Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

David Palmer
Computing and Management
2005/2006

The candidate confirms that the work submitted is their own and the appropriate credit has been given where reference has been made to the work of others.

I understand that failure to attribute material which is obtained from another source may be considered as plagiarism.

(Signature of student)___________________
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

Summary

This report attempts, through extensive research of physical and IT security networks, to ascertain the technological feasibility of an integrated security system. Having researched the technology it was then important to identify software capable of running an integrated system. With the technology understood the report identifies two potential clients and their requirements for such a system. Whether to implement such a system is a big decision for an organisation to make and therefore it is critical to identify other areas such as political, legal, economic, and sociocultural factors that could affect the systems success or failure.
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

Acknowledgements

Most of all I’d like to thank Sarah Fores who has been my tutor for this project. I would also like to thank Prit Rehal who acted as my client and helped give me the foundations to start this project and Tony Jenkins who as my assessor helped me to critically view my final system. Thanks also go to everyone who proof read my report.
# Contents

1 Introduction to Physical and IT Security  
   1.1 Physical and IT Security Networks  
   1.2 Methodology  
   1.3 Evaluation Criteria  

2 Physical Access  
   2.1 Lock and Key  
   2.2 Keypad Access System  
   2.3 Solenoid  
   2.4 IT Related Access Keys  
      2.4.1 Smart Card  
      2.4.2 Biometrics
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

3 Network Security

3.1 Desirable Properties

3.1.1 Confidentiality

3.1.2 Authentication

3.1.3 Message Integrity

3.1.4 Non-Repudiation

3.1.5 Availability

3.1.6 Access Control

3.2 Cryptography

3.2.1 Symmetric and Asymmetric Cryptography

3.2.2 Authentication Protocol

3.2.3 Digital Signatures

3.3 Firewalls

3.4 Summary

4 LDAP (Lightweight Directory Access Protocol) Software

4.1 Directory
4.2 Directory Applications ........................................... 20

4.3 Microsoft Active Directory ...................................... 21

4.4 Summary .......................................................... 22

5 Clients Requiring an Integrated Solution ............... 23

5.1 New Client .......................................................... 24

5.2 Summary .......................................................... 25

6 Analysis framework .................................................. 26

6.1 Stakeholders ....................................................... 26

6.2 Political Considerations ......................................... 27

6.2.1 Disability Law .................................................. 27

6.2.2 Data Protection Act ........................................... 28

6.2.3 Freedom of Information Act ............................... 29

6.2.4 Computer Misuse Act ....................................... 29

6.3 Economic Considerations ....................................... 30
6.4 Sociocultural Considerations

6.5 Technological Considerations

6.6 Summary

7 Integrated System

7.0.1 Managing the System

7.1 Limitations
Chapter 1

Introduction to Physical and IT Security

1.1 Physical and IT Security Networks

Companies have traditionally built separate networks that deal with their physical access security and their logical access security [1]. The physical security network involves technology that deals with access control such as ID badges, access cards, as well as CCTV, security guards alarm systems, perimeter protection systems, fire alarms [1]. The IT security network uses technology such as passwords, access cards and digital certificates to control logical access [1]. Looking at both the networks from this high level it appears that it may be possible to integrate the two in one networked system. The problem is to ascertain the feasibility of implementing such a system. A general system is defined by Somerville [2] as:

‘a purposeful collection of interrelated components that work together to achieve some objective’

Somerville [2] then mentions that there are two specific types of system; the technical computer based system that “includes software and hardware... has no procedures or process” and the sociotechnical systems that “include one or more technical systems but, crucially also include knowledge of how the system should be used to achieve some broader objective.”
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

However, for the purpose of this problem “system” refers to a technical system. The people aspect that is included in the sociotechnical system will be investigated once both the hardware and software aspects have been discussed fully.

The main reason for having a single integrated system is that it may lead to lower costs in terms of maintenance and administration; one network could possibly mean one team maintaining and administrating it rather than two, and equipment; as there is only one network there will be less equipment required. There may also be a gain in management efficiency as any ambiguous areas that existed between the two networks previously will be removed by having a stronger definition of responsibilities.

1.2 Methodology

In order to ascertain the feasibility of an integrated solution effectively a methodology must be employed. The methodology for this problem will be as follows:

- Investigate physical security. This will include a discussion of current technologies used for controlling physical access as well as some technologies that may be employed in the near future. Understanding these technologies may also lead to their employment in controlling logical access.

- Investigate the network security. This will look at the desirable properties of networks and an explanation of methods used to ensure these properties are apparent in the network. This is important to understand the issues for the current IT network team and for any future integrated solution.

- Investigate directory application software. Having discussed both the physical and IT network issues there needs to be an understanding of the software that will allow the two to integrate.

- Find a client. Having evaluated the technological feasibility it will be important to find a client who can add information about the desirability and requirements of such a system.

- Create a case study. If, as expected, finding a commercial client proves difficult, then a case study will be developed in order to provide a basis for investigation into and evaluation of any other aspects that may affect the feasibility of such a system.

- A decision making framework will be used to help capture all the information that should be considered before making a decision on whether to integrate or not.
A possible solution will be constructed and evaluated against the technologies to be used and any other factors highlighted by the employment of the suggested framework.

1.3 Evaluation Criteria

The possible technologies that can be employed to control logical and physical access shall be explained, with the help of a table, highlighting the features that are relevant to clients. A decision making framework will be developed against which any final solution can be compared. The information gained from the employment of this framework will also be used to help choose a technology that will be able to best fit a clients requirements. The chosen technology will then be discussed with all reasoning and assumptions clearly outlined. Any limitations foreseen with the proposed solution will also be specified, with a discussion of possible alternatives and the reasons for their rejection.
Chapter 2

Physical Access

The existence of security providing companies such as ADT prove that for many businesses controlling physical access has and always will be a major concern, not just in terms of preventing potential intruders from entering the building but also controlling employee access within the building. Many areas may hold confidential information or be deemed dangerous and therefore effective access control is required. There will always be a requirement for some type of key or identifying technology that controls access and thus acts as a means of securing the area.

2.1 Lock and Key

The most basic system is a metal key and lock that is used in homes all over the world. With this system each employee would be issued with a metal key for each area that they were authorised to access. However, there are a number of problems with the lock and key system: If the key is lost then whoever finds it can potentially enter the secure area; it is possible to pick a lock to open a door without a key; keys are very cheap, quick and easy to copy thus a key could be taken, copied, and returned before anyone noticed it was missing.
2.2 Keypad Access System

Another mechanical rather than electronic system for access control is the keypad access system. This is where a keypad is installed by the secured door and in order to gain entrance a specific numbered code must be entered [3]. As there is no physical key there are no issues with loss or picking of the lock. However, it does still have other issue of copying the code as it is possible for a potential intruder to watch when the code is entered. Another point is that when people have access to many areas all with different access codes it is very likely that they will store a list of the codes somewhere just in case they forget one. Having this list is essentially the same as having a set of physical keys. Anyone who possesses this list has the potential to access all the areas. It is worth noting that now there are electronic keypad systems available [4], but these still have the same problems as the mechanical systems.

2.3 Solenoid

‘Locks are just a delay device, only offering a delay in access to assets. The time delay established for a warded lock is zero seconds. A disk or wafer lock takes three minutes to pick, a pin tumbler takes ten minutes, and a lever lock can be compromised in thirty minutes.’ [5]

Due to this fact that all lock types can be picked, relatively quickly and easily by anyone who has trained themselves, other ways to secure a door have been developed.

