Global Information Assurance Certification Paper

Enhancement of Airport ID Security Badge Environment

Results of 9/11

by Kenneth Mack

January 19, 2004

SANS GAIC GSEC Practical Assignment Ver 1.4b Option 2

Contents

1 Abstract

The events of 9/11 shook up the entire air transportation industry. Many airports have undergone a major re-evaluation of their security infrastructure, practices, and personnel evaluations. This has affected the way the airlines do business with their passengers and the way the airports do business with the airlines.

This paper is an overview of how the security of the badging system, its interfaces and its processes have changed as a result of the heightened security atmosphere. The identification and consideration of both short-term and long-term security requirements are presented as well as the impact they are expected to have on the system security and functionality. Sensitive information has been omitted to protect system security.

2 Introduction

Major metropolitan airports around the country have undergone a major change in security. Most of the news has been focused on the changes that affect the passenger.

What is not in the news are the changes that have taken place to the supporting network, servers and workstation infrastructure within airports and the way the airports now must process individuals that work or do business with the airport.

Before 9/11 getting an ID badge for access to the AOA (Air Operations Area) of the airport only involved being employed by the airport or a company that has a contract with the airport, showing two forms of ID, and passing a SIDA test. Today fingerprint scan background checks and identity verification are mandatory, and biometric data capture is becoming more commonplace.

The infrastructure of an airport badging system has been greatly affected by the heightened demand on a more secure environment. A typical system includes badge-processing workstations, servers, LANs (Local Area Networks), WAN (Wide Area Network) and the Intranet and Internet. In addition, there are impacts to the interfaces that the badging environment maintains with the systems inside and outside the airport while guarding the system against intrusion.

As a member of the airport IT support staff for over 10 years, and with 20 years experience in networking and IT support, I was assigned as system administrator for an airport badging system, supporting network and infrastructure. I was a member of the communications team that supported the airport during and after the events of 9/11, including the identification of requirements for improving the security of the badge production environment. The implementation of the requirements was the responsibility of the corporate network support staff.

3 Original Environment

The badge production environment of a typical metropolitan airport prior to September 11th 2001 consisted of database servers and several badge workstations located on the main backbone of the airport LAN.

3.1 The Badging Process

The badge process had been in place for several years with little or no change to the workflow or process automation. In the current state of heightened security, many new processes, procedures and requirements, which are being placed on airports and the industry in general, cannot be met unless we change the way that we do business.

A high level diagram of the current badge process flow is shown in Figure 1. The upper part of the diagram shows a small part of the Company process and below that is the process for an employee of that company.

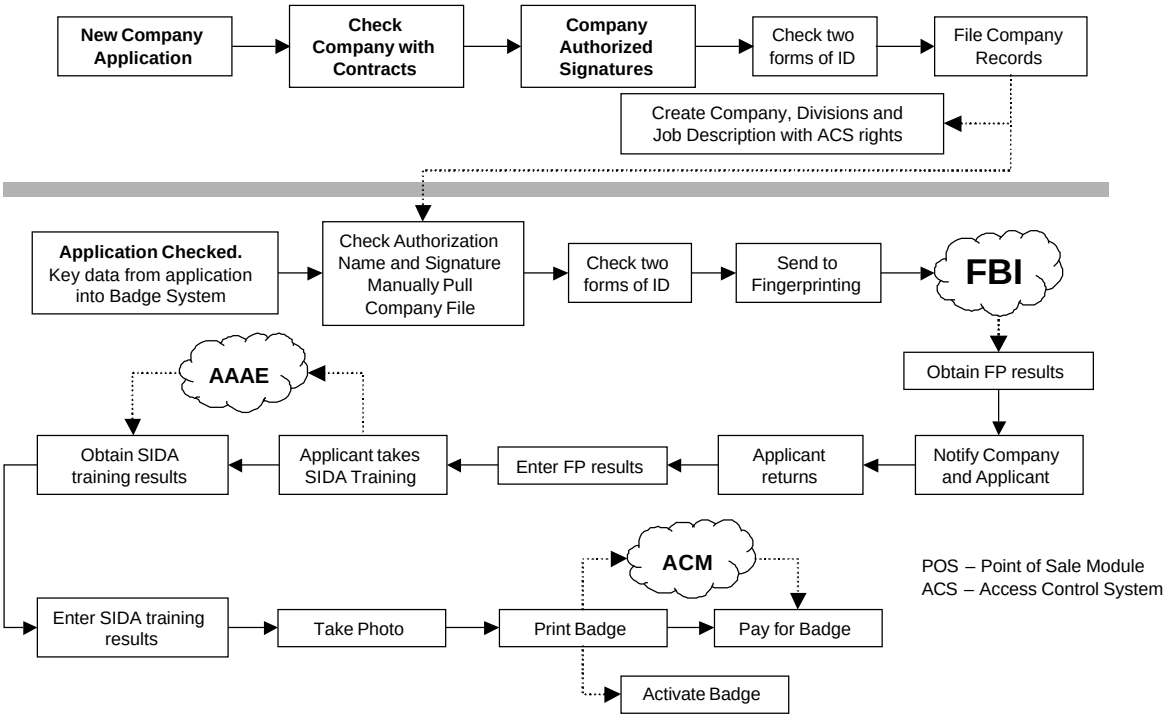

Figure 1 - Badge ID Process

Once all the applicant's personal and company data has been entered, the badge record is sent to the database. After all fingerprint and training obligations have been met, the badge record is ready to print and the information is collected and sent to the print server. Once a successful badge print has been acknowledged the activation record for this badge is sent to an Activation Processor (AP). This is the badge database interface to the Access Control

System (ACS) application. Each transfer either creates a new or modifies an existing applicant record in the ACS database, which gives them access to specified doors throughout the facilities.

