ANALYSIS OF AIRPORT SECURITY BASED ON THE FIVE COMPONENTS OF INFORMATION SYSTEMS

Juyun Cho, Colorado State University-Pueblo, joey.cho@colostate-pueblo.edu
Tom Velazquez, Colorado State University-Pueblo, tomvelazquez@hotmail.com
Benedikt Kraus, Colorado State University-Pueblo, b.kraus@colostate-pueblo.edu
Korakod Aphipanya, Colorado State University-Pueblo, k.aphipanya@colostate-pueblo.edu

ABSTRACT

Since the attacks of September 11, 2001, the United States has declared a global war on terrorism and has strived to make the nation secure. However, as revealed in the 2009 Christmas Day attack, the government did not have a capable system to defend the country against terrorist attacks. This paper discusses the current issues and problems of airport security in terms of hardware, software, data, procedure, and people. This paper also suggests solutions that would potentially solve security problems which reside in the five components of current information systems.

Keywords: Information systems, Security, Airport security, Transport Security Administration, Terrorist screening database, Hardware, Software, Data, Procedure, People.

INTRODUCTION

After World War II, the martial and economic boom that the United States experienced during the 1950s and 1960s resulted in a nationalistic belief that the United States of America could not be attacked within its borders. The Cuban Missile Crisis and the Cold War were the closest threats of an attack on the United States, yet there was a sense that because of the military might of the United States, the country could not be invaded or attacked from within its borders.

It was not until after the fall of communism that a new threat began to emerge – the threat of terrorist acts within the United States. Extremist groups had conducted attacks against the United States dating back to the early 1980s with the Hezbollah truck bombings on the U.S. Embassy and the U.S. Marine Corps barracks in Lebanon, the 1984 bombing of the U.S. Embassy Annex in Beirut, and the hijacking of TWA Flight 847 in 1985 (Mueller, 2006). At that time, terrorism's strong presence was being felt throughout the world, but never on United States soil. Soon, however, the first attack within the borders of the United States occurred on the World Trade Center Buildings in 1993. A group of Muslim terrorists detonated a car bomb beneath the North tower killing six people and injuring over 1,000 others.

Despite the aforementioned attacks, the United States government was slow to react to the lack of security and vulnerability the nation faced to threats posed by terrorist groups within the country. The egocentric sense of invincibility still permeated the American mentality. It was not until the April 19, 1995, attack on Oklahoma City that a truly successful strike was carried out on American soil. Timothy McVeigh and Terry Nichols, two American citizens, destroyed the Alfred P. Murrah Federal Building in downtown Oklahoma through the use of a truck bomb. The attack killed 168 people and injured 680 more. The blast destroyed and damaged 324 buildings and 86 cars. The bomb was estimated to have caused at least $652 million worth of damages (Mueller, 2006). Consequently, this act of terrorism was noticed around the world and exposed key weaknesses in the United States' security and infrastructure to terrorist groups.

All the while in the background, underfunded, technologically outdated agencies such as the Federal Bureau of Investigation (FBI) and Central Intelligence Agency (CIA) were trying to prevent a similar attack on the country. According to the FBI Counter-terrorism Report (2006), the FBI and its partners had adverted attacks on New York City land marks in 1993, the bombing of a U.S. aircraft in the Far East in 1995, pipe bombs on New York subways, letter bombs in 1997 and the infiltrations and stoppage of a Los Angeles International Airport bomb plot in 2000 (Mueller, 2006).

During the same period, the use of communication and collaboration technology mushroomed throughout the world as a result of the Internet and the dot com boom. This also made it easier for terrorists to actively organize themselves, communicate, and spread radical ideas and propaganda. As these groups expanded their influence, ideology and capabilities, the organizations

that were supposed to be protecting the country were lagging behind instead of moving to the forefront of innovation and use of technology that could prevent further attacks on the United States.

The remainder of this paper is organized as follows: The next two sections describe the most recent two attacks which occurred in the U.S. Next, analysis of information systems used in an airport security is discussed, and suggestions and conclusions are followed.

