

# **The Role of Technology in Homeland Security**

**Brian Danis**

**December 9, 2004**

## Table of Contents

<b>SECTION</b>	<b>PAGE</b>
Research Objective and Scope	3
Introduction	4
Biometric Technology	7
The Biometric Process	7
Retinal Recognition Systems	10
Iris Recognition Systems	11
Fingerprint Recognition Systems	11
Facial Recognition Systems	12
Hand Geometry Recognition Systems	13
Speech Pattern Recognition Systems	14
Signature Recognition Systems	14
Biometric Research	15
Biometric Technology Applied: The US-VISIT Program	17
Geospatial Information Systems Technology	23
Cyberterrorism	26
Threats to Network Security	27
Methods of Network Defense	30
Conclusion	36
References	37

## **Research Objective and Scope**

This paper examines the ever-increasing role that information technology is playing in enhancing homeland security and fighting the "War on Terror." Tools such as biometric technology and geospatial information systems are quickly becoming valuable resources in addressing the constant threat of terrorism. In addition, numerous other programs utilizing information technology have been enacted in order to better secure our ports and borders. This paper will provide an overview of some of these programs and technologies, describing the benefits of each and analyzing their overall effectiveness, as well as consider the role of cyberterrorists and cybercriminals as it relates to both network and homeland security.

## **Introduction**

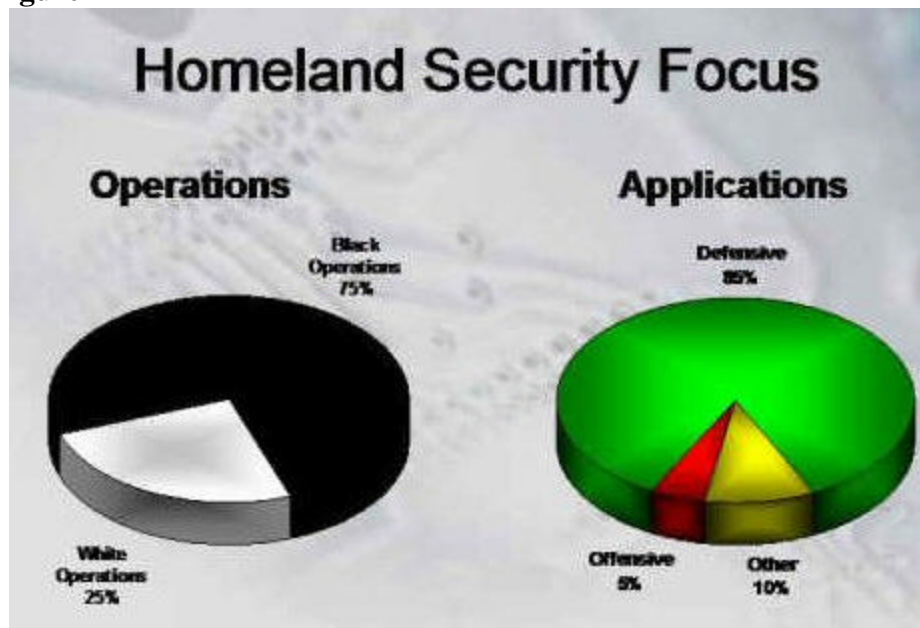
In addressing the United States Congress on December 8, 1941, President Franklin Roosevelt spoke of the attack on Pearl Harbor as "a day which will live in infamy." Nearly sixty years later, the previously unfathomable notion of a terrorist attack on American soil became a reality as, on the now equally infamous date of September 11, 2001, three hijacked commercial airliners struck the World Trade Center in New York City and the Pentagon in Washington D.C. while a fourth hijacked plane crashed in a field just outside Pittsburgh. The United States had received a horrific lesson in an ideology that, while familiar to other parts of the world, was previously a distant concept to Americans: terrorism. Immediately following the 9/11 attacks, many Americans were left feeling vulnerable and wondering when the next act of terrorism would occur. To combat these threats, information technology has stepped to the forefront and become a major weapon in fighting the "War on Terror." The IT community is providing the means to both improve systems within our country's current security infrastructure as well as developing new systems that promise to enhance security.

In his article "Technology and Homeland Security" which appeared in the March 6, 2003 online issue of *Directions Magazine*, author Kevin Coleman categorizes the applications used in homeland security as offensive and defensive. Offensive applications are resources and technologies that are used to physically destroy an enemy. These would include weaponry such as tanks, bombs, and missiles. Defensive applications, on the other hand, are those technologies which limit the destructive capability of an enemy, including intelligence gathering networks, radar, and various types of sensors. Coleman further divides defensive applications into two subcategories:

tools of detection and tools of protection. Tools of detection include the aforementioned intelligence gathering networks and sensors to detect the presence of biological, chemical, or radioactive agents. Tools of protection are more physical entities such as vaccines, protective clothing, and blast absorbing materials. However, measures of network security such as anti-virus software, firewalls, and intrusion detection systems can also be categorized as tools of protection.

As the figure below illustrates, the focus of homeland security is clearly on defensive applications which presents many challenges and opportunities for those in the field of information technology.

**Figure 1**



Source: "Technology and Homeland Security" Kevin Coleman

Although these applications may be termed defensive, not all defensive applications are as reactive as the name would lead one to believe. Regarding intelligence gathering systems, many programs set forth by the United States government and the Department

of Homeland Security, in particular, take a very proactive stance in obtaining vital intelligence that can be used for the purpose of data mining and threat detection. Some of these programs will be addressed in subsequent sections. However, regardless of the type of application being utilized, offensive or defensive, tool of detection or tool of protection, it is clear that the role of information technology is and will continue to be vital in the development of the homeland security system.

## **Biometric Technology**

One such defensive tool of detection that has come to play a major role in homeland security is biometric technology. The fundamental theory behind biometrics is that each person possesses certain traits, both physiological and behavioral, that uniquely identify them. Biometric proponents argue that the proper collection of these traits for visitors entering the United States as well as those deemed as possible threats is a significant step in enhancing homeland security. However, the collection, storage, and proper use of these unique biometric traits as a means for improving security provide a significant challenge for security and IT organizations in terms of overall project scope, system accuracy, and system interoperability.

