Case Study in Automating Branches of a Bank

Tim Rhome

August 27, 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b

Option #2

1. SUMMARY

This case study will highlight points that were addressed while automating 85 locations for a bank. These branches had three separate networks, one for each: Automated Teller Machines, IBM developed Systems Network Architecture (SNA) mainframe applications, and a PC based network at eight locations to operate a mortgage application. All three of these networks had outdated technology and were to be combined into one network for increased redundancy, improved security measures and reduced cost.

Although we addressed many aspects to complete this project, this document will focus on two specific areas that posed significant security challenges: wireless security and access control/password management.

2. BACKGROUND

The bank was formed in the mid-80's from several failed Savings and Loans and merged together with help from the FDIC. Although a mainframe was in place as the "system of record" for the banking applications, there had never been a hardware and software business needs analysis performed in the branches. Branch personnel performed standard banking transactions (cash, checks, savings, small loans, mortgage loans, etc.) through multiple antiquated systems and many of the activities were done manually or on a stand-alone PC. The ability to communicate with all branch personnel, whether it be regarding fraud or signature verification on an account, became a necessity. As PC costs went down and bandwidth costs became more reasonable, operational efficiencies became a priority to upper management.

3. BEFORE

The bank's three antiquated networks had many operational limitations in the branches. Some of the business shortcomings were:

- Antiquated method (faxing) to share signature verification cards among branches
- Time and error inefficiencies
- Wire transfer requests were not automated
- There were very limited disaster recovery capabilities
- No centralized electronic journal research option for banking transactions
- No fraud tracking system in place
- No way to view reports on optical system
- There was no tracking system for fee income
- There were no computer based training abilities

3.1 Security Concerns

In addition to the above operational deficiencies, we found many areas where information security could be enhanced. For example:

- The Teller system, which is used to conduct banking transactions with customers, password handling/administration was controlled in each individual branch. User ID and password information was stored on diskettes at each branch and not adequately controlled. Although the data that the bank maintains on the mainframe is the "system of record", an entry point existed with the teller system exposing potential vulnerabilities. These diskettes contained the account and password information and stayed in the unsecured disk drives at all times. These diskettes also contained a journal of all transaction for that branch's work each day potentially exposing sensitive bank or customer data to unauthorized access.
- There was no centralized management of the three networks and a different department controlled each. User ID and password guidelines were not consistent across these platforms and the information security policy had not been reviewed or updated in quite some time. Further, the systems were totally autonomous causing user ID and passwords to be different and out of sync. Interviews with the users revealed they were writing down their passwords and sharing with other users to conduct daily business. Some users had as many as seven ID and passwords.
- Revocation issues existed in that there was no way to ensure terminated employees were removed from the systems in a timely manner. If there had been a way to know that an employee was terminated, there was no way to restrict the user from accessing the system in the remote branches.
- Many policies and procedures were not up-to-date and none were centralized for prompt distribution and access.
- Access issues were present since mainframe access was reviewed periodically, but access to the other networks was not. Additionally there was no way for the Data Security Administrator or Audit Department to perform regular reviews.
- There was a PC with a modem in each branch for electronic communications – the modems were not secured in any way, they were not inventoried, there were no restrictions on who could use the modem and for what.
- The PCs were not secured from illegal software installation and there were no audit features in place to identify possible licensing issues.
- Internet access, if any, was limited in the branches via dial-up by each branch PC. These PCs allowed unrestricted Internet activity, no audit trail, and firewalls were non-existent.
- Virus scanning programs were not consistent on each PC if at all present and the virus definitions were certainly not kept current.

The initial focus was to begin replacing the 10-year old archaic Teller equipment that ran a proprietary operating system and applications. The hardware was becoming obsolete and parts were getting much harder to find. It was for these reasons that I was asked to direct a branch automation project and collapse the three networks down to one. As the project scope began to unfold, it became apparent that there were many security related issues that needed to be addressed as well.

4. DURING

We formed a committee to conduct a technical review of several new teller systems. This committee was comprised of members from all of the functional business areas of the bank including information services, back-office operations, users, training, and branch administrators. After we satisfied all the aspects of the bank's *Software Acquisition* procedure (features, ease of use, training, implementation support, post-installation support, cost, product references, financial viability of the vendor, etc.) a new teller system (from here on referred to as TP) was selected and approved by the bank's executive management team. At the same time we selected IBM desktops, Compaq servers, HP and IBM printers, and Cisco routers. Novell NetWare was the network operating system for the eight locations already connected and another vendor provided the core financial system running on IBM 3090 hardware. The challenge was now to interconnect all of the new technology from the various vendors and make it function in a secure environment. This would include communications to each branch, user authentication on the desktop, and controlled Internet access to all users.

4.1 Wireless Implementation

It was now time to select a communications vendor to connect all of the branches together. After reviewing proposals from Sprint, Qwest, MCI, Broadwing, and AT&T, the MCI Frame Relay technology was selected based on price and performance. However, not all branch locations were accessible on the MCI network. For some locations this was due in part to their remote locale and for other locations the monthly recurring cost was not economically feasible. However, since each location needed to be on the network, we had to find alternatives. Wireless Local Area Network (WLAN) technologies appeared to be a viable option. Since Cisco routers were selected for the branch routers, we researched the Cisco Aironet 802.11b technology.