9/11 Attack

As a result of the government's slow response to various attacks and threats aforementioned, on September 11, 2001, the most catastrophic, deadly attack occurred on U.S. soil. The Al Qaeda terrorist organization, headed by Osama Bin Laden, hijacked four U.S. commercial aircrafts with the aid of 19 suicide bombers. Two of these aircraft were used as battering rams and were crashed into the two World Trade Center towers in New York City, killing all its passengers and destroying the two buildings. These towers were targeted because they stood as a symbol of America's economic wealth. The third plane was crashed into the Pentagon, the headquarters and symbol of America's military might, and the fourth plane was crashed into a field, when passengers heard of the other attacks and began to fight back against the hijackers. It was believed that this last plane was headed for the White house, the symbol of America's government. In effect, Al Qaeda had attacked every facet of American society by attacking America's military, political, and economical institutions. Thus, the 9/11 attacks were very effective from the terrorist's perspective. In total, 2,973 innocent victims died as a result of these attacks.

In addition to the lives lost, this attack was a huge blow to the U. S. economy. According to the Institute for the Analysis of Global Security (2003), the losses suffered on 9/11 for property damage and lost production exceeded $100 billion dollars. When stock market losses and the Global War on Terror are considered, projections range from 1 to 2 trillion dollars. The United States citizenry also suffered a severe blow to their national psychology. The mindset of American invincibility had been replaced with fear. The weaknesses of U.S security infrastructure was exposed to the entire world. As a result, the people of the United States turned to the government for answers. What could be done to prevent this from happening again? Hence, the 9/11 attacks affected every facet of American life and dramatically changed the perception of U.S. security, transportation and business procedures. The United States had entered a new era: the post 9/11 era and the Global War on Terrorism. Table 1 shows the economic cost of 9/11 attack.

Christmas Day Attack

On Christmas Day 2009 the U.S. was attacked again. Umar Farouk Abdulmutallab, a Nigerian man with known connections to terrorist organizations was allowed to board Northwest Flight 253 in Amsterdam en route to Detroit, Michigan. He purchased his one-way airline ticket with cash in Ghana on December 16, all of which are security red flags.

Table 1. Economic Costs of 9/11attack (Source: NATO, 2004)

Contents	Economic Loss
9/11 Attack	• ~$34 bill. plus uninsured losses • ~$576 million for Pentagon • ~2,973 dead
Combating Terrorism	• $53 bill. by U.S.
Afghanistan	• ~$50 billion plus for DOD • ~$3.3 billion for reconstruction & $4.5 bill. pledged by other countries • ~140 Americans killed
Iraq	• ~$125 billion plus for DOD • ~$21 billion for U.K. for year • ~$21 billion for construction & $13 billion pledged by other countries • ~1,058+ Americans killed ~$3.3 billion for reconstruction
Macroeconomic Effects	• Up to $300 billion in lower world growth in 2001 & 2002
Insurance	• 5% increase in premiums on property in U.S. Higher increases oversees
Travel & Tourism	• 279,000 U.S. jobs lost 2002
Shipping	• 1-3% of shipment value for security

During the flight, as the plane approached Detroit, Abdulmutallab spent about 20 minutes in the

bathroom and returned to his seat covered in a blanket. He then attempted to detonate a plastic explosive. A passenger onboard jumped onto Abdulmutallab and fought with him as flight attendants used fire extinguishers to put out the fire caused by the failed ignition. The bomb that he used consisted of a six-inch packet containing the explosive powder PENT, which when mixed with TAPN becomes a plastic explosive. He used a syringe with acid liquid as his detonator (Wikipedia, 2010). It was later revealed that the plastic explosives he possessed were enough to destroy the plane and kill all the passengers onboard.

Again, the government had been exposed as not having a capable system to defend the country against terrorist attacks. The National Security Agency had given information to the National Counterterrorism Center (NCTC) that a Nigerian man, with ties to Al Qaeda was going to attack the U.S. Furthermore, American diplomats in the U.K. were warned by Abdulmutallab's father that his Nigerian son had been radicalized by a group in Yemen and should be considered a threat (Shane, 2009). However, these two key pieces of information were never connected together by the U.S. intelligence agencies. Thomas H. Kean, chairman of the 9/11 commission said, "It's almost like the words being used to describe what went wrong are exactly the same." (Shane, 2009). Eleanor Hill, staff director of the joint Congressional inquiry into September 11 attacks also said, "It's eerily similar to disconnects and missteps we investigated. There seems to have been the same failure to put the pieces of the puzzle together and get them to the right people in time." (Shane, 2009).