One of the most common security systems used in business today is the use of a solenoid. A solenoid is a loop of wire wrapped around a metallic core, which produces a magnetic field when an electric current is passed through it [6]. This means that they can create controlled magnetic fields and therefore can be used as electromagnets. It is apparent from visiting companies, for example IBM UK headquarters in North Harbour, that many of their security systems now use a door either made of metal or that has some metal that connects to this solenoid. An electrical current is constantly passed through the solenoid creating an electromagnet. The force needed to open the door is greater than a human can exert. When the correct key is presented the electrical current ceases for a set period of time and the door can now be opened.
2.4 IT Related Access Keys

There are a number of different physical access keys that have been developed and are in widespread use such as smart cards [7]. There are also some newer emerging technologies that can be implemented but are not as of yet so common.

2.4.1 Smart Card

‘Smart cards are plastic cards that resemble credit cards, but which include an embedded chip to store and process information.’[8]

These were originally used as identity cards or loyalty cards in stores but are now being used more frequently by companies for security purposes as suggested by IBM [9]. The smart card is placed in a reader which, using contact springs, makes a connection to the contact surfaces of the card. Via these contact surfaces the card is supplied with a clock pulse and energy. Using a bidirectional serial port also known as an input/output port data transfer takes place. There are two types of smart card stated by Cardwerk [10]: the basic memory card; and the microprocessor card.

Memory cards can store a variety of data, including personal information and access codes. According to Finkenzeller [11] They are a superior alternative to the original magnetic strip card, as they: are more reliable, durable and secure, can store up to one hundred times more information, and they can perform multiple functions. However as they typically use one type of memory EEPROM (Electrical Erasable and Programmable Read-Only Memory) it is not possible for them to process any information. The microprocessor card is more powerful than the memory card in that it “offers multiple functions such as encryption, advanced security mechanism, local data processing, complex calculation and other interactive processes” [12]. This is because the microprocessor in the card has segmented memory consisting of ROM (Read-Only Memory), RAM (Random Access Memory) and EEPROM segments. ROM incorporates an operating system for the microprocessor and is inserted during chip manufacture. As this memory is read only its contents must be determined during manufacture. The EEPROM is where the application data is stored, while the reading and writing to this is controlled by the operating system [11]. This increases the flexibility of the card as the application specific parts of the programme are no longer loaded in at the manufacturing stage but afterwards.
When used in a security system the smart card will act as a key. This means that the key is never visible
and therefore difficult to copy, especially as both types of card allow a level of encryption. If the card is lost
then whoever finds it will have access. However, if the card is reported lost or stolen it can simply be deleted
from the system thus rendering it useless. As each card will have a unique key this can be used to identify
whoever is using it, allowing companies to know who exactly is onsite at any time. The problems that arise
when using smart cards are due to the physical contact between the reader and card as both products can
suffer from wear, corrosion and dirt [13]. Replacing a smart card is fairly cheap as their cost is low, replacing
a reader on the other hand can be quite expensive and therefore costly to maintain. Due to this, contactless
smart cards have been developed that are very similar to contact cards but use Radio Frequency technology
[13]. This technology will be discussed later.

2.4.2 Biometrics

Biometric technology is defined as

‘automated methods of identifying a person or verifying the identity of a person based on a
physiological or behavioural characteristic’ [14]

There are a number of biometric identifiers in use in the world today: Fingerprint scanning; signature dy-
namics; facial recognition; Iris recognition; and voice authentication are all noted by Shutt [15]. Although it
is important to understand all biometric identifiers there will be a detailed discussion of fingerprint scanning,
the first widely used biometric technology, and iris scanning, one of the fastest growing technologies in use
today, to better understand the implications for physical access security.

Signature dynamics is concerned not with what the signature looks like, but how it is written in terms
of speed, stroke order, relative speed, stroke count and pressure [16], as it is these factors that when used
together can uniquely identify a person. Facial recognition “analyzes the spatial geometry of distinguishing
features of the face” [17] in order to create a template that can be used for verification and identification.
These can be used by CCTV cameras to identify people and so can be used for surveillance. However, this
technique has been found to only yield satisfactory results in controlled conditions [18].

‘Voice authentication captures a person’s voice - the physical characteristics of the vocal tract
and its harmonic and resonant frequencies - and compares it to a stored voiceprint created during
an enrollment process’ [19]
Voice authentication however is seen as one of the less accurate biometric devices as it has to allow for day to day changes in the voice of a person [19] as well as the changes that happen when a person is unwell, for example with a sore throat.

Fingerprint Scanning is not a new technique; it was originally developed for use in the police force in the late 19th Century and it is still the most common form of biometric identification in use today [20]. The technique originally used ink and paper but, more recently, an electronic scanner is used to take the copy of a person’s fingerprint. Whorls, arches, and loops are recorded along with the patterns of ridges, furrows, and minutiae [21]. Every fingerprint is unique and therefore allows a means of identifying a person. However there are problems with fingerprint scanning:

‘A blister on the finger, sweaty hands or dirt on the scanner can all interfere with a device’s ability to read a fingerprint. Nor do they work well in high-traffic environments’ [22]

Access to a building at 9:00am is definitely a high traffic environment and so fingerprint scanning may not be a suitable solution for physical access control in a workplace.

Iris Scanning is ‘widely considered the most accurate way to identify people through biometrics” [22]. This is the reason that it is used not only as a verification technology but also as an identification technology. A camera is placed up to a metre away from the person it is trying to identify. The person then looks at their own eye while the camera captures the image of the eye. The process of Iris Scanning is:

‘to describe circular contours of increasing radius in order to create zones... examine texture of iris for distinguishing features within zones... provide information about orientation and spatial frequency’ [23]

Ashbourn [23] discusses the following issues relating to Iris Scanning. As the iris is close to the brain it is one of the first organs to decay and so a dead eye cannot be used. Many scanners also vary the light going into the eye to check for pupil dilation to prove the eye is working correctly. The actual image is not what is stored on the database, a code that uses a 512 byte template known as an Iriscode is stored instead [23].
2.4.3 RFID

RFID or Radio Frequency Identification is a technology that has been around since the 1970s, for example, many cars that use toll roads regularly have been fitted with transponders that are connected to their credit cards, thus allowing them to drive straight through the check points without having to stop for payment [24]. However, it is only recently that the cost has decreased sufficiently for their use to be incorporated into other areas such as inventory management. The US army has, for example, implemented RFID along with other technologies in order to track their vehicles and equipment and have seen one unit reduce its inventory value from $127 million to $70 million [25].

Figure 2.1: The reader and transponder are the main components of all RFID systems [11]

All RFID systems are made up of two components, see figure 2.1.:  

- The reader which, depending upon its purpose, can be used to read and write to a device or just to read.
- The transponder, located on the identifying object

The transponder uses its coupling element, which is made up of a coil and a microwave antenna, to receive its energy, clock pulse and data from the reader. It can also use this to send data; this is very similar to the way that the contact smart card works. The transponder is often encased in a plastic housing known as a fob [26].
RFID technology has all the advantages of a smart card without the drawbacks. It has a faster reading speed than the smart card, there is no influence of dirt and damp and there can be a distance of up to about 20-30 feet between the carrier and the reader depending on the specifications used [24]. The reason for both RFID technology and biometric technology not being widely used is the cost. Both technologies costs have significantly fallen over the past 20 years, the cost of a reader can start at as little as $500 [27], and are now within the price range of many large companies. However, this price may still prove to put the technology out of reach, financially, for medium and small sized businesses.

2.5 Summary

This chapter has discussed all the technologies presently available for controlling physical access. The means of securing entrances has been discussed through an explanation of a lock and key system and a discussion of solenoid implementation. Keypads have also been discussed, but have been found to share weaknesses with passwords in that; they are often noted down somewhere, as employees find difficulty in remembering all the codes for all the doors, and it is possible to learn the correct code by simply watching employees enter it.

A number of technologies could be used in the future to help control not only the physical but also the logical access of an integrated solution. Biometrics have been identified as the only technology that leads to total non repudiation, due to the fact that they can uniquely verify a person. However, they have been seen to be both expensive an unreliable at the present time. RFID technology and smart cards are the most secure alternatives, as they allow encryption and are therefore very difficult to replicate.
Chapter 3

Network Security

Tanenbaum [28] describes Network Security as:

‘a broad topic and covers a multitude of sins. In its simplest form it is concerned with making sure nosy people cannot read or worse yet, secretly modify messages intended for other recipients.’