WLAN in its simplest form is an extension of the existing wired LAN using radio waves instead of copper or fiber. Since the same data that is protected by the wired corporate security infrastructure is traversing the WLAN, the same security standards still apply. One problem with this model is that WLAN usage is now the corporate LAN and can easily be extended beyond the physical security perimeter.

Additional challenges exist that make securing wireless data more difficult. For example, eavesdropping and unauthorized authentication are two primary issues. As stated in Security Architecture: Design, Deployment and Operations[1] "two primary security safeguards that should be considered when implementing WLANs are the degree of control that is required in identifying the remote user and the degree to which the network traffic must be safeguarded". Further, "several levels of security can be implemented to safeguard the WLAN". Therefore, the best way to secure the branches utilizing WLAN technologies was to utilize a defense in-depth strategy and not rely on a single piece for total security.

4.1.1 Wireless Defense in-Depth

We decided to implement multiple security measures in the installation of the Cisco Aironet radios. The first measure was the suppression of the broadcasts of the Extended Service Set ID (ESSID) by the wireless bridges. Although there are limited ESSIDs available and it traverses the WLAN in clear text, this is somewhat of a deterrent for a hacker to associate with the radios. Additionally, we configured MAC address restrictions on the radio hardware. We only allowed the two radios to talk to each other, and did not allow these radios to be aware of any other radios whose paths might cross ours.

Next, we implemented Wired Equivalent Privacy (WEP), which is typically used to pass network traffic back and forth between the protocol endpoints. However, several publications had recently surfaced stating that the WEP algorithm has a number of flaws. Nikita Borisov, Ian Goldberg, and David Wagner from University of California at Berkeley in their article "Security of the WEP Algorithm"[2] state:

> We have discovered a number of flaws in the WEP algorithm, which seriously undermine the security claims of the system. In particular, we found the following types of attacks:
>
> - Passive attacks to decrypt traffic based on statistical analysis.
> - Active attack to inject new traffic from unauthorized mobile stations, based on known plaintext.
> - Active attacks to decrypt traffic, based on tricking the access point.
> - Dictionary-building attack that, after analysis of about a day's worth of traffic, allows real-time automated decryption of all traffic.
>
> Our analysis suggests that all of these attacks are practical to mount using only inexpensive off-the-shelf equipment. We recommend that anyone using an 802.11 wireless network not rely on WEP for security, and employ other security measures to protect their wireless network.

According to Borisov, Goldberg, and Wagner Intercepting Mobile Communications: The Insecurity of 802.11[3] "WEP fails to accomplish its goals: Confidentiality, Access Control, and Data Integrity". These are fundamental for basic data security so additional measures had to be introduced.

In an effort to strengthen WEP shortcomings, we elected to implement four different (maximum allowed by Cisco) WEP keys that are rotated at certain time intervals. This would further deter packet hijacking due to the constant key changes. However, we still wanted higher encryption algorithms and looked for external encryption routers to serve this purpose.

We selected another Cisco product, the 1710 Encryption Router with 56-bit DES and ESP-MD5-HMAC authentication algorithm. We used this algorithm based on Cisco recommended implementation found in "Cisco Easy VPN Client for the Cisco 1700 Series Routers"[4.] Further, we used RFC 1827[5], RFC 2085[6], and RFC 2104[7] to understand and validate these algorithm variants.

For the final step in our defense in-depth strategy, we had to prevent unauthorized associations with the wireless hardware via the network numbering scheme. On the subnet between the 1710 routers on each end we used a long subnet mask (255.255.255.252) 10.100.x.0/30 to prevent IP spoofing. The subnet used to connect the two branches only allow the two 1710 routers behind the Aironet radios to communicate with each other.

Now that the WLANs were secured with a defense in-depth strategy, We began the planning the access control and account management phase.

4.2 Access Control and Account Management

We began to address data security and user authentication on the various applications. The bank had already established Data Owners, System Administrators, and separation of duties for it's various information system applications. By examination of the subjects (users) and objects (data), the bank used a role-based model for data security. However, the process for the myriad of systems, both centralized and decentralized, contained several security flaws. For example there were no standards for password length, password expiration, failed login attempts, and password history limitations across the various platforms. Additionally, each individual branch handled security differently exposing the bank to unauthorized access and potential fraudulent transactions. As noted in Network Security: Private Communication in a Public World[8], "user authentication consists of a computer verifying that you are who you claim to be. There are three main techniques: *what you know, what you have, what you are*". Since passwords are the first line of defense that fall into the "*what you know"* category and there were known/documented incidents of password sharing and written-down passwords, the bank needed to centralized its access control and account management. There was an overall Information Security Policy that addressed these items, but nothing specific for each system.