ANALYSIS OF FIVE COMPONENTS OF INFORMATION SYSTEMS IN AIRPORT SECURITY

This section analyzes the aviation security in terms of five components of information systems. According to Kroenke (2009), an Information System is a combination of hardware, software, data, procedure, and people. We will use this definition for our analysis.

Hardware Issues

This section discusses different types of hardware used by U.S. security agencies and U.S. airports and airlines. There are several types of hardware that need to be looked at because of the weakness of the system being used. This hardware includes security cameras, metal detector, full body scanner, X-ray machines, and Computed Tomography (CT) scanners.

Security Barriers and Security Cameras: Security cameras are used to detect persons or objects that are undesirable at the airport or in any location that needs security surveillance. Currently, barriers to enter an airport are along the entire parameter, and cameras are located at critical areas such as entrances and exits, fueling docks, and luggage loading areas (Tyson, 2001).

Although security barriers are in place to deter unwanted people from entering secured areas of an airport, it is still possible to penetrate these areas by cutting a fence or by attacking planes from outside the airport with a rocket launcher that could be shot at incoming planes as they descend for landing. Currently, there are not security measures in place that secures all outside areas of the airport where it could be strategically attacked by terrorists.

Also, the ability of cameras to recognize unwanted individuals and criminals within an airport and track them is still not perfect. For example, on September 4, 2004, a suspect in police custody asked to use the restroom at La Guardia airport. He was accompanied to the restroom by one officer and managed to escape the bathroom around 7:15 p.m. As of midnight that night, the man had not been located despite an extensive search of the airport by the police. It was believed the man had found a way out of the terminal and perhaps had fled the airport (New York Times, 2004).

Similarly, even after the recent Christmas Day attack and increased security, a man was able to breach a security checkpoint exit at Newark airport. This was reported to the Transportation Security Administration (TSA) by a passenger, which resulted in the airport being shut down for six hours while police and airport security searched for the man. The man was later observed leaving the terminal by a separate surveillance camera 20 minutes after the initial incident. Surveillance cameras at the airport had not recorded the breach because the Digital Video Recorder (DVR) was not set up and updated correctly. TSA was forced to use Continental Airlines' backup security cameras to find the suspect because of this mistake. The man was later apprehended by police (MSNBC, 2010).

To ensure that airports are secure for everyone, the amount of security surveillance cameras installed should be enough for airport security guards to monitor the entire airport. Airport security systems

have to be able to protect more than just the airport terminals. They should guarantee the security of the airport, the perimeter of the airport, as well as each plane. Also, the surveillance cameras should be connected with each other and controlled by a single system. Based on the current technology, the IP network cameras are very suitable for the airport industry over the old technology, the analog camera or CCTV. According to Bryant (2006), an IP-based camera digitizes the video signal using a specialized encoder that contains an onboard web server. This allows the IP camera to act as a network device, thus allowing captured video images to be viewed not only through an existing network but also through a web browser that can be accessed through the Internet. Therefore, use of an analog camera system, by its very nature, does not provide the flexibility or integration with computer networks that an IP-based camera system does. The failure of video recording of the security camera system is another topic that one must pay attention to. The cameras, controlling units and storage components should be periodically checked, maintained, and updated to make sure that they are working correctly. One feature that airport security checkpoint surveillance cameras must have is an internal memory that can temporarily store video sequences in case of computer server failure. When the server comes back again, it should be automatically updated.

Metal Detector and Full-Body Scanner: All passengers at airports are required to go through airport security before entering the terminal. Passengers must walk through metal detectors. However, the problem that exists here is that Al Qaeda is not attempting to bring metal objects onto plains. The shoe bomber and the Christmas Day attack both were attempted by use of plastic explosives which are not sensed by metal detectors.

Currently, full-body imaging machines are being installed into American airports, but not without controversy because of their ability to reveal naked images of the body. According to John Schwartz (2009), these are used in 19 airports throughout the U.S. with 150 more ready to be installed. Even so, the plan is to use these machines only as secondary scanning devices. Consequently not all passengers will have to pass through this type of technology screening, only suspicious ones. Furthermore these passengers can refuse to be scanned, and if so will receive a full-body pat down. The obvious problem is that twice since 9/11, Al Qaeda terrorists were not given secondary screening and made it through into the terminal by only passing through a metal detector. Furthermore, another weakness of the full-body scanner is that it is unable to detect objects that are concealed within the body's orifices or under the folds of an obese person's flesh (Schwartz, 2009). Accordingly, neither metal detectors nor full-body scanners are infallible. However, the full-body imaging machines should be used as a primary device for every airport as soon as possible because these are the best scanners currently available. Passengers who reject this screening method should receive an equivalent level of screening, which is a pat-down procedure.