There are a number of desirable properties of secure communication: confidentiality, authentication, non-repudiation, message integrity, availability and access control [29]. Although this project will focus on access control, in order to evaluate the feasibility of integrating network and physical security there needs to be an understanding of all these areas.

3.1 Desirable Properties

The following properties are all important to network security. It is important to understand what is required for the existing IT network and how these could possibly affect any attempted integration between this and physical networks.
3.1.1 Confidentiality

Confidentiality is concerned with one person being able to send messages to another without anyone else being able to read or modify what is being sent [30]. In order to do this there must be a means of encrypting and decrypting messages so that only intended recipients can understand them. Any information that is stored either on servers or potentially on access cards in the final system will need to be confidential and so there will probably need to be some type of encryption in place to ensure this.

3.1.2 Authentication

When communicating participants need to be able to ensure that who they are communicating with is who they say they are. There are three categories for using authentication techniques; proof of property, proof of possession and proof of knowledge [31]. Proof of property is where a claimant can prove their identity via a biometric characteristic. In a face-to-face communication this is easy as voice recognition and other biometric cues can be used for identification. However, in a network it is often a communication between routers and other hardware that needs to be authenticated. Proof of possession is something a claimer possesses such as physical keys or a smart card. It is very difficult for a physical item to be used in a network or distributed system due to problems with production and management of these items. Proof of knowledge is something a claimer knows for example a password or a cryptographic key. It is worth noting that passwords have the same problems as keypads in that they are often easy to remember as humans have to remember them. When attempting to design an integrated solution there will need to be a means of authenticating the user for both the physical access and for the logical access. It may be that the two means of authentication are different, for example, a smart card for physical access and a password for logical access, or it may be that both authentications can be completed using the same unique identifier.

3.1.3 Message Integrity

It is vitally important any message that is received is exactly the same as the one transmitted by the sender. There is a possibility for the content of the message to be altered either accidentally or maliciously in the period of its travel across the network [30]. If, for example, an encrypted smart card has a code that when decrypted reads 1234, and that this code was needed for access into the office, then it is important that the reader on the entrance to the office correctly decrypts this card therefore receiving the correct access code of 1234 and allowing the owner of the card to enter the office.
3.1.4 Non-Repudiation

Repudiation can lead to many problems in organisations. For example if a participant was trading goods with another they would want a means of proving that the participant they were trading with had received their communication and agreed to whatever contractual obligations had been set down [32]. This would prevent any ambiguity as to who was at fault if the contract terms were breached. In the context of this problem it is important that if there is a theft that takes place within an area then any evidence gathered, whether it may be from the use of a legitimate users access, CCTV, or some other security measure, is correct and not able to be repudiated. This is where the use of a smart card that has a unique identifying code for each user is superior to having a lock and key system where it is not known who exactly the key used for access belonged to.

3.1.5 Availability

It is a requirement of all networks that the resources on the network are available to the legitimate users [29]. This means that the network will have to be robust and have built in redundancy to deal with any hardware issues. In terms of the software one of the main problems that a network administrator will have is preventing attacks on the network from other illegitimate users. This may be through a variety of techniques such as viruses in emails, Trojan Horses, and Denial of Service (DOS) attacks where the network is flooded to prevent its use. An issue that may arise from integrating the two networks is what happens to the physical network when the IT network crashes or has scheduled down time, as people may still need to enter and leave the building.

3.1.6 Access Control

As each network has a number of legitimate users authorised to use its resource it must manage the access permissions [29]. This will include ensuring appropriate access rights are only distributed to these legitimate users. For example, the payroll software should be accessible by Human Resource employees only. Therefore the system will have to verify users before granting access permissions. Most commonly this is through the use of passwords or perhaps more recently biometric identification techniques.
3.2 Cryptography

Cryptography is derived from the Greek words for ‘secret writing” [28]. It may use codes or ciphers. Codes were used more regularly when humans had to perform the necessary transformations. For example [28] during World War II the US military employed Najavo Indians to act as communicators as they could use their language for communication. As it had no written form the Japanese were unable to crack this particular code. However, ciphers are now frequently used as computers have the necessary power in terms of calculations per second to use complex encryptions.

There are two tools that are needed in order to encrypt and decrypt messages; an algorithm and a key. The algorithm is almost always universally known while, depending on the type of cryptography the key may be known universally, by both participants or by only one of the participants in the communication [28]. These tools are put into practice in order to improve confidentiality. For example participant A firstly writes what it is they want to communicate in plain text, then uses a key and an encryption algorithm to convert this into cipher text. Participant B receives the message in its cipher text format and then uses a decryption algorithm with a key to convert the message back into plaintext. Anyone listening into the communication can read the cipher text, but without the correct key they cannot convert it into the correct plaintext message, thus rendering the cipher text message useless to them. There are two different types of key that can be used to perform this confidential communication; a private key or a public key. The choice of key will lead to one of two cryptographic techniques known as symmetric cryptography and asymmetric cryptography. [31]

3.2.1 Symmetric and Asymmetric Cryptography

In symmetric cryptography both sender and receiver have identical private keys for encryption and decryption. These are likely to be exchanged either manually, distributed through a trusted third party or a key distribution centre. The sender then uses the encryption algorithm and key to encrypt the message and the receiver will use a decryption algorithm and the same key to produce the original plaintext from the sender. In asymmetric cryptography there is a public key, that will be universally available, and a private key, that only one of the participants will have knowledge of. For example the receiver has a public key B that the sender uses along with the encryption algorithm to create the cipher text. The receiver is the only participant who has the private key and therefore the ability to decrypt the cipher text into the original plain text [33]. This means that unlike the symmetric cryptography there is no need for a secret key to be shared between the two parties. When deciding upon what technology to use for physical and logical access a decision...
will need to be made upon whether to use a public or private key system for encrypting the system. This
decision may have been made for the company by whoever provides the access keys but it is still important
to understand the two types of encryption.

### 3.2.2 Authentication Protocol

Through the use of cryptographic techniques it is also possible to authenticate a participant. An appropriate
technique to do this is through the use of a nonce and public key cryptography. A nonce is a number that a
protocol will use only once in a lifetime and is used to check that the participant making contact is live [31].
A demonstration of this system in use can be seen in fig 3.1

![Figure 3.1: In this diagram the nonce is represented by T. Participant A's private key is Ka- and their public
key is Ka+. Participant B uses the public key Ka+ to decrypt the encrypted nonce therefore authenticating
participant A. Adapted from [28].](image)

### 3.2.3 Digital Signatures

According to Oppliger [34]:

‘Digital Signatures provide an electronic analog of handwritten signatures for electronic doc-
uments... digital signatures must not be forgeable, recipients must be able to verify them, and
signers must not be able to repudiate them later.’
Digital signatures are much like handwritten signatures in that they lead to non repudiation and act as a means of authentication. However, they do have one distinct difference, unlike handwritten signatures they must not be constant or else due to their electronic makeup copying would be a trivial task. They are in fact created as a function of the document upon which they appear [34]. A digital signature can also ensure message integrity through the use of public key cryptography and a hash function [29]. A hash function takes a message m and computes a fixed-sized string known as a hash. An example of how this works is explained in Figure 3.2 below.

![Diagram of digital signature process](image-url)

**Figure 3.2: A diagram showing how digital signatures work [29]**

1. Participant A takes a message m and uses a cryptographic hash function to compute H(m). They then encrypt H(m) using their private key Ka-. The result is what is known as a digital signature. The message m and digital signature are sent to participant B.