### ***The Biometric Process***

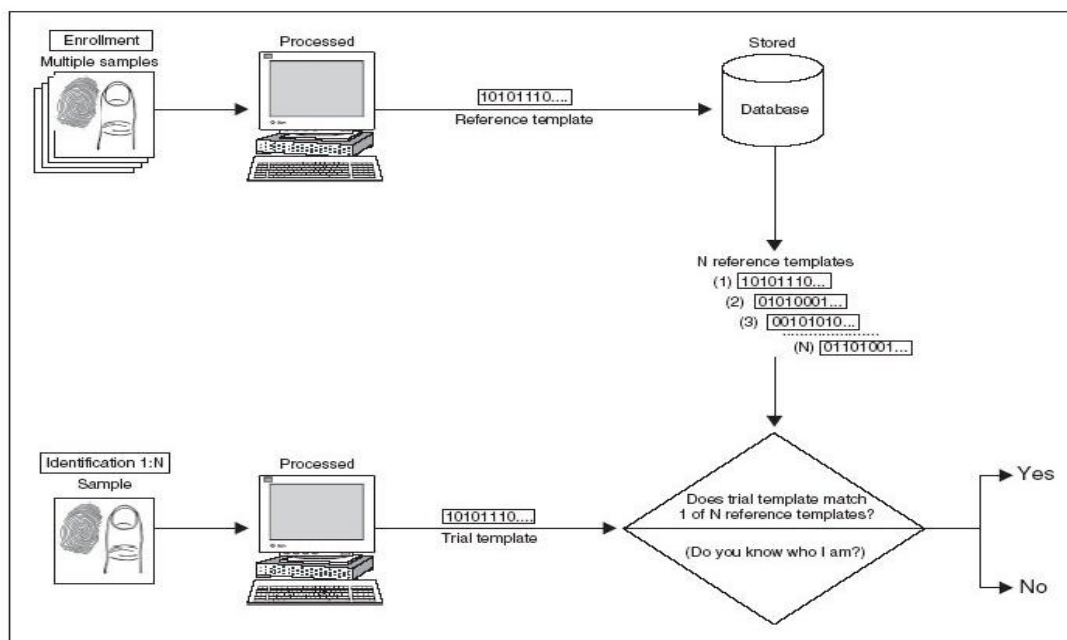
Regardless of the type of trait examined, physiological or behavioral, and the type of recognition system used, most biometric applications can be divided into two distinct categories: identification or verification. Identification applications focus on **determining** an individual's identity. They seek to answer the question, "Who are you?" Verification applications are used to **confirm** an identity, looking to verify that a person is who they say they are.

The first step in both identification and verification is what is known as enrollment. Basically, enrollment is the phase in which initial biometric data is collected from a subject. First, the subject provides some form of proof of identity, known in biometric circles as an identifier. The biometric data collected will be linked to whatever identity is listed on the identifier. The subject then provides the collector with the

necessary biometric data through the available recognition system. The data is collected, analyzed, encoded, and stored on a template for future reference. These templates can be stored either within the biometric recognition device itself or in a central database. Clearly, the most important piece of the enrollment process is the identifier that the subject presents. If the identifier is false, the subject's biometric data will be linked to the false identification which can have potentially disastrous security implications. (Rhodes, p.2-3)

Following enrollment, the process may branch into identification in which the goal is to identify who a person is. It is important to note that an identifier does not need to be provided when undergoing identification. Instead, an individual's biometric data is obtained and compared to a database of stored templates utilizing the same recognition system. This type of comparison is known as 1:N, or one to many. The identification process is illustrated in Figure 2.

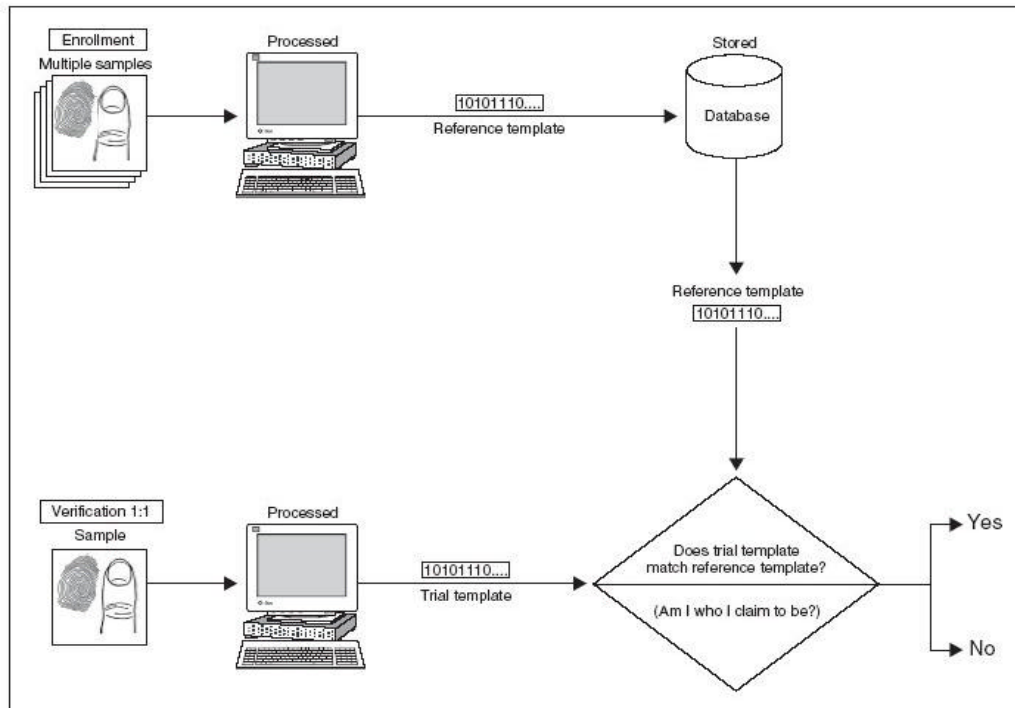
**Figure 2**



Source: "Challenges In Using Biometrics" Keith Rhodes, p. 6

Unlike the identification process, verification **does** require that the individual present the identifier used in enrollment. To begin the verification process, the subject provides the biometric data that they were enrolled with. For example, an iris scan of subject A is taken at the point of entry and this data is stored on a trial template. The trial iris scan template of subject A is then compared to the reference iris scan template that was stored during enrollment. Completing the comparison can usually take less than one second. A result of match or no match is returned and the question of "Are you who you say you are?" is answered. The verification process is shown in Figure 3.