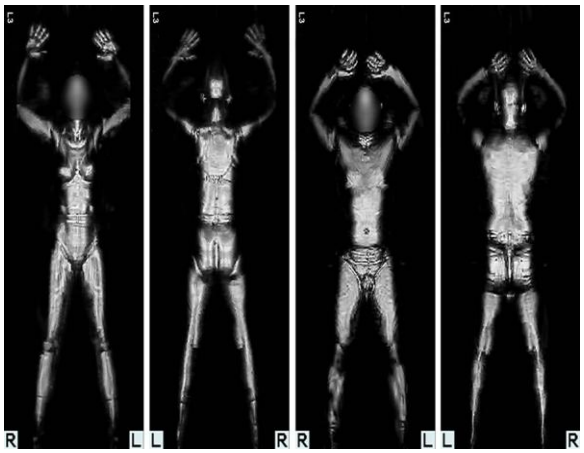

Figure 1. Example Image of Millimeter Wave Technology (Source: Transportation Security Administration)

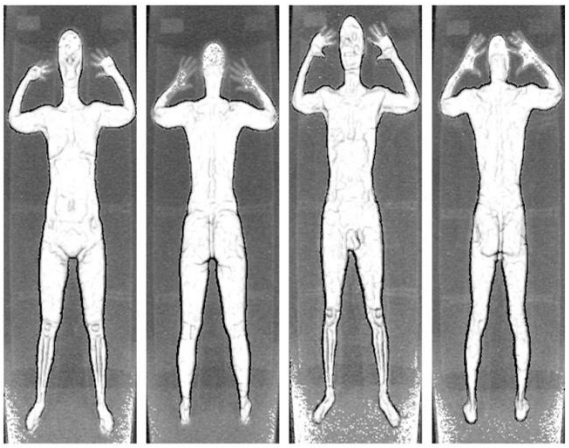

Figure 2. Example Image of Backscatter Technology (Source: Transportation Security Administration)

There are two screening technologies being used with the full-body scanners: Millimeter wave and Backscatter. Millimeter wave technology produces an image that resembles a fuzzy photo negative. Backscatter technology produces an image that resembles a chalk etching. Both technologies can be

viewed by a Transportation Security Officer in a remote, secure location. Furthermore, these advanced imaging technologies do not store, print, transmit, or save the image. Figures 1 and 2 show the example images of these two methods.

***X-Ray Machine**:* While passengers are walking through metal detectors, their luggage and carry-on items have to pass through X-ray machines. Machines employed at airports use a dual-energy X-ray system. Items are displayed on a monitor to represent one of three categories: organic, inorganic and metal. The colors used to signify inorganic and metal vary between manufacturers, but all use shades of orange to represent organic, because most explosives are organic (Tyson, 2001). However, X-rays are also not fully automated and thus rely on individuals to use them to detect potential threats. Human error and the lack of automation are the biggest problems to the current X-ray system. For example, Konrad (2001) mentioned, "The technology is only as good as the people who use it. It's a mind numbing experience to watch 300 bags cross the screen and try to determine if that's a hair dryer or an explosive device." In addition, electronic devices such as laptop computers, cellular phones and digital cameras are compacted with many small components, causing difficulty in determining whether or not a bomb is stored within them. This is why laptops are required to be uncovered while they are passing through security and why one may be asked to turn on their device (Tyson, 2001).

Similarly, checked baggage and airline cargo also pass through X-ray machines. Airports use three different types of these X-ray systems to scan luggage: medium X-ray systems, mobile X-ray systems, and entire building systems. If a bag is deemed to be a further threat when it passes through these, it then moves through a secondary screening called a Computed Tomography (CT) scanner. This scanner calculates the mass and density of objects within a bag. If something in the bag's mass or density falls within the range of dangerous materials, the CT scanner sends out a warning. CT scanners are much slower than the other types systems previously discussed. This is why they are not used to check every bag, but only used as a secondary screening device (Tyson, 2001).