2. Participant B then uses the same hash function H upon m. They then use the private key Ka+ to decrypt the digital signature. The result of these two operations should be H(m) therefore proving that
the message was transmitted by participant A

3.3 Firewalls

There are two desirable properties of a secure network that have still to be looked at in detail: availability and access control. Installing a firewall will help although not ensure that these two ideals are met. According to Goncalves [35]:

‘A firewall separates a protected network from an unprotected one, the Internet. It screens and filters all connections coming from the Internet to the protected (corporate) network, or vice versa, through a single, concentrated security checkpoint.’

Any packets travelling over the Internet have to pass through this firewall in order to gain access to the network. A firewall may consist of some packet filtering routers or an application gateway or both. The packet filters are usually driven by tables that list sources and destinations that are permitted, sources and destinations that are blocked and rules about what to do with packets coming from or going to other machines. These tables are configured by the systems administrator to adhere to the security policy of the company. The source or destination will usually consist of a port and an IP address [28]. The port indicates what service is being requested for example telnet is port 23. The application gateway, as is suggested by the name operates at the application level. This may check the content, the header or the file size in order to decide whether to transmit or discard the message [35]. In an integrated system a firewall will help to prevent access being granted to unauthorised users on the Internet, while also helping to allow secure remote access for legitimate users.

3.4 Summary

This chapter has aimed to provide an understanding of what is required for a network to be both reliable and secure. There has been a discussion about the six desirable properties of networks followed by specific techniques that help ensure their existence. This knowledge will play an integral part when attempting to design a integrated network solution.
Chapter 4

LDAP (Lightweight Directory Access Protocol) Software

Having researched both the physical security technologies and the key points for network security it is time to research applications that will enable the two to merge onto one network. It is now becoming a common practice for companies to use a directory application in order to help management of their IT networks [36].

How does it do this? Consider a company that wants to delete an employee’s user details after they have left work. It may be reasonably quick to delete them from the database where the usernames are stored, but then they also have to be deleted from the company phone lists, mailing list, HR, payroll and possibly many more. This means that the same data is being stored in a number of different places, and this in turn means that updating or deleting information can become very time consuming. A directory will allow all this data to be stored in a single location, thus leading to significant administrative savings [37].

Due to their growing use in IT networks it is important that directories and directory applications are firstly understood before evaluating whether the physical security network can, and perhaps more importantly should, be managed on them.
4.1 Directory

A directory is made up of entries; these are the basic unit of a directory, such as people or workstations. These entries in turn have a number of attributes much like a database. For example, a people or person entry may have attributes such as first name, surname, date of birth etc. Each attribute contains a pair of elements; the first known as the attribute type defines the kind of information stored whilst the second known as the attribute value stores the actual data [36]. For example, an attribute may have dob = 11/02/83 where dob is the attribute type and 11/02/83 is the attribute value. However, unlike a database it is possible for each attribute in a directory to have a number of values rather than just one [36]. This helps to increase the flexibility of the directory and can make searching much easier. In every entry there is an attribute known as ObjectClass. This is the attribute that defines all the rules about an entry and includes optional as well as mandatory rules [36]. At the most basic level these rules will state the different attribute types allowed in the entry. An entry or a number of entries are commonly placed inside another special type of entry known as a container.

![Diagram showing container structure](image)

Figure 4.1: This diagram shows how a container can be used to split entries into their relevant areas [36]

The two containers, labelled "People" and "Workstations", establish a parent child relationship between themselves and the entries, as can be seen from Figure 4.1. One advantage of having theses designated containers is that searching will be quicker and more efficient, for example, if a user is attempting to search
for information on an employee then only the people container will need to be searched rather than the whole system. There is a special type of container known as an Organizational Unit that has the added advantage of being able to set permissions so that only certain users can have access to certain information. The team responsible for maintaining all IT related hardware will need access to the workstations container but not to the people container. If these containers are in fact Organizational Units then it is possible to set passwords and access rights for each of them so that a company can ensure information is only available to those who require it. As will be discussed later this is both a legal requirement for companies as well as good ethical practice.

4.2 Directory Applications

Having discussed directories it is now important to understand how directory applications work. Directory applications now use a protocol known as LDAP. Arkills [36] states that:

‘Lightweight Directory Access Protocol (LDAP) is a set of protocols that has become the standard for accessing information directories’

The reasons for it being known as lightweight are due to its ties with the X.500 directory service. X.500 is the original set of standards that were developed around directory services. The main problem with X.500 is that it is based around OSI (Open System Interconnection) protocol stack and not TCP/IP, which is the standard for the Internet [37]. It also implemented many features that clients never needed, making it overly complex. LDAP was designed to be easier to utilise, as it left out many of the features of X.500 that were never needed, and in 1995 the University of Michigan released the first LDAP directory server [37].

There are a number of LDAP-based directory servers available including OpenLDAP, Microsoft Active Directory, SunONE Directory Server and Novell’s eDirectory. As these products use the same set of protocols it can be assumed that they are very similar in their functionality. It is therefore sufficient to choose one product and attempt to gain an understanding, rather than analyse all the strengths and weaknesses of each. The chosen product to be looked at in more detail is Microsoft Active Directory. The reason for this is not that it is the superior product, as can be seen from [38] Novell certainly believe their product to be superior, it is purely because two projects undertaken in the University of Leeds School of Computing [39, 40] integrate IT security with physical security using Microsoft Active Directory.
4.3 Microsoft Active Directory

Microsoft Active Directory is based around some core concepts, such as Domains and Domain Trees, Forests, Organizational Units; mentioned earlier in the general discussion of a directory, section 4.1, and Groups [37]. There are in fact two others: Group Catalog, used for forest wide searches; and Flexible Single Master of Operations (FSMO), used for specific roles that require there to be only a single domain controller [37], whose functionality will not affect the implementation of an integrated security network and are therefore not discussed in detail.

Domains are made up of four components, a DNS domain name that acts as a unique identifier, a hierarchical structure of containers and objects, a security service to authenticate any requests for access to resources or trusts with other domains, and policies to dictate functionality restrictions placed upon users or equipment, e.g. workstations or printers, within that domain [37].

![Diagram showing both the hierarchical structure of a domain tree and the DNS unique identifier for each domain](image-url)

Figure 4.2: Diagram showing both the hierarchical structure of a domain tree and the DNS unique identifier for each domain [37].
The benefits of having a domain tree like that shown in fig 4.2 are that a user in one domain within the
tree is able to access information or resources from any of the other domains in the tree as well as their own
[37]. This can potentially prevent resources having to be allocated onto all the separate domains and thus
make management much easier.

When the domain tree in Fig 4.2 was created a forest containing that tree was also created, automatically.
It is possible to have a number of domain trees in one forest, all of which would trust one another and share
resources [37]. For example a company that has many subsidiaries, like Unilever, may require that some
of their subsidiaries have access to the resources of others. By placing these subsidiaries within the same
forest they can fulfil this requirement. On the other hand a company may have a legal obligation to prevent
unauthorised access to certain information within certain business units. In order to ensure this, the domains
for each respective unit must have their own forest [37]. If the security network was integrated with the
existing network then there would need to be some way of ensuring that only security personnel could view
and alter information regarding the access for employees to areas of the building. It can be seen by looking at
the information above that this would definitely be possible if Active Directory or one of the other directory
services was used.

4.4 Summary

Before attempting to understand LDAP software it was important firstly to discuss the concept of a directory
with some example of how it might work. LDAP was then explained with reference to a number of vendors
that incorporate it within their directory applications. Microsoft Active Directory was then chosen as a
specific application and was explained in more detail to provide a more specific example of how directory
applications actually work including a brief discussion of how it could provide a means to integrate the two
existing networks.
Chapter 5

Clients Requiring an Integrated Solution

Now that all the technologies have been detailed and understood, and a possible means of merging them identified, it is time to look at whether there is a business need and what sort of integrated solution may be needed. The most obvious means of assessing these questions is to have communication with a possible client. However, many businesses of varying size and stature have been approached as possible clients but all had responses along the lines of: ‘We are sorry, but we are not willing to discuss any of our security issues whether physical or IT related with persons outside our own business.’ This potential scenario was however, foreseen, as it is understood that security plays a key part of many businesses and thus discussion around its specific implementation or even more general issues may, in a businesses view, help lead to a future breach.