Another process within the badge application sends information to the Revenue Control System (RCS) where the applicant's data can be pulled up using the Point of Sale (POS) application. Neither the AP nor the POS have the ability to communicate back to the badge application telling of a successful activation or payment.

3.1.1 Company Application

Before an employee of a company is issued a badge, the company must have a business relationship with the airport. Once the company is established to do business with the airport, a formal letter, on company letterhead, is provided to Pass and ID that designates the individuals with the authority to sign a request for a badge. The letter is then filed for future reference.

Once paperwork is checked, a company profile is created in the badge application. The profile includes:

- Company name
- Company number (different than that in any other airport's system)
- Company divisions
- Job positions, and
- Access control codes required for each Job position.

Now employees for the registered company can apply for a badge.

3.1.2 Employee Application

An applicant for an ID badge must first complete an application. The applications must be typed and signed by the employee. The badge application must be presented to Pass and ID by the applicant and be accompanied by

1) Two forms of ID (valid divers license, social security card, birth certificate, military ID, green card, INS documents, etc.) and

2) Company letter signed by one of the individuals authorized to approve a badge and whose signature is on file with Pass and ID.

Pass and ID personnel visually check all of this documentation. Once all the documentation is validated, the applicant is sent to be fingerprinted.

3.1.3 Fingerprinting and Adjudication

This current Fingerprint and Adjudication process is shown in Figure 2 and the associated process system connectivity is shown in Figure 3.

As can be seen, the process is mostly a manually intensive one with multiple data entry and data retrieval steps. The process starts with (1) Enter Applicant Data. At this point, the applicant data is manually entered into the badge database. Once the company letters and the two forms of ID are verified, the

applicant is sent to fingerprinting. At point (2) the applicant's data is re-entered into a stand-alone database and again into the Identix TouchPrint 3000 Live Scan Terminal. [1] The fingerprints are then taken.

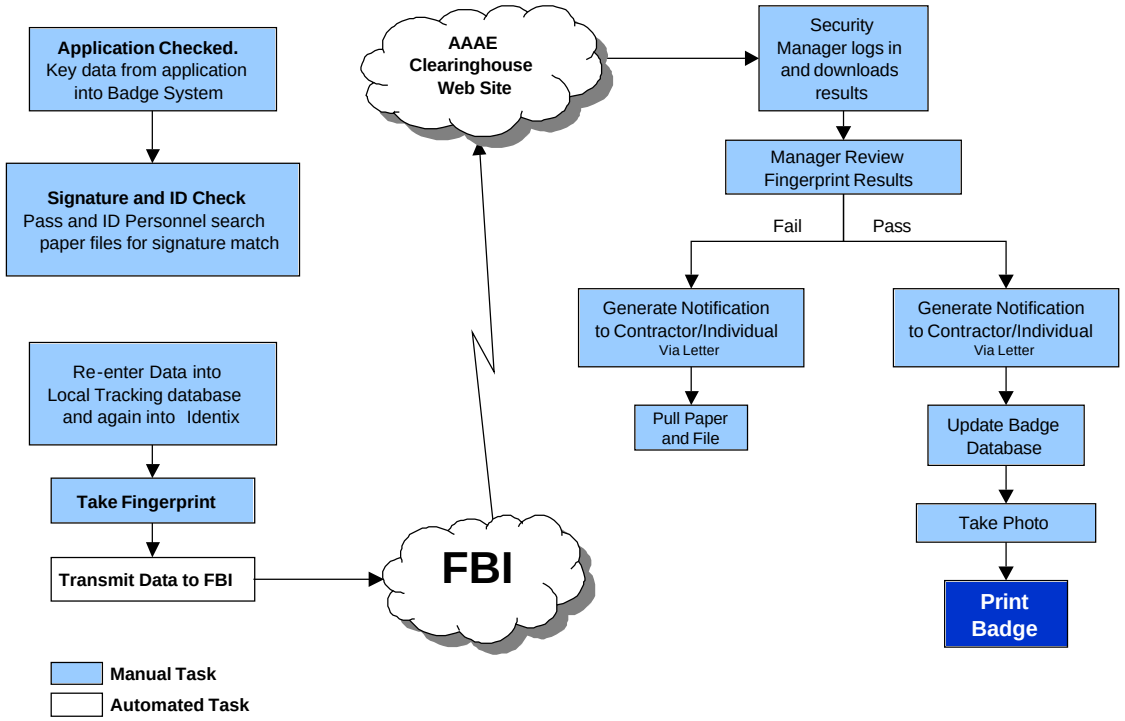

Figure 2 - Fingerprint Process Flow

The set of fingerprints are transmitted to the FBI (3) and, about 3 days later, received by AAAE. The airport security manager in charge of adjudication, logs into the AAAE site (4) on a daily basis and opens the "rap sheet" e-mails that have been posted. E-mails are manually examined (5) to identify which contain "rap sheets" and what kind of offenses are associated with an applicant's profile.

