

Commercially Available Access Control Systems

Eric Schmiedl

Mike Spindel

July 2, 2007

Abstract

“Access control” describes a broad category of devices used to control the movement of people through particular locations. There are a plethora of applicable technologies that range from guards, to keys, to biometric systems. At times it seems like every design conceived in the last century is still in production by someone, somewhere. The object of this paper is to give a technical description of the most common, and most interesting, technologies available and to provide the reader some insight into their specific strengths and weaknesses.

1 Selecting an Access Control System

It's important to have a clear set of requirements and metrics when evaluating an access control system. Without them, it's too easy to get lost in a sea of marketing. [1] characterizes systems in terms of the system's error rate, it's throughput, environmental requirements, and general feature requirements.

1.1 Error Rate

A system's tendency to make mistakes is typically characterized by two metrics: the False Reject Rate (FRR) describes the frequency of errors that reject an authorized user, and the False Accept Rate (FAR) describes the frequency of errors that accept an unauthorized user.

False accept errors can be thought of as either accidental or intentional; an accidental false accept occurs when an unauthorized user is granted access without the user attempting to bypass the system. A false accept is intentional if the user was purposely attempting to bypass the system. False reject errors don't typically represent an immediate security risk. However, they can affect morale and cause delays [1]. Perhaps even worse, an excessively high FRR encourages people to circumvent the access control system because it's inconvenient.

Although the FAR and FRR are extremely important when evaluating biometric solutions, the concepts can be generalized to give insight into other systems.

1.2 Other Factors

[1] also lists a series series of planning questions to aid in understanding a system.

- What is the expected volume of personnel that will use the system, and how often can the system be expected to experience maximum or minimum load?
- What security requirements need to be taken into account for each secure area?
- Do users need to have different levels of access?
- Are there special environmental considerations for the control point, such as extreme weather or vandalism?
- How fast can the system process users, and will it handle the expected load?
- Can the system be integrated into an existing security infrastructure, such as an alarm system?

- What maintenance requirements does the system have? How often can the components be expected to fail? Can the system be maintained by existing staff?
- How long does it take to enroll a user into the system? Is the enrollment process user friendly? What qualifications does the person managing the enrollment need?
- Can the system be expanded to meet the requirements of future growth?
- What will happen to the system during a power outage?
- Will the system detect tampering or other physical attacks? Especially in unattended applications, it is important to prevent an attacker from circumventing the system entirely.
- What are the audit requirements? Systems that are connected to a central computer typically have extensive auditing capabilities.

2 Photo ID

The least technical system is simply a guard who looks at badges. CCTV systems can additionally be used to reduce manpower requirements. In such systems, the guard compares the person shown onscreen with the picture stored in a computer database.

The FRR tends to be low because guards are unlikely to deny access to a legitimate user unless the photo is extremely outdated. On the other hand, studies of photo ID systems have shown that guards are very reluctant to deny access to anyone provided that the photo bears even a passing resemblance to the person standing before them [2]. This means that even accidental false accept error rates can be quite high. To make matters worse, it is relatively easy to forge even high-security identity cards that use features such as watermarks, holograms, or magnetic stripes. Although there is an international registry of holograms used for identification designed to prevent an unauthorized user from commissioning the production of holograms for counterfeit identification, techniques have been developed by fake-ID manufacturers that can duplicate most common security features.

3 Knowledge-based systems

Knowledge-based systems require the user to remember a code or password of some sort. Most use a numeric code or PIN, entered via keypad. However, other methods of numeric code entry are available.

Electronic knowledge-based systems can have audit trail capabilities on par with any other electronic access-control system. Standalone mechanical systems, such as Simplex locks, do not have any logging or audit trail capabilities.

3.1 Mechanical locks

Mechanical push button locks are designed for high-traffic, low- to medium-security applications. They offer no audit trail capability and can have only one access code at a time. To increase security, they can be programmed with “special” access codes that require the users to depress more than one button at a time, or to depress a button only half way. Models are available with key bypass, using a wide variety of removable-core locks. The Unican 1000 series locks are compliant with the Americans with Disabilities Act standards, and are commonly used in institutional settings. Many universities use them to secure labs and other areas.

