Evaluation of Physical Security at IDA

Muhammad Salman Khan
Email: khamu937@student.liu.se
Supervisor: Juha Takkinen, { juhta@ida.liu.se }
Project Report for Information Security Course
Linköping Institute of Technology, LiTH
Linköpings Universitetet, Sweden

Abstract

This report is a detailed study of physical security methods available for protecting a data center. A preliminary analysis has been done on the data center located at the Department of Computer and Information Science (IDA) of Linköping University, Sweden. Various traditional methods for physical security are discussed in this report along with their implementation. The two appropriate solutions are proposed for the data center of IDA are biometrics and CCTV these methods recommended for the physical security of IDA. The combination of these two methods has capability to provide access and monitoring control to IDA facility.

1. Introduction

The aim of this report is to make physical security analysis of IDA and to identify vulnerabilities and recommend some possible solutions to safeguard against physical attacks in future. The proposed solution is based on the theoretical analysis of traditional attacks and their possible prevention methods.

By reviewing the design and construction process for a data center from a physical security perspective, this report shall identify and describe the counter measures needed to make IDA's data center fully secure.

Physical security is basically the protection of assets from significant physical damages. The recent development in the computer security area has changed the meanings of physical security. Physical security is the technology to protect the computing system from unauthorized access. The technological solutions must provide high rate of success as compare to failure cases. [1]

Some common examples of assets include backup hard disks, servers, and backbone routers. There is no standard definition of physical security. However, the domain of physical security starts when an attacker plans to perform a physical attack on the system.

No system can be ideally foolproof. IDA is a department of Linkoping University (LiU). IDA has important assets which includes database servers, gateways, routers, and ISP backbone. IDA has physical security system but we cannot rely on the current system in future. Also, physical security requirements change over time because of newly discovered attacks and scenarios. Therefore continuous analysis is necessary to identify vulnerabilities in the system in order to make it secure against possible physical security attacks.

During the preparation of this report, a deep analysis has done. The analysis was theoretical and consisted of several phases. The sole purpose the analysis phase was to identify the best possible solutions to protect the data center from physical security attacks. During the analysis phase, most secure methods were selected for the protection of the data center at IDA.

2. Background

Physical security provides the methods to protect the valuable assets from serious circumstances. The assets play a key role in the working of an organization. It is necessary to identify the critical resources and provide the security for them. It is also necessary to use specialized security solutions in parallel to the

traditional solutions. It is also important to consult security experts to remove the security flaws and update the system in a professional way.

It is interesting to note that physical security is often overlooked by many organizations. These organizations often give their attention to more technical issues such as viruses, spy wares and Intrusion Detection Systems (IDS) systems. Due to the lack of knowledge and interest, the attacker can easily find the way to the importance assets and performs serious attacks. Therefore, analysis of physical security and its implementations is crucial in order to propose a feasible and effective solution.

2.1 Purpose of Physical Security

The purpose of physical security is to describe both measures that prevent or deter attackers from accessing a facility, resource, or information stored on physical media, and guidance on how to design structures to resist various hostile acts. It is not possible to guarantee the ideal and 100% level of physical security. However, it can be optimized and reach an acceptable level if proper and effective methods are used. Also, no method is perfect or ideal. It depends on the nature of assets, protecting environments, and scenarios that form the basis for the analysis.

2.2 Resources to be protected

There are various resources to which ‘evil forces' are interested in gaining access at organizations site. Some of these are theft of information or purchase of information from personnel. These also includes theft from records, files, documents, or related sources, gaining access to working models, sample products, processes, or equipment, and making copies. There are some other non-physical types of resources that are necessary to protect. The most important one is personal information. The attacker can use skillful means to obtain information from employees at social events, gathering information after gaining access to facilities, searching through discarded records, waste, trash cans, etc.

There is no standard defined for the types of physical security attacks, however, they can characterized on the basis of their sources. There are two types of physical security attacks.