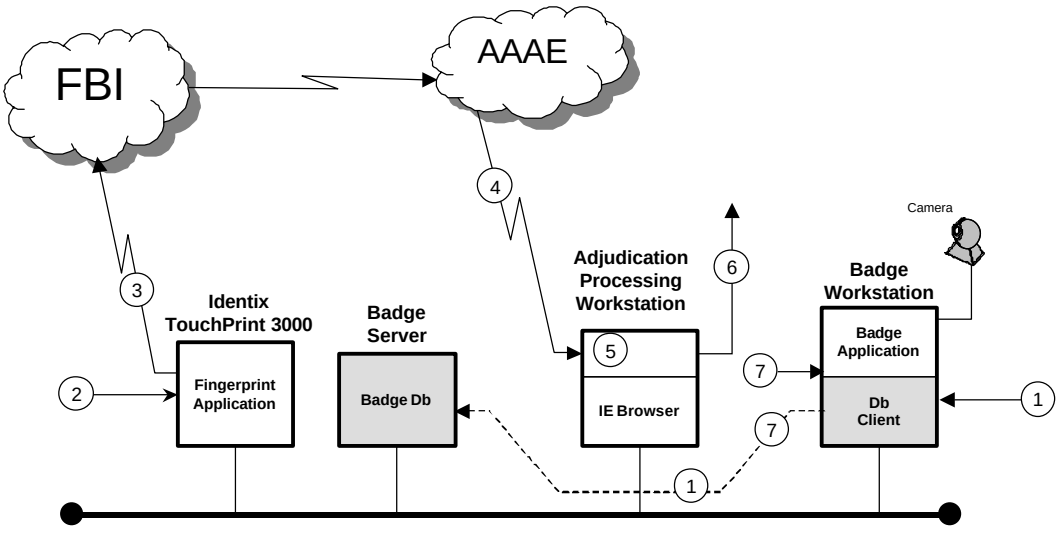

Figure 3 - Fingerprint Process Connectivity

Applicants without a "rap sheet" associated with the profile are sent to the administrative assistant to generate a letter (6) to the company stating that the badge application for the employee is approved and requests the employee to return to Pass and ID to complete the badging process. When the employee returns to the Pass and ID desk, the remaining information is manually entered (7) into the badge database.

3.1.4 SIDA Training

The next step for the badge applicant is to attend the SIDA training course. The training is self-paced and given on Interactive Employee Training (IET) workstations. [2] The connectivity of the IET SIDA training stations is shown in. Figure 4. The applicant's data is already entered into the badge database (1). The video on the IET SIDA stations is interactive and can be controlled by the student (2). At the end of the video training, there is an exam, which the student must pass to close the training session. When the student passes the test, the results are transferred via FTP (3) to the AAAE server for grading.

The applicant returns to the Pass and ID office where personnel there can retrieve the test scores (4) via browser interface, from the AAAE server. These results are then noted in the applicant's record (5).

At this point in the process, as shown in Figure 1, the only items that remain to be completed are to:

- Capture the applicant's image,
- Print the badge
- Activate the badge and
- Pay for all the items.

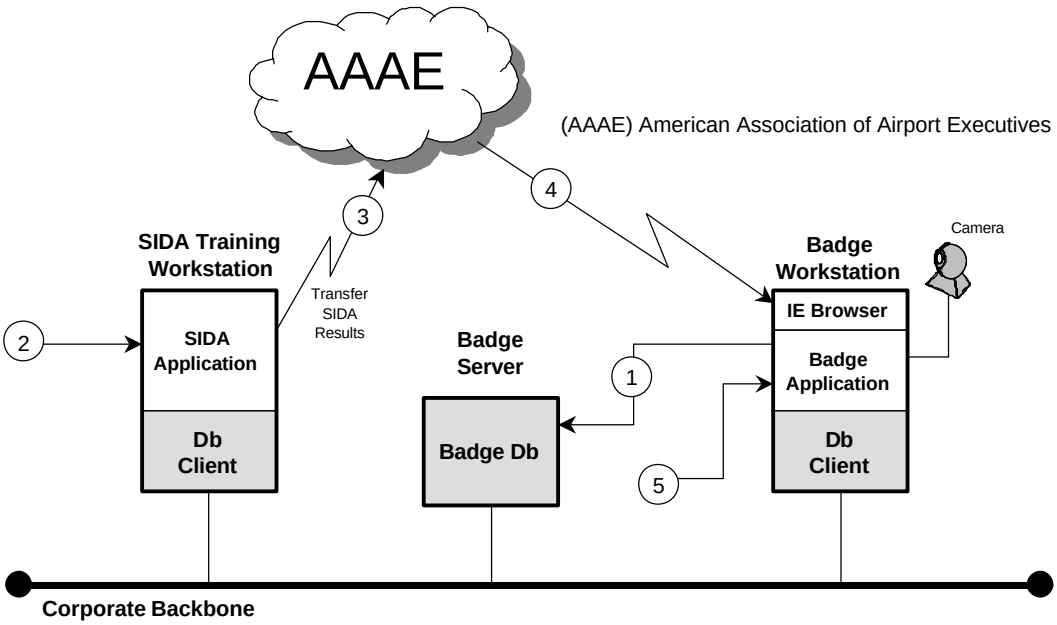

Figure 4 - SIDA Training

3.2 Badge Network

Backbone LAN – The entire corporate network prior to 9/11 was comprised of Cisco Catalyst 5500 series of Ethernet switches, Multi-mod fiber uplinks between wiring closets and Cat 5 cabling to the nodes. The switch that supported the Airport Operations area was a model 2900 that had a fiber uplink to the main Cisco 5509. The Catalyst 5509 has nine slots and supported high density 10/100/1000 Ethernet switching. Only the protocols in the IP suite were used and a Class B private addressing scheme was used across the entire campus.