**Figure 3**



Source: "Challenges In Using Biometrics" Keith Rhodes, p. 4

It should be noted that there are a number of factors which can contribute to errors within a biometric system, resulting in a false negative outcome. For example, there may be a temporary change in the biometric trait taken during enrollment such as voice changes due to respiratory illnesses or possible cuts or scars on fingertips. Environmental conditions may also play a role if there is a difference in lighting during a facial recognition scan or dry climate conditions could result in weak fingerprint impressions. Also, a change in the type of sensor being used from enrollment to identification or verification could also be the cause of a false negative outcome. Finally, improper subject interaction such as a change in facial pose in facial recognition systems or relaxed eyelids during an iris or retinal recognition scan are other possible sources for error. (Ross and Jain)

As stated above, biometrics can examine both the physiological and behavioral traits of an individual. Among the physiological measurements currently monitored by biometric systems are the distinguishing characteristics of the retina and iris, fingerprints, facial and hand geometry, and others which are described in greater detail in this section.

### **Physiological Traits**

#### ***Retinal Recognition Systems***

Retinal scanning systems record the patterns of blood vessels on the narrow nerve at the back of the eyeball. These retinal patterns are very distinctive as every eye has a unique pattern, including those of identical twins. They are also fairly stable over time, although retinal patterns can be affected by such diseases as glaucoma, diabetes, and AIDS and conditions such as high blood pressure. Capturing retinal images is much

more difficult than other biometric systems as the eye must be placed very close to the lens of the scanning device, look directly into the lens, and remain still while a small camera scans the retina through the pupil. Even the slightest movement can result in having to restart the process. Although times can vary, enrollment with a retinal recognition system typically takes over one minute. (Rhodes, p. 9)

### ***Iris Recognition Systems***

Iris scanning systems look at the approximately 173 of the 266 distinctive characteristics of the iris, the colored band encircling the pupil of the eye. In this system, a high-resolution, black and white image of the iris is captured by a high-quality camera. Then, the boundary of the iris is defined, a coordinate system is established for the particular iris, and zones for analysis are then defined within the established coordinate system. (Rhodes, p. 8) Many within the security community feel that iris recognition systems may be the best form of biometric identification available as many different research studies have yielded very positive results. These studies have consistently found that iris recognition systems return false rejection rates of under two percent, some even having a zero percent rate, and false match rates of zero in over 1.2 million.

### ***Fingerprint Recognition Systems***

Fingerprint recognition systems are among the most widely used biometric systems, primarily used by members of law enforcement until recently. In fact, fingerprint recognition systems are the leader in mass-market biometric-ID systems. These systems analyze impressions taken of the unique ridges on the fingertips. The

common characteristic in acquiring fingerprints for analysis is that they are taken either flat or rolled. The drawback of taking flat fingerprints is that only the central area of the fingertip is captured whereas a rolled fingerprint gives a more complete impression of ridges on both sides of the fingertip. The fingerprint image is taken by a scanner and converted to a template. These scanners can be either silicon, optical, or ultrasound. Although ultrasound is the most accurate method of scanning, it is not widely used due to its high cost. According to the United States Government Accountability Office, optical scanning is the most frequently used form of fingerprint acquisition. Fingerprint capture and analysis can be a timely process. The initial capture of the fingerprint at a security post will take about 30 seconds. From here, however, the image must be circulated through a post server, the State Department server, and the Department of Homeland Security server before returning with a result. This circulation can take over 30 minutes. In addition, if the fingerprints need additional analysis by a fingerprint expert, an additional 24 hours may be needed. (Rhodes, p. 7-8) Users of fingerprint recognition systems are also forced to deal with negative subject perceptions as fingerprinting is commonly associated with police booking and criminal activity.

### ***Facial Recognition Systems***

Facial recognition systems analyze an individual's facial features that that cannot be altered easily such as the sides of the mouth, the outlines of the eye sockets, and the areas around the cheekbones. This is a more versatile system as it can both compare a live image to a stored template as well as to a static image such as a digitized passport or visa photograph. Facial recognition is also the only biometric measurement technique

that can be used for surveillance purposes because video cameras are able to obtain facial images. (Rhodes, p. 7) They are designed to be strong enough to conduct one-to-many searches in databases containing thousands and even hundreds of thousands of individuals. Facial recognition systems are gaining popularity as they are quickly becoming more inexpensive, unobtrusive, and faster in terms of overall system speed, especially when compared to other biometric systems. The user perceptions of facial recognition are also more positive than with other biometric systems as people already identify each other based upon facial appearance.

### ***Hand Geometry Recognition Systems***

Hand geometry recognition systems take 96 measurements of an individual's hand, including the dimensions of the fingers, shapes of the knuckles, and the distance between the joints. An optical camera is used to obtain two-dimensional images of the sides and back of the hand. Like the retina, the shape of one's hand remains fairly constant over time although slight changes can occur. (Rhodes, p. 8) Currently, hand geometry recognition systems are primarily used for time and attendance applications as well as physical access control applications. Hand geometry recognition systems are known for being durable. Not only is system performance unaffected by factors such as soiled or dirty hands, certain hand geometry recognition systems are able to function in such extreme temperature ranges as -30 to 150 degrees Fahrenheit, making it possible to store them outside of the physical access area. Among the disadvantages of implementing hand geometry systems are high implementation costs and the large,

impractical size of hand geometry scanners. In addition, hand geometry technology does not allow for one-to-many identification and database mining. (Frost and Sullivan)

In addition to physiological traits, biometric technologies are also able to record and analyze certain behavioral traits of a person. The most commonly measured behavioral traits are speaking patterns and signature patterns.

## **Behavioral Traits**

### ***Speech Pattern Recognition Systems***

People's voices sound different because of learned speaking habits as well as the shape of the vocal tracts. In speech pattern recognition systems, an individual is prompted to state a predetermined phrase into a microphone. The phrase is recorded and converted from analog to digital sound. The unique attributes - tone, pitch, cadence - are then taken from the sample and recorded to a template for future reference. (Rhodes, p. 9)

An advantage of speech pattern recognition is that, like facial and hand recognition, it is relatively unobtrusive. Also, it can be language independent. However, speech pattern systems must consistently address the issue of background noise as this can obviously have a serious impact on authentication results. In addition, results can be affected by the subject's health, level of stress, and emotions.