1) First one includes natural disasters like fire, earthquakes, flood, blizzards, volcano etc.
2) Second type includes intentional attacks from human beings such as burglary, theft, vandalism, and terrorism.

2.3 Components of Physical Security

There are multiple strategies to prevent physical security attacks. These strategies can be categorized into three main components, based on the step-by-step security level framework. [2]

- The first and the initial component of physical security, is to keep an attacker far away from the protected assets. This strategy can have psychological effect on the attacker. The methods include physical locks, high walls, fire proof sites along with fire alarm detectors, water sprinklers, and security guards.
- For the second and intermediate component of physical security, monitoring and notification system is appropriate. This type of physical security also includes surveillance systems. Proper lighting at the place to be protected, fire and heat sensors especially smoke detection, mobility detection, and CCTV cameras are best examples of this category of components.
- The third component of physical security identifies an attack when it happens and takes appropriate steps. The methods in this component are not preventive but they are recovery methods. Proper and effective backups are mandatory for this component.

The first and second components belong to the physical security prevention phase and the third one is the part of the recovery phase.

2.4 Traditional Physical Security Methods

It is necessary to discuss the traditional physical security methods so that we will have some idea about the working of these methods before the analysis.

2.4.1 Identity Card

Identity card is a small-size document used for authentication and identification of a person. It is simple and suitable way to authenticate the identity of any person. Identity card is one of the most famous and old way of security identification. Traditionally, Identity card consists of some personal information along with a photograph on it. However, some technological features are also included in identity cards such as bar code, and embedded micro chips. Plastic cards are best examples of modern identity cards. [3]

Figure 1: Student ID card [4]

2.4.2 Safety Alarms

Safety alarms are electrical house alarms designed to alert the owner to danger. Sensors are connected to a control unit via a low-voltage hardwire or narrow band RF signal which is used to interact with a response device.

Figure 2: Fire safety alarm [5]

The most common security sensors indicate the opening of a door or window or detect motion via passive infrared (PIR). [6]

2.4.3 Biometrics

Biometrics is a method/technique that is used for recognizing human beings based on their physical and behavioral characteristics.Biometric-based human identification are classified into two major categories:

- Physiological characteristics concern the physical characteristics of human beings, like shape, size, height, and geometry. Some famous examples are DNA, retina, and fingerprint.
- Behavioral characteristics refer to behavioral changes or set of unique identifications of human beings like voice, typing style, and facial expression.

- ***Features of Biometric Systems***

Biometrics can play a vital role in understanding the human characteristics on the following particular parameters. [7]

- Universality: Each person has universal and predefined set of characteristics.
- Uniqueness: The biometric ability to identify the individual.
- Permanence: How much the biometric occurrence changes with the passage of time.
- Collectability: How well the related biometric human information can be available and organized.
- Performance: How much work is done in a particular time with respect to speed of respective technology.
- Acceptability: How well the biometric methods are accepted in daily life of human beings.

- ***Basic Functions of Biometric Systems***

The two most important and basic functions of a biometric system are as follows: [7]

- Verification: This is the process of identifying an individual by mapping

different characteristics of it. The authentication mechanism of verification includes the one-to-one mapping of all the concerned records stored in a particular database. Examples are fingerprints and the iris.

- Identification: This is the process of recognizing the individual on the basis of its personal information like, identity and secret questions. Biometrics record gives the closest available entry from the database.

The sensor is the first component of the system that provides the interface between the real world and the rest of the system. The purpose of the sensor is to gather all the required data from the real world and send that data to the preprocessing phase of the system. The second block is responsible for preprocessing of incoming data i.e. to remove all the irregular signals and noise. In the third step, correct features are extracted. This step is an important step because it extracts all the related information from the data. The purpose of this stage is to give the correct features to next phase. In the fourth step, a template is generated from the extracted features. A template is basically a synthesis of all the characteristics of data generated from the source. The generated template is then enrolled in the database of template section and then used for matching the identification. The result is then forward to the application device to activate the response. The main operation of the biometric system is enrollment and test. In enrollment, the generated template (or biometric information) is stored. During the test, the biometric information is then checked against the stored information. [7]