A 3Com premises switch, which was located in the departmental communications closet, supported all the Pass and ID workstation and printers. This had a fiber uplink connection to a Cisco 5509 that was located in the computer/communications room. The badge servers were connected directly to the Cisco 5509. This 5509 was just one of many that made up the corporate environment.

Our primary area of concern was having the badge network accessible to the corporate network. Another issue was the network architecture itself. It was essentially a flat campus IP network. If an intruder did get into the servers it would be difficult if not impossible to trace where the intruder was located. In addition, the network used DHCP to manage the IP addressing of devices. This means that any person with a PC or laptop could plug into the corporate LAN, receive an IP address, and start snooping.

Badge Servers - There were two servers (badge database server and badge print server), and a gateway (activation processor) involved in the badging process. These were connected to the backbone LAN via Cat 5 cabling back to the 5509 switch.

The server security was up to specification. All operating system and security patches were up to date. Anti-virus was also installed and updates applied. The only issues were the lack of firewall software, and Security Event logging was turned off. Therefore, it could be possible to hack into the server using commonly available utilities many of them mentioned during class.

Badge Workstations – The system is an image capture workstation with Windows 2000 OS, WS Office 2000 with Outlook 2000. The workstations were part of the corporate Windows 2000 domain and had the password, folder, file, and protocol group policies of a standard user. The only additional badge processing software on the workstation was the badge application.

Workstation security was up to corporate security standards with respect to password, file, folder, and group policies.

Badge Application – The application maintained a database of all companies, employees, photos, and personal information as well as the ability to print and activate the badge. The badge software that was used was adequate for the security requirements of the 90's. However, during the crisis of 9/11 it became obvious to those working with the system that there were features that were lacking. Immediately after the events of the day, the FAA mandated a change in

all airport IDs. This required the mass deactivation, collection, destruction, production, and re-activation of many thousands of ID badges. In most cases, this was a totally manual operation. Many improvements needed to be made to the application to allow for such emergencies in the future.

3.3 Badge Support Infrastructure

Prior to 9/11, airports also had additional systems that were an integral part of the badging process. These systems included fingerprinting, training and collection of payments.

Finger Printing - The fingerprinting operation consisted of one standalone (un-networked) Identix TouchPrint 3000 Live Scan Terminal fingerprinting station with modem. In addition, there was one standard corporate workstation like those mentioned above. This workstation had the same complement of software and connectivity, as did the badging workstations. However, it did have a custom database application that kept track of all the personal data of those that had their fingerprints taken.

Beyond fingerprint identification, there was no other method in place to verify that the person receiving the ID badge was who they said they were. The only thing that the fingerprints did was to validate that the person getting the ID was not a known felon who had committed any of the 36 crimes listed in the 49 CFR Parts 1542 and 1544 of the Federal Aviation Regulations and Public Law #106-526. This list is on the badge application for many airports.[3]

There was great need for improvement in verifying the identity of the person receiving the ID badges that allowed access to the Air Operations Area (AOA)

SIDA (Security Identification Display Area) Training – It was and still is a requirement that all personnel receiving a badge must go through training on the use and display of the ID badge as well as the regulations on entering the AOA.

The training facility was in an area set aside from the badging operation. It originally consisted of 10 stand-alone SIDA training stations with touch screens. (mouse and keyboard are locked). The training application is AAAE's Interactive Employee Training (IET) System and requires a complement of specialized software. [2]

The training workstations themselves were not part of the corporate domain but did reside on the corporate backbone. However, the IET System had to establish FTP connection to the AAAE server to transmit the test results.

To accomplish this, the workstations were given static IP addresses and a hole was put in the corporate firewall to allow only FTP from those addresses to pass to the IP address of the AAAE server collecting the results. Pass and ID personnel could then access the results via the Internet from their workstation to verify that the applicant had fulfilled the training requirement and passed the exam.

Revenue Control - This operation in the badge process is where everyone goes to pay for the badge once all the requirements are met. The point of sale

workstation was a standard corporate PC except it had POS software and a connection to the corporate accounting system. The badge applicant's information is sent to the accounting system and can be accessed by using the applicant's social security number. This avoids the redundant entry of employee and company information and minimizes data errors.

This interface was maintained by a background process running on the badge server that pushed employee, company, and account information to the corporate accounting system.

4 Security Implementation

The physical security of all the Pass and ID workstations and servers was not a concern. The workstations are located in "card access" area that has an additional alarm that can only be disarmed with an ID badge with the proper "credentials". When unoccupied, the area is always locked.

