Interested in learning more about security?

SANS Institute InfoSec Reading Room

Iris Recognition Technology for Improved Authentication

One area where security can be improved is in authentication. Iris recognition, a biometric, provides one of the most secure methods of authentication and identification thanks to the unique characteristics of the iris. Once the image of the iris has been captured using a standard camera, the authentication process, involving comparing the current subject's iris with the stored version, is one of the most accurate with very low false acceptance and rejection rates. This makes the technology very useful in areas such as...

Iris Recognition Technology for Improved Authentication

By

Penny Khaw

SANS Security Essentials (GSEC) Practical Assignment
Version 1.3

Table of Contents

Summary

The pressures on today's system administrators to have secure systems are ever increasing. One area where security can be improved is in authentication. Iris recognition, a biometric, provides one of the most secure methods of authentication and identification thanks to the unique characteristics of the iris. Once the image of the iris has been captured using a standard camera, the authentication process, involving comparing the current subject's iris with the stored version, is one of the most accurate with very low false acceptance and rejection rates. This makes the technology very useful in areas such as information security, physical access security, ATMs and airport security.

The technology is accurate, easy to use, non-intrusive, difficult to forge and, despite what people may think, is actually quite a fast system once initial enrolment has taken place. However, it does require the co-operation of the subject, needs specific hardware and software to operate and administrators need to ensure they have a fall back plan should the resources required to operate the system fail, for example power. Iris recognition technology does provide a good method of authentication to replace the current methods of passwords, token cards or PINs and if used in conjunction with something the user knows in a two-factor authentication system then the authentication becomes even stronger.

Introduction

In today's information technology world, security for systems is becoming more and more important. The number of systems that have been compromised is ever increasing and authentication plays a major role as a first line of defence against intruders. The three main types of authentication are something you know (such as a password), something you have (such as a card or token), and something you are (biometric). Passwords are notorious for being weak and easily crackable due to human nature and our tendency to make passwords easy to remember or writing them down somewhere easily accessible. Cards and tokens can be presented by anyone and although the token or card is recognisable, there is no way of knowing if the person presenting the card is the actual owner. Biometrics, on the other hand, provides a secure method of authentication and identification, as they are difficult to replicate and steal. If biometrics is used in conjunction with something you know, then this achieves what is known as two-factor authentication. Two-factor authentication is much stronger as it requires both components before a user is able to access anything.

Biometric identification utilises physiological and behavioural characteristics to authenticate a person's identity. Some common physical characteristics that may be used for identification include fingerprints, palm prints, hand geometry, retinal patterns and iris patterns. Behavioural characteristics include signature, voice pattern and keystroke dynamics. A biometric system works by capturing and storing the biometric information and then comparing the scanned biometric with what is stored in the repository. The diagram below demonstrates the process followed when using a biometric system for security:

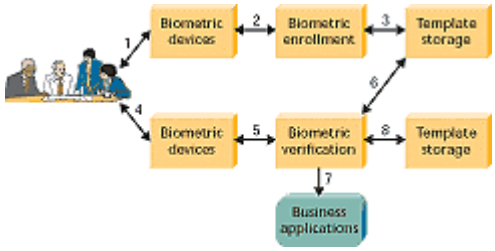

Figure 1: Biometric System Process[1]

Out of all the various physical characteristics available, irises are one of the more accurate physiological characteristics that can be used.

History

In the mid 1980s two ophthalmologists, Drs Leonard Flom and Aran Safir, proposed that no two irises are alike, even in twins, thus making them a good biometric. This belief was based on their clinical experience where they observed the distinctive features of irises including the "many collagenous fibres, contraction furrows, coronas, crypts, colour, serpentine vasculature, striations, freckles, rifts and pits" [2]. After researching and documenting the potential use of irises as a means of identifying people they were awarded a patent in 1987. They then approached Dr John Daugman, a Harvard mathematician, in 1989 to assist with creating the mathematical algorithms required for digitally encoding an image of an iris to allow comparison with a real time image. By 1994 the algorithms had been developed and patented and are now used as "the basis for all iris recognition systems and products"[3] currently being developed and sold. These processes are owned by Iridian Technologies who develop products and license the processes to other companies.