Mechanical push button locks have an excellent FRR and accidental FAR because they rarely breakdown and they never accept invalid codes. However, they can be bypassed through both brute-force [3] and manipulation [4] attacks. The design of the mechanism is such that the number of possible combinations is surprisingly limited; numbers only be used once and codes with half-presses are rarely used. As a result, an attacker can try the all possible combinations in the space of ten minutes.

3.2 Conventional keypad

Keypads are the most common access control system in use today. Versions are available to handle nearly any environment, and they are often used to complement biometric or token-based access control systems. They often can be linked with a central computer for any desired auditing capability.

FRR and accidental FAR error rates are extremely low, barring forgetful users. Traditionally, the attack on keypad systems has involved the application of fingerprint or UV-fluorescent powder on the keys prior to a legitimate user's use of the keypad. A brief examination of the keypad afterwards allows the attacker to determine which keys were pressed. This requires the attacker to try all possible permutations of the numbers, and can be foiled by reusing the same number in the combination. Many systems will lock out or trigger an alarm after a set number of incorrect codes. To circumvent this, a technique was discovered (which we believe has not been discovered and made public before) that involves the use of yellow highlighter ink to track the movement of fingers across the keypad. The ink is applied to a single key at a time, the legitimate user allowed to enter the combination, and the keys examined under UV light to determine where the highlighter ink has been tracked to the next key in the combination. Standard yellow office highlighter will still adhere enough to the fingers for this technique to work some time after the application, though results may vary depending on different ink formulations.

Sophisticated attackers have also been known to plant inconspicuous video cameras to record access codes. As a result, high-security systems require a shield around the keypad to prevent observation. Very high security systems will use a dynamically changing keypad to protect against examination of latent fingerprints or other marking. Rather than having the numbers etched or printed on the keys, each key has a digital display on it that allows the keypad to change the layout of the keypad each time it is used. This technique, combined with an anti-observation shield, renders it impossible for an attacker to determine the code surreptitiously.

3.3 Safe-type mechanical and electronic locks

Safe-type mechanical and electronic locks are used in cases where resistance to surreptitious entry is paramount. They use standard electronic or mechanical safe locks mounted to special fittings designed to work on normal doors. (High security doors and vault type doors are available.) The FAR and FRR are similar to keypad-based systems. False reject errors are limited to those caused by user error. Department of Defense regulations specify the use of Federal Specification FF-L-2740 compliant and approved locks for storage of classified material, and to date the only locks that so qualify are the Mas-Hamilton X-07, the Kaba Mas X-08 (shown in Figure 4), and the Kaba Mas X-09. Conventional "safe-type" locks, especially UL Listed Group 1 and 1R locks, offer excellent resistance to surreptitious entry, but do not have any auditing capability. The Mas-Hamilton / Kaba Mas locks offer audit-trail capability and at the time of writing have no publicly known vulnerabilities.

4 Token-based Systems

Token-based access control systems use a card or other token encoded with data that is scanned by a reader at the entry control point. Many different methods of identifying each token are used, ranging from barcodes to microprocessor chips, and with options for nearly any security level or budget.

Audit trail capabilities with these systems can be extensive. In systems where each control point is connected to a central computer, auditing information may be accessible the moment the user passes the control point.

Token-based systems have the key vulnerability that the token may be used at the access point and then passed back to an unauthorized user. Higher security systems will detect this pass-back and deny the second user access and/or trigger an alarm.

4.1 Barcode technology

Bar code cards use a series of stripes to encode binary data. The encoding was originally developed so that a laser beam swept across the barcode would cause the detector to output an easily-decoded bit-stream, though many modern scanners use more diffuse light and a CCD image sensor. Variants on the barcode principle are available that encode data two-dimensionally. Two-dimensional barcodes are capable of storing considerable amounts of data, and have been adopted

by the shipping industry to encode pertinent information regarding a package or shipment. Bar codes are usually read optically by a photo-detector cell (in the case of laser-based one-dimensional systems) or the aforementioned CCD image sensor.

