Global Information Assurance Certification Paper

Matthew Newell
SANS GSEC Option 1
Submission 1.4b
Washington DC, Dec 2003
18 May 2004
Biometrics: Retinal Scanning: Out of Sight

Abstract

The purpose of this paper is to provide to the reader an in depth understanding of the processes involved with Retinal Scanning and to determine if its benefits outweigh its shortcomings in biometrics. The methods introduced will cover the biometric authentication process, an in depth walk through of retinal scanning and concerns behind the use of this reliable form of biometrics. These concerns are manifested in the way of personal safety, privacy and efficiency of the methods in discussion. The alternate methods of biometrics will be introduced and briefly discussed in terms of process and credibility. The technology explored in depth will only pertain to retinal scanning, as this is the only technology under investigation. Although the technology surrounding the other biometric options will be mentioned, there will be analysis of these methods only in regards to safety, privacy and efficiency.

Introduction

The concepts involving every realm of security are tied together by a common goal. This desired state of security is an objective that should translate across each entry point and anything that could become one. To construct a 60 ft cement wall, 15 ft thick, around a facility and have a single firewall[1] as a network boundary[2] solution would guarantee that no one would physically walk in. However, they might buy a book on hacking firewalls for numbskulls, and eventually gain access to all the information. The reverse situation should be considered equally foolish; a single armed guard to address authentication measures surrounding a private network with, let's say, banking information stored on its servers. Even the most feeble, hacker could casually approach the armed guard, under disguise, and make their way to the server, and be off with sensitive and lucrative information.

These and other inconsistencies come to mind when we read about the awesome power of the dedicated, well funded hacker who whips up a tool that is nothing short of brilliant in outsmarting network security infrastructures. A little further into the same article, one could discover a link, leading to the preventive measure or detection measure that should have been taken and how if we were just a little more mindful of the technical aspects, the damage could have been avoided. These things sound disturbing to a network security engineer but we learn as we sit in a secure lab that has several layers of security between us and the outside world. Should the same drastic measures be taken upon authentication of users who enter the premises?

Of course they should. In the next sections we will discuss user authentication, its importance and techniques. As we approach an understanding of the need for a more sufficient means of authentication, the ideas and practices of modern biometrics will be introduced. The final biometric introduced, retinal scanning will be examined in depth for its effectiveness, shortcomings, physiological aptitude

and concerns surrounding safety of use. The idea of retinal scanning does indeed push the envelope as far as invasiveness and efficiency goes in the overall process of authentication. Through the research performed, we will see that until the next technological breakthrough, there is a place for all biometric applications. Authentication is the subject by which we begin to introduce the topics surrounding biometric methods before covering the specifics behind retinal scanning.

Authentication

Authentication[1] methods are a security concern in 360 degrees of access. We will concentrate on authentication pertaining to the access that is granted to users with the desired credibility. The goal is to prove genuine, the user who seeks passage. As the automated methods of authentication appear in our offices, our cyber space and our government, there are those who seek to counter these efforts on every respective level. These authentication methods are independently brilliant but not absolute. As the different methods are explored, the fact is that for each one to provide the best measure of defense, it must be coupled with other forms of authentication in order to mitigate each shortcoming. These supplementary strategies, when grouped, form what is called Defense in Depth[3]. The following provides examples of authentication and illustrates a clearer picture of Defense in Depth.

Johnny User drives into work, shows his photo ID to the security guard at the entrance to the parking facility, swipes the magnetic badge to gain access to the building, punches in his code to get into the lab he works in, sits in his assigned workstation on a chair that is calibrated to trigger Johnny's access according to the weight applied to the seat (plus or minus 10lbs, of course). Once "big brother" has added up and verified that all the previous four security measures were taken and passed in sequence, he can key in his simple, lazy password and get to work surfing the web.

How do we know this is really Johnny User? He presented something he had that proved him genuine, his photo ID and magnetic badge. Then, Johnny punched in the code on the door to get in the lab which was something he knew and hopefully is not written on a post it next to the door. Finally, we get to the biometric, his weight or "something he is". Certainly the weight applied to the chair at Johnny's terminal alone is, not by any stretch, a means to verify that Johnny is who he says he is. Perhaps if there were something that Johnny "was" that was also sophisticated and more importantly, unique to him and no one else, we might be getting somewhere with a more subtle method of secure authentication[4].