Iris Recognition Technology

The Iris

The iris has many features that can be used to distinguish one iris from another. One of the "primary visible characteristic is the trabecular meshwork, a tissue which gives the appearance of dividing the iris in a radial fashion"[4] that is permanently formed by the eighth month of gestation. During the development of the iris, there is no genetic influence on it, a process known as "chaotic morphogenesis" that occurs during the seventh month of gestation, which means that even identical twins have differing irises. The iris has in excess of "266 degrees of freedom"[5], i.e. the number of variations in the iris that allow one iris to be distinguished from another. The fact that the iris is protected behind the eyelid, cornea and aqueous humour means that, unlike other biometrics such as fingerprints, the likelihood of damage and/or abrasion is minimal. The iris is also not subject to the effects of aging which means it remains in a stable form from about

[1] http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm
[2] http://www.rycom.ca/solutions/pdfs/iridian/iris_whtppr.pdf
[3] http://www.cl.cam.ac.uk/users/jgd1000/history.html
[4] http://www.stanford.edu/~bjohara/iris.htm
[5] http://www.mi5.co.nz/mi5/docs/iridian.pdf

the age of one until death. The use of glasses or contact lenses (coloured or clear) has little effect on the representation of the iris and hence does not interfere with the recognition technology. The picture below demonstrates the variations found in irises:

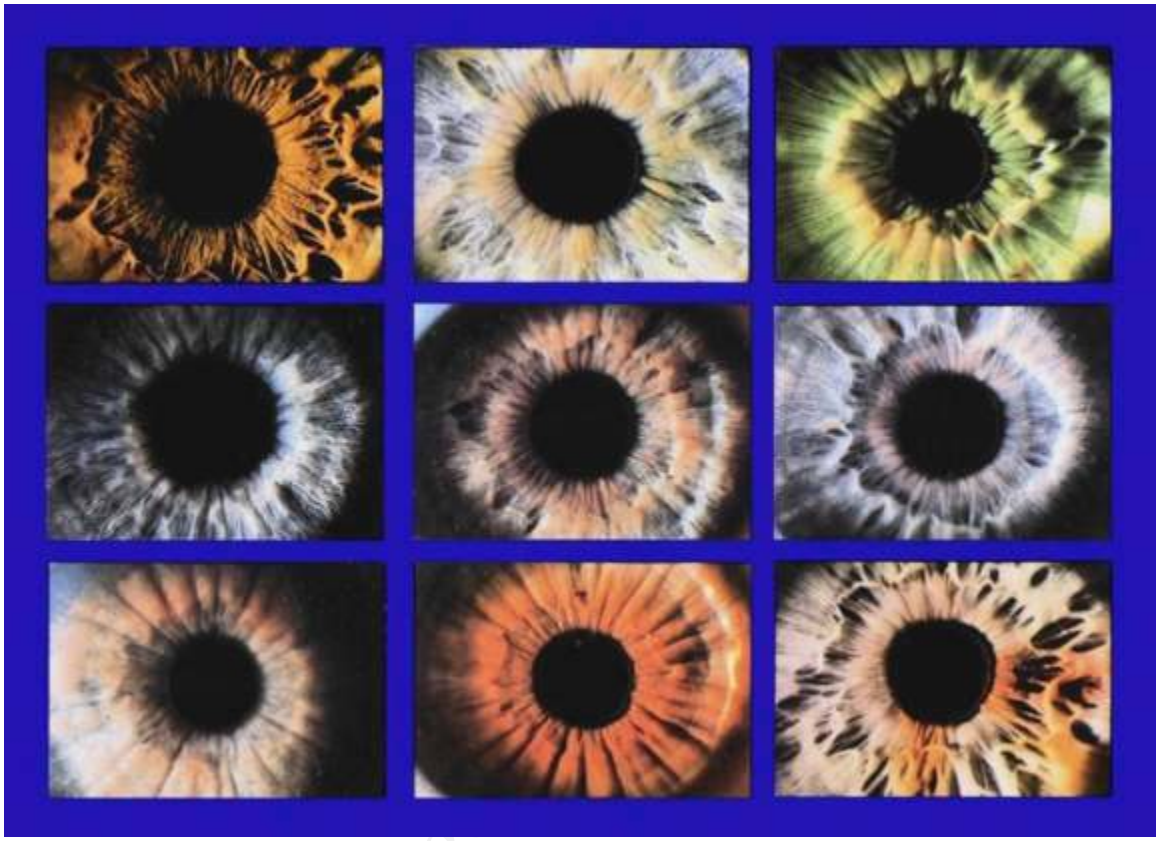

Figure 2: Collage of Irises[6]