False reject errors can happen when the reader or the barcode is dirty. In general though, the technology is inherently resistant to false reject errors. Intentional attacks are a different matter. Checksums make alteration of an existing card difficult without reprinting the barcode, but the nature of barcodes is that they can be easily duplicated. It may even be possible to use of a telephoto lens to record the barcode of an exposed card. As a result, conventional barcode systems are generally used in low-security applications such as customer identification and employee timekeeping.

Slightly more secure barcodes exist that can't be duplicated as easily. These systems print the barcode in UV-fluorescing ink or in infrared-blocking ink with an infrared-transparent overprint (resulting in the appearance of a solid block under normal light, but revealing the barcode when read via infrared). The latter technique is more commonly used in access control card applications, while the former is generally used for document marking.

4.2 Magnetic cards

Magnetic stripe cards encode data on a rewritable magnetic stripe, using a process similar to the one used to encode data on magnetic audio tape. They have excellent audit trail capability. Due to the maturity of the technology, magnetic stripe card systems are very inexpensive. Most ID card printers are capable of encoding magnetic strips at the same time the ID card is being printed. Due to the cost of the technology, they are one of the most common token-based systems.

Magnetic cards can be corrupted or erased by accidental exposure to magnetic fields, such as found both in common magnets and in the presence of an MRI (Magnetic Resonance Imaging) scanner or certain other scientific equipment.

The system can be attacked by stealing, cloning, or emulating cards. The risk of forgery is higher with magnetic stripe cards as the equipment to read and write magnetic stripe codes is readily available. To raise the barrier against forged or stolen cards, cardholders may be required to use a personal identification number or biometric identifier at the time of access.

The other option is the MagnePrint [5] system from MagTek. Aimed primarily at Point of Sale applications, the technology uses the unique pattern of ferrous oxide particles that make up the magnetic stripe on the card to create a 54-byte fingerprint value at the time the card is read. This fingerprint value is compared to a centrally-stored fingerprint that was recorded at the issuance or first use of the card; provided the fingerprint matches within certain parameters, the manufacturer claims that the card read can be positively identified as the original issued card. The manufacturer claims an FRR of 0.027% when the threshold is set low enough to give a zero FAR [6].

4.3 Barium Ferrite

Barium ferrite is a high coercivity ferromagnetic material that is commonly used today in high coercivity (HiCo) magstripe cards [7]. However, its use in access control predates standardized HiCo magstripes by almost 30 years: early designs for barium ferrite cards were patented in the 1970's [8] but HiCo magstripe cards were standardized by ISO 7811-6 in 2001. The cards are formed by sandwiching barium ferrite between two layers of plastic and polarizing particular regions during the encoding process. The magnetized regions can be read with either physical tumblers or coils. Although they're interesting from a historical perspective, the cards have been completely obsoleted by magstripes. Magstripe cards today are thinner, cheaper, and can hold considerably more data.

Like other magnetic tokens, barium ferrite cards can be decoded by visualizing the magnetic field in the vicinity of the card.

4.4 Wiegand Wire

Wiegand wire is a ferromagnetic wire made from an alloy of iron, cobalt, and vanadium that was invented by John Wiegand [9]. The wire has two uniform magnetic domains: an outer high coercivity shell and a low coercivity core. The two run the length of the wire and interact at a single domain wall [10]. A strong magnetic field will align both the shell and the core, but a relatively weak magnetic field in the opposite direction will only reverse the core. When the core is realigned with the shell the magnetic flux changes sharply, which induces a strong pulse in the read coil [11].

In access control cards, short Wiegand wires are placed in two parallel tracks that represent binary zeros and ones [12]. The wires are completely encased in the plastic, so both the cards and the readers are robust to extreme environmental conditions, and have a correspondingly low FAR and FRR.