### ***Signature Recognition Systems***

Even a person's handwritten signature contains biometric information. Signature recognition may take two forms: simple signature comparison and dynamic signature

verification. The simple signature comparison only takes into account how the signature was made. Dynamic signature verification, on the other hand, focuses on the speed, pressure, and timing while signing. Although someone may be able to duplicate how a signature looks, it is virtually impossible to recreate the speed, pressure, and timing of the signature. Also, the false acceptance rates of signature verification are extremely low. When utilized, an individual will sign their name on a digital graphics tablet or PDA which will analyze the pressure, speed, and stroke of the signature and convert the signature and data to a template. In addition, as a person's signature may change over time, the signature recognition systems are able to record these variations. (Rhodes, p. 9)

Although there are clearly numerous methods for obtaining biometric measurements and data, most biometric systems share four similar components: sensor module, feature extraction module, matching module, and decision-making module. The sensor module is simply the means of acquiring the biometric measurement from an individual. The feature extraction module extracts a feature set representative of the biometric trait by processing the data acquired from the sensor module. The matching module compares the extracted biometric data, in template form, of the individual in question to a database housing similar biometric traits. Finally, the decision-making module either validates the individual's identity or refutes their claim. (Ross and Jain)

### ***Biometric Research***

A number of studies have been conducted which address the validity and accuracy of biometric technologies. One such study, "BioFace: A Comparative Study of Facial

Recognition Systems," was co-coordinated by the Federal Office for Information Security in Bonn, Germany and the Federal Office of Criminal Investigation in Wiesbaden, Germany. The BioFace report was released by the German organization Bundesamt für Sicherheit in der Informationstechnik in June of 2003. Divided into two parts, BioFace I and BioFace II, the study examined the performance of facial recognition systems. The overall objective was to analyze the functionality of the system when handling large amounts of data as well as the influence of external "noise" factors. In addition, the researchers sought to measure the overall effectiveness of facial recognition systems. (BioFace, p. 5)

The BioFace project studies were initially conducted using laboratory tests in the areas of identification, using one-to-many comparisons, and verification, using one-to-one comparisons. The researchers next proceeded to testing in more practical settings where the facial recognition systems would be utilized. In the identification portion of the study, the BioFace team conducted searches of 116 individuals in databases of varying sizes using 305 different images of the same 116 individuals. The databases used contained 1000, 5000, or 50,000 filler images, images of other people. The test results found that there was a direct correlation between the size of the database and system performance. When looking for the ten best matches, the larger databases were more likely to insert non-matches in the top ten positions in place of correct matches. In the verification portion of BioFace, one image of a test subject was placed in a search database while a second image of the same test subject was placed in the reference database. The verification scenario databases contained images of 5,000, 10,000, 20,000, and 50,000 people. Unlike the identification scenario, the size of the database had no

significant effect on correct matches in verification. In addition, age differences of the test subjects did not play a major role in altering the test results. However, researchers did find that the quality of the image captured by the facial recognition device was a significant factor in non-match results. (BioFace, p. 7)

Another study, "Biometric Sensor Interoperability: A Case Study in Fingerprints," examined the effectiveness of fingerprint recognition systems in terms of their ability to exchange common data across different platforms. Authors Arun Ross and Anil Jain argue that although progress has been made in terms of developing common data exchange formats for biometric feature sets to accommodate the numerous vendors of biometric recognition systems, the actual issue of matching these feature sets has been ignored. Because so many biometric recognition systems are currently in place with more scheduled for implementation in the near future, the need for biometric sensor interoperability has become more imperative, both from cost and security perspectives. (Ross and Jain)

### ***Biometric Technology Applied: The US-VISIT Program***

On January 5, 2004, the Department of Homeland Security launched the United States Visitor and Immigrant Status Indicator Technology, or US-VISIT, program. The overall mission of the US-VISIT program is to gather, preserve, and share information on foreign nationals through the use of biometric data collection, including fingerprint and facial identifiers. In collecting this data, the Department of Homeland Security hopes to create an integrated system that will allow officials at U.S. ports of entry to determine if a foreign national should be allowed or banned from entering the United States; can receive

or alter immigration status; has violated their terms of admission; should be detained by law enforcement officials; needs particular attention or protection, as with political refugees seeking asylum in the U.S. (DHS RFP)

According to the Department of Homeland Security's Request for Proposal which was issued in November of 2003 to all contractors bidding on the US-VISIT project, the US-VISIT program has established four primary goals in implementing this project:

1. US-VISIT will enhance the security of U.S. citizens as well as its visitors.
2. US-VISIT will facilitate legitimate travel and trade.
3. US-VISIT will ensure the integrity of the U.S. immigration system.
4. US-VISIT will protect the privacy of visitors to the United States. (DHS RFP)

Civil liberties organizations have argued that the US-VISIT program has the potential to impinge upon privacy rights. The issue of the disregard of privacy rights, however, is a non-issue for U.S. citizens in the US-VISIT program as biometric data is only collected for **visitors** to the United States. In addition, it is difficult to argue against any measure such as US-VISIT whose sole purpose is to ensure our nation's security in the post-9/11 world we live in.

The US-VISIT project was officially awarded to Accenture LLP on May 28, 2004. For the project, Accenture will lead the Program Management, Business Transformation, Business Architecture, and Overall Transition work. However, Accenture is not alone in the development and implementation of US-VISIT. It was through the strength of their Smart Border Alliance with member companies including Raytheon, SRA International, and The Titan Corporation that they won the contract. Raytheon will aid in systems engineering, biometrics, deployment activities, and the

overall enterprise architecture structuring. SRA International's primary areas of contribution will be in data analysis, data privacy, and program security. Finally, The Titan Corporation will support the project through their expertise in quality and configuration management, systems testing, systems engineering, systems design and development, and deployment. ("DHS Press Release")

The US-VISIT program itself begins with a pre-entry/enrollment process when a foreign national formally requests entrance or applies for a visa or the expedited travel program. At this time, biographic and biometric data is collected as well as prior travel and visa information. This accumulated data is then used to verify identity, compare to various watch lists, and provide assistance for the issuance of visas or other travel documentation. ("DHS Press Release")

The second stage of US-VISIT occurs as the foreign national attempts to board either an airplane or ship destined for a U.S. port of entry. The identity on the airplane/ship manifest is checked against identity and various watch lists in order to make advanced decisions whether or not to admit the individual in question into the United States. This advanced arrival data also serves to aid in the inspection process and aid inspectors monitoring the primary ports of entry. However, land border ports of entry will not have the same ability to monitor and review the advanced arrival data. ("DHS Release")

Upon arrival at a U.S. port of entry, travelers begin a formal inspection process in which machine-readable, tamper-resistant travel documentation is read, individual biometric data is collected, and entry data such as duration of visit is recorded. Those who pass inspection are allowed entry into the United States while those individuals who

fail are sent to a secondary inspection area for further processing. Inspection failure can occur for numerous reasons such as inability to verify identity, appearing on a watch list, or attempting to enter the U.S. using false documentation. During the duration of their stay in the U.S., foreign nationals can obtain immigration benefits. As information supporting those immigration benefits may change, the US-VISIT system will record the changes as well as tracking individuals who may have overstayed the recorded length of their visa. Finally, as a foreign national departs, their exit is recorded and, if necessary, they are detained depending on the results of a watch list screen. In addition, entry and exit records are coordinated and visa compliance is determined. ("DHS Press Release")