Iris Recognition Process

The process of capturing an iris into a biometric template is made up of 3 steps:

1. Capturing the image
2. Defining the location of the iris and optimising the image
3. Storing and comparing the image.

1. Capturing the Image

The image of the iris can be captured using a standard camera using both visible and infrared light and may be either a manual or automated procedure. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the iris in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. The automatic procedure uses a set of cameras that locate the face and iris automatically thus making this process much more user friendly.

[6] http://www.cl.cam.ac.uk/users/jgd1000/iriscollage.jpg

2. Defining the Location of the Iris and Optimising the Image

Once the camera has located the eye, the iris recognition system then identifies the image that has the best focus and clarity of the iris. The image is then analysed to identify the outer boundary of the iris where it meets the white sclera of the eye, the pupillary boundary and the centre of the pupil. This results in the precise location of the circular iris.

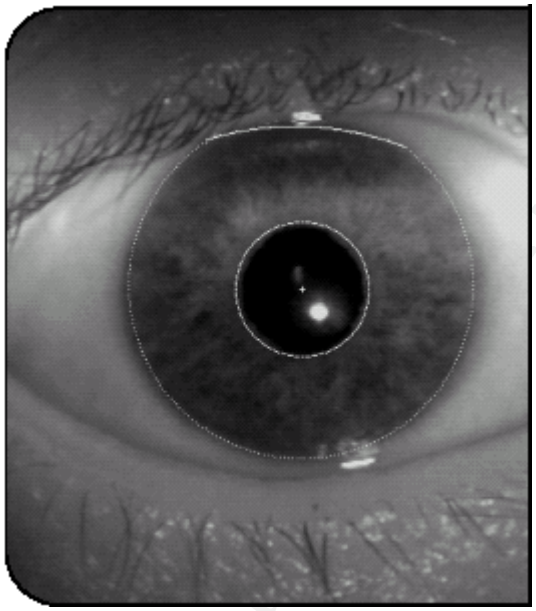

Figure 3: Circular Iris Location[7]

The iris recognition system then identifies the areas of the iris image that are suitable for feature extraction and analysis. This involves removing areas that are covered by the eyelids, any deep shadows and reflective areas. The following diagram shows the optimisation of the image.

[7] http://www.rycom.ca/solutions/pdfs/iridian/iris_whtppr.pdf

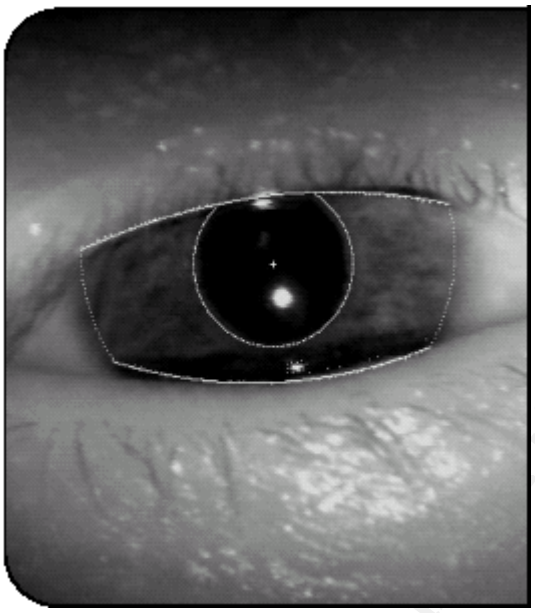

Figure 4:Optimising the Image[8]

3. Storing and Comparing the Image

Once the image has been captured, "an algorithm uses 2-D Gabor wavelets to filter and map segments of the iris into hundreds of vectors (known here as phasors)"[9]. The 2-D Gabor phasor is simply the "what" and "where" of the image. Even after applying the algorithms to the iris image there are still 173 degrees of freedom to identify the iris. These algorithms also take into account the changes that can occur with an iris, for example the pupil's expansion and contraction in response to light will stretch and skew the iris. This information is used to produce what is known as the IrisCode®, which is a 512-byte record. This record is then stored in a database for future comparison. When a comparison is required the same process is followed but instead of storing the record it is compared to all the IrisCode® records stored in the database. The comparison also doesn't actually compare the image of the iris but rather compares the hexadecimal value produced after the algorithms have been applied.