The servers are located in a computer/communications room. This area is also only card accessible and is never left unlocked. The servers themselves have the consoles locked with secure logins and passwords.

4.1 Phase 1 – Network Security

The highest priority items on the agenda for the airport security team were any issues that concerned network security, and of most concern to Airport Operations was the ID badge operation and the isolation of the Badge LAN from the backbone network. Several alternatives were proposed by myself and examined by the network security team.

4.1.1 Total Isolation

This would obviously be the most secure. It would place all the workstations and servers on the same switch. There would be a router between the corporate LAN and the badge LAN to allow the badge server access to the accounting servers and the badge workstations access to the corporate resources. This is a good possibility because the workstations are located just within 100 meters of the Cisco switch. However, this option would limit the bandwidth of the workstations to 10Mb. This may prove to be a problem in the future when the workstations and camera are upgraded. There is a new requirement form the TSA for higher resolution image capture for photo IDs. This means that more network traffic would result from the increased photo resolution in both sending the data to the database to be stored and then the printing of the photo ID itself on the badge.

4.1.2 Server LAN

This option would require separate single switch to be located in the computer room for both the badge and print server connectivity. The server switch would connect to the backbone network via a router. The router access list would need

to have all the Pass and ID workstations included along with the addresses of the accounting servers.

There was a concern about the Pass and ID workstations "visibility" on the corporate network. It could be possible for someone to "take over" one of the Pass and ID workstations and get into the badge system. This may allow the intruder access to all the personal information in the badge database and could possibly allow them to print an ID badge. The ID badge would only print in the Pass and ID office but this is still one step too close for comfort.

4.1.3 Pass and ID LAN

Each Pass and ID location would have two workstations, one for the corporate network and one for the Badge network. The pair of PCs would share a common keyboard, mouse, and monitor. The corporate workstation would have the standard software and network installation, with access to the servers, e-mail and the Internet. These workstations would be connected to the premises switch located in the departmental communications closet.

The badge workstations would have additional cable pulled from the computer room and be directly connected to a separate Cisco 5509 switch. This switch would then have a router connection to the corporate backbone Cisco 5509.

The access list on the router would only allow IP traffic to and from the badge server and the accounting servers. This eliminates the need for the additional entries in the access list for the workstations to get to corporate resources.

4.1.4 Pass and ID VLAN

The difference between this solution and the LAN solution is that the Badge Isolation LAN is on the same physical box as the corporate backbone. The Cisco 5509 would have to be configured for the VLAN but the router configuration would remain the same as that of the LAN solution. The advantage of this solution is it does not require a separate box in the equipment rack.

This option was the one chosen by the network security team to implement. It gave the best balance of cost and security. The disadvantage with this solution is the security issues that are inherent with VLAN configurations.

4.1.5 VLAN concerns

There are several security concerns that arise when VLANs are used on Layer 2 switches.[4 5] These issues included:[6 7]

- MAC Flooding Attack
- 802.1Q and ISL Tagging Attack
- Double-Encapsulated 802.1Q/Nested VLAN Attack
- ARP Attacks
- Private VLAN Attack
- Multicast Brute Force Attack

- Spanning-Tree Attack
- Random Frame Stress Attack

However, because of the heightened security environment and the requirement for multimedia support, the entire corporate network was upgraded from Layer 2 to Layer 3 switches (Cisco 6500 series).

4.1.6 Layer 3 Network

The implementation of the Layer 3 network was accomplished by following the Cisco SAFE guidelines for Enterprise Networks.[8] In concurrence with the upgrade from Layer 2 to Layer 3 switching, the corporate IP addressing scheme was reconsidered by the network security team. The decision was made to change the IP addressing form its original private Class B address to a private Class A addressing scheme. This allowed a more creative use of subnetting and filtering so that IP addresses could be more easily assigned based on the location. For example (Campus, building, floor, workstation).

This also required the re-examination of the DHCP implementation. These changes were made by the server group using the requirements established by the network security team. The DHCP and network services were tightened. 1) Have static IPs for servers, printers and a few mission-critical workstations. 2) No client can obtain an IP address without authentication. 3) IP address lease of extended period which simulates a static IP. 4) All unused ports on the switches were disabled.

One of the final security measures that the network group implemented was the installation of IDS modules in all Cisco switches.[9] [10] [11] The implementation of the IDS will help detect some of the common threats used to compromise a network such as Exploits (failed login attempts, TCP hijacking), Denial of Service attacks (DoS) (TFN, and SYN floods), probing or mapping activity, or the misuse of network services (FTP, Telnet).

The result of the network security upgrade was tested very recently by an independent firm. They were contracted to try to penetrate the network from inside the firewall on the corporate backbone. After 3 days of trying, there was no penetration of any system anywhere within the corporate network or any or the isolated LAN segments.

4.2 Phase 2 – Badge Application

The next most critical area was the badge application itself. The original application was built around a technology that was 6 years old, and lacking capabilities that were direly needed. The requirements for the new badge application were developed by the airport operations staff and me. The requirements included:

1. Before a badge is printed, an applicant must meet the requirements for
    a. SIDA training
    b. Background investigations

c. Identification
d. Compliance to corporate business rules
e. Payment

2. Advanced features for the mass deactivation, activation and printing of badges by company, department, job function, etc.
3. Interface to existing Access Control System
4. Track employee violation information.
5. Configurable security permissions and business rules
6. Financial Functions (Point of Sale)
7. Design and printing of professional badges with capability of several methodologies of encrypting information. (Magnetic Stripe, 2D Optical Scanning, and Smart Chip)

The application that was chosen was WinBadge Aviation. [12] This product was designed specifically for the aviation industry and met or exceeded the requirements.