Although the scenario indicates the use of several layers of authentication before the user can access network information, a motivated, well funded, and well-organized effort can slip right through this security system. On the basis that

each method can be captured and reproduced, this rather meticulous security set-up is considered vulnerable. Sounds like a long shot? The same philosophy applies to network security professionals who are hounded to read each and every transaction log that displays on their monitoring system. If IP addresses couldn't be spoofed, would we need to worry so much about the large assortment of DDoS[5] attacks that are waiting in the shadows of cyberspace? Many of us would be in another line of work. This same philosophy should apply to all dimensions of security. Going back to the scenario, we could spoof the user's badge, photo, appearance, weight and in some unmentionable fashion gather the necessary information from him to gain access to his computer. After all, the fact is that not every cleared technology guru is trained in combat torturing avoidance and submission techniques. The facts surrounding different instances where authentication with little or no margin of error is heavily relied upon are what perpetuate the surging research in biometrics.

Biometrics

Biometric authentication methods are reinventing security procedures across commercial and private industry and across federal, state and local government and in the military. "Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic"[21]. In this document we will explore some of the more common sources of biometric recognition: face, fingerprints, hand geometry, handwriting, iris, retinal and vein. Each method uses a database to store a template, which is acquired at the initial reading and later used to compare proceeding authentication attempts for access. Before we engage in the depths of retinal scanning we will first summarize and briefly explore the alternative methods of biometric authentication.

When looking at biometric methods from a distance, we can ascertain that the measuring of human expanse, initially, is complex and invasive at best. Although the idea is quite ancient, the goal has remained a constant. In the late 1800's, Alphonse Bertillon, a clerk at a police desk in Paris, created a technique that actually measured exterior portions of the human body such as height, length of limbs, digits and a host of other tangible symmetries to authenticate criminals[20]. At that point in history, the technology involved was nothing short of the metric system. About 400 years before that, an explorer, Joao de Barros, in China discovered a technique to identify children by printing their footprints and palm prints on paper to distinguish young children from one another[7]. Advancements in technology would soon provide alternative methods, extinguish the previous solutions and lead to proficiency in verifying that users/subjects are indeed who they claim to be. Since the foundation of biometrics resides at the hands of accuracy and precision, there exists a margin of error that must be reckoned with. There will be temper mental occurrences during attempts at authentication in which the system either read a true user as false and a false user as true. The rate at which a machine reads a valid user as false, or invalid, is called the false rejection rate, or FFR[8]. The rate at which an invalid user is identified as true, or

valid, is referred to as the false acceptance rate, or FAR. Now let us take a look at some of the different methods of biometrics[8].

Face Recognition

Face recognition is executed by examining the features of a person's face by way of digital video imagery[22]. The concept first underwent research in the 1960's and later began further research and testing in the 1980's. This process measures characteristics such as the distances of the subject's facial construction points such as the pupil distance, dimensions of the nose, and the mouth and dimensions of the jaw[22]. Terminals designed to verify face structure are constructed with either a single camera or multiple cameras which capture the image of the subject from many angles using 3D capability and assemble the biometric points for verification or by the use of a single camera in which the user looks directly at one lens. The initial read is used to create a template for which the proceeding reads will be compared to[22]. Either method demonstrates the strong selling point of facial recognition, non-intrusiveness, which has been a major concern of biometrics as a whole[9]. In essence, this mechanism simply provides a visual Identification of the subject just as another human would, given the assignment of memorizing everyone who enters and exits the premises. The expression on a user's face can be a factor even with today's technology[22]. The instance of false positives, or when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action[10], is still relatively intolerable among the possible fields of deployment. When people are waiting in line in a delayed airport, it is reasonable to assume that their facial expression may be a little different from the template created, and be, therefore, difficult for the device to read. This could potentially cause a delay or lack of faith of the security personnel monitoring the reads[11].

Fingerprint

Fingerprints are read by using "an image of a person's fingertips and recording its characteristics"[7]. The skin on the tips of the fingers is different from the skin everywhere else on the body. The exterior layer of the skin, or epidermis, fold into deep ridges forming unique patterns of arches, loops and swirls[12]. These patterns make up minutiae points on the surface of the fingers that are the building blocks of fingerprints. Once the points are identified, a computer searches a database for matches to the minutiae points[23]. To process a subject's fingerprints, there are slightly more proactive measures needed on the part of the subject. They must place their finger on the surface of a scanner/reader. The scanner is connected to a system that transfers the read to a matching program and queries the databases for a match[13]. The entire process is relatively non intrusive and takes little time to complete verification. However some of the disadvantages can present a hindrance or even prevent authentication form taking place. In the instance of a huge database in which the templates are stored, it could take a relatively troublesome length of time to

access the correct file[14]. If a user's hand is unclean or the skin is cut or scraped, it could present a problem in the reading process contributing to the false positive rate[14].