The US-VISIT program is being implemented through a series of phases known as increments. The first phase, Increment 1A, was completed on January 5, 2004. In Increment 1A, the initial operational entry capability for the US-VISIT program was put in place at 114 airports and 14 seaports as well as all 211 international visa-issuing posts. Increment 1B will address the issue of exit stations at both air and sea ports. A number of pilots are currently being evaluated at airports and seaports across the country. In one exit pilot, foreign nationals exiting the U.S. will check out of the country at exit stations situated within the airport or seaport. At the exit station, travel documents are reviewed, a digital picture of the individual is taken, their two index fingers are scanned, and the traveler receives a receipt documenting that they have properly checked out. Another exit pilot is identical to the previously mentioned pilot with one added requirement: verification at the departure gate following check-out at the exit station. In this form of verification, the visitor is required to present the receipt received at check-out from the exit station to an attendant at the departure date. From here, the attendant will scan the

receipt and scan an index finger of the visitor to verify identity. Provided that identity is verified, the receipt is returned to the visitor and they are allowed to board.

The next increment, Increment 2A, delivers the ability to read all biometrically-enabled travel documents, a capability required at all ports of entry. In Increment 2B, which is scheduled for delivery by December 31, 2004, entry capability at the fifty busiest land ports of entry should be implemented. Also included in Increment 2B is the collection of two index finger scans as well as digital photographs for visa holders and those traveling under the Visa Waiver Program. Increment 2C entails the development of automated entry and exit stations at select primary entry and exit lanes at the fifty busiest land border crossings. Radio Frequency technology will be utilized in Increment 2C in order to collect entry and exit data at land border crossings in an efficient manner. Finally, Increment 3 will deliver the functions of Increment 2B to all other land points of entry not initially included in 2B. ("DHS Press Release")

As it currently stands, US-VISIT is supported by nineteen key IT systems across numerous agencies. These IT systems include:

1. ADIS/VWPASS: Arrival Departure Information System
2. APIS: Advance Passenger Information System
3. BVS: Biometric Verification System
4. CCD: Consolidated Consular Database
5. CIS: Central Index System
6. CLAIMS: Computer-Linked Application Information Management System
7. CLASS: Consular Lookout and Support System
8. GES: Global Enrollment System
9. IAFIS: Integrated Automated Fingerprint Identification System
10. IBIS: Interagency Border Inspection System
11. IDENT INS: Automated Biometric Identification System
12. INSPASS: Immigration and Naturalization Service Passenger Accelerated Service System
13. NAILS II: National Automated Immigration Lookout System
14. NEXUS NEXUS
15. NIIS: Non-Immigrant Information System

- 16. OARS: Outlying Area Reporting Station
- 17. PALS: Portable Automated Lookout System
- 18. SENTRI: Secure Electronic Network for Travelers Rapid Inspection
- 19. SEVIS: Student Exchange and Visitor Information System ("DHS Press Release")

Integration is clearly an issue for US-VISIT given the number of systems that support it.

In addition, many of these systems are older, are paper-based, and do not easily support the latest technologies. It will be a significant challenge for the US-VISIT project team to enhance the interoperability of these support systems in order to achieve the objectives set forth by the Department of Homeland Security. However, once these obstacles are overcome, the full implementation of the US-VISIT program and its associated biometric technologies will prove to be a valuable tool in securing U.S. borders.

## **Geospatial Information Systems**

Although not as widely recognized by the general public as biometric technology, geospatial information systems, or GIS, are another critical technology currently being utilized for homeland security purposes. The National Science Foundation defines a GIS as "a computerized database management system used for the capture, storage, retrieval, analysis, and display of spatial (defined by location) data." GIS databases have been used by various organizations at the federal, state, and local levels of government for decades. However, the 9/11 attacks and the subsequent push for enhanced disaster awareness and preparation have increased its importance as a homeland security tool. GIS provides decision-makers with the data they need to properly address threats such as sabotage, terrorist attacks, and natural disasters. (Ferketic)

GIS enables its users to view important features and potential terrorist targets such as bridges, buildings, water supply facilities, or even vehicles and people. However, GIS applications are not limited to simply displaying the location of features and objects. They also have the ability to predict how those features may react to certain stimuli as well as describe how the objects and land features relate with each other. (Ferketic)

A standard GIS consists of several transparent layers of information on a map. At the foundation of the GIS is the landbase or base map which consists of the physical and cultural features of the land such as buildings, roads, bodies of water, and other features that can serve as reference points for general orientation. From here, other features such as nuclear facilities, hospitals, or water treatment plants can be placed over the base map for further analysis. In addition, aerial photography or satellite imagery can also serve to supplement the base map and provide further support in analysis. Global Positioning

Systems, or GPS, can also be integrated with GIS in order to provide precise locations on assets such as search/rescue personnel or emergency response vehicles. (Ferketic)

Every aspect of homeland security can be addressed through the use of GIS. It possesses **detection** capabilities that allow users to perform accurate threat analysis so that likely targets and scenarios can be properly identified and anticipated. The possibility of a terrorist attack as well as its impact on life and property fall under the category of detection. Emergency planners and responders can be considerably more **prepared** through the implementation of GIS as it provides data that is vital to the success of any emergency situation. Plans can be developed to save lives and minimize the amount of damage inflicted by an attack. Because of its ability to identify possible patterns regarding security threats and potential terrorist attacks, GIS serves as an important tool of **prevention** as well as **protection**. Finally, GIS is already utilized by organizations such as FEMA and the Red Cross for the purpose of **response and recovery**. Response can best be defined as the events immediately following an attack or disaster situation while recovery involves the activities to return all systems to their pre-attack state. (FGDC)

Immediately following the 9/11 attacks on the World Trade Center, New York City rescue workers needed rapid access to accurate information about the disaster site. However, the information that they needed went far beyond basic maps of the area. Information with data about potential hazards such as fires and debris was imperative to assist rescue workers in rescue and recovery operations. Emergency coordinators were able to turn to GIS to obtain and analyze this data. GIS applications were able to analyze data that had been gathered through heat-sensing aerial photography. These photographs

were then superimposed on base maps that showed the location of underground fuel tanks. As a result, "hot spots" could be identified and the sources of numerous existing fires could be determined. GIS applications were also able to produce a detailed map of the World Trade Center site so that the ever-increasing amount of information that was coming from the site could be properly stored and analyzed.