As it became apparent that all business corporations would be responding in much the same vain the area of the search was changed towards the public sector. The University of Leeds School of Computing was approached to identify their current physical and IT security situation. A formal interview was conducted with Mr Prit Rehal to discuss the School’s current security situation in order to try and ascertain whether an integrated solution may be viable for them and, if not, what issues are preventing this.
The School currently has a physical and an IT network running completely separate to one another. They are already using Microsoft Active Directory in their IT network to manage both their Linux and Windows client logins. Mr Rehal also commented that the current software associated with the physical security devices such as fob readers and solenoids are substandard, not allowing the products to work effectively. Mr Rehal also understands that one system may potentially allow both a more centralised control of both physical and IT security and lower running costs than the current infrastructure. He intimated that the School may be interested in products that lead to the integration of it’s current two security systems.

If the School decided to try and integrate their two current systems there would be a sizeable initial cost for purchase and installation of the necessary equipment. However, the long term maintenance costs would decrease as only one system would be maintained rather than two. Some economic questions the School would need answering are “What would the initial cost be?” and “How much would the maintenance costs decrease by?” Mr Rehal stated that at the present time it is likely that the installation costs will be too great to justify pursuing the matter further. It is my judgement that as the School are not a commercial organisation that they will not invest in such technologies whilst the current system is believed to be satisfactory.

5.1 New Client

The point of this project is not to find a perfect solution for merging physical and IT security but to ascertain whether it has the potential for a market. Therefore having considered a client with an existing infrastructure it is also important to consider one without. Due to the difficulty of finding cooperative ‘real world’ clients it is suggested that a ‘dummy’ client will be investigated. From now on all references to the ‘dummy’ client will be simply termed our client. As some of the economic considerations have been mentioned and taken into account earlier, certain assumptions will be made with respect to the client to aid the exploration of other factors influencing feasibility. These will be based on:

- Company size.
- Whether the company owns or rents the building.
- Whether the company shares the building with others.
- If the integrated solution is going into a new building for a company or if they are going to have to look at re-networking their existing building.
The following will be assumed: the company is of medium size, more than 100 employees so that the potential saving is worthwhile; is looking to move to a new location in a brand new building, so networking the whole building needs to be undertaken regardless of what option is chosen; will own the building, so all costs relate to them and them only; and will not share the building with any other companies, so the whole building can have the same system. These assumptions ensure that initial networking cost is no longer a prohibitive factor, thus allowing other aspects to help decide feasibility. One further assumption that will be important is the type of business that the client is in. For example a company in the manufacturing industry may have a low percentage of its employees with computer access, and so an integrated network may not provide a significant advantage to them. However, a small management consultancy company where everyone has access to a personal computer may find the solution much more viable. It is for this reason that the latter will be assumed about our client.

5.2 Summary

This chapter provided specific information about a client who currently has two networks running separate to one another and what their limitations are with regard to pursuing an integrated solution. A new client was then developed, with a number of assumptions outlined, so that all factors, and not just economic ones, could be discussed and evaluated.
Chapter 6

Analysis framework

When considering decisions as important and complex as moving to a new site and using a new technology it is important to use some sort of decision framework to help. In many businesses a team may be employed to make this type of decision and then to present its recommendations to board members, senior managers and other stakeholders. When presenting these recommendations it is important that both the choice can be understood, and that the reasons for making that choice are clear and understandable. This is where the use of a recognised decision making framework can be invaluable; therefore it is proposed that one will be employed for our client. The chosen framework is known as PEST. PEST stands for Political, Economic, Sociocultural and Technological [41]. The context of each of these factors will need to be considered by our client before considering whether to go ahead with the integrated network in their new site or not. Before employing this framework however, it is also important for our client to consider the perspectives of all their stakeholders and not just, for example, the senior management.

6.1 Stakeholders

All businesses have a number of stakeholders: shareholders, employees, customers, suppliers, local and national governments, competitors etc. When making important decisions that affect the company as a whole it is often important to consider some if not all the views of the stakeholders. A small management consul-
tancy firm like our client, who is looking at investing in this new integrated networking technology, would have to consider the following stakeholders: government; they would be concerned with the political and legal considerations, shareholders; they would be concerned with the economic considerations, employees; they may be concerned with many, but especially the sociocultural and economic impacts of the decision. Other stakeholders such as customers and suppliers however would probably not be affected sufficiently for them to be considered. These will be the people who are involved in the sociotechnical system.

6.2 Political Considerations

The political considerations will also include any relevant legal issues. Due to the nature of this decision there are no real political issues worth considering. However, there are a few issues surrounding the legal requirements of a business that are worth some consideration. Whenever a company builds a new site there are many legal requirements that need to be met, for example meeting building regulations, gaining planning permission, and providing disabled access. Although the construction laws are not necessarily a direct influence on how the company networks the building, there may be some factors that they need to consider when deciding upon the security, access, and information management.

6.2.1 Disability Law

It is often the case that definitions of disabled people are far too narrow, and therefore before discussing the various regulations that have been introduced to prevent disability discrimination, it is important to understand the legal definition of “disabled people”. Powell-Smith and Billington’s definition [42] is an example of one that is too narrow. They define it as those people with

‘a) a physical impairment which limits their ability to walk or makes them dependant on a wheelchair for mobility b) impaired sight or hearing’

However, the Disability Discrimination Act (DDA) [43] defines a disabled person as one:

‘who has a physical or mental impairment that has a substantial and long-term adverse effect on his or her ability to carry out normal day-to-day activities.’

Although this definition encompasses all disabilities, it is on its own quite vague and so therefore further clarification is given [43]:
‘substantial means neither minor nor trivial. Long term means that the effect of the impairment has lasted or is likely to last for at least 12 months (there are special rules covering recurring or fluctuating conditions). Normal day-to-day activities include everyday things like eating, washing, walking and going shopping. A normal day-to-day activity must affect one of the ‘capacities’ listed in the Act which include mobility, manual dexterity, speech, hearing, seeing and memory’

Now it is understood what classifies a person as disabled the duty of employers can be explored more accurately. The Act explicitly outlines that an employer must not cause a disabled person to be substantially disadvantaged when compared to persons who are not disabled. This includes any arrangements made by or on behalf of the employer as well as any physical features of the premises that the employer occupies. If this is the situation at any point, then the employer must work with the disabled people in question to rectify this. There are many steps this may involve, but two which an employer looking at access and security may have to consider are: making physical adjustments to the premises and acquiring or modifying equipment. For example, if swipe cards are used for entry to the building it is possible that a disabled employee may not have the necessary dexterity to use the swipe card in a reader. Therefore, the employer must consider creating another way for the employee to enter the building. This may be through employing different technology, or possibly by having a member of the security team aid the employee in using such a device.

The point being stressed is not to find a piece of technology that is usable for all persons, as this may not prove to be viable, it is instead to decide upon the most appropriate and then actively seek adaptations to help accommodate any person who may experience any difficulty.

6.2.2 Data Protection Act

The Data Protection Act of 1984 is explained by Sizer and Newman [44]. They state that an individual is entitled to be informed by anyone who holds any personal data about them, to have access to that data, and to correct or erase that data if appropriate. The Data Protection Act 1998 [45] updates its predecessor by adding that the individual also has the right to know the purpose for which the information is being processed as well as who may receive this information. However, it also states that the person holding the data only needs to disclose this if they have received a written request and are satisfied as to the identity of the person making the request.
The implications of this for our client are that whatever information is gained from the security system, whether it may be from log files showing when people are at work or identifying the position of an employee using RFID tracking, can be used as the company wants internally and does not have to be disclosed unless a written request is made. For example, it is possible when using a security system that logs people in and out of the building for this information to not only be used for security purposes, but also to check hours worked for each employee. Employees would not have to be told of this practice unless they explicitly asked what the information being gathered was used for. There are however, some other issues, including company ethics and practicality, that will need some consideration before attempting to implement an example like this. These will be discussed later.