Hand Geometry

Hand Geometry is measured by using specialized hardware to read specific characteristics of a subject's hand to verify authenticity[7]. The hardware is constructed of a metal surface equipped with pegs used to direct the subject's hand placement. Once the subject's hand is in the desired position, the reader takes the required measurements[7]. These measurements are then referenced on the database and a match is queried. The entire process is hardly considered intrusive and takes only a few seconds[14]. The shortcoming associated with this method is its static design. The process has been relatively unaffected by technological advancements as it requires a larger area to install and use. The products designed with hand geometry authentication points are typically less discrete compared to the other methods used. The hand geometry scanner's capability to only utilize a 1-to-1 verification limits its applications as well. The features of a person's hand are not permanent and can rather easily be damaged, as injuries to hands are not uncommon[11]. This aspect of biometrics is, however, effective when coupled with other methods or layers of recognition[7].

Handwriting

There are two methods of identifying subjects by examining the way they write. The first considers the handwriting an image complete with texture. The evaluation of this texture uniquely identifies the author of the handwriting[4]. This method uses a sophisticated filtering technique to determine the difference in texture throughout the writing strokes. This filtering is coupled with a classification system to form a means for which to identify each point of consistency. The miniscule variables that identify the author are also accounted for in the way of speed of the strokes used to create a signature and the pressure that is applied to each mark. These two factors are not readily visible to the unsuspecting writer[7]. The stability, however, of a user's handwriting is a potential cause of false positives. Many factors play a role in how much pressure is placed on the signing device or the stylus as well as the speed of each stroke[4]. These inconsistencies can play a role in producing a higher number of false positives and cause the efficiency of the system to sharply decrease[24].

Iris Scanning

Iris scanning is one of the more sophisticated techniques in biometrics. The iris, much like a snowflake, is unique in makeup and is the part of the eye that determines the color[17]. Even the two eyes you're using to read these pages are suited with irises unique to one another[13]. At the exterior portion of the eye, the cornea is the first layer that receives light. It stretches over the iris and the pupil.

The iris controls how much light enters the eye by reacting to the current intensity of light[17]. When the amount of light is greater than needed, the iris constricts to a smaller diameter. When there is a shortage of available light, the iris dilates to a larger diameter harvesting even the faintest light sources[15]. These changes in diameter are significant as a means of protection against subversion attempts. The image interpreted by the machine scanning the iris can first identify the fact that the iris is responding to the light of the scanner before initializing the scan of the iris[13]. The actual authentication method is executed by capturing what is usually a black and white video image of the iris. If the process included capturing the color of the iris for evaluation as well, it would potentially fault on anyone with eyes that do not maintain a constant color. Then the measurements of the exterior circumference and interior circumference are taken with respect to the pupil, which lies in the center, or behind the iris. The pattern within the iris is mapped and measured to establish an IrisCode. This code is stored in a file independently or with another identifier on a database. One true disadvantage of this is the unknown health risks that, at this point are almost reduced to myths. Much like the onset of LASIK eye surgery[15], many users are concerned with the potential long-term damage that could occur over a continued use of the scanning system. Vendor's claims on the success of Iris recognition have made claims of such a level of effectiveness, the implication is that it is a one for all cure for authentication purposes. One item to keep in mind is that should a company consider using Iris recognition as their sole means of access, the users who become comfortable with not carrying access cards or badges will be in for a troubling surprise should the system be out of service[11]. The users, who care not to be ready for such an instance, will be locked out or even worse, locked in. The primary delay in the installation of this method would reside in the lack of understanding and the reluctance of the potential users[11]. After all, the mechanism obtains information from a most precious sense, vision.

Vein Recognition

Vein recognition methods involve the capturing of images as most of the previously discussed methods of authentication. The veins located on the back of a hand are targeted for the measurement. An image of this community of veins is captured in black and white and stored in a template[6]. Some of the applications abroad use a rather basic system of PC-based software and smartcards combined with a digital camera. This model uses a collection of images and filters to enhance the contrast between the veins and the rest of the hand. Vein recognition vendors can make a claim for the fastest known recognition time of all biometric recognition systems[6]. These vendors, such as VeinID, have constructed systems that verify the user/subject in less than 0.5 seconds[18]. The registration time, equally proficient, resides at approximately 0.5 seconds[18]. While this method of authentication has proven extremely efficient, there are feasible methods to forge the process and trick the scanner into thinking that the image is real. As far-fetched as this might sound, the

technology engineered to provide authentication itself was once considered far-fetched at best.

