Document released in part; withheld in part as (b)(5).

From ???@??? Thu Mar 07 10:10:00 2002
To: "Cosgrave, Paul" <Paul.Cosgrave@ost.dot.gov>, "'Jay Dombrowski'" <Jay.Dombrowski@nwa.com>, "Zarur, George" <George.Zarur@ost.dot.gov>
From: "Thomas H. Hinke" <thinke@mail.arc.nasa.gov>
Subject: RE: NASA - TSA introduction
Cc: "Torbeck, Mark" <Mark.Torbeck@ost.dot.gov>, tom_Edwards,huy Tran <htran@mail.arc.nasa.gov>, bob Rosen <rrosen@mail.arc.nasa.gov>
Bcc: "Patricia M. Jones" <pmjones@mail.arc.nasa.gov>, "John Melton" <jmelton@mail.arc.nasa.gov>, "Mark Schwabacher" <mark.schwabacher@mail.arc.nasa.gov>, "Linda Connell" <lconnell@mail.arc.nasa.gov>, "Jeffrey C. Becker" <becker@nas.nasa.gov>, "Ray Gilstrap"<rgilstrap@mail.arc.nasa.gov>, James Bell <jhbell@mail.arc.nasa.gov>, thinke@mail.arc.nasa.gov;
X-Attachments:
In-Reply-To: <23C309FEA282A943AE132127AABBC1E702A7B05D@ostex001.ad.ost.dot.gov>
References:
Message-Id: <4.3.2.7.2.20020307090414.00b8bdb0@mail.arc.nasa.gov>
X-Eudora-Signature: <Standard>

<html>
All,

I appreciate the introduction from Jay Dombrowski and would like to provide you with some background on NASA's work on the aviation security effort that I am leading here at the Ames Research Center. I am currently leading an effort that is performing research on the application of information technology to the passenger threat assessment problem. As you may or may not know, the NASA Ames Research Center (which is located in the San Francisco Bay area) is the NASA Center of Excellence for Information Technology. In addition to various core technologies that Ames has developed that may be applicable to this problem, we are located in the heart of Silicon Valley, which provides us with an excellent opportunity to easily interact with many universities and companies that are playing a major role in the development of new technology that may also be applicable. With that as background, I would like to provide you with a brief overview of our effort.

NASA has embarked on a project to develop an Automated Passenger Threat Assessment and Security Reporting System. This system has the following two primary goals:

* To integrate information technology into the passenger flow, with the goal of ensuring that passengers who may pose a threat to a commercial aircraft will be identified prior to takeoff.

* To use information technology to provide a means to capture information as to the effectiveness of the overall aviation security system through an extension of NASA's current Aviation Safety Reporting System (ASRS).

NASA's understanding of the passenger threat assessment problem is that an effective system must do the following:

1. Detect people who are known threats
2. Detect people who may pose a threat but are unknown
3. Ensure that people cannot bypass screening by
<x-tab>   </x-tab>* Using false names and/or forged credentials

<x-tab>   </x-tab>* Having substitute passenger board the aircraft in place of a screened passenger
4. Have an acceptable
<x-tab>   </x-tab>* Pd (probability of correct detection)
<x-tab>   </x-tab>* Pfa (probability of false alarm)
<x-tab>   </x-tab>* Tp (throughput)

In addition, in order to be acceptable, the system must be sensitive to the following:

1. Must address privacy and "big brother" issues to the extent possible
2. Must recognize that due to sensitive data, some agencies may not be willing to release information on known threats, but, they may be willing to do red-light/green-light processing on passenger biometric, some universal ID or name.

NASA's current work in applying information technology to this problem includes work in the following areas:

1. Developing a system to acquire and integrate information from multiple sources
2. Developing a system to perform data analysis and data mining on this integrated information
3. Integrating the technology in a security laboratory the mirrors passenger flow in an airport
4. Addressing the problem of how to scale the technology to 600+ million passengers per year spread over 430 airports.

Each of these will be described in what follows.

Information Acquisition and Integration

Believing that information holds an important key to passenger screening, in cooperation with Voquette (a commercial vendor), NASA has developed a system to automatically acquire information from various external sources and integrate this information into a system that can serve as a testbed for exploring various types of threat assessment techniques. The system monitors various government sources to acquire information about people who have been identified as potential threats. This information is enriched through the acquisition of additional information from various web-accessible sources, in an effort to identify other people and organizations that are associated with these threat people.

The system also acquires information from various commercially available databases in order to augment the information that airlines normally have about passengers. The goal of this augmented passenger information is to provide richer information than is currently available, in order support improved methods of passenger screening, including the determination as to whether any link exists between passengers and known threats.

Data Analysis and Mining

Data mining represents one of the core technologies at NASA Ames, which is one of the top research labs in the country in statistical machine learning and

unsupervised machine learning. NASA also maintains very close ties to the broader academic and industrial research communities in these areas. With this background, NASA Ames is applying various data analysis and data mining techniques to the augmented passenger information (described in the previous section) in order to identify passengers who either fall into groups that can be considered safe or groups that require additional scrutiny. Data mining seeks to automatically discover previously hidden information from large databases. Our goal is to use these discoveries to improve information-technology-based passenger screening techniques. A number of different analysis and mining techniques are being investigated and will be briefly described.