In order to compare the stored IrisCode® record with an image just scanned, a calculation of the Hamming Distance is required. The Hamming Distance is a measure of the variation between the IrisCode® record for the current iris and the IrisCode® records stored in the database. Each of the 2048 bits is compared against each other, i.e. bit 1 from the current IrisCode® and bit 1 from the stored IrisCode® record are compared, then bit 2 and so on. Any bits that don't match are assigned a value of one and bits that do match a value of zero. Once all the bits have been compared, the number of non-matching bits is divided by the total number of bits to produce a two-digit figure of how the two IrisCode® records differ. For example a Hamming Distance of 0.20 means that the two IrisCode® differ by 20%.

With all biometric systems there are two error rates that need to be taken into consideration. False Reject Rate (FRR) occurs when the biometric measurement taken from the live subject

[8] http://www.rycom.ca/solutions/pdfs/iridian/iris_whtppr.pdf
[9] http://www.iris-scan.com/iris_technology.htm

fails to match the template stored in the biometric system. False Accept Rate (FAR) occurs when the measurement taken from the live subject is so close to another subject's template that a correct match will be declared by mistake. The point at which the FRR and the FAR are equal is known as the Crossover Error Rate (CER). The lower the CER, the more reliable and accurate the system. In iris recognition technology, a Hamming Distance of .342 is the nominal CER. This means that if the difference between a presented IrisCode® record and one in the database is 34.2% or greater then they are considered to have come from two different subjects. During recognition mode, this comparison has to occur between the IrisCode® record from the live subject and every IrisCode® stored in the database before the live subject is rejected. The following table shows the probabilities of false accept and false reject with iris recognition technology:

Hamming Distance	False Accept Probability	False Reject Probability
.28	1 in 10^{12}	1 in 11,400
.29	1 in 10^{11}	1 in 22,700
.30	1 in 6.2 billion	1 in 46,000
.31	1 in 665 million	1 in 95,000
.32	1 in 81 million	1 in 201,000
.33	1 in 11 million	1 in 433,000
.34	1 in 1.7 million	1 in 950,000
.342	1 in 1.2 million	1 in 1.2 million
.35	1 in 295,000	1 in 2.12 million
.36	1 in 57,000	1 in 4.84 million
.37	1 in 12,300	1 in 11.3 million

Figure 5: Hamming Distances & Error Probabilities[10]

System Usage

Enrolment in an iris recognition system is normally quite fast. The actual capturing and testing of the image, administrative requirements and training of the subject can usually be accomplished in a couple of minutes. Subjects who wear glasses should remove their glasses during the initial enrolment in a recognition system to ensure that the best image is captured without any reflection from the lenses in the glasses. Contact lenses, on the other hand, do not need to be removed as they sit flush with the eye and hence have no reflections to impede the initial scan. After the initial enrolment most users are able to go through subsequent scanning without any additional instruction or assistance. Those who wear glasses no longer have to remove them after initial enrolment and wearing clear or coloured contact lenses pose no problems. Note that the same eye used during enrolment must be used during subsequent comparisons.

The comparison of a live subject IrisCode® record with all the IrisCode® records in the database may seem like a large amount of data to process, in reality it normally only takes a few seconds. This comparison speed is obviously affected by the speed of the system processor the database is running on and the size of the database itself.

[10] http://www.rycom.ca/solutions/pdfs/iridian/iris_whtppr.pdf

The proximity a user needs to be to the scanning system is usually dependant on the lens in use and the illumination. For example, systems scanning at the desktop PC level can operate with the subject seventeen to nineteen inches from the unit.

Advantages of Iris Recognition Technology

The physiological properties of irises are major advantages to using them as a method of authentication. As discussed earlier, the morphogenesis of the iris that occurs during the seventh month of gestation results in the uniqueness of the iris even between multi-birth children. These patterns remain stable throughout life and are protected by the body's own mechanisms. This randomness in irises makes them very difficult to forge and hence imitate the actual person.