Review: Methods of Biometrics

Several alternatives have been mentioned to providing authentication under this reinvented, technological breakthrough called biometrics. Each instance has resourced the use of imagery to measure the uniqueness of either an exterior or interior subtlety of the human body. Another common characteristic of each method is that each process is constructed to promote the presence of a log of who is successfully reaching authentication. This notion provides a mechanism for detection[3], objective number one in network security. Should a system be 'outsmarted', it is equipped with the capability of recording when the subversion occurred, which entity in the database, or who, was compromised as well where the occurrence took place if there are indeed multiple authentication points. Each of the methods introduced has a shortcoming no matter how trivial or likely it may seem. These imperfections are typically supplemented with other methods of authentication as in the example in the Biometrics section of this document. The methods harboring issues involving efficiency and excessive false positives do have their respective places in security and can provide an invaluable degree of security in the right settings. There are instances in the security field that require the highest levels of security. These instances, such as Banking and Military Intelligence Installations, require the services of the most accurate form of authentication regardless of shortcomings not related to accuracy or false negatives. A false negative is referred to as a Type I error and occurs when a system rejects an authorized user[9]. The most effective approach to biometric authentication available is retinal scanning.

Retinal Scan Reasoning Behind Exactness

The question still remains the same as it does for all forms of authentication: Are we absolutely sure? This question is, more than ever, being sought in cutting edge technology under the research of methods such as retinal scanning. While this method of biometrics may prove to be the closest thing to absolute, the notion weighing in heaviest is, "Is it really worth it?" Is it worth the intrusiveness or the potential damage? After all, the results are the closest to absolute, but not absolute.

The concept of retinal scanning was actually first introduced nearly seven decades ago. Research as far back as the 1930's suggested that the blood vessels at the back the eye form patterns unique to each individual[6]. Much later, in 1984, a company called EyeDentify made the first successful retinal scans. The Eyedentification 7.5 was the first retinal scan developed for commercial use[6]. Since then, many advancements in technology have obviously taken place, which have contributed a more sufficient version of retinal scanning. The time it takes to create a template or execute an attempt at authentication has decreased simply out of the faster computer systems.

As in other frontiers of research and development, there is one avenue that embraces a philosophy strictly catering to perfect outcome under the truest representation that technology can provide. In biometrics, this is retinal scanning. The stride for absolute verification/identification short of an autopsy is the philosophical grounds under which this method is based. While retinal scanning provides the most reliable method out of those introduced, it has its disadvantages. Before we introduce the process of the retinal scan itself we will first take a snapshot of the eye and what happens to light as it passes through in efforts to better understand the educated concerns behind retinal scanning.

Physiological Process of the Retina

Retinal scanning involves the reading of vascular patterns found on the back of the eye[13]. This method requires light to pass through each physiological layer of the eye that provides vision. The following segment will walk us through the path of light as it enters the eye, on its way to the retina.

Light approaches the eye and moves through the cornea. The cornea is the clear surface of the eye on which the eye re-hydrates every time you blink. Because the cornea lines the exterior portion of a sphere it is convex by definition. The fact that it is a clear layer means it causes light to bend, or refract, as it passes through.

Behind the cornea, the Anterior Chamber is the portion that has a slightly higher convexity allowing further refraction as the light passes through. Beyond this portion is the iris. The iris is in the shape of a doughnut and is the portion of the eye that holds color[17].

As the iris senses the amount of light entering, it expands and contracts to let more or, in other cases, less light in. Next, the light rays pass through to the iris. The interior circle of the iris is known as the pupil. The pupil is the window in which light passes through to the crystalline lens. The crystalline lens is mechanism that focuses light as it passes through to the retina. Unlike the vascular pattern found inside the eye, the crystalline lens changes throughout the life of an individual. It gradually grows thicker and thicker causing eventual nearsightedness in someone who was born with perfect vision. This is why some patients in the optical industry need glasses up until a slightly advanced age group and then suddenly don't need them anymore. The crystalline lens grew to a magnification that actually corrected the previously imperfect vision. Once the light source and images carried by it reach the retina, they are suited for interpretation. To interpret these images the retina is lined with photoreceptors. In regards to the objective of this document, this is the extent to which we will explore the physiological survey of the retina.