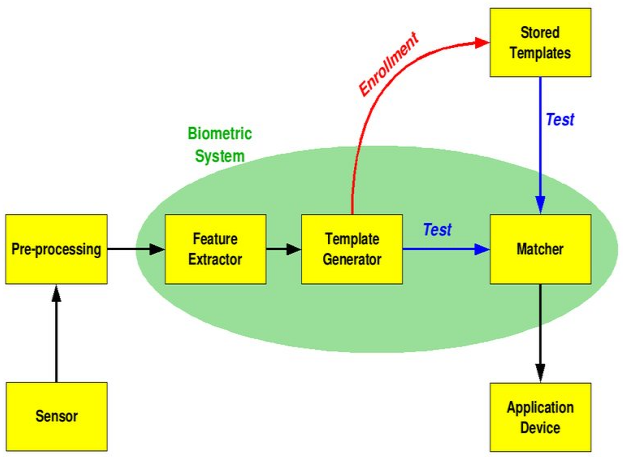

Figure 3: Biometric system [8]

2.4.4 Closed-circuit television (CCTV)

Closed-circuit television (CCTV) is the use of video cameras to transmit a signal to a specific place, on a limited set of monitors. CCTV is often used for surveillance in areas that may need monitoring such as banks, casinos, airports, military installations, data centers, and convenience stores. [9]

Figure 4: Surveillance cameras [10]

- ***Significance of CCTV***

The Closed Circuit Television (CCTV) market is one of the fastest segments of the security industry today. One reason for this is the fact that a picture is worth a thousand words. This is especially true in a court of law where an eye witness is required who can place the criminal at the scene of a crime. Otherwise, chances are the criminals will not be convicted. CCTV systems are also helpful in the residential security market. They allow homeowners to see their callers, thus establishing their identity before they open an outside entrance door. This is an important feature too, because otherwise, they might open their door to a criminal.[11]

Figure 5: Monitoring room [12]

2.4.5 Impact of Social Engineering on Physical security

Physical security is concerned with social engineering. Social engineering is a collection of techniques which involves deception and manipulation of people to get their secret and personal information. The common techniques includes the glancing of password entries, recording password key strokes through some device such as movie camera, searching password notes in the personal pads of users, and calling system operators and saying that he/she is an employee who forgot his/her password and ask for a new one. The goals of social engineering are the same as of hacking in general i.e. to gain unauthorized access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network. Social engineering based attacks mostly focus on large companies and organizations. Example of these targets is financial institutions, military, government agencies and hospitals. [13]

3. Analysis

A data center is a centralized repository, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business**.**

3.1 Phase 1: Identification of Assets and Resources

A data center consists of numbers of servers, routers, cables, and server racks along with maintenance and monitoring system. The size of a data center depends upon a number of factors such as the size of an organization (in terms of number of client nodes connected), the number of specialized applications and most importantly the role of the data center in day-to-day work. The importance of data center cannot be underestimated because it acts like a central operation unit for the organization.

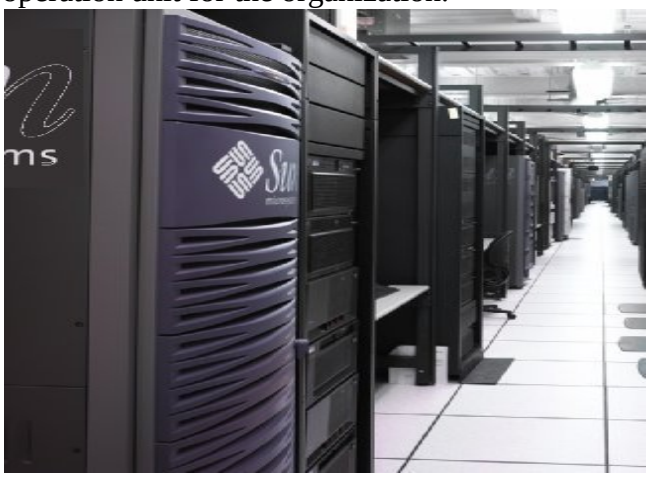

Figure 6: Data Center of Sun Microsystems [14]

3.1.1 Importance of Data Centers

Some of the reasons behind the physical security of data centers are as follows:

1. The data centers are responsible for running the core applications of the organization. These applications handle the core business and operational data of the organization.
2. The data center is also used for the fundamental and necessary server function and their services. These include domain controller, active directory services, file server, dynamic host control protocol (DHCP) server, and web server.