GIS is also playing a major role in security in the local government sector. For example, in Boston, local officials have begun a pilot program known as the Boston Preparedness Pilot. The Boston Preparedness Pilot utilizes the smart database and digital mapping capabilities of the National Imagery and Mapping Agency, or NIMA. Boston law enforcement officials are using 100 digital mapping files from NIMA in their pilot program. Included on these mapping files are detailed locations of every school, hospital, grocery store, government building, fire and police station, major landmark, industrial facility, bridge, street, and highway. Boston Police Department officials hope that the collection and proper maintenance of such data will better assist their emergency personnel in preparing for and responding to a terrorist attack. (Verton)

The collection of data vital to government infrastructures on local, state, and federal levels is a valuable tool for homeland security. GIS applications support this purpose as they can better prepare emergency workers and law enforcement personnel to deal with detection, prevention, protection, preparedness, and response and recovery in disaster situations.

## **Cyberterrorism**

Dr. Dorothy Denning, Professor of Computer Science at Georgetown University and a leading authority in the field of cyberspace security issues, defined cyberterrorism in testimony before the Special Oversight Panel on Terrorism, on May 23, 2000, as follows:

Cyberterrorism is the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. (Denning)

On the surface, this definition appears directed at government systems which is indicative of the date of her testimony, over one year prior to the 9/11 attacks. The world has changed considerably since that time and that definition now has a greater scope - business and financial institutions. Clearly, an attack launched against the network of a major business or financial center could have devastating results for a nation's economy.

As the United States and the world in general has become more dependant on information technology and we advance to a true global community through the use of information technology, the opportunity for attack and overall vulnerability through these systems has increased. However, the degree to which government and business systems are vulnerable is a source of great debate within their respective communities. Some will say that while the threat of cyberterrorism is present and should be properly addressed, the probability of an attack seriously disabling a government or business network is minimal. Others have gone to great lengths to prove the opposite. For example, in 1997, the Pentagon simulated a scenario in which a cyberattack occurred and discovered that

cyberterrorists could disrupt military communications, 911 networks, and the electrical power systems in major U.S. cities using simple computers and easily accessible software. Unfortunately, hacking knowledge and tools have developed even further and become readily available to any willing participant since this simulation was conducted. ("Terrorism: Q & A")

Related to cyberterrorism is what has come to be known as cybercrime. Cybercrime can best be described as an attack against a person or persons or an organization for financial gain. The FBI estimates that \$10 billion is lost every year due to "electronic crime." Also, nearly all of the Fortune 500 companies have had system invasions at some point by cybercriminals. However, only about 17 percent of these instances are reported out of the fear of decreasing stock values and consumer confidence. ("Cybercrime...Cyberterrorism...Cyberwarfare")

Clearly, the threat that cyberterrorists and cybercriminals pose is significant to every government and business network. Though their purposes may be different (i.e. political versus financial disruption), the effects of these acts can be equally disastrous.

### ***Threats to Network Security***

The most well-known threat to network security is probably the virus. Computer viruses can take many forms such as the straight virus, e-mail viruses, Trojan horses, and worms. In computer terms, a virus is a self-contained piece of software, usually fairly small in size that attaches itself to another document or application. Once the virus is executed, its true power is unleashed and it begins to infect other documents and applications. (Brain)

In network terms, a virus is able to spread through the use of shared resources, including folders and drives, or other network servers or ports. Often, network viruses are able to locate and exploit weaknesses in the network operating system or in other network applications. In addition, some viruses are spread through network ports such as port 80, which is reserved for HTTP, port 135, reserved for DCOM RPC, and port 1434, reserved for SQL. Among the most well-known and noteworthy viruses are CodeRed, MSBlast, Nimda, and SQLSlammer. The CodeRed virus targets network port 80 and attacks a weakness in the Microsoft Internet Information Service by spreading as a group of packets in the system memory. The MSBlast virus targets network port 135 and attacks a vulnerability in the DCOM RPC interface. In addition, MSBlast exploits port 69 (UDP) and port 4444 (TCP) as well. The Nimda virus, like CodeRed, targets network port 80 and also attacks a weakness in the Internet Information Service but is also able to spread across the infected network through e-mail attachments and shared drives. Finally, SQLSlammer infiltrates a network through port 1434 and takes advantage of a vulnerability in Microsoft Desktop Explorer and Microsoft SQL Server 2000 by spreading as packets in the system memory. ("Glossary of Virus Terms")

The e-mail virus shares all of the characteristics of a straight virus with one exception: the method of spreading. An e-mail virus spreads through individual e-mail messages, as attachments, and replicates by mailing itself to most, if not all, of the e-mail addresses in the victim's e-mail address book. Two of the most popular e-mail viruses are the Melissa and ILOVEYOU viruses. Launched in March of 1999, the Melissa virus spread in .doc (Microsoft Word) files that were attached to an e-mail. Once the infected attachment was downloaded, the virus began and replicated itself in a similar e-mail to

the first fifty people in the victim's e-mail address book. So as not to arouse suspicion, the replicated e-mail message included the initial victim's name. Assuming that the e-mail was non-threatening, the recipient would open it and download the attachment, which led to another fifty people from the recipient's address book receiving the same e-mail and continuing the vicious cycle of the Melissa virus. Melissa spread so rapidly that many large companies were forced to shut down their e-mail systems until the problem could be resolved due to the excessive traffic. On May 4, 2000, the ILOVEYOU virus was launched. This time, the victim would open an e-mail, click the attachment, and unknowingly launch the virus. Not only would files be corrupted on the victim's machine, the virus would replicate by sending itself to every e-mail address in the victim's address book. (Brain)

Besides the aforementioned viruses, another threat to network security is the Trojan horse. All Trojan horses are executable programs, meaning that they will perform some sort of pre-defined action when opened by a user. A Trojan horse has been defined by one source as a "malicious, security-breaking program that is disguised as something benign." (Lo) Trojans can be disguised as any sort of program that the user would be willing to open, including multimedia applications, games, movies, or music. In this fashion, Trojans are usually downloaded from the World Wide Web or through File Transfer Protocol although they can also be acquired through peer-to-peer (P2P) network file exchanges, instant messaging, or through an e-mail attachment. Once in the system, a Trojan can have devastating effects. For example, Trojans can allow others to access private files or can turn your computer into a "slave" machine that can be used by hackers to attack other computers. (Lo) A particular type of Trojan is a logic bomb, though it

often delays its malicious features. A logic bomb is programming code that can be inserted into a program either overtly or covertly that, once activated, can corrupt or delete data or have other negative effects. Triggers for logic bombs vary but can include a lapse of time or inactivity by a program user. ("Logic Bomb")