Retinal Scanning Process

The most current technology involves three steps in executing a retinal scan. First, the image is acquired by locating the optic disk and a photograph is taken[16]. Second, a circular barcode is constructed using software, which translates the different sizes of the blood vessels into a summary pattern[16]. Lastly, the pattern of the image is matched against the database[16]. Each of these basic steps has subsequent steps which provide the gathering and verification of the unique information represented by the eye.

The first of the three basic steps previously listed, is where the template is gathered from the user for future queries. The user removes their glasses if they are eyeglass wearers and places their eye approximately three inches away from the lens and maintains an open eyelid for several moments[13]. At this point a low intensity light is directed through the eye to the interior regions of the retina. In the next moment, the mechanism reads the vascular pattern on the back of the eye. When the user is initially enrolled in the system it can take up to 20 seconds to read and store the record[13]. This is the most tedious process for the user and mechanism to execute, as this most likely is the user's first encounter with the device during this particular session of authentication[6]. Once the image is captured, the device moves on to the next step, creation of the barcode.

The different points created by each change in the path and or thickness of each vessel in the eye is translated into a sequence of bars to represent a code that defines the uniqueness of the image. This barcode is then sent for a matching process to the database in search of a corresponding registered barcode[16].

The match can be queried at 1-to-1 or 1-to-many[16]. This flexibility is essential in creating the quickest processing technique in the entire session of authentication. The confidence in the uniqueness of each record in the database is the highest in the business[16]. This confidence is passed along to every user in the form of a recognition error rate of 1:10,000,000. This is more than 75 times more accurate than iris scanning at a distant second at 1:131,000[13].

Worth a Look

This is by far the most intrusive method available in biometrics[6]. It does require the active participation and full cooperation of each user. There is no conclusive evidence that the current technology used has damaging effects on the eye. There are instances in which the application of retinal scanning does have a place in securing information and physical access. Retinal scanning provides the highest accuracy rating available and are yet to be out done by any other standard method of authentication. Each method has its own shortcoming or disadvantage. The effort to strive for the most secure conventions where they are needed remain justified and worthy of the investment in settings, which demand the foremost security.

Conclusion

In the information uncovered in this paper, we can see that there is indeed a place for the installation and use of retinal scanning. The reluctance of some areas or particular users to subscribe to a method as involved as retinal scanning will be met with a more informative approach. The security sectors that necessitate a device with services such as a retinal scan will inherently be in a community in which there is not significant information that is not initially known by the security department. As a result, the users who are concerned with privacy literally don't have anything to hide. Retinal scanning does, and will, play a role in security today and in the near future. It is simply up to the community to associate this, like all other resources, to its optimal opportunities for application.

Notes

[1] Stallion Support, Quick Navigate 2002 to 2004 Glossary of Terms 15 April 2004 http://www.stallion.com/html/support/glossary.html

[2] "Jasomi Enhances Network Boundary Traversal Capabilities for Microsoft Office Live Communications Server" 15 April 2004 Jasomi Networks 25 April 2004 http://www.jasomi.com/pr_microsoft04.html

[3] "Perimeter Defense-in-Depth: Using Reverse Proxies and other tools to protect our internal assets"
18 February 2002 Morrison, Lynda 25 April 2004
http://www.sans.org/rr/papers/35/249.pdf

[4] Kuhn
http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf

[5] Cisco Systems "Strategies to Protect Against Distributed Denial of Service (DDoS) Attacks"
http://www.cisco.com/warp/public/707/newsflash.html

[6] Jain, A K., et al.
http://www.biometrics.org

[7] Steketee
http://www.ncsconline.org/

[8] Olsson
http://www.sans.org/rr/papers/index.php?id=1226

[9] Charles
http://faculty.capitol-college.edu/~kacharles/CS401-Fall-2003-syllabus.pdf

[10] Imparato
http://www.intelligententerprise.com/020416/507bus_impact1_1.jhtml

[11] The Biometric Group
http://www.biometricgroup.com/reports/public/reports/hand-scan_strengths_weaknesses.html