Although the mechanism is fascinating, the cards fell out of style years ago, and their major distributors have re-focused on proximity and contactless smart cards. Yet, the cards were marketed as high security and HID Corp. continues to make the claim that “due to the complexity of manufacturing the Wiegand wire, Wiegand cards are virtually impossible to duplicate and remain one of the most secure access control technologies” [13], even though a simple method [14] to duplicate the cards was posted to the cypherpunks mailing list in 1998: cut up another card and rearrange the slivers containing wires into the desired code. Moreover, the coils on the Wiegand read head are essentially the same as the ones in a magstripe reader and are generally vulnerable to emulation style attacks as well. The only complication is the larger field strength that the Wiegand reader expects.

4.5 Proximity cards and RFID technology

The term proximity card refers to access control cards based on RFID technology. The cards contain embedded circuitry that’s powered via induction by a magnetic field emitted by the reader. They don’t need to be inserted in or swiped through the reader, which allows more flexibility in reader placement and card use. The convenience and verification speed of proximity cards has made them an extremely popular access control technology, and they are widely used by institutions and corporations as access control for buildings or secure areas. The same technology can also be used to tag goods and other objects for identification and tracking. Long-range readable RFID tags are used to identify vehicles for the purpose of opening security gates or recording access on toll-roads (known as the EZ-Pass system).

False reject errors can be caused by damage to the card’s electronics and environment factors. Anecdotal evidence suggests that a large system should have a stock of replacements available.

With respect to intentional attack, conventional proximity cards are intrinsically vulnerable to interception and cloning attacks because they don’t perform any sort of cryptography handshake during authentication. Rather, they simply transmit stored data to the reader. It is also possible to impersonate a card reader and obtain the ID number from a proximity card in the field, allowing an attacker to clone the access card of an authorized user simply by holding the (concealed) device near that user’s proximity card. For example, the device could be concealed in the attacker’s sleeve, and passed near the legitimate user’s wallet during an “accidental” collision on the street. Alternately, the device could be hidden near a proximity reader, where it would be able to intercept the ID numbers of the cards that are used.

Newer generation 13.56 MHz contactless smart cards effectively close this vulnerability through the use of cryptographic handshake (mutual key) authentication. Furthermore, observation of the radio traffic becomes an ineffective way of bypassing the system. Therefore, applications requiring significant security should ensure that the older proximity cards are passed over in favor of newer contactless smart card technology. The newer cards can be considered extremely secure, especially in conjunction with a biometric or knowledge-based system.

4.6 CPU tokens

CPU tokens contain a chip inside a protective enclosure such as the Dallas Semiconductor iButton system or the common smart card. For the purposes of physical access control, the operating principles of both technologies are very similar. Each user is issued with a token, whether an iButton or smart card, that contains an electronic serial number. The user inserts the token into the reader, which reads the serial number and grants or access based upon a database of valid numbers. The convenience of this system combined with the relatively low cost of smart cards has made them popular in the pay-TV and phone-card industries, while the high security of the technology makes them suitable for banking applications.

False rejection errors are rare with this kind of token. If they occur, it’s usually caused by environmental factors. Smart cards are vulnerable to environmental factors such as abrasion or corrosion. The stainless-steel chassis of the iButtons provides significant protection, and they are often used in applications where resistance to the elements is important.

It is very difficult to create a counterfeit token with the same serial number as a target. However, cryptographic authentication isn’t typically used, so a “virtual token” could conceivably be created and used if the attacker is able to connect a portable computer to the access control point. Some tokens and many smart card systems do use cryptographic

authentication and thus such an attack is made considerably more difficult. (Albeit not impossible. In the pay-TV market, the extreme demand for a successful bypass technique resulted in a hardware/software combination that would give the TV pirate all channels for free, if the pirate was able to procure an expired access card.) Also, the systems are like any other token-based access control systems vulnerable to tailgating and pass-back unless measures are taken to prevent either.

4.7 SecurID tokens

Though they are generally used for dual-factor authentication on computers, a summary of access control systems would be remiss to omit the RSA SecurID. The SecurID system consists of software running on a central server, which verifies the authenticity of the tokens, and a SecurID token carried by the end user. When users attempt to access the system, they are prompted to enter both their normal username and password, and the number displayed on the SecurID token. The number changes every minute and is synchronized with the central server using a time-based random number generator and a secret seed value that is not exchanged during the login process.