Yet another very serious threat to network security is the Denial of Service attack, or DoS. A DoS attack can be categorized as a Trojan type of attack that interrupts the regular flow of information into and out of a system. Once a DoS attack has begun, the resources of a system are consumed and rendered useless in a relatively short period of time. DoS attacks involving World Wide Web systems are similar in that a Web site under attack will be accessed repeatedly at an extraordinarily high volume from many different locations and tying up the site so that regular users are unable to access and retrieve information. ("Glossary of Virus Terms")

In TCP SYN flood attacks, SYN-ACK packets are sent to either one or many hosts who are in no way involved in the attack but eventually become victims of the attack as well. When there is an unknown or inaccessible source address in a TCP SYN flood attack, additional host resources are wasted as the target host is trying to set aside resources waiting for a response while the fake source address is constantly changed by the attacker when each new SYN-ACK packet is sent. (Ferguson and Senie)

### ***Methods of Network Defense***

Fortunately for businesses and government organizations, there are numerous methods available in the market to better protect a network system against the previously

mentioned threats as well as other threats to network security. While costs may vary, the benefits for enhancing the security of a network are invaluable.

As stated earlier, viruses pose a very serious threat to network security. It is estimated that over 87% of all viruses enter a network through e-mail. ("The Real Cost of a Virus Outbreak") The table below examines the typical costs associated with a virus attack on a network.

ACTION	COST
Cost for an IT manager to be informed of and take action on one virus incident	\$500
Cost for one workstation to be stopped, scanned, and cleaned of virus	\$1,000
Cost for one workstation to detect and clean a virus infection locally	\$100
Average number of times hackers will attempt to crack a network per month	2

Source: "The Real Cost of a Virus Outbreak: Why is Anti-Virus Needed?" Trend Micro White Paper

This table clearly illustrates the need for all networks to be adequately equipped with anti-virus protection. If it costs \$1,000 to inspect and clean a single workstation from a virus attack, a virus that infects dozens of workstations can cause significant financial damage to an organization. Therefore, anti-virus software should be viewed as a necessity for every business and government institution. To further illustrate this point, the following table shows the comparative costs of virus outbreaks over time.

		<b>COMPANY A</b> (no email protection)	<b>COMPANY B</b> (with email virus protection)
<b>TIME PERIOD</b>	<b>VIRUS INCIDENTS</b>	<b>TOTAL COST</b>	<b>TOTAL COST</b>
1 year	24	\$540,000	\$12,000
5 years	120	\$2,700,000	\$60,000
10 years	240	\$5,400,000	\$120,000

Source: "The Real Cost of a Virus Outbreak: Why is Anti-Virus Needed?" Trend Micro White Paper

Reviewing this table further reinforces the point that anti-virus protection is imperative for every network-based organization. Two well-known anti-virus software manufacturers, Symantec and McAfee, are compared in the table below. While the costs vary slightly due to the number of features offered, it is obvious that the cost of equipping a network with such software is minimal compared to the costs that can be incurred as a result of a virus attack.

<b>MANUFACTURER</b>	<b>EDITION</b>	<b>NUMBER OF LICENSES</b>	<b>COST</b>
Symantec	Corporate	50	\$1945.65
McAfee	SMB	50	\$2839

Sources: [www.symantecstore.com](http://www.symantecstore.com) & [www.shopmcafee.com](http://www.shopmcafee.com)

Another relatively inexpensive form of network security is a firewall. A firewall is a hardware device or an application that filters the information entering a network from an outside connection. Information deemed threatening by the firewall is not allowed access to the network. There are three primary methods in which a firewall filters network traffic. First, there is proxy service in which information from the Internet is retrieved by the firewall, reviewed for threats, and sent to the requesting system and vice versa. Secondly, in packet filtering, small pieces of data known as packets are reviewed

by filters. Any packet viewed as non-threatening is passed on to the requesting system. All other packets are not allowed access and discarded. Finally, there is stateful inspection. Similar to packet filtering, stateful inspection also examines each packet that is attempting to gain access to the requesting system. However, the difference lies in that stateful inspection only examines certain key components of the packet, not the entire packet as in packet filtering. The key packet components are then compared to a database of trusted information. If the key component and database results correspond, the packet is allowed through. If there is no match, the packet is discarded. (Tyson)

In the table below, five separate firewalls are compared. All were priced with a single-user license as multiple-license prices were not available from all manufacturers.

<b>MANUFACTURER</b>	<b>EDITION</b>	<b>LICENSE</b>	<b>COST</b>
BlackICE	PC Protection	Single-User	\$39.95
McAfee	Personal Firewall Plus 6.0	Single-User	\$30.39
Symantec	Norton Personal Firewall 2004	Single-User	\$18.14
Sygate	Personal Firewall Pro	Single-User	\$47.95
ZoneAlarm	Pro	Single-User	\$49.95

Source: [www.compnetworking.about.com](http://www.compnetworking.about.com)

Again, as was the case with anti-virus software, the costs of implementing a firewall within a network in comparison to the costs associated with a virus attack are minimal. In addition, the benefits achieved through anti-virus software and the utilization of firewalls are immeasurable, in terms of both cost-savings and information security.

Another method of defending against network attacks is the method of protocol filtering. When protocol filtering is utilized, ports are recognized on a protocol basis. A port can be a member of one or more protocol groups. For each individual protocol

group, flood traffic is allowed access out of a port only if that particular port is a member of the proper protocol group. Protocol filtering prevents certain protocol traffic from exiting switch ports. Both unicast and broadcast flood traffic are filtered based on the membership of the respective ports in separate protocol groups. Protocols categorized as Layer 2, including Cisco Discovery Protocol, or CDP, and Spanning Tree Protocol, or STP, are not affected by protocol filtering. Ports that are members of all protocol groups include dynamic VLAN ports and ports that have port security enabled. Ports can be configured with any of the following modes: on, off, or auto. As expected, when configured to **on**, all flood traffic for a particular protocol will be received by the port. Conversely, when configured to **off**, no flood traffic for the protocol is received by the port. In the **auto** configuration, a port receives membership to the protocol group only after the device connected to the port transmits packets of the particular protocol group. ("Configuring Protocol Filtering")

Yet another method of enhancing network security is what is known as an intrusion detection system, or IDS. There are three categories of an IDS: the network intrusion detection system, or NIDS; the system integrity verifier, or SIV; and the log file monitor, or LFM. The NIDS screens to see if a hacker is attempting to gain access to a network system or cause a denial of service attack by observing packets along the network wire. An NIDS can run on either a target machine that may be susceptible to attack or on an independent machine that oversees the network traffic. The SIV looks for changes in system files when a hacker modifies them. In addition, a SIV may also monitor other components such as a Windows registry and detect when a regular user mysteriously obtains administrative-level authority. As its name indicates, the LFM

monitors log files produced by network applications. The LFM looks for patterns or indications that a hacker may be present. (Graham) In general, an IDS is another valuable tool in the fight to protect network security.