6.2.3 Freedom of Information Act

The Freedom of Information Act 2000 [46] has guidelines similar to the Data Protection Act 6.2.2, regarding the provision of requested information that is held, but only applies to information held by public authorities such as; government departments, armed forces of the Crown, the House of Commons, the House of Lords. It therefore does need to be considered the client. If one of the above mentioned public authorities happened to be thinking about network integration then they would need to consult the Act in detail.

6.2.4 Computer Misuse Act

The Computer Misuse Act 1998 [47] states that any person is guilty of an offence if

1. ‘he causes a computer to perform any function with intent to secure access to any program or data held in any computer
2. the access he intends to secure is unauthorised; and
3. he knows at the time when he causes the computer to perform the function that that is the case.’

Any person found guilty of such an offence can be imprisoned or fined. Therefore anyone, whether they be employee or not, found attempting to gain access to information on a system for which they do not have access may be prosecuted.
6.3 Economic Considerations

Due to the fact that the company is moving to a new location there is going to be a requirement to network the building whether they choose to use the integrated technology or not. Much of the cost of networking will be down to the purchase of cabling, switches, and routers. All of these pieces of equipment will be needed for both solutions and so the installation costs of the two should be quite similar. The possible difference will be that networkable security technology, such as CCTV cameras with network cards, will need to be purchased for the integrated solution and it is possible that these may be more expensive as newer technology is often more costly. However, even if the traditional solution is chosen it is possible that these technologies may be requested in order to run the security network. Using this information a financial analysis could be run to estimate the relevant administrative costs over a long term period of five years and the initial installation costs for both the integrated solution and the traditional two network solution.

The integrated network solution may also require some investment in staff training. This may include training security personnel how to navigate and use a directory server application, and training the administrative team on the requirements of the new security technology.

6.4 Sociocultural Considerations

When investigating the social and cultural impact of this particular decision it may be useful to understand the perspectives of the lower level employees and the senior management separately, rather than simply classifying them as one single stakeholder. A manager job would be made easier if they knew where all their employees were at all times and therefore from a management perspective the more information available about employee activity the better. However, an employee might feel intruded upon and therefore less motivated to ‘go the extra mile’ for a company that they feel is always looking over their shoulder.

Due to these different perspectives it is important to understand what will be the effect of merging the two technologies. There are some key questions that need to be answered about the proposed solution:

- Is the technology simply going to be integrated to cut future costs of administration?

- Will the new system allow more information to be held about an employee, for example if RFID technology is used then will it be possible to track the employees movement around the company and if so then what benefit can this give to the company?
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network

- Will it improve safety, for example, if there was a fire in the building could the system be used to ascertain whether employees were still in the building and if so exactly what is their location?

- Will Human Resources use the information to act as a way of calculating hours worked?

- Will it increase security within the workplace?

The answers to these questions may strongly affect the opinions and preferences of both employees and managers. If the use of RFID technology for tracking was incorporated to increase security and improve safety then employees and managers would likely both agree that this is a good thing. However, if it was employed to assess how many hours are worked and therefore affect payment, employees might perceive this as a lack of trust from the senior management and therefore be less happy. There is also an argument that it may not be possible to assess amount of work done by simply looking at hours in the building or hours an employee is at their desk. This is especially true when considering the current trends for flexible working and task based, how much work is completed rather than the amount of time spent at a desk, employment.

Will the system be able to log people who are connected to the network but are working from home? How will the system allow for meeting clients outside of the company location? It may be possible to employ this sort of system in a call centre where work must be completed at the desk, but it is not really a feasible idea for our client where work often takes place on customer sites, at home or even on the golf course. Any company looking to use this integrated solution must be prepared to answer questions relating to the role of the technology to their employees.

The company also needs to understand both the culture of the country in which the company works and the culture of the company. In the UK where human rights is a major issue it may be that employees are less welcoming to a system that acts as a “big brother”, always wanting to know where you are and what you are doing. However in a country such as Russia, where for many years under the communist regime that is how government had been working, then there may be a more less resistance. However, just because the idea would be more readily accepted does not necessarily mean that it is morally correct.

It is also important to understand that there may be employees of different cultures within the organisation, who will have different views. It may be the case that the company has its own culture and this may be very important. If, for example, our client has a culture of assessing employee performance on results and not methods then there may be considerable opposition to some sort of tracking system. In this case it may be a
good idea to use information only for security and safety whilst also looking to reassure employees that all
the information will only be used for these purposes.

A separate issue that will arise from integrating the technologies is who will now control the system. In
the traditional system security personnel would have managed the physical security network while the IT
department would have controlled their own network. When the system is integrated the physical security
network would probably be integrated into the existing IT network, as this is likely to be the larger of the two.
Using Active Directory it is possible to set permissions so that only security personnel could access security
information. However, in this scenario there must be an administrative team who run Active Directory and
have overriding control if there are serious network errors. It may be that one of the security team will
become a member of this team or will help train the team to understand the issues surrounding physical
security.

6.5 Technological Considerations

Technology is at the core of this decision, without it there is no decision to make. Using the earlier research
it is apparent that the technology needed to implement the integrated solution is readily available. This state-
ment is also backed up by the fact that a similar project has been implemented in a number of educational
facilities across the world by Cisco [48].

There is however one worry that has not been addressed and that is about the vulnerability of only having
one system. The traditional system means that the physical security network does not have access to the
Internet as there is no need. This means that illegitimate users cannot attempt to gain access to and manipu-
late this system through the use of Internet hacking techniques. This is a major plus point for the traditional
system as it decreases risk of unauthorised access. Therefore as the two networks are to be integrated into
one in the proposed solution, it could be argued that it will now be easier to for illegitimate users to gain
unauthorised access as these techniques can be used. This is a valid argument and a good point, but as the
whole system will now be centrally managed with highly defined responsibilities for all security staff, the
administrative team will find that it will become easier to detect any such attempts. Whereas the original
system may have some ambiguity with regard to who exactly is accountable for what, through centralisation
the proposed solution combats creating clear sets of responsibilities for all involved personnel.
No matter how secure the proposed system is a manual override system will need to be implemented on all fire escape routes. This is so that if, for some reason either accidental or malicious, the system does have problems, then employees will still be able to exit the building.

6.6 Summary

The aim of this chapter was to ensure that consideration was given to all the issues the client may have with an integrated solution. This was achieved by employing a decision making framework. Using this framework all the relevant stakeholders were identified as it is important to understand the viewpoints of more than merely the management. The framework ensured that three was a discussion of the political and legal, economic, sociocultural, and technological issues facing the client, therefore increasing the chances of a more effective and personalised solution being developed.
Chapter 7

Integrated System

Assuming that our client has decided to go ahead and integrate the two networks in their new building they will require a system that meets their personal requirements. Management consultancy is a service industry and this means that much of the work done is front office; this is to say that customers see many of the processes, and so image is very important. The client would therefore require a system that was seen to be using technology that was state of the art. Having already noted that the client only employs about 100 people and having completed a PEST analysis it is apparent that there will be some considerable economic constraints.