The advantage of the SecurID system is that interception of particular passwords is less important. Of course, the tokens do little to protect against man-in-the-browser attacks.

4.8 Hollerith Cards

Hollerith cards use a pattern of holes punched in the card in order to encode data. Cards used for access control are made of plastic to resist wear. The vast majority of the readers in use are mechanical, although they can be optical. They are intended for applications where the locks require frequent re-keying to deny access to previously authorized personnel. Hotel locks such as the VingCard system are an excellent example.

Hollerith cards in these applications have been almost entirely replaced by magnetic stripe cards, but are still available and live on in large legacy installations [15]. The chief disadvantage of Hollerith cards is that they can be decoded by sight. Hotel thieves have been known to photograph maids' keys in hotels that use the VingCard system in order to create their own keys [16, 798]. In mechanical systems this vulnerability is compounded by the fact that the holes are read through mechanical pins, rather than optically. As a result, the lock system can be decoded quickly and surreptitiously using a specially made device [17].

5 Biometric Systems

Biometric systems use features of the body that vary from person to person in order to authenticate users. In theory, biometrics provide absolute verification that the person passing through the control point is the person that is authorized to enter the secure area. That said, the difficulty of accurately quantifying physical features of the body has prevented technology from meeting that goal.

5.1 Voice Recognition

Voice patterns are characteristics of a person's voice that are recorded when the person is given access to a facility. The shape and movement of the tongue, throat, and vocal cords make a person's voice unique, and it is these characteristics that are represented in the digitized voice pattern.

False rejections are a genuine challenge in all biometric systems, and voice recognition is no different. Things like illness and recent dental work can dramatically change a person's voice. Further false rejection errors can be introduced as a result of background noise or whether the system can actually depend on the user speaking a particular phrase. False accept errors can occur if the attacker is able to record the user's voice, digitally edit it if necessary, and play it back in place of the attacker's own.

5.2 Face recognition

Facial recognition systems use computer algorithms to identify a person by comparing their face (as captured through a camera) to a stored template.

Automatic facial recognition is fraught with problems due to the nature of photographs. Photographs taken explicitly for identification have controlled lighting, angles, and recording media. Images from video tape or surveillance cameras are even more difficult to process effectively. Movement, lighting, viewing angle, perspective, and facial expressions all contribute to the difficulty.

Error rates (both FAR and FRR) of one percent or less are almost impossible to achieve with facial recognition, in comparison with other forms of biometrics.

Facial recognition systems can often be compromised by using photographs and video images of the authenticated user. In one scenario, notebook computers with images that are displayed in front of the sensor in a facial recognition system can defeat security. To combat this, some manufacturers have introduced liveness checks. However, these can be defeated by adding motion to a short video clip. This suggests that information from an individual that is captured by a video camera in public could be used to simulate that individual at an unsupervised access point.

5.3 Fingerprint recognition

Fingerprint recognition systems digitize the user's print by recording the relative position of key points in the print. Variations in these key points are compared to a stored template. Some systems can read fingerprints from dirty or otherwise partially illegible fingers, reducing false reject errors. However, they can occur if the users are involved in manual labor or other activities that wear down fingerprints – in addition to false reject errors caused by the algorithms or sensing methodology used in the system.

Most fingerprint scanners are vulnerable to spoofing attacks. Some systems can be fooled by simply breathing on the sensor, and thereby revealing the previous user's fingerprint. Other latent-print attacks include the use of fingerprint-dusting techniques to lift the latent print, or the use of a thin-walled water-filled bag placed on the scanner. "Swipe" style scanners (in which the user draws his or her finger over the scanner) are not vulnerable to this type of attack. If an attacker can make an impression of the fingerprint, Second Skin (tm) burn treatment film can record the fingerprint while being very difficult to detect even if the fingerprint terminal is supervised by trained guards. If an attacker does not have access to an authorized fingerprint, then a latent print from the surrounding surfaces could be lifted and an artificial fingerprint made using photo-etching techniques.