Although CT scanners are slow compared to other types of X-ray machines, they should be used as a primary device for checking passengers' luggage and carry-on items because they are better than any other x-ray machine currently used in the U.S. The CT scanners should be located around the entrances of the terminals and before passengers approach the check-in counters, so every luggage and carry-on item is scanned at this location.

Biometrics: To better combat terrorism, merely examining a photo ID such as passport or driver's license may not be enough to validate a person's true identity. Implementing biometrics with security equipment is a good methodology to be considered. Biometric authentication uses personal physical characteristics such as fingerprints, facial features, iris, retina, palm blood vessel type, and Deoxyribonucleic Acid (DNA) to examine if someone is who they say they are or if they match a watch list individual. Biometric authentication is the best technology available for authentication but leads to the requirement of advanced hardware and more complex information system. However, the biometric method is currently in the early stage of development. It will definitely be used more in the future due to its strength, and therefore the U.S. should be looking into innovative ways to implement this technology into human identification

Software Issues

The key element to software is that it should support the goals and the objectives of an organization. Thus, U.S. security agencies and airline security must be able to select software that facilitates the defense of aviation and the American public. According to Blair and Leiter (2010), director of national intelligence and director of the national counterterrorism center respectively, the U.S. Intelligence Community must constantly strive for and exhibit three characteristics for security organizations to be effective:

> The Intelligence Community (IC) must be integrated: a team making the whole greater than the sum of its parts. We must also be agile: an enterprise with an adaptive, diverse continually learning, and mission-driven intelligence workforce that embraces innovation and takes initiative. Moreover, the IC must exemplify America's values: operating under the rule of law, consistent with Americans' expectations for protection of privacy and civil liberties, respectful of human rights, and in a manner that retains the trust of the American people (Blair & Leiter, 2010).

Nevertheless, this has not been the case in regard to software and technology within the IC. There are many problems that exist with the implementation, use, abilities, and adaptation of their software. Currently, the software programs that are in use are

unable to put together multiple bits of information, such as the case was with the Christmas Day attacks. Lipton (2010) mentioned that, "Despite the government's having spent billions of dollars since 2001 to strengthen the nation's defenses against the terrorist attack, analysts inexplicably still cannot do a simple Google-like search of various computer databases to automatically search for links." The software that they currently use does not enable them to accomplish a simple task – like links – that would enable them to more easily and accurately do their job.

Another good example of the lack of effective software can be observed through the inadequacy of the FBI's technology. Muller (2006) stated that "Over the years, we have failed to develop a sufficient capacity to collect, store, search, retrieve, analyze and share information." According to the report, some of this is due to outdated technology. Also, this is a result of the IC's inability to adapt to 21st century technologies. They even admit that these technological problems cannot be fixed overnight. As a result, they have embarked on a comprehensive overhaul and revitalization of their information technology (Mueller, 2006). It is yet to be seen if their endeavors will accomplish their goals and mission, but they must nevertheless address the extensive gaps that currently exist. If Google, Las Vegas casinos and many other industries are able to incorporate software to meet basic search needs, connect data and use software to provide security, governmental security agencies should not lag so far behind.

Intelligent Database Management Systems: The government security agencies have been developing a software application to effectively and accurately manage multiple bits of information. In other words, they want to successfully collect, store, search, retrieve, analyze and share information among agencies. Unfortunately, the Christmas Day attack proved that they are not even close to the desired outcome. The solution to this problem is to create an intelligent Terrorist Screening Database (TSDB) program. The government must seek out and collaborate with private parties who specialize in this field such as IBM, Microsoft and Oracle. Also, they should ask for help from companies that have expertise in search engines such as Google and Yahoo. Once the government and private parties collaborate with each other, there should be a better and suitable software program for coping with a security database.

To be able to efficiently use the TSDB, it is necessary that its DBMS meet several criteria. First, the DBMS should be easy to handle. Every user should be able to create effective database queries and have access to well-designed tools. Second, the DBMS should have the ability to generate database queries that show when not all criteria fit a specific search. For example, when a TSA agent creates a database query and only 7 out of 10 attributes are exact, he should receive the result in 70% agreement with a searched person in the database. Hence, the TSA agent could decide whether or not he would undertake further steps to identify the individual in question.

Furthermore, some reports show only matches when all attributes correspond to the search. Thus, the reports should weight the different attributes based on importance. As a result, agents would receive a better fitting report result. Lastly, it should be possible to easily create relationships with other tables of the database. All in all, the users of the TSDB would benefit from these improvements that make it possible to create precise, effective and easily generated reports.