In summary, the risks posed by the many types of viruses, Trojan horses, denial of service attacks, and other network threats are serious for all business and government institutions. Recent history has proven that cyberterrorists and cybercriminals are more than equipped with the knowledge and technology to inflict massive damage to any network system. However, through the utilization of such resources as anti-virus software, firewalls, protocol filtering, and intrusion detection systems, network administrators are well-equipped to combat the malicious intentions of those hoping to capitalize politically or financially through the misuse of information technology. In addition, the benefits of implementing the aforementioned resources, as well as others, far outweigh the financial costs incurred.

## **Conclusion**

Since the 9/11 attacks, the issue of homeland security has affected the life of every American in one way or another. For some, it may mean longer delays for airline travel while for others, homeland security may have been the deciding factor in voting for a presidential candidate. Although homeland security may be viewed as a nuisance in some instances, it is difficult to refute that it is now a necessity given the current state of the world today.

Information technology is and will continue to be a vital tool in many homeland security applications. Given the age of many of the current systems in use by government organizations as well as their lack of interoperability, IT professionals have many opportunities to be on the front line in the "War on Terror" to both improve these systems and facilitate communications among all government systems and organizations. In addition, technologies such as biometrics and geospatial information systems will continue to advance and new applications will be developed so that they can further enhance homeland security.

Government organizations have shown themselves to be incredibly slow to change, as shown by their continued use of outdated information systems. It is imperative that government, as a whole, embraces information technology as a resource and a weapon in the "War on Terror" and allows for the continuous development and implementation of the latest technologies available.

## References

- "BioFace: A Comparative Study of Facial Recognition Systems." Bundesnt für Sicherheit in der Informationstechnik. June 2003.
- Brain, Marshall. "How Computer Viruses Work." <http://computer.howstuffworks.com/virus.htm>, viewed October 5, 2004.
- Coleman, Kevin. "Technology and Homeland Security." Directions Magazine: March 6, 2003. [http://www.directionsmag.com/article.php?article\\_id=302](http://www.directionsmag.com/article.php?article_id=302), viewed September 28, 2004.
- "Configuring Protocol Filtering."  
[http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/rel\\_6\\_1/conf/protfilt.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/rel_6_1/conf/protfilt.htm), viewed October 10, 2004.
- "Cybercrime...Cyberterrorism...Cyberwarfare..."  
<http://www.csis.org/pubs/cyberfor.html>, viewed October 10, 2004.
- Denning, Dorothy E. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy." [http://www.totse.com/en/technology/cyberspace\\_the\\_new\\_frontier/cyberspc.html](http://www.totse.com/en/technology/cyberspace_the_new_frontier/cyberspc.html), viewed October 29, 2004.
- Denning, Dorothy E. "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism." <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html>, viewed October 10, 2004.
- "DHS Press Release." [http://www.dhs.gov/dhspublic/interapp/editorial/editorial\\_0442.xml](http://www.dhs.gov/dhspublic/interapp/editorial/editorial_0442.xml), viewed November 15, 2004.
- "DHS Request for Proposals for US-VISIT Program." US-VISIT Program Office: November 28, 2003.

Ferguson, P. and Senie, D. "Network Ingress Filtering: Defeating Denial of Service Attacks Which Employ IP Source Address Spoofing." January 1998.

<http://www.faqs.org/rfcs/rfc2267.html>, viewed October 15, 2004.

Ferketic, John A. "Applying Spatial Technology to Homeland Security: A White Paper." James W. Sewall Company: 2002.

Frost and Sullivan. "Hand Geometry Technology Holds It's Own Biometric Technologies." April 13, 2004.

[http://www.findbiometrics.com/Pages/hand\\_finger/%20articles/handfrost.html](http://www.findbiometrics.com/Pages/hand_finger/%20articles/handfrost.html), viewed November 30, 2004.

"GIS for Homeland Security: An ESRI White Paper." ESRI: November 2001.

"GIS and Homeland Security." <http://www.c-b.com/information%20center/security/ic.asp?tID=16&pID=10>, viewed October 22, 2004.

"Glossary of Virus Terms."

<http://www.trendmicro.com/en/security/general/glossary/overview.htm>, viewed October 15, 2004.

Graham, Robert. "FAQ: Network Intrusion Detection Systems." 2000.

<http://www.robertgraham.com/pubs/network-intrusion-detection.html>, viewed October 15, 2004.

"Homeland Security and Geographic Information Systems."

<http://www.fgdc.gov/publications/homeland.html>, viewed October 3, 2004.

"Homeland Security and Geographic Information Systems: How GIS and Mapping Technology Can Save Lives and Protect Property in Post-September 11th America." Federal Geographic Data Committee: 2002.

Jain, Anil and Ross, Arun. "Biometric Sensor Interoperability: A Case Study in Fingerprints." LNCS: May 2004.

Lo, Joseph. "Trojan Horse Attacks." <http://www.irchelp.org/irchelp/security/Trojan.html>, viewed October 10, 2004.

"Logic Bomb: A Whatis.com Definition." [http://searchsecurity.techtarget.com/sDefinition/0,,sid14\\_gci815177,00.html](http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci815177,00.html), viewed October 15, 2004

Rhodes, Keith. "Challenges in Using Biometrics." United States General Accounting Office: September 9, 2003.

Sarkar, Dibya. "Experts Push GIS for Homeland Security." <http://www.fcw.com>, viewed October 22, 2004.

"Terrorism: Q & A." <http://www.terrorismanswers.org/terrorism/cyberterrorism.html>, viewed October 29, 2004.

"The Real Cost of a Virus Outbreak: Why is Anti-Virus Needed?" Trend Micro Inc. White Paper, March 1, 2002.

Tyson, Jeff. "How Firewalls Work." <http://www.howstuffworks.com/firewall.htm>, viewed October 15, 2004

Verton, Dan. "GIS Plays Key Role in Homeland Security." <http://www.computerworld.com/printthis/2002/0,4814,74071,00.html>, viewed October 10, 2004.