The new badge application software and database were installed and implemented over the past several months. The new application a much improved interface and database performance. It has greatly increased the ability to track an applicants progress in obtaining an ID badge and improved the overall reliability of the system by decreasing the number of points of failure. This was done by eliminating the stand-alone print server by using the print services available on the server.

4.3 Phase 3 – External Interfaces

The last and final phase of the security upgrade is the enhancement of the applicant's company and personal ID verification. The interfaces involved are between the badge application software and several of the corporate financial and contracts systems. These interfaces will have to be internally developed with the assistance of WinBadge support.

The planned badging process follows the same flow as the current process except for the addition of several enhanced and automated elements. These elements include:

- Company information management
- Enhanced company verification interface
- Employee information validation
- Biometric data capture
- Automated fingerprint adjudication
- Automated SIDA training reporting
- Enhanced Access Control System interface

4.3.1 Company Information Management

When a company establishes a business relationship with the airport most of their employees will require access to either “sterile” and/or “non-sterile” areas of the facility. These areas vary according to job position and the company’s areas of responsibility.

As previously discussed in Section 3.1.1, the current company application process is a manual paper process. The planned process will help to minimize the amount of paper that needs to be retained, speedup the employee validation process, and add a company validation check.

Companies that come into the Pass and ID office have to present letters on official company letterhead. The letters must be signed by the appropriate company officials and state the personnel authorized to approve badges for new employees.

The letters will be scanned into the badge system’s company profile. Items that will be captured and retained include:

- Company logo
- Signatures of company officials (with names keyed into the system)
- Signatures of the personnel that have employee authorization privileges (with names keyed into the system)
- Signatures of any airport authorization
- Company number

Alternatively, the entire document scan can be stored but must be electronically referenced using signature lookup on the names of any of the people that signed the document as well as company name or number.

4.3.2 Enhanced Company Validation

This interface is to the corporate accounting system and is designed to validate whether a company has a contract with the airport. The interface will periodically retrieve company information (company name, contract number, etc.) and store it in a table within the badge ID system.

When a company representative arrives to register a new firm with Pass and ID, the accounting information will be accessed to validate that a business relationship exists with the airport. Once validation is complete, Pass and ID will be able to create a new company profile in the badge ID System

Existing company profiles within the badge system will also be periodically checked against this table. Those that do not have a corresponding entry in the corporate accounting system will have the company profile deactivated in the badge system. Any badges associated with this company will immediately be deactivated.

4.3.3 Social Security Number Verification

What is the difference between validation and verification?

Validation:

Validation means the social security number (SSN) is a valid number. Validation can be, and usually is, determined by a mathematical calculation that determines that the number MAY BE A VALID NUMBER, along with the state and year in which that the number MAY HAVE BEEN ISSUED. However, this process does not ensure that the number: has actually been issued, does not belong to a deceased person, or that the number was issued by the Government to your candidate. In this type of process, there is no actual access to real data from the Social Security Administration attempted or implied. In an employment situation an SSN Validation will not provide any useful information about the actual status of an applicant's social security number.

Verification:

Verification means that the Social Security Administration (SSA) actually:

- Verifies that the number has been issued,
- Verifies state of issue has been provided by the SSA, and the
- Year of issue has been provided by the SSA.

If the SSN is not the exact name as presented in your request the SSA will not tell anyone to whom the SSN is actually issued. However, the SSA will give you a report which indicates:

- "Possible fraud" at the top in a starred box
- SSN has already had death benefits paid
- SSN is drawing SSI disability payments
- Any of the possible 17 classes of fraud has been issued

4.3.4 Name Verification

Several services are available that perform SSN and Name verification. They provide a combination of information from the national credit bureaus and Social Security Administration data. If the national credit bureaus have received identical full credit application data on a person from at least two different merchants, they declare that the SSN has been verified. The credit bureaus can also further verify a SSN number by comparing each request for information made to them against a copy of the current quarter's master tape from the SSA.

This provides a more complete picture of where the applicant has lived by matching the applicant's information against a half billion credit summaries. Name Verification provides names and addresses associated with a social security number. It is a valuable tool to help reveal discrepancies in information provided by the applicant.

Currently there is no social security number (SSN) or name verification other than a visual check of a social security card, if one is even presented.

Implementing the SSN feature would require a subscription to one of many external services available. The cost of the subscription varies but the turn-around of the verification service for a SSN name check can be as short as 24 hours. However, the results would be available within the period allotted to receive the fingerprint results.

4.3.5 Biometric Data Capture

The badge system will eventually be able to capture and store on the badge some kind of information on "what we are". These elements may include:

- Finger prints
- Hand geometry
- Iris scan

This information will be stored on the badge in the form of the programmable smart card. The main drawback of using much of the biometric data for access control is the cost of implementation. It could run as high as $1,000 per access point. This is a significant figure if you consider that an airport facility can have over 300 access points. Obviously the number of access points can be reduced to those AOA access but a study has to be conducted on the security risks of non AOA access to system such as elevators, mechanical rooms, communications points of presents (POPs) etc.