It is assumed that the client much like the University of Leeds School of Computing, is currently using Microsoft Active Directory as their IT network management software. This software, as was explained in section 5, will allow the integration of the two networks. It is also suggested that although there will be separate security teams and IT teams there should be regular meetings between senior members from each team to allow for discussion of issues relating to the system. Before integration it is strongly suggested that security personnel are consulted with regards to their requirements from the system.
Figure 7.1: Table comparing key technologies that could be employed to control logical and physical access.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Smart Cards</th>
<th>RFID</th>
<th>Biometrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cost</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Security</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Non-Repudiation</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Ease of Use</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Allow Tracking</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Reliability</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
</tbody>
</table>

Figure 7.1 has been constructed using information gathered in chapter 2. Although there are six features that are highlighted for the comparison of the three technologies these features do not have equal importance to the client. The most important factor for the client is reliability followed by cost and security. The new system may face some initial opposition and therefore proving the system to be reliable and secure will help to ease these fears. Initial cost will be an issue for the client as it needs to consider its shareholders, mentioned in section 6.1, and maintain profitability but it is more important to get the right system working reliably. This in turn may lead to future maintenance costs being significantly lower.

The integrated system aims to combine the benefits of both smart card and RFID technology. Entering the building and various rooms within the building should be easy for legitimate users to do. As can be seen from figure 7.1 RFID technology is the easiest to use and is therefore the chosen technology for physical access. This will also help the client to comply with the Disability Discrimination Act mentioned in section 6.2.1. The key benefit of smart card technology is its low cost. Logical access will require readers at every PC or laptop and with so many readers required smart card technology will be used here to keep costs minimal. The system will consist of a smart card that uses two separate RFID transponders; for physical access and tracking, as well as a contact chip; for logical access. The reason for two RFID transponders is that they will need to have different ranges.

The first transponder will have a maximum range of 30 centimetres and be used to access rooms within the building, while the second transponder will have a maximum range of 20-30 feet and be used for tracking employees around the building. The tracking transponder has this longer range in order to minimise the amount of readers needed within the building, thus keeping the costs at a minimum. The reason for the
tracking of employees is for safety; in case of fire the client will be able to advise the fire brigade as to any employees in the building and their location to within 30 feet, and for security; if an employee is in a room for which they do not have access a flag will be seen on the system showing this see Figure 7.2. It is possible to only have this longer range transponder on the card, but this could lead to security weaknesses. For example, consider a scenario where an employee with full building access is walking through a corridor, every door within 30 feet of their card will be unlocked, potentially allowing other employees the opportunity to access rooms for which they do not have the correct security pass. Another advantage to employees of having the two transponders is that they will not be expected to be as vigilant with regards to people tailgating within the building; this is where an employee enters a room behind another employee without using their access card. From experience it has been noted that employees often feel uncomfortable confronting a colleague and asking to see their I.D. after having had them tailgate. As can be seen from Figure 7.2 a flag will come up on the system to show if an employee is in an area for which they do not have the correct access privileges. The short range RFID on the door will not have allowed access to Person B while the long range RFID in the room will locate them as present. This anomaly causes the system to flag the presence of an unauthorised employee in the room.

Figure 7.2: 3 Stage diagram showing how an unauthorised employee, Person B, attempting to tailgate an authorised employee, Person A, to gain access into a room will be flagged by the system.
The smart card will be inserted into a reader, on a laptop or PC, in order to gain logical access. There will also be a requirement for a password once the smart card is inserted. As mentioned earlier in section 3.1.2 authentication, there are three possible types of proof for authenticating a user and two of these will be needed for logical access; something you have and something you know. The cost of a contact reader is much lower than the contactless reader, as was discussed in sections 2.4.1 and 2.4.3, and as there will be many laptops and PCs within the company it is judged that this saving will be substantial.

All the technologies that are used on the smart card allow for encryption, therefore meeting many of the requirements mentioned in Network Security in section 3. No biometrics are to be used in the system at present and so CCTV will be installed at key areas within the building to help meet the requirement of non-repudiation, section 3.1.4. With regards to availability, section 3.1.5, there are two issues affecting the integrated network. It is possible that the network may be unavailable due to malicious or accidental actions, or that there will be a requirement for maintenance work to be carried out. The areas of the network that relate to physical access will be separated on the network by their own set of switches so that hopefully there will be minimal disturbance during these times.

7.0.1 Managing the System

Having proposed the system for the client it is important to mention how its implementation will be managed. The key to the success of this system is not just having the right technology in place it is also having the commitment from employees, as was discussed in section 6.4.

As mentioned in section 6.3 before the system is implemented there will need to be some training of staff who will be responsible for maintaining and running the system. It may be a good idea to get key staff members involved in the implementation of the system so that they can better understand how the system works. If the system is implemented by an outside source then it will be a good idea to have some consultancy arrangement with this source to provide assistance for a period of time.

As was briefly mentioned in section 6.5 CISCO [48] have produced similar systems that are tailored to their specific clients in the education industry. They have included in their system the ability for security personnel to control the opening and locking of doors. This is also proposed for this solution. If, for example, an employee lost their access card and reported it the security personnel could simply cancel all of its access permissions. However, if they believed the loss to actually be down to theft they could track...
the individual until they entered into a room or office and then simply lock the door. This would then allow them to enter the room and apprehend the suspect.

As mentioned in section 6.2 there are legal obligations that the system has to abide by. The contact smart card requires the user to manipulate the card within the reader and this is another reason why it is only being used for logical access and not physical access. When trying to gain logical access the user can be sat at their desk and will find manipulation of the card easier in this environment. It is possible that an aid can be manufactured for any people who still have difficulty with manipulation. As the physical access is contactless this means that access should be easy for all employees. The readers will however, need to be placed at a level reachable by employees in wheelchairs, therefore complying with legal obligations mentioned in 6.2.1. If a contact card was used for tracking and employees had to use this for exiting rooms, then in the event of a fire it is possible that a malfunction of the card could lead to an employee being trapped. However as the tracking system is done using contactless RFID technology, there will be no requirement for employees to use their cards upon exiting the building, it can be guaranteed that this scenario will never happen.

Although it is noted in section 6.2 that the company has no obligation to inform their employees what the tracking data is being used for, in section 6.4 a strong case is made for being open and honest with employees in order to gain their trust and cooperation. If it is stressed that this data will not, under any circumstances, be used to assess employee performance or work hours and that it will be only be used for security and safety issues then there should be less opposition from employees. Holding a meeting with employees from all levels, to discuss any issues, before the solution is accepted is strongly recommended. In this meeting it is suggested that the system be demonstrated to both show the employees how to use it correctly while also highlighting how it will may make life easier for them. Demonstrating the benefits rather than just talking about them can act as an affective tool for persuasion.

7.1 Limitations

Although it is believed that this is the best solution for the client there are some limitations. The first is that as biometrics are not used employees are able to repudiate any claims made against them. If, for example there was a burglary and an access card had been used then although some of the blame can be placed upon the employee whose card was used it does not necessarily mean that it was them who conducted the burglary.
In order to uniquely identify the employees biometric technology would be needed.

There are however, a number of reasons for biometrics not being used at present. The first is that the relative cost of reliable techniques such as iris scanning is currently too high for small or medium sized firms. As mentioned in section 2.4.2 fingerprint scanning is not suitable for high traffic environments, however, this is also true of most biometrics as even the fastest techniques cannot compete with the relative speed of RFID technology. Fingerprint scanning is a solution that could be used for logical access due to its relatively low cost, however, when discussing the IBM thinkpad X41’s fingerprint reader Mitchell [49] states that:

‘while there’s only a 1 in 10,000 chance that it will accept a wrong fingerprint, there’s a 1 in 20 chance that it will reject a valid fingerprint’

This level of unreliability seems to be the current trend in many biometrics at this time and although their use in the future seems inevitable they are not, at present, competing in terms of price and reliability as well as other technologies.

As CCTV will be in operation at the entrances to the building there may be the possibility to identify any intruders as they enter the building. There will be log files that detail entrance times to the building and so it would be possible to find the time the intruder entered using the card and view the CCTV footage of this period.