In addition to the physiological benefits, iris-scanning technology is not very intrusive as there is no direct contact between the subject and the camera technology. It is non-invasive, as it does not use any laser technology, just simple video technology. The camera does not record an image unless the user actually engages it. It poses no difficulty in enrolling people that wear glasses or contact lenses. The accurateness of the scanning technology is a major benefit with error rates being very low, hence resulting in a highly reliable system for authentication.

Scalability and speed of the technology are a major advantage. The technology is designed to be used with large-scale applications such as with ATMs. The speed of the database iris records are stored in is very important. Users do not like spending a lot of time being authenticated and the ability of the system to scan and compare the iris within a matter of minutes is a major benefit.

Disadvantages of Iris Recognition Technology

As with any technology there are challenges with iris recognition. The iris is a very small organ to scan from a distance. It is a moving target and can be obscured by objects such as the eyelid and eyelashes. Subjects who are blind or have cataracts can also pose a challenge to iris recognition, as there is difficulty in reading the iris.

The camera used in the process needs to have the correct amount of illumination. Without this, it is very difficult to capture an accurate image of the iris. Along with illumination comes the problem with reflective surfaces within the range of the camera as well as any unusual lighting that may occur. All of these impact the ability of the camera to capture an accurate image. The system linked with the camera is currently only capturing images in a monochrome format. This results in problems with the limitations of greyscale making it difficult to distinguish the darker iris colourations from the pupil.

Although there is minimal intrusiveness with iris recognition, there is still the need for co-operation from subjects to enrol in the system and undergo subsequent authentication scans. Enrolling a non-cooperative subject would prove very difficult indeed. Inadequate training of users at the initial enrolment period will cause problems both at the initial enrolment time and subsequent authentications. Frustrated users will not help make the system any easier to use and will not be accepted by users as a convenient authentication method. Communication with users plays a major part in introducing such a system successfully.

As with all authentication methods it's important to remember to have a backup plan. Normal day-to-day problems such as system failures, power failures, network problems, and software problems can all contribute to rendering a biometric system unusable. Once users get accustomed to such a system it is unlikely that they will remember to bring their other forms of identification with them to the office. System administrators also have the additional pressure of ensuring the system that stores the iris record database is properly secured to prevent tampering with the data stored. Although these are not major hindrances to the actual iris recognition system it is important to take these things into consideration and have a backup plan.

Applications of Iris Recognition Technology

The most obvious use of iris recognition technology is within the computing environment. There is a lot of valuable data stored on a company's network and being able to access the network with a username and password is the most common method of authentication today. If a username and password is stolen then this gives the thief all of that person's access privileges and this can be detrimental to a company in today's competitive environment. Implementing an iris recognition system to authenticate users on the network means that there are no passwords to steal and no tokens to lose. Users are only able to access the systems they have privileges to access and it's very difficult for someone to replicate an iris for authentication. The technology can not only be used for securing log on but also in areas such as file and directory access, web site access and key access for file encryption and decryption. In a network environment, a system may be configured to compare the live template to the stored template and if a match is found then the user's access privileges are passed back to the client. In other implementations, after a match is found, the server returns a username and password to the client, which then transmits this information to the network server to allow access to the systems the user has privileges to. Enterprise applications are also being worked on in the areas of e-commerce, healthcare applications for medical records protection, insurance and brokerage transactions.

Another area iris recognition is useful with is physical security to data centres or computer rooms. Mounting a scanner by the access door and authenticating people via their iris is a good method of ensuring only those whose templates are in the database for computer room access are actually allowed in. This helps to alleviate problems associated with swipe card access where some systems have to be manually programmed with specific card numbers and robust processes need to be in place to ensure access lists are regularly reviewed. Swipe cards are also easily lost, stolen or borrowed.

Iris recognition is also being utilised or considered in other areas of daily life. ATMs are a major area where iris recognition is being trialled. The use of this technology with ATMs means that customers can discard their plastic cards and PINs thus eliminating the possibility of having cards and/or PINs stolen or lost. The banking industry is also involved in looking at implementing the technology in over the counter transactions with customers. This would reduce the requirement for customers to produce identification, bank books, account numbers etc and would result in faster transaction times that leaves the bank teller with more time to concentrate on the level of service provided to the customer.