Face Recognition Software for Security Surveillance Cameras: Another feature and capability that the surveillance camera system of airports should have is the face recognition. Face recognition software can help transfer the standard surveillance video camera system into a proactive crime prevention tool. Face recognition is used to compare people by matching names to faces; hence, operating this software with a well managed IP-based camera system will help enhance airport security.

According to Bryant (2006), "Face recognition software actually captures an image of a person's face and then uses that image to compare to a database of facial images. This software makes it possible for law enforcement officials to proactively identify and monitor persons of interest." Once a suspicious person is detected by the system, further investigation should be applied immediately. Figure 3 shows an example of how facial recognition works

Data Issues

Data duplication, erroneous information, incorrect tracking codes as well as the insufficient linking between the watch list and agencies are considered main factors for occasional undesirable events. For example, the former Assistant U.S. Attorney General and former head of the Justice Department's criminal division – who had top-secret security clearance – was delayed and put through further screening as a result of his name being on the watch list (Zetter,

2008). To address these problems, one has to analyze the failure chain from beginning to end. This analysis will begin with the data collection and processing and finish with the management and usage of the database. As the saying goes in the information field, "Garbage in, garbage out." Therefore it is important to ensure that the data used and information retrieved is adequate to reach desirable results. Nevertheless, numerous newspaper articles and governmental publications demonstrate that the quality of data in the TSDB is a major problem. The TSDB program should make sure that the data is neither duplicated nor interferes with other data. In accordance, to determine responsibility, the TSDB content management system should track and report any changes to data, the date of the changes, the reasons for the changes, as well as who made the changes. Moreover, this content management system should administer access control of the content based on predetermined security measures and responsibilities. Consequently, it will be ensured that only authorized security agents have access to, and the ability to change, confidential data.

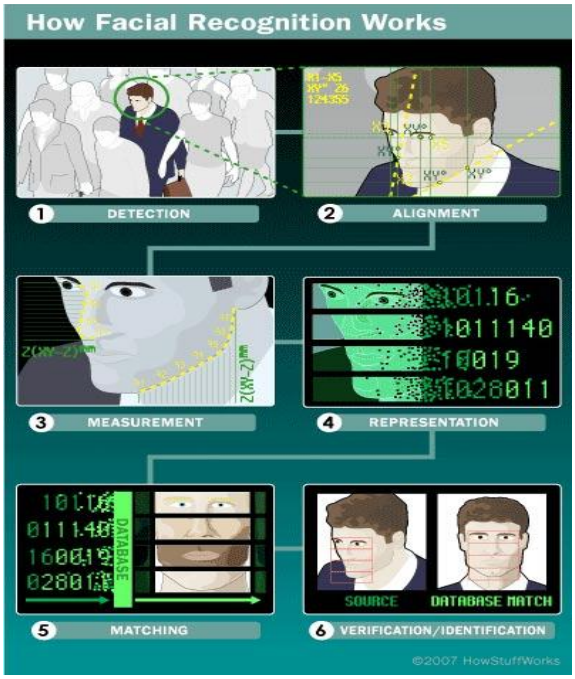

Figure 3. Facial Recognition Systems (Source: Tyson, 2001).

Due to the fact that good information relies basically on good data, as well as people who are capable of interpreting that data, it is important to have certain criteria concerning data that makes it useful during later analysis. Therefore, it is important that the data within the counterterrorism database meets the criteria of accurate, timely, relevant, just barely sufficient, and worth its cost (Kroenke, 2009).

Procedures Issues

Currently, people who would like to come to the United States must obtain a visa. The most common visas are as follows: student, tourism, work, and immigration. In order to obtain a visa, an applicant must go to an American embassy or a consulate and be interviewed by a consular officer. At the office, fingerprints are taken and a background check is run to find out if the applicant is a terrorist or a criminal (Ervin, 2009). However, a crystal clear problem in this procedure is the fact that the Umar Farouk Abdulmutallab's visa was not revoked when his father reported him as having ties to a terrorist organization. For that reason, U.S. security agencies need to do a better job at tracking individuals who already have obtained a visa and who may also be a threat.