3. Data centers are also used for offsite backups. The organization may subscribe to backup services provided by a data center. Backups can be taken of servers locally on to tapes. However, tapes stored on site pose a security threat and are also susceptible to fire and flooding. Larger companies may also send their backups off site for added security. This can be done by backing up to a data center. Encrypted backups can be sent over the Internet to another data center where they can be stored securely.
4. Data centers contain a set of routers and switches that transport traffic between the servers and to the outside world. Some of the servers at the data center are used for running the basic Internet and intranet services needed by internal users in the organization such as e-mail servers, proxy servers, and DNS servers.

3.2 Phase 2: Physical Attacks and their Classification

In the second phase, I began my analysis of the traditional physical security attacks and their prevention mechanisms. As my target was data centers, I limited my analysis to the physical security attacks concerned with the data center only.

Now, the next thing was how to discover the physical attacks to the data centers. Without knowing the possible attacks their prevention methods cannot be determined. Environment (in which a data center is working) is also an important factor for attacks. Therefore, in the second phase, I searched different possible attacks to data centers**.**

3.2.1 Nature of Physical Security Attacks

There are large numbers of possible attacks to data centers. It is impossible to analyze all the attacks and their causes because the occurrences of these attacks are based on their environments, purposes and their sources. However, classification of these threats based on their sources is possible. Attacks from human beings are classified into two subcategories. These are:

1. The first type of attacks is from human beings with the use of some tools, machines or devices. This type of attacks includes bombing, attacking and terrorist activities etc.
2. The second type of attacks is from human beings and called personal attacks. These attacks are launched personally.In these attacks, an attacker is physically present at target location.

During the analysis, I noticed that man-made personal attacks are the most frequent attacks. These attacks are easy to launch and require fewer resources than any other physical attacks. However, the success factor of this type of attacks requires extensive skills and analysis of a victim or target in order to be launched. The interesting thing to notice is the damage level. These attacks are very dangerous and sometimes may cause more serious damage than any other physical attack. Therefore, I decided to continue my analysis on personal attacks.

3.2.2 Social Engineering and Man-made Personal Attacks

Before understanding the personal attacks and their types, the method of social engineering should be analyzed first. Social engineering is a set of techniques that are used to build the user confidence to stealing the confidential information. Through social engineering, an attacker makes an attempt to defraud a person or group by gaining their confidence. An attacker uses different confidence-gaining tricks on victim based on his/her personality. Persons of any level of intelligence are vulnerable to deception by an experienced social engineer. Confidence tricks exploit human weaknesses like greed, dishonesty, and vanity, but also virtues like honesty, compassion, or an expectation of good faith on the part of the attacker.

3.2.3 Physical Attacks Specific to Computer Systems

There are also many physical security attacks specific to computers. These type of attacks are and harmful for computers, specially servers and other dedicated machines. Some of them are given below.

- **Ultraviolet Attacks:** Using ultraviolet lights to destroy electrically erasable programmable read-only memory (EEPROM) or using a strong magnet on magnetic storage.
- **Hard-disk Damaging:** A physical attack on storage devices is a popular attack. These attacks are launched to destroy valuable data from storage such as hard disks.
- **Other Types of Attacks:** Computer CRT signals can be picked up from distances of up to several hundred meters with simple, cheap equipment. Ordinary phone wires are prone to both active attacks (using alligator clips and listening to the signal), which can be detected, or inductive attacks which are harder to notice. Fiber optic cables can be compromised by splicing a repeater, bending or nicking the wire, or placing the wire in high-refractive liquids and allowing the light to escape.