4.3.6 Automated Fingerprint Adjudication

The fingerprint adjudication process is one of the more manually intensive processes (3.1.3) that is required before a badge is issued to the applicant. The current fingerprint process flow was outlined in Figure 2 while Figure 3 shows the current process connectivity.

The planned fingerprint adjudication process has four steps that require manual intervention (Figure 5), but has a much higher connectivity requirement which is diagramed in Figure 6.

As before, the process starts with the entry of data (1). However, the majority, if not all, of the initial data input will be a possible combination of:

- Scanned with OCR data capture
- Web form with field transfer
- PDF form with field transfer
- Word form with field transfer

Part of the data entry process with the planned system will include the validation of the company information and authorization signatures that are presented when an employee applies for a badge. Pass and ID personnel will have the ability to electronically pull up the company letter that was presented and scanned when the company profile was created. This profile also includes the names and signatures of people within the company that are authorized to approve an employees badge application.

Other steps that are complete at initial data entry is the employee's presentation of two forms of ID and the initiation of the SSN and name verification process (Section 4.3.3).

When the initial data entry is completed, the applicant is sent to be fingerprinted. At this point, the Pass and ID operator will indicate on the form (via button or other means) that this applicant is going to have their fingerprints taken. The software will transfer, via secure protocol, the required information to a holding area to await the arrival to the applicant.

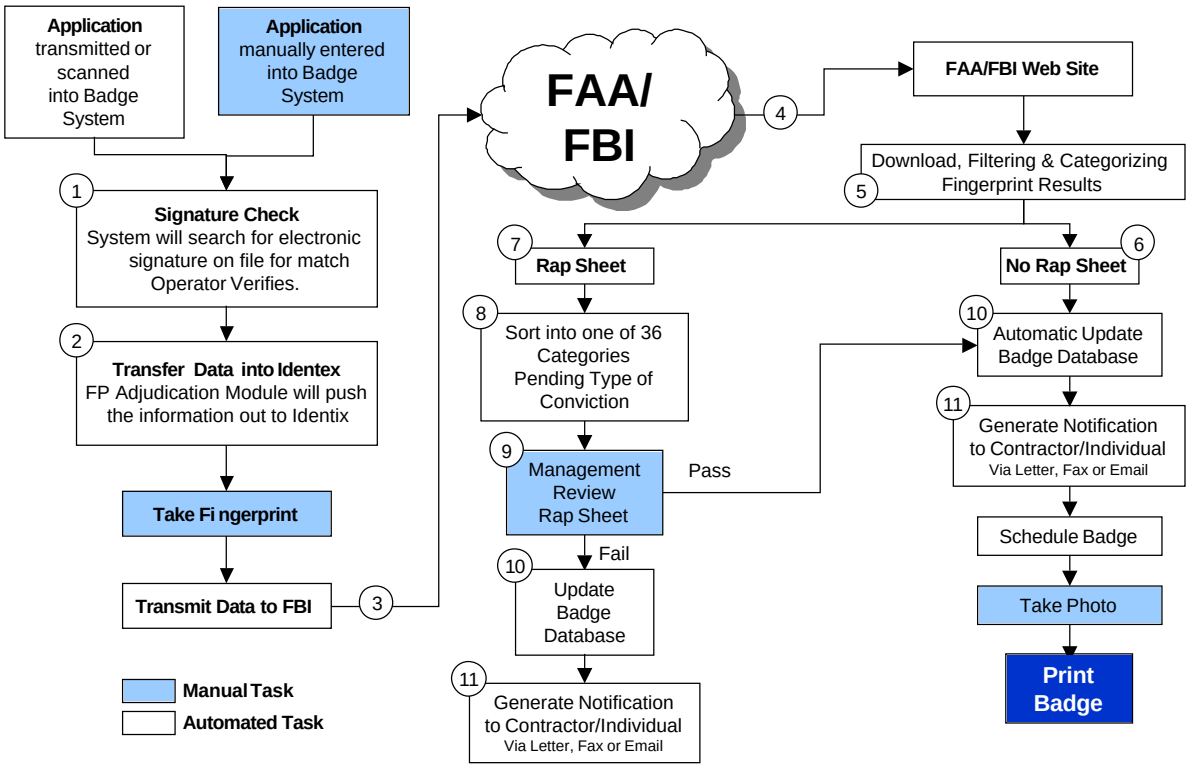

Figure 5 - Fingerprint Adjudication Process Flow

Upon applicant arrival in fingerprinting, his/her information will be requested from the system and transferred to the Identix TouchPrint tation (2). At this point, the fingerprint is physically taken and the information is transmitted (3) to the FBI for processing.

Results that have been processed are currently sent to a clearinghouse. However, it is our desire to attempt to retrieve the fingerprint results directly from the source. In any case, the badge software will have to periodically poll the server (4) that contains the results and transfer them, via secure protocol, to the badge software (5) for further processing.

Once the Finger Print Module (FPM) receives the data, it will process it according to applicant ID and identify if a "rap sheet" is present. Applicant data results that do not contain a "rap sheet" do not need any further evaluation. The information

is passed to the badge database (6) and the applicant's profile is updated accordingly.