Iris recognition is being considered in areas where there is a need for large throughput and queuing. For example border clearance, ticketless air travel, transportation and airport security. Airport security has seen a huge increase in focus after the recent events of September 11, 2001. Heathrow airport is already testing a system that scans a passenger's iris rather than the passenger needing to provide their passport. The aim behind the trial is to speed up processing of passengers and to detect illegal immigrants into the country. Currently, approximately 2000 passengers are participating in the trial that is due to run for five months. Passengers participating will have one of their irises stored in a database. When arriving at the airport, instead of presenting their passport, they proceed to a kiosk where their iris will be scanned by a camera and matched with the record stored in the database. Once a match is confirmed a barrier will open and the passenger is able to proceed as normal. More of these stations are due for trial at New York's JFK airport and Washington's Dulles airport.

Iris Recognition Products

Iridian Technologies, Inc of Moorestown, NJ and Geneva Switzerland holds the exclusive US and international patents for the core concepts and technologies behind iris recognition technologies. Iridian then license these processes to other companies who undertake systems development and integration with iris recognition.

There are a number of companies currently using the Iridian technology to produce systems. These include Iridian themselves in conjunction with LG Electronics and Panasonic, and EyeTicket Corporation. These products cover the areas of physical access, information security and the requirement for an authentication server to store the iris records.

Physical Access

Iridian have worked with LG Electronics to design a system to identify and authenticate user access to physical environments known as IrisAccess®. This system uses Iridian Technologies' iris recognition software and LG's imaging platforms to produce a system that has "superb accuracy, speed, scalability and convenience"[11].

EyeTicket Corporation produces a system known as EyePass™ that is primarily targeted at the aviation industry. This system is designed to control the movements of airport staff such as airport officials, ground staff, airline staff etc. The company also produces a product known as EyeTicket™ that is used for authenticating passengers travelling on airlines. It is used in conjunction with reservation systems and allows travellers to check in and board an aircraft simply by using the iris recognition system. This system can also be used for sporting and other events as a means of admission for people, thus reducing the need to have tickets, passes or other means of identification. As a result of this, costs are therefore greatly reduced and the speed at which people can be processed reduces the time waiting in queues. This product was successfully used during the Sydney Olympics 2000 with the German Olympic team to authenticate athletes, media, National Olympic Committee officials and dignitaries into the German Haus.

[11] http://www.iriscan.com/products.php?page=1&sub=a

Information Security

Iridian Technologies has combined with Panasonic to develop a system specifically designed to address the issues associated with passwords, PINs and token cards. The Panasonic Authenticam™ utilises PrivateID™ iris recognition software developed by Iridian Technologies. This software is designed to allow "an iris recognition camera to capture, select and secure iris images"[12]. The Panasonic Authenticam™ allows administrators to secure PCs, files, folders, and applications etc to only authorised users within the company. It helps to reduce the costs associated with password management and reduce the risk of fraudulent activities. An added benefit of the product is the ability of the camera to be used for video conferencing and online collaboration.

Authentication Server

A key component to any iris recognition system is a server to store the iris records on and to process the authentication. Iridian Technologies produce a system known as KnoWho™ Authentication Server designed specifically to store iris images created by the PrivateID™ software. This system can be integrated into "transaction systems, mission critical applications and/or network environments requiring high performance authentication capabilities"[13]. The system has two major functions: it has a storage function for IrisCode® records and an enrolling and real time matching system. When a match is found within the system it provides only a unique identification number, it does not release any personal information thus preserving the privacy of the individual.

In the past, iris recognition technology has been quite costly to implement. However, as with most technologies, the cost of hardware and software is decreasing. A device for a single PC that provides information security can be purchased for as little as US$239 and the minimum requirements for the PC to install the software on is a standard Pentium MMX class 333MHz PC with a minimum 64MB RAM and 30MB free hard disk space.

Conclusion

The need for secure methods of authentication is becoming increasingly important in the corporate world today. Passwords, token cards and PINs are all risks to the security of an organisation due to human nature. Our inability to remember complex passwords and tendency to write these down along with losing token cards or forgetting PINs all contribute to the possible breakdown in security for an organisation.