The second limitation involves the information that is kept by the client. Although the client will be claiming that the information will not be used for finding out employee work patterns there may be some scepticism from employees about the validity of this statement. This scepticism could possibly lead to misconduct from employees, for example, swapping access cards with one another. In order to help prevent this, it is suggested that the information gained from the access cards be stored for a short time period of, say, one working day. There should also be guidelines in place outlining the discipline procedures for misuse of any company property. As mentioned in section 6.2.4 unauthorised access of computers is prosecutable by U.K. law. If the legal definition of a computer includes the integrated system then employees swapping cards could be possibly tried in breach of the Act.
Another limitation involving the information is that if the transponders are tracking every employee at regular intervals then there will be a great deal of information being produced and so there will need to be a high amount of memory available for this. The security of information being kept on RFID technology has also, very recently, been questioned. Research, conducted at Amsterdam Free University under the guidance of Andrew Tanenbaum, has shown the possibility of installing viruses on RFID technology [50]. However, Greg Day, a security analyst for McAfee [51], is unworried stating that

“the reality of such an attack it’s unlikely… as a virus propagation method it’s useless you’ve already cracked the RFID scanner”

So the RFID technology does have a possible security flaw, but it is judged, by the experts, to be a minor one.

Due to fire escape it has been suggested that exiting a door does not require use of the access card. This could potentially lead to a problem if the tracking transponder fails. The only way an employee would know that their access card had stopped working would be when they passed through a door. If an employees transponder does not communicate with the reader then the system will assume that the employee has left the building. One solution may be to ensure that at the main entrance and exit employees have to show their card to leave the building. However, if there was a fire then the door can be opened like a normal fire door.

The final and possibly biggest limitation is fundamental to the idea of integration. As there will now only be one network and not two it could be argued that a security breach is more likely. It seems logical that it would be easier to breach one network than two. The counter argument however, is that having only one network means management is easier and any anomalies will be highlighted earlier, therefore increasing the overall security.

7.2 Feedback from Mr Prit Rehal (University of Leeds School of Computing Representative)

The integrated system that has been produced is for the ‘dummy’ client, thus meaning there is no feedback from the client. Therefore the system was presented to Mr Prit Rehal, the representative from University of Leeds School of Computing, who was the original client in order to gain feedback from a marketable source.
Mr Rehal was very impressed with the system being proposed and stated that if it were not for the economic constraints placed upon the University he believed that there would be a definite interest in acquiring a similar system. He did however, have two concerns over the system. Firstly there is the issue of resilience and redundancy. What happens if there is a complete crash of the system? The second point is to do with the people aspect of the system. Universities act like a business in many ways, such as charging tuition fees for student attendance, but they are not fundamentally interested in profits as they are exist to aid education, research, and learning opportunities. Many university employees have sought to work in a less pressured and constrained environment than the one offered in many commercial organisations. As academics have a genuine interest in their research and subjects they are trusted to work to a satisfactory level without being directly supervised. Mr Rehal believes that there may be greater opposition, to a system that tracks users, from university employees than what will be seen in the commercial business environment because of this culture difference.

The first point made by Mr Rehal about redundancy and resilience is valid not only for his situation but for all prospective clients. In order to prevent the situation mentioned earlier arising it is proposed that the system work with a dual server architecture. This will have a main server running the system with a backup server mirroring the system so that if there is a need for maintenance or the main server does come into difficulties then the system can be run off of the backup server. The recommendation of how to deal with Mr Rehal’s second point, about greater opposition from employees in a university environment, is the same as it is for all clients. That is to involve employees from different levels in an organisation, before accepting a system, to help demonstrate the potential benefits and alleviate any worries.

Mr Rehal finally mentioned that although the cost installing a new integrated system would be too high, there may be interest in a system that allowed migration from existing networks. Many organisations may be in the position where they have two networks running separately and would like to integrate but cannot afford a completely new system. Therefore a market may exist for applications that enable the migration of two networks into one integrated system without requiring extensive re-networking.

7.3 Conclusion

Although the solution has limitations it is believed that this is the optimal solution for the client at the present time. This solution may not fit the needs of other clients and it is important to state that although integration
of logical and physical access is suggested for this client it may not be of benefit to all organisations. Any organisation that is interested by the possibility of producing their own integrated system would be advised in following a similar analysis to the PEST undertaken in section 6, to help highlight what issues need to be considered.

It is difficult to assess if there is a market for integrating solutions due to the unwillingness of almost all organisations in divulging their current status and information relating to their security requirements. However, as stated by CISCO [48] 75% of the cost of a buildings lifecycle occur in the maintenance and operating period. This fact means that the proposed solution and ones of a similar vein, that enjoy lower maintenance and operating costs, can lead to significant savings for organisations.

7.4 Further Work

This work could be furthered by looking at the possibility of tracking equipment in conjunction with employees. This would look at the possibility of checking that any equipment being removed from the building does actually belong to those removing it. Organisations where many employees have laptops and often work from home may find such a system beneficial.

Another aspect that could be investigated could be the cultural differences of different countries, industries, and organisations to assess how similar solutions are received by employees and management in each.

Having investigated the integration of the IT and physical security networks the next stage may be to investigate integrating the Human Resource network, and discussing the possibility of networking and integrating the heating, lighting and power in all rooms, much like what CISCO [48] has been installing in some education facilities. There are potentially massive cost savings arising from more efficient energy use and the ability to undertake remote maintenance work. Two important question being posed for anyone investigating such ideas are ”Where do the lines between privacy and convenience begin to blur?” and ”Who is getting the most benefit, employees or employers?”
Chapter 8

Appendix A

When starting my project I found that the first problem I encountered was not knowing the exact direction of the project. This ambiguity created a problem for planning. The initial idea was to attempt to find a client who could provide a set of requirements so that a solution could be worked towards. However, it became clear very soon that organisations are unwilling to share any information about their security systems with outside sources such as myself. It was important to make some progress with the project and so it was decided that concentrating on researching what technologies were available for physical security and how they could be integrated with the IT network should be undertaken before again tackling the problem of client.

I found researching physical security technologies difficult as there were very few books written containing the information required. This is probably due to the fact that the technologies researched were new, and as they are not unique to security it is unclear where a detailed explanation of how they work should take place. The majority of information was therefore gathered from technical publications and white papers.

As commercial organisations were unwilling to act as a client I turned to the education industry and found The University of Leeds, School of Computing to be a willing client. Although they did not have immediate requirements for an integrated system due to economic limitations they did provide information as to what
technologies they were employing at the time and what they felt needed improving. Due to the lack of commercial client it was decided to create a client, stating any assumptions made, who could be analysed to provide requirements for a solution. Rather than being a hinderance creating a client possibly allowed me a more thorough investigation. Whereas a real client may have only revealed their technological and economic requirements for the system, having a created client meant that it was possible to investigate other factors such as what the social effect of the system may be, any legal factors needed to be considered and what differences would there be between how the system was meant to be used and how it actually was used.

8.1 Lessons Learnt

Due to the ambiguous nature of the project at the start there was a methodology and a fairly unstructured plan. It is important before starting work to define how the project will take shape and analyse how long each factor will take in order to work efficiently. As the project develops revisions to the initial plan be made. This is not a bad thing as it helps to keep focus and provides more accurate progress information to a candidate.

I met with my tutor once a week and found these meetings invaluable. Tutors can act as a sounding board for ideas, help to guide candidates in the right direction while prevent veering off course, or they can simply act to rebuild confidence when the project seems to be going nowhere.

8.2 Avoiding Problems

Anyone looking at undertaking a similar project that involves a client or a potentially marketable solution should be advised to develop links with an organisation before starting the project. Finding a client was the biggest obstacle that I faced, and although I managed to get around the problem through the creation of a client and the analysis of other similar solutions to aid solution evaluation I feel that having a client from the start would be an advantage. The information gathered from them is non-reputable and can help understanding of specific organisational or general market requirements. If there are other factors that need to be investigated then a case study can always be created later and these two would compliment one another.
Bibliography


Report on the Feasibility of Integrating Physical Security Access with an existing IT Network


David Palmer - jhs2dp
Report on the Feasibility of Integrating Physical Security Access with an existing IT Network