5.4 Hand Geometry

Hand geometry access control systems examine various features of the hand, such as finger length and hand proportion. Unlike fingerprints and retinas, the hand geometry is not particularly unique; hand geometry cannot be used for identification, only verification. While this can be a disadvantage due to a higher accidental FAR, this can also be a feature. In applications such as customs or biometrics used by the public, the privacy protection that this aspect provides may prove a critical advantage. Furthermore, the amount of data storage required to store each user's parameters is the lowest by far among access control systems, making it easy to store biometric identifiers on smart cards or other tokens.

False rejections could happen in cases of extreme weight gain or industrial injury. Hand geometry-type access control systems may also be incompatible with certain disabilities or medical conditions that cause permanent disfigurement of the hand. The FAR is higher than other systems due to the non-unique nature of hand geometry. Intentional errors are time-consuming to produce, because the attacker needs to create a fake hand with the geometry of a target user.

5.5 Retina

Eye retinas are unique from person to person. Retinal scanners use low-intensity infrared light to digitize the pattern of blood vessels on the retina. Using a technique similar to the one used by fingerprint scanners, the retinal scanner records the distance between a set of checkpoints on the retina. When the user seeks entry, the measured data is compared with the stored checkpoints.

False reject errors can occur as a result of physical changes. Medical problems, or industrial accidents (for example, losing an eye or otherwise damaging the retina) may cause a user to change their retinal signature. Attacking the system is difficult due to the problem of presenting the scanner with a forged retina. However, it is possible to induce a false reject error by putting an allergen in one's eye some time before being scanned: the swelling of the blood vessels on the retina can cause the scanner to read a different retinal code.

5.6 Iris

Iris recognition is potentially the most reliable method of biometric access control because the iris code is much more complicated and random than a fingerprint.

There are a few disadvantages to iris scanning, however. In order to capture an acceptable image for processing, several hundred pixels must be available [18, 270]. This means that, as in retinal scanning, the individual has to be close to the scanner, which raises some issues with respect to privacy and intrusiveness. Distances between eye and scanner can vary from a few inches to two or three feet. Within a controlled environment, the distance between individual and scanner is less important, but in a retail or commercial setting, it can become a problem. Other issues that can cause problems would include blinking, eyelashes, nystagmus, and sunglasses.

Iris recognition offers the lowest false accept rate for any biometric authentication system. The Department of Energy has conducted extensive tests and found an accidental FAR of zero. The equal error rate is better than one in one million [18]. However, iris scanning systems can be bypassed.

In cases where the iris scanner is operating in an unattended environment, a photograph of the target iris can be presented to the scanner; in some cases, it may require that a hole is cut for the pupil area and a live subject used for the pupil [19]. In cases where the iris scanner is supervised in operation, the target iris pattern could be printed on contact lenses.

5.7 Signature Recognition

Signatures vary considerably between signings, so signature recognition systems do not compare the actual form of signature. Rather, they record the characteristics of the lines and the dynamics of the writer. In the enrollment process, users provide several signatures in order for the system to store a baseline average to compare against a signature provided at the access control point.

The chief drawback to signature-based systems is their FRR. Due to the challenges of recognizing a signature, the systems are not suitable for large-scale use, such as public terminals, banking, or point-of-sale applications. In these cases, the 1% FRR found in some versions would result in far too many annoyed customers to be successful [20]. On the other hand, signature systems might be appropriate in small-scale applications with trained users, especially if support or security staff is readily available.

5.8 Hand Vascular Scanner

Hand vascular pattern identification is an emerging technology that identifies users based on the pattern of veins and capillaries on the back of the hand. Since the system uses an infrared sensor to penetrate the skin without contact with the user, hand vascular pattern identification is well-suited to applications where hygiene is important. The manufacturer, Identica Corporation, claims that the technology shows no performance degradation under harsh environments. This makes the system very promising for access control in the mining, chemical, and construction industries. Furthermore, the FAR and FRR are claimed to be 1 in 1,000 and 1 in 1,000,000, respectively, with an 0.4 second verification speed and 99.98% usability [21].

Due to the fact that it is a relatively new and obscure technology, hand vascular pattern identification has been the subject of very little research in the security community, and no bypass technique exists that has been successfully tested.