The problem in the procedure for approving visas can be improved. At the U.S. embassy, before issuing visa to anyone, the U.S. embassy should be more restricted than previously. For example, the officials who interview and record the information of passengers should be qualified and well-trained. Any mistakes such as misspelling the names of visa applicants should not be acceptable in this process. Historical records of not only passengers but also their family should be thoroughly checked. Also, if someone like Umar Farouk Abdulmutallab's father reports terrorist activity of a family member, the officials should take appropriate action. Today, many countries are changing their regular passports to E-passports. However, the electronic chip's capability and capacity are still limited and require improvement. If U.S. airports were to follow the methodologies that Israeli airports use, it would result in higher security. There, every traveler is subjected to personal questions by well-trained agents and is tested by screeners who will look travelers straight in the eye for signs of deception before check-in. It is believed that doing so could enhance aviation security (CNN, 2010).

Furthermore, profiling is another interesting method that if implemented could help prevent other terrorist attacks. Profiling would be used to isolate airline passengers for more intensive security searches before they board the U.S. flights, based on their age, ethnicity, or gender. According to Jones (2010), "Each attempted terrorist attack seems to bring a renewed call for heightened security measures. It is not certain that the U.S. government would ever seriously consider adopting profiling of air

passengers based on their personal characteristics as a means of preventing terrorism. But despite concerns about the practice, most Americans seem inclined to favor it."

Lastly, airlines should be involved in screening people. It may be roughly assumed that people who do not have a special purpose for coming to the U.S. such as studying or working should not stay very long and should buy a round-trip ticket. Thus, people who buy one-way tickets with cash should be a concern to security. As a result, when the airlines sell a ticket to a person who falls into these criteria, airlines should report this to the TSA immediately. When the TSA receives an alert message from the airlines, they can investigate in further detail if that person should be considered suspicious. If the TSA finds something wrong, the U.S. embassy should then reject the visa and the airlines should cancel the ticket.

People Issues

U.S. security personnel work hard day in and day out to protect U.S. citizens from numerous threats around the world. Nevertheless there is always room for improvement. Top security personnel need to take the blame when problems such as in the Christmas Day attack are exposed. The Obama administration proclaimed that human error was the biggest lapse concerning Umar Farouk Abdulmutallab because no one with information put him on the no-fly list. Furthermore, the misspelling of his name led to the State Department's belief that he didn't have a visa (Zeleny &Cooper, 2010). Thus, the current lack of collaboration is still evident between agencies, even though this was their primary mandate after the 9/11 attacks. Security leaders must find innovative measures to collaborate and share information with each other. They must constantly hold not only themselves to high standards and rigor, but also their subordinate personnel.

The United States must also seek to collaborate with other countries. International collaboration and treaties are a must to curb the threat of terrorism. The following is a statement made by Secretary Napolitano of the Department for Homeland Security during her recent visit to Toledo, Spain: "The attempted attacks on Dec. 25 threatened the lives of individuals from 17 foreign countries, including more than 100 citizens of European nations. The international dimension of this incident - and the international threat posed by radical extremism - requires international aviation security standards and procedures." (Homeland Security, 2010)

Although the beginning of dialog with friendly nations to create international aviation security measures and standards is a start, much more needs to be done in the area of collaboration and policy to help prevent similar attacks. People can be the biggest weakness of an information system, as well as the biggest strength. Therefore, it is important to make sure that the people factor becomes a strength instead of a weakness. In the past, most undesirable security outcomes were the result of the poor work done by humans.

The best system is useless without the expertise and capability of the users who apply it. According to the Department of Homeland Security, one should "take further steps to enhance the rigor and raise the standard of intelligence analysis designed to uncover and prevent terrorist plots." (Blair & Leiter, 2010) It is important to invest at least the same amount of money for training and education of the users as it is for systems and technical components. Intelligence agents should be trained and instructed to supply the database with required data and information. All securities agencies from the CIA to TSA agents at the airport should be able to use all components of the information system, as well as to understand the security processes. Thus, all security personnel will able to create and interpret the reports that supply the required information to identify possible terrorists.

As a result of the discovered problems in cooperation between the different counterterrorism agencies, one should consider collaboration as way to create future improvements. Collaboration is a teamwork process in which all involved agencies would interactively work together and review each other's actions. Agency collaboration would be considered successful when the inter-collaboration between agencies provides feedback on the actions of other departments. They communicate their failures in the past and work together for a better future solution.