An attacker knows all the traditional physical security implementations. Intelligent attackers always plan with the possible physical security methods in their mind. Also, no single strategy is perfect to safeguard against these attacks. Therefore, some other way of thinking is necessary.

3.3 Phase 3: Prevention Methods and their Classification

The best strategy to prevent an attack is to identify an attacker in an early stage, preferably as early as possible.

3.3.1 Biometrics-based Prevention Methods

The best way is to use biometrics system. Biometrics system has the ability to recognize the physical and behavioral characteristics of human beings. Biometrics based solutions provide the advantage to uniquely identify an attacker. The basic function and features of the biometrics system are described in section 2.5.3. The famous biometrics-based physical security solutions are as given in detail. [15]

- *Fingerprint Recognition*

Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identities.

- *Facial Recognition*

In facial recognition system, the specific characteristics of a human face are detected. The data concerned with facial characteristics is then compared to the database. The database contains the stored values of the faces, scanned before. Digital images and video sources are used as input for the facial recognition system.

- *Iris Recognition*

Iris recognition system is similar in its operation as the facial recognition system. In the iris recognition system, high resolution images of the eyes of human beings are necessary to identify the individual.

There are some other biometrics-based prevention methods in use. The selection of a particular biometric method is based upon the requirements, environment and nature of the asset to be protected.

- ***Advantages of Biometrics Systems***

The main advantages of biometrics systems are:

- The fact that one will have to personally be present in order to authenticate oneself.
- The finger prints or retina of the eyes of one person does not match with anyone else. Therefore, there is absolutely no chance of other people to use one's identity.

- Logs are maintained for future use.

- ***Disadvantages of Biometrics Systems***

Some of the disadvantages are given below.

- The people that are directly involved in chemical industries are not suitable for fingerprint identification. Their fingerprint characteristics are badly affected by the use of chemicals.
- The eyes of most people are badly affected with diabetes. It is difficult to the use iris recognition system with diabetes persons.
- Biometric machines are expensive. Therefore they are often avoided in many small organizations.

3.3.2 Multi-Levels Security

We know that biometrics-based security is not easy to break or bypass but at the same time we also know that the attacker is an intelligent person. Therefore, second level security should exist after the biometrics security. The second level physical security should be at least similar or more intelligent than the first level so that an attacker has to consume more efforts and time to break or bypass the security. In the same time, we will have a greater probability to stop an attacker. The second level of security should have the capability to monitor facilities. One clever method for this is CCTV.

3.3.3. Closed-Circuit Television (CCTV)

Closed-circuit television (CCTV) is the method of physical security that uses video cameras to transmit a signal to a specific place, on a limited set of monitors.

- ***Advantages of CCTV***

The advantages of CCTV include:

- CCTV allows the user to instantly retrieve relevant data without going through hours and hours of videotape.
- Digital video images are superior to video recorded on analog tape. Also, digital video images can be enhanced and copied virtually endless times without losing their original quality.
- Sharp images can be stored, which can be replayed over and over without image deterioration.
- Important information can be archived on to many types of media, including CD-R or DVD for later retrieval even years later.
- One can transmit and retrieve stored data across cities or even across the world. The digital video images can be remotely viewed, saved, retrieved, displayed, copied, printed, faxed, and even e-mailed.
- The digital CCTV images can be stored in a database that can be searched by camera ID, time, date, alarm activation, or even motion type.
- With digital CCTV, one does not use tapes. Digital storage media has almost an unlimited lifetime.

- ***Disadvantages of CCTV***

The disadvantages of CCTV include:

- Data protection violation (one has to ensure media kept in a secure place).
- People might be uncomfortable being watched so this will affect motivation and attitudes.
- May cause people behaving in controlled ways.
- Good quality CCTV is costly.

The combination of these two methods can provide the best protection against physical security attacks on the data centers.