6 Appendix A: Increasing security

The combination of systems and the availability of system options are numerous. By combining token-based, knowledge-based, and biometric access control systems, it is often possible to increase the level of security provided.

For example, by combining a PIN keypad with a magnetic stripe reader, the system cannot be compromised immediately by the theft of a legitimate user's card. The addition of a secure biometric authentication system (such as a retinal scan) would ensure that users are not able to pass on their security credentials to unauthorized persons.

References

- [1] "Physical security equipment guide," U.S. Dept. of Defense, User's Guide UG-2045-SHR, Dec. 2000.
- [2] R. Kemp, N. Towell, and G. Pike, "When seeing should not be believing: Photographs, credit cards, and fraud," *Applied Cognitive Psychology*, vol. 11, no. 15, pp. 211–222, 1997.
- [3] S. Skinner and E. Goldstein, "Simplex locks: An illusion of security," 2600, *The Hacker Quarterly*, no. 3, 1991.
- [4] *Hobbit*. (1986, Oct.) Simplex 5-button combination locks: *hobbit*'s in-depth evaluation. [Online]. Available: <http://www.indra.com/archives/alt-locksmithing/hobbit.html>
- [5] R. S. Indeck and J. Marcel W. Muller nad Robert E. Morley, "Method and apparatus for fingerprinting and authenticating various magnetic media," U.S. Patent 5 920 628, July 6, 1999.
- [6] K. Gandhi, "Magneprint: A real time risk management tool," *Card Manufacturing*, no. 6, Nov. 2003. [Online]. Available: <http://www.icma.com/info/magneprint111203.htm>
- [7] J. J. Coelho, "Analyzing magnetic stripes for reliability and iso specifications," *Card Manufacturing*, no. 6, Nov. 1998. [Online]. Available: <http://www.icma.com/info/magstripes.htm>
- [8] D. D. Riggs, "Magnetic identification card," U.S. Patent 3 808 404, Apr., 1974.
- [9] J. R. Wiegand, "Switchable magnetic device," U.S. Patent 4 247 601, 1981.
- [10] R. Hollis and D. Thompson, "Switching behavior of stressed vicalloy wire," *Magnetics, IEEE Transactions on*, vol. 15, p. 1848, 1979. [Online]. Available: <http://ieeexplore.ieee.org/iel5/20/22838/01060397.pdf>
- [11] D. J. Dlugos, "Wiegand effect sensors: Theory and applications," May 1998. [Online]. Available: <http://archives.sensorsmag.com/articles/0598/wie0598/index.htm>
- [12] J. E. Opie, C. D. Sloan, and J. R. Wiegand, "Read head for wiegand wire," U.S. Patent 4 736 122, Apr., 1988.
- [13] (2007, June) HID - Wiegand cards and readers. [Online]. Available: <http://www.hidcorp.com/products/wiegand/>
- [14] B. Payne, "Counterfeiting wiegand wire access credentials," Oct. 1996. [Online]. Available: <http://marc.info/?l=cypheerpunks&m=95279373321048&q=p3>
- [15] (2002, Apr.) Press release: Horwood House, England. [Online]. Available: <http://www.vingcard.com/page?id=36&key=3036>
- [16] M. W. Tobias, *Locks, Safes, and Security: An International Police Reference*, 2nd ed. Springfield, Illinois: Charles C. Thomas Publisher Ltd., 2000.
- [17] —, "Method and apparatus for decoding a pin tumbler lock," U.S. Patent 5 355 701, Oct. 18, 1994.
- [18] R. Anderson, *Security Engineering*. USA: John Wiley & Sons, 2001.
- [19] L. Thalheim, J. Krissler, and P.-M. Ziegler, "Biometric access protection devices and their programs put to the test," *ct*, p. 114, Nov. 2002. [Online]. Available: <http://www.heise.de/ct/english/02/11/114/>
- [20] "Finger minutiae system leaps the 1:100,000 false refusal barrier," *Fraud Watch*, no. 2, pp. 6–9, 1996.
- [21] VEID Pte Ltd. - hand vascular pattern identification system. [Online]. Available: <http://www.veid.net/Product/VPIIS.htm>