The uniqueness of the iris and low probability of a false acceptance or false rejection all contribute to the benefits of using iris recognition technology. It provides an accurate and secure method of authenticating users onto company systems, is a non-intrusive method and has the speed required to minimise user frustration when accessing company systems. Users no longer have to worry about remembering passwords and system administrators no longer need to worry about the never-ending problem of users disclosing passwords or having weak passwords that are easily cracked. If a two-factor authentication system is implemented, for example iris recognition

[12] http://www.iriscan.com/products.php?page=2&sub=a&sec=1
[13] http://www.iriscan.com/products.php?page=3

with a smart card, then the strength of authentication increases and provides another part to "defence in depth" for the company.

References

1. Iris-scan.com. Iris Recognition: The Technology.
   URL: http://www.iris-scan.com/iris_technology.htm (11 February 2002)
2. Iris-scan.com. Iris Recognition: Issues.
   URL: http://www.iris-scan.com/iris_cautionary.htm (11 February 2002)
3. Iris-scan.com. Iris Recognition in Action.
   URL: http://www.iris-scan.com/iris_recognition_applications.htm (28 February 2002)
4. Daugman, John. History and Development of Iris Recognition
   URL: http://www.cl.cam.ac.uk/users/jgd1000/history.html (19 February 2002)
5. Daugman, John. Some Possible Applications of Iris Recognition
   URL: http://www.cl.cam.ac.uk/users/jgd1000/applics.html (28 February 2002)
6. Daugman, John. Advantages of the Iris for Identification and Disadvantages of the Iris for Identification.
   URL: http://www.cl.cam.ac.uk/users/jgd1000/addisadvans.html (11 February 2002)
7. Daugman, John. Iris Collage.
   URL: http://www.cl.cam.ac.uk/users/jgd1000/iriscollage.jpg (4 March 2002)
8. Ashbourn, Julian. The Biometric White Paper. 1999.
   URL: http://homepage.ntlworld.com/avanti/whitepaper.htm (13 February 2002)
9. Ashbourn, Julian. Vulnerability with Regard to Biometric Systems. 2000
   URL: http://homepage.ntlworld.com/avanti/vulnerable.htm (13 February 2002)
10. Dye, Brian. Gerttula, Jeff. Kerner, Jonathan. O'Hara, Brian. An Introduction to Biometrics.
    URL: http://www.stanford.edu/~bjohara/iris.htm (11 February 2002)
11. Iridian Technologies. Science Behind the Technology.
    URL: http://www.iriscan.com/basics.php?page=5 (14 February 2002)
12. Iridian Technologies. Physical Access products. 2001.
    URL: http://www.iriscan.com/products.php?page=1&sub=a (26 February 2002)
13. Iridian Technologies. Information Security products. 2001.
    URL: http://www.iriscan.com/products.php?page=2&sub=a&sec=1 & http://www.iriscan.com/products.php?page=2&sub=a&sec=2 (26 February 2002)
14. Iridian Technologies. Authentication Server. 2001.
    URL: http://www.iriscan.com/products.php?page=3 (26 February 2002)
15. Eye Ticket Corporation. Iris Recognition
    URL: http://www.eyeticket.com/technology/irisrecog.html (19 February 2002)
16. Eye Ticket Corporation. EyePass™
    URL: http://www.eyeticket.com/eyepass/index.html (26 February 2002)
17. Eye Ticket Corporation. EyeTicket™
    URL: http://www.eyeticket.com/eyeticket/index.html (26 February 2002)
18. Eye Ticket Corporation. EyeTicket™ - Sport
    URL: http://www.eyeticket.com/sportscan/index.html (26 February 2002)
19. Eye Ticket Corporation. EyeTicket Corporation and German Haus Team to Provide High-Tech Admissions at 2000 Olympics. 2 August 2000
    URL: http://www.eyeticket.com/company/press-room/80200.html (26 February 2002)