* Expert Systems: This is a rule-based approach in which human experts on aviation security are asked how they would assess the threat level of a passenger. Their methods for threat assessment are then encoded into a set of rules. For example, the experts might say that a passenger who pays cash for a one-way first-class ticket is more likely to be a threat. This approach has a capability that is equivalent to the approach used to build CAPPS (Computer Aided Passenger Prescreening), which is currently being used for passenger screening. [redacted]

* Inductive Learning: Under this machine learning approach, inductive learning software is trained on both normal and threat passengers. The software learns the characteristics of normal passengers and those of threat passengers. When a new passenger makes a reservation, this software would analyze the information available about the passenger and categorize the passenger as normal or threat. While this technology has been used very successfully for fraud detection, where there are a relatively large number of fraudulent activities (in comparison to known threat passengers), the applicability of this technology for passenger threat detection may be more limited do to the very small number of known threat passengers.

* Anomaly detection: Anomaly detection software looks for cases where information about a passenger deviates significantly from all other passengers.

* Link analysis: The goal of link analysis is to discover if a passenger has a connection or link to a known threat.   Two people are linked if, for example, they have the same previous address (which could be determined from our commercially available data), they flew together (which can be determined from airline data), one made a phone call or sent an e-mail to the other. A passenger is more likely to be a threat is he/she is linked to a suspected terrorist, and less likely to be a threat is he/she is linked to someone who is believed to be safe. Under this approach, threat scores are propagated across links based on the weights of the links.

* Clustering: This technique is used to automatically group people, based on various characteristics. The objective is to discover clusters that correspond to classes of "good" passengers, such as business travelers and tourists. This is accomplished by using a clustering (or unsupervised classification) algorithm to find clusters of similar passengers. Passengers who do not fit into any of the clusters of "good" passengers will be subject to additional screening.

* Hybrid mining: Under this approach, two or more of the previous approaches would be combined in order to provide improved screening

* Group threats: Under this approach, the goal is to explore methods for detecting groups of high-threat passengers on the same flight, or across multiple flights.

In cooperation with LexisNexis, pseudo-passenger data was augmented with data retrieved from the LexisNexis commercial databases of 180 million Americans. This LexisNexis data included previous addresses and phone numbers, license information and real estate information. Starting with name and address information associated with the pseudo-passengers, the Voquette software was used to retrieve additional data on them from the LexisNexis Web site. We are using this data to test the applicability of various commercially available data analysis and mining packages. We have recently received three months of actual passenger data from Northwest Airlines which will also be used in our work.

Our challenge is to

1. Investigate the applicability of existing analysis/mining techniques for passenger threat assessment,
2. Investigate how existing analysis/mining techniques can be modified to support passenger threat assessment
3. Investigate the need for new analysis/mining techniques that may be needed to perform effective passenger threat assessment.

Aviation Security Laboratory

<font face="Times New Roman, Times">Various types of information technology must be applied at appropriate places in the passenger flow from reservation to boarding. To investigate the various options for applying information technology, NASA Ames has established an Aviation Security Laboratory. This laboratory contains various processing stations including the following: reservations/checkin, security checkpoint, boarding, security officer screening and security control room. The first three stations mirror current points in the passenger flow process, but augmented with additional technology such as biometric devices where appropriate.

The security officer screening station provides a place to provide a behind-the-scenes view of the type of threat assessment techniques that are being developed, such as link analysis. In addition, the security officer screening station could be used to provide a security officer with information about a particular passenger that could be of value for interviewing those passengers for whom the automated system has indicated that additional scrutiny is required. It is recognized that only a small portion of the total passenger load can be selected for additional screening if the system is not to cause a major burden on the passenger screening system.

The security control room illustrates the application of information technology to assess the threats across all of the passengers on a particular flight and to look across the entire national airspace to assess the aggregate threats associated with all flights that may be in concurrent operation. The control room processing capability provides a place to investigate analysis and mining associated with group threats. This system could also be integrated with a flight path anomaly system under development here at NASA Ames, so that the passengers and associated threat information of the anomalous flight could be readily displayed to decision makers.

The laboratory will also provide a place to experiment with various types of biometric devices and smart cards (for trusted passengers) to understand how they can be effectively integrated into the overall passenger threat assessment system and where they can be placed in the passenger flow, balancing both effectiveness and overall cost.

Scalability

Any technology developed for automated passenger threat assessment must scale to 600 million passengers per year (growing to one billion in the future) spread over 430 airports across the country. To this end, NASA is investigating how one of its core technologies, grid computing, might provide the basis for supporting such scalability. Grid computing has developed international interest as the European Union, the United Kingdom, the U.S. Department of Energy, NASA, and various high-performance computer groups in Japan and Korea collaborate in developing standards and best-practices for integrating large number of computers, including high performance computers, into a seamless computational and data environment that can effectively handle some of the most challenging applications in the world. NASA Ames has played a significant role in the development of grid computing with its Information Power Grid project. The applicability of grid computing for handling the large amount of processing anticipated to support these passenger loads are an important component of the NASA effort in passenger threat assessment.

Using NASA's ASRS for Security Reporting

For many years, NASA's successful Aviation Safety Reporting System (ASRS) has been soliciting, processing and analyzing reports that describe aviation safety problems. In the last few months, tASRS has been receiving security reports. NASA has initiated a program to begin to solicit and analyze security reports. Formal data analysis methods will be used to identify system risks and vulnerabilities. These will be communicated back to the aviation industry, but as with the current safety reports, the identity of the person reporting the incident will be protected. This guarantee of anonymity is one of the strengths of the current ASRS system.