Bioscrypt™ Core"**
    http://www.bioscrypt.com/products/bioscrypt_core.shtml **(15/07/04)**

12. **"INTERPRETING FINGERPRINT AUTHENTICATION PERFORMANCE"**
    12/18/2001,
    http://www.fidelica.com/Documents/Interpret_Finger_Auth_Perf.pdf **(15/07/04)**

13. V´aclav Maty´a¡s and Zden¡ek ¡R´ýha Faculty of Informatics, Masaryk University Brno, Czech Republic
“BIOMETRIC AUTHENTICATION —SECURITY AND USABILITY”
http://www.fi.muni.cz/usr/matyas/cms_matyas_riha_biometrics.pdf **(15/07/04)**

14. **“Best Practices for Privacy-Sympathetic Biometric Deployment 2003”**
http://www.bioprivacy.org **(15/07/04)**

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
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
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
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
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
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
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event