CONCLUSIONS

The transformation of the current information system and all of its components used by security agencies is no easy endeavor. Nonetheless, the Christmas Day attacks brought the inefficiencies of the security agencies to the center of U.S. attention. This paper addressed the vulnerabilities and problems of current information security information systems, and suggests solutions that are necessary to ensure national security. The United States should investigate all potential solutions related to the airport security, including effective strategies for implementing information systems that close gaps

and meet the needs and objectives of the different stakeholders involved in security.

REFERENCES

1. Blair, D. C., & Leiter, M. E. (2010). Intelligence reform: The lessons and implications of the Christmas Day attack. Retrieved January 13, 2010, from http://www.dni.gov/testimonies/20100120_1_testimony.pdf

2. Bryant, L. (2006). IP versus analog cameras--what are the advantages and disadvantages of each? Retrieved January 16, 2010, from http://www.video-surveillance-guide.com/ip-versus-analog-cameras.htm

3. CNN. (2010). How the Israelis do airport security. Retrieved February 6, 2010, from http://www.cnn.com/2010/OPINION/01/11/yeffect.air.security.israel/index.html

4. Ervin, C. K. (2009). After eight years, terrorists still fly. Retrieved January 12, 2010, from http://www.nytimes.com/2009/12/29/opinion/29ervin.html

5. Homeland Security. (2010). Secretary Napolitano discusses enhancing international aviation security measures and standards with European counterparts in Spain. Retrieved January 21, 2010, from http://www.dhs.gov/ynews/releases/pr_1264099539740.shtm

6. Institute for the Analysis of Global Security. (2003). How much did the September 11 terrorist attacks cost America? Retrieved February 6, 2010, from Institute for the Analysis of Global Security: http://www.voanews.com

7. Jones, J. M. (2010). Americans back profiling air travelers to combat terrorism. Retrieved February 8, 2010, from http://www.gallup.com

8. Konrad, R. (2001). Airport security technology under scrutiny. Retrieved February 11, 2010, from http://news.cnet.com

9. Kroenke, D. M. (2009). *Using MIS*. Upper Saddle River, New Jersey: Pearson.

10. Lipton, E. (2010). Officials regret curbs on adding to terror watch list. Retrieved February 6, 2010, from http://www.nytimes.com

11. MSNBC. (2010). Police arrest man in Newark security breach: Incedent at airport delayed flights for several hours. Retrieved February 6, 2010, from www.msnbc.msn.com/id/34682282

12. Mueller, R. S. (2006). FBI counter-terrorism report. Retrieved March 4, 2010 from http://ww.classbrain.com

13. NATO. (2004). NATO and the fight against terrorism. Retrieved February 19, 2010, from http://www.nato.int/cps/en/natolive/topics_48801.htm

14. New York Times. (2004). Suspect escapes police at airport. Retrieved February 6, 2010, from http://query.nytimes.com/gst/fullpage.html?/res=9E01EEDC1131F937A3575AC0A9629C8B63

15. Schwartz, J. (2009). Debate over full-body scans vs. invasion of privacy flares anew after incident. Retrieved April 10, 2010, from http://www.nytimes.com/2009/12/30/us/30privacy.html?scp=1&sq=Debate%20over%20full-body%20scans%20vs.%20invasion&st=cse

16. Shane, S. (2009). Shadow of 9/11 is cast again. Retrieved March 3, 2010 from http://www.nytimes.com/2009/12/31/us/31intel.html

17. Transportation Security Administration. (2010.). Imaging technology: Innovation & technology. Retrieved February 6, 2010, from http://www.tsa.gov/approach/tech/imaging_technology.shtm

18. Tyson, J., & Grabianowski, E. (2001). How airport security works. Retrieved February 6, 2010, from http://science.howstuffworks.com/airport-security.htm

19. Wikipedia. (2010). Northwest airlines flight 253. Retrieved February 6, 2010, from http://en.wikipedia.org/wiki/Northwest_Airlines_Flight_253

20. Zeleny, J., & Cooper, H. (2010). Obama details new policies in response to terror threat. Retrieved February 6, 2010, from

http://www.nytimes.com/2010/01/08/us/politics/08terror.html

21. Zetter, K. (2008). Former DoJ official caught on terror watchlist. Retrieved April 2, 2010, from http://www.wired.com/threatlevel/2008/07/former-doj-pros/