The applicants' information that have "rap sheets", will require further processing. The FPM will take the "rap sheet" information and sort it according to one of the 36 categories listed by the TSA 1500 Series [3] regulations (8) and one additional miscellaneous category. The fingerprint results that need a manual review are ready to be displayed (9) on the Security Officer's workstation. The Security Officer should be the only one that has access to this module and a role will be created that will include rights to this module.

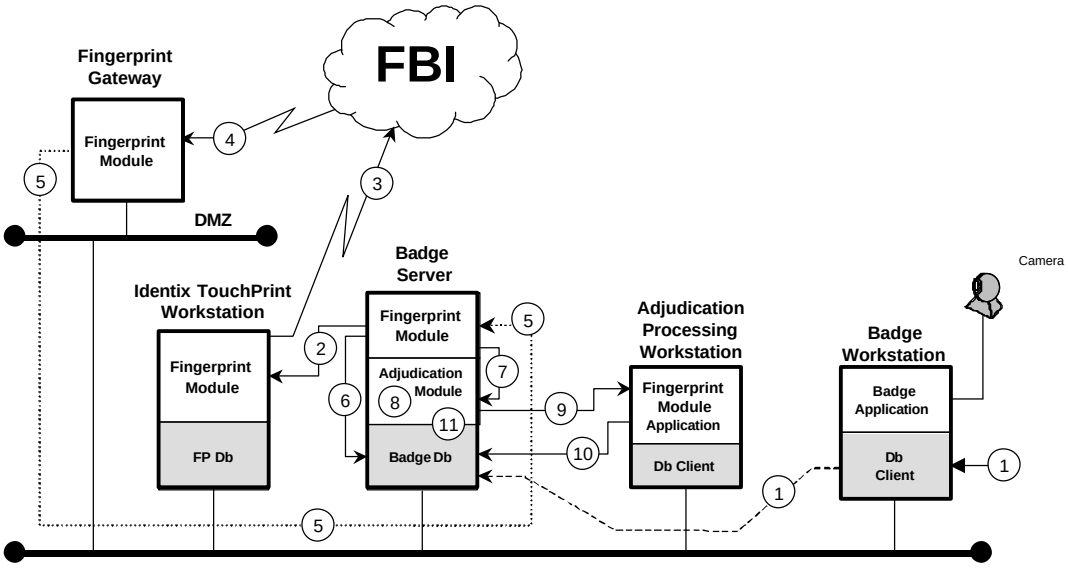

Figure 6 - Fingerprint Adjudication Process Connectivity

During the review process, the Security Officer will either approve with comments or disapprove with comments. Approvals and comments will immediately update the applicant's profile (10) so it can be accessed by the Pass and ID personnel. In addition, the system will generate a letter (11) that will be printed, e-mailed or faxed to the company sponsoring the applicant.

Disapprovals and comments will immediately update the badge system database with the applicant's information. However, the system will also flag the profile so a badge cannot be printed. Notification of the sponsoring company of the results will be handled in the same way.

5 Conclusion.

The events of 9/11 forced many in the industry to re-evaluate our security strategies and work together within the organization to identify weaknesses, provide solutions and implement the best solution for the amount of money that is allocated.

Much work has been done to prevent a re-occurrence of these events but much work needs to be done to streamline the networks, processes and procedures that the Federal Regulations will require of us in Airport Operation security.

6 References

[1] Identix TouchPrint 3000 Live Scan Terminal
URL: http://www.identix.com/products/pro_livescan_3000.html accessed on (1/15/04)

[2] AAAE's Interactive Employee Training (IET) System
URL: http://www.airportnet.org/depts/training/interactive/ accessed on (12/15/03)

[3] Federal Register / Vol. 67, No. 36 / Friday, February 22, 2002 / Rules and Regulations pg 21
URL: http://www.airportnet.org/depts/regulatory/security/fartotsa.pdf accessed on (12/20/03)

[4] Configuration Examples Related to VLAN Features
URL: http://www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eescg8x/aleakyv.htm accessed on (12/16/03)

[5] VLAN INSECURITY by Rik Farrow
URL: http://www.spirit.com/Network/net0103.html accessed on (12/15/03)

[6] Virtual LAN Security Best Practices
URL: http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/prodlit/vlnwp_wp.htm accessed on (1/15/04)

[7] SAFE Enterprise Layer 2 Addendum
URL: http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml accessed on (12/15/03)

[8] Cisco SAFE: A Security Blueprint for Enterprise Networks
URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns128/c649/ccmigration_09186a00800a3016.pdf accessed on (12/20/03)

[9] Cisco Catalyst 6500 IDS Service Module
URL: http://newsroom.cisco.com/dlls/IDSM2DS.pdf accessed on (1/5/04)

[10] Cisco IOS IDS software App Overview
URL: http://www.cisco.com/en/US/products/sw/secursw/ps2113/products_white_paper09186a008010e5c8.shtml accessed on (12/15/03)

[11] Cisco Intrusion Detection System
URL: http://www.cisco.com/en/US/products/sw/secursw/ps2113/index.html
accessed on (12/15/03)

[12] Goddard Technology – WinBadge® Aviation
URL: http://www.goddard-tech.com/Home/Products/Aviation/aviation.html
accessed on (12/15/03)