20. Cambier, James L. Iris Recognition and Network Security.
URL: http://www.mi5.co.nz/mi5/docs/iridian.pdf (19 February 2002)
21. Williams, Gerald O. Iris Recognition Technology. February 2001
URL: http://www.rycom.ca/solutions/pdfs/iridian/iris_whtppr.pdf (11 February 2002)
22. Liu, Simon & Silverman, Mark. A Practical Guide to Biometric Security Technology.
URL: http://www.computer.org/itpro/homepage/Jan_Feb/security3.htm (11 February 2002)
23. International Biometric Group. Iris Recognition
URL: http://www.biometricgroup.com/a_bio1/technology/cat_iris.htm (11 February 2002)
24. BBC News. Airport tests passenger eye IDs. 8 February 2002.
URL: http://news.bbc.co.uk/hi/english/uk/newsid_1808000/1808187.stm (26 February 2002)
25. McMordie, Dave. Texture Analysis of The Human Iris For High Security Authentication. December 3 1997.
URL: http://www.cim.mcgill.ca/~mcmordie/iris_recognition.html. (11 February 2002)
26. Malmsten, Valerie. Eye Scans – Authentication with Biometrics. 21 November 2000.
URL: http://rr.sans.org/authentic/eye_scans.php (11 February 2002)

Last Updated: July 31st, 2014

Upcoming SANS Training

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

SANS San Antonio 2014	**San Antonio, TXUS**	**Aug 11, 2014 - Aug 16, 2014**	**Live Event**
Cyber Defense Summit & Training	**Nashville, TNUS**	**Aug 13, 2014 - Aug 20, 2014**	**Live Event**
SANS SEC401 Bootcamp @ Malaysia 2014	**Kuala Lumpur, MY**	**Aug 18, 2014 - Aug 23, 2014**	**Live Event**
SANS Virginia Beach 2014	**Virginia Beach, VAUS**	**Aug 18, 2014 - Aug 29, 2014**	**Live Event**
SANS Chicago 2014	**Chicago, ILUS**	**Aug 24, 2014 - Aug 29, 2014**	**Live Event**
SANS Pen Test Bangkok 2014	**Bangkok, TH**	**Aug 25, 2014 - Aug 30, 2014**	**Live Event**
SANS Delhi 2014	**New Delhi, IN**	**Aug 27, 2014 - Sep 02, 2014**	**Live Event**
SANS Tallinn 2014	**Tallinn, EE**	**Sep 01, 2014 - Sep 06, 2014**	**Live Event**
SANS Brisbane 2014	**Brisbane, AU**	**Sep 01, 2014 - Sep 06, 2014**	**Live Event**
Security Awareness Summit & Training	**Dallas, TXUS**	**Sep 08, 2014 - Sep 17, 2014**	**Live Event**
SANS Crystal City 2014	**Crystal City, VAUS**	**Sep 08, 2014 - Sep 13, 2014**	**Live Event**
SANS Bangalore 2014	**Bangalore, IN**	**Sep 15, 2014 - Sep 27, 2014**	**Live Event**
SANS Albuquerque 2014	**Albuquerque, NMUS**	**Sep 15, 2014 - Sep 20, 2014**	**Live Event**
SANS ICS Amsterdam 2014	**Amsterdam, NL**	**Sep 21, 2014 - Sep 27, 2014**	**Live Event**
SANS Baltimore 2014	**Baltimore, MDUS**	**Sep 22, 2014 - Sep 27, 2014**	**Live Event**
SANS DFIR Prague 2014	**Prague, CZ**	**Sep 29, 2014 - Oct 11, 2014**	**Live Event**
SANS Seattle 2014	**Seattle, WAUS**	**Sep 29, 2014 - Oct 06, 2014**	**Live Event**
SANS Hong Kong 2014	**Hong Kong, HK**	**Oct 06, 2014 - Oct 11, 2014**	**Live Event**
SOS: SANS October Singapore 2014	**Singapore, SG**	**Oct 07, 2014 - Oct 18, 2014**	**Live Event**
SANS Perth	**Perth, AU**	**Oct 13, 2014 - Oct 18, 2014**	**Live Event**
GridSecCon 2014	**San Antonio, TXUS**	**Oct 14, 2014 - Oct 14, 2014**	**Live Event**
SANS Network Security 2014	**Las Vegas, NVUS**	**Oct 19, 2014 - Oct 27, 2014**	**Live Event**
SANS DHS Continuous Diagnostics and Mitigation Workshop with Training	**OnlineDCUS**	**Aug 01, 2014 - Aug 08, 2014**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**