[12] Babler
http://www.ridgesandfurrows.homestead.com/FSG2.html

[13] Dunker
http://www.sans.org/rr/catindex.php?cat_id=6

[14] English
http://www.bsu.edu/web/awenglish/SCHOOL/ITEDU_510/ta.html

[15] Knobbe
http://www.eyemdlink.com/EyeProcedure.asp?EyeProcedureID=8

[16] Heacock
http://www.retinaltech.com/index.html

[17] National Eye Institute
http://www.nei.nih.gov/photo/eyean/index.asp

[18] VeinID
http://www.veinid.com/product/index.html

[19] The Biometric Consortium, Introduction to Biometrics
http://www.biometrics.org/html/introduction.html

[20] Moenssens, Andre A., Forensic-Evidence.com 2002 Identification Evidence
http://www.forensic-evidence.com/site/ID/ID_bertillion.html

[21] The Biometric Consortium, Introduction to Biometrics
http://www.biometrics.org/html/introduction.html

[22] Tanzeem, Choudhury, "History of Face Recognition", 21 January 2000 MIT Technical Reports 15 April 2004
http://vismod.media.mit.edu/tech-reports/TR-516/node7.html

[23] Prabhakar, Salil and Jain, Anil 2003 Mississippi State University Computer Science Dept. 15 April 2004
http://biometrics.cse.msu.edu/fingerprint.html

[24] Mainguet, Jean-Frances 2001 January Biometric Handwriting 15 April 2004
http://perso.wanadoo.fr/fingerchip/biometrics/types/handwriting.htm

Works Cited

Babler, William J. Frictional Skin Growth. 03 Nov. 2001. Forensic Forum. 15 Apr. 2004 <http://www.ridgesandfurrows.homestead.com/FSG2.html>.

Biometric Group. 05 Jan. 2004. Biometric Group. 29 Apr. 2004 <http://www.biometricgroup.com/reports/public/reports/hand-scan_strengths_weaknesses.html>.

Biometrics: A Technology Assessment. <http://www.bsu.edu/web/awenglish/SCHOOL/ITEDU_510/ta.html>.

Charles, Kellep A. CS 401 E01 Network Security. 21 Aug. 2003. Capitol College. 15 Apr. 2004 <http://faculty.capitol-college.edu/~kacharles/CS401-Fall-2003-syllabus.pdf>.

Crews, Clyde W. Cato Institute. 01 Jan. 2004. Cato Institute. 18 Apr. 2004 <http://www.cato.org/pubs/pas/pa-452es.html>.

Dunker, Mary . SANS Reading Room. 08 Mar. 2004. SANS Institute. 05 Apr. 2004 <http://www.sans.org/rr/catindex.php?cat_id=6>.

English, Alex W. Biometrics: A Technology Assessment. 22 Apr. 2004. IS Dept., Ball State University. 29 Apr. 2004 <http://www.bsu.edu/web/awenglish/SCHOOL/ITEDU_510/ta.html>.

Heacock, Greg, and David Usher. Retinal Technologies. 06 Nov. 2001. Retinal Technologies. 15 Apr. 2004 <http://www.retinaltech.com/index.html>.

Imparato, Nicholas. Intelligent Enterprise. 16 Apr. 2002. Dept. of Marketing, University of San Francisco. 05 Apr. 2004 <http://www.intelligententerprise.com/020416/507bus_impact1_1.jhtml>.

Jain, A K., et al. The Biometric Consortium. 04 Apr. 2003. The Biometric Consortium. 15 Apr. 2004 <http://www.biometrics.org>.

Knobbe, Chris A. M.D. 2000 EyeMDLink 15 April 2004 <http://www.eyemdlink.com/EyeProcedure.asp?EyeProcedureID=8>

Kuhn, Markus. Security - Biometric Identification. 13 Mar. 2003. Computer Lab, University of Cambridge. 21 Apr. 2004 <http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf>.

Normal Eye Anatomy. 01 Jan. 2004. National Eye Institute. 02 Apr. 2004 <http://www.nei.nih.gov/photo/eyean/index.asp>.

Olsson, Tricia. SANS Reading Room. 26 Aug. 2003. SANS Institute. 05 Apr. 2004 <http://www.sans.org/rr/papers/index.php?id=1226>.

Perry, Bill. Biometrics and ID. 12 Nov. 2002. Digital Identification Forum - London. 01 Apr. 2004 <http://www.consult.hyperion.co.uk/PubWebFiles/DigID_02/08BillPerry.pdf>.

Steketee, Martha W. NCSC, National Center for State Courts. 13 May 2004. National Center for State Courts. 15 Mar. 2004 <http://www.ncsconline.org/>.