4. Discussion

The biometrics-based security methods and CCTV is an ideal combination. These methods provide access control and monitoring at the earlier stage of physical attack. One of the great advantages of these methods is that they can be implemented almost everywhere and in parallel with other physical security methods. In addition, a proper backup mechanism is required for a satisfactory physical security setup.

5. Physical Security at IDA

After the analysis and the results extracted from it, two physical security methods were selected. However, it is also necessary to know the present physical security situation of a data center located at IDA.

It was discovered that the basic security of the servers at IDA consists of a locked room to which only the Technical Maintenance and Service (TUS) group have access. All officers from TUS use key cards to access the data center. These key cards are of the similar type as the of student ID card. There are neither physical locking or access mechanism on the servers themselves nor CCTV cameras for monitoring.

It is now clear that the servers of IDA are vulnerable from a physical security's viewpoint. Therefore, an appropriate solution is necessary to avoid possible physical attacks. The biometrics and CCTV methods can be helpful in this regard.

6. Conclusion

The present situation of the data center at IDA is not satisfactory. There are physical security flaws for the access and monitoring control. The biometrics and CCTV methods can provide the satisfactory level of security. However, the suggestions from experts are necessary for the implementation.

7. Future Work

My study is based on theoretical analysis. For implementation purposes, this report can play a key roll. However when implementation takes place then environmental constraints should be taken into account such as IDA policy related to physical security. It is important to consult with the experts to examine the implementation cost. Biometrics-based solutions are costly than other physical security methods. Also, a more thorough investigation would be interesting to perform in future.

References

[1] Weingart, S. H. White, S. R. Arnold, W. C. Double, G. P, (1990), *An evaluation system for the physical security of computing systems*, IBM Res. Thomas J. Watson Res. Center, Yorktown Heights, NY, IEEE.

[2] Components of physical security, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci1150976,00.html.

[3] Carey Leyton, 05/19/2009, *Uses Of Plastic Cards*,http://www.amazines.com/article_detail.cfm/887686?articleid=887686.

[4] Figure 1: *Student ID card*, http://audaciousness/library/libserv/images/studentcard_number.jpg.

[5] Figure 2: *Fire safety alarm*, http://www.indiamart.com/jawala-safetyengineers/pcat-gifs/products-small/response-indicators_10411687.jpg.

[6] Trimmer, H.William, (*1981*), *Understanding and Servicing Alarm Systems*, Stoneham: Butterworth.

[6] *Features of biometric systems*, http//en.wikipedia.org/wiki/Biometric.

[7] Jain, A. K, Ross, Arun; Prabhakar, Salil, (January 2004), *An introduction to biometric recognition*, IEEE Transactions on Circuits and Systems for Video Technology.

[8] Figure: *Typical biometric system*, http://upload.wikimedia.org/wikipedia/commons/3/3c/Biometric_system_diagram.png.

[9] Jain, A. K, Ross, A, Pankanti S, (June 2006), *Biometrics: A Tool for Information Security*, IEEE Transactions on Information Forensics and Security.

[10] Figure 4: *Surveillance cameras*, http://upload.wikimedia.org/wikipedia/commons/a/a1/Three_Surveillance_cameras.jpg.

[11] Al Colombo, *CCTV - Video Surveillance Cameras Monitors Security Monitoring Devices*,

http://www.infosyssec.org/infosyssec/cctv_.htm.

[12] Figure 5: *Monitoring room*, http://upload.wikimedia.org/wikipedia/commons/3/34/SoMSurveillance_.jpg.

[13] Bob Samson, *Social Engineering*, (july 1, 2008),www.cfcpa.org/downloads/SocialEngineering.doc, Central Florida Crime Prevention Association.

[14] Figure 6: *Datacenter of Sun Microsystems*, http://www.sunlandunixguru.com/SunlandUnixGuru.com_files/h_datacenter.png.

[15] *The biometrics article by wikipedia*, (May 2009), http://en.wikipedia.org/wiki/Biometric.