4.2.1 Single Point Authentication

The new TP system was designed for a user and PC to authenticate over a Wide Area Network (WAN) to an AS400 for electronic journal transaction history and gateway to the mainframe for actual bank account manipulation. Although the branches would no longer be using the old "Teller" system and its security shortcomings, the PCs, network, and AS400 posed more challenges to keep good access control processes.

We turned to the bank's core network operating system, NetWare, to find solutions to a centralized administration model and to resolve the shortcomings of the previous systems' account management. Novell's design goal was to simplify the access control process by providing a central service that performs authentication and/or authorization functions. Since NetWare's Directory Services (NDS) was already in use at the bank, expanding into the branches based on the NDS model and the role-based/least privilege access method employed by the bank would be a good fit. All user logon ID and passwords would authenticate to the NetWare tree and be centrally administered.

4.2.2 Password Standards Updated

Now that the infrastructure software was selected, we had to focus on the various applications security framework. I formed a committee to evaluate the best practices for password administration. It was comprised of the CIO, MIS Director, Data Security Officer, several business analysts for the various systems and me (Manager of Network Services). A gap analysis was performed on all the applications to determine if any system limitations existed that would restrict strong password policies from being enforced.

There were some limitations with the IBM Resource Access Control Facility (RACF) security package regarding password length, but all the other 28 applications could be reconfigured to meet the new standards. We set a date 60-days out and put a plan in place to synchronize all user IDs on the various bank applications. We used the Federal Financial Institutions Examination Council (FFIEC) [9] and Department of Defense Password Management Guideline[10] as guiding principles to develop the new password standards. The new bank standards met or exceeded the guidelines as set forth in these documents.

The new standards that apply to all users are as follows:

1. Must be a minimum of eight (8) alphanumeric characters with at least one character being an embedded numeric character
2. Must start and end with an upper case or lower case alpha character
3. Cannot contain redundant (repeating) characters
4. Cannot contain a trivial character sequence (i.e. abcdefgh)
5. No dictionary words or proper names (this applies to English, Spanish and other foreign languages)

The new standards that apply to **Administrative** level accounts are as follows:

1. All of the items in the above standard plus
2. Must be a minimum of ten (10) characters in length
3. At least one or more lower case characters and one or more upper case characters
4. At least one (1) embedded numeric and at least one (1) embedded special character such as @, %, *.

System settings standards:

1. Maximum password age: 60 days
2. Minimum password age: 1 day
3. Passwords must be unique
4. Lock account after three (3) failed login attempts
5. Enable logging of successful and failed logon attempts

To address the issue of Security Awareness, we distributed e-mail to all employees outlining the new password policies and guidelines. This memo included examples of good and bad passwords to help users further understand the changes. Additionally each user signed a Security Acknowledgment of receipt and understanding of these new policies.

5. AFTER

Once the network was fully installed in all locations and PCs were put into place the bank saw many benefits both from operations and security perspectives.

5.1 WLAN Considerations

The WLAN implementation has worked as expected. The bank was able to significantly reduce monthly costs to many bank locations while still providing a good network connection that is secure. In fact, the bank is starting to convert ATM units to this technology to further reduce costs.

Although security in the WLAN field is constantly changing, the defense in-depth approach has allowed the bank to keep its data secure. As one piece may become compromised with newer/cheaper technology to hackers, this method ensures the bank is not relying on one particular piece to keep its data safe. Additionally, as new technologies are being developed, the bank is able to implements new layers of security while not having to remove and/or compromise the existing defense mechanisms.

Future enhancements to the WLAN include upgrading the Cisco 1710 encryption routes to 3DES and considering converting to Wi-Fi Protected Access (WPA) on the radios. WPA uses Temporal Key Integrity Protocol (TKIP) as the protocol and algorithm to improve security of keys used with WEP. It changes the way keys are derived and rotates keys more often for enhanced security. It also adds a message-integrity-check function to prevent packet forgeries.

5.2 Access Control and Account Management

NetWare's NDS continues to be a good central management tool for account maintenance and a single point of authentication to the network. Centralized management has streamlined account administration, maintenance, monitoring and revocation to the network. Additionally, we have auditing capabilities and have implemented a network-reporting tool, KANE Security Analyst, to assist with detection and reaction of abnormal network access and activity.

To assist users with the new access control and password standards, I e-mailed all users with the standards with examples of good and bad passwords attached. Additionally, we distributed the updated Information Security Policy that each user must read and acknowledge every year. This has proven to be beneficial in enhancing user awareness of general information security and specifically password management and security. Although we still deal with the human factor (users) we have seen a decrease in password sharing and password compromise.

For future enhancements we plan to expand Novell's Lightweight Directory Access Protocol (LDAP) capabilities of the NDS Tree to incorporate RACF and Intranet applications. Novell's eDirectory 8.5 features an improved native implementation of LDAPv3 running over SSL, which provides fast searches, auxiliary classes, referrals, and controls that we are planning to review. EDirectory 8.5 also has biometric capabilities that will take network authentication (*what you know, what you have, what you are*) one-step further to incorporate "what you are".

We have been able to protect our investment in hardware and software with Novell's NDS model. eDirectory 8.5 is a truly cross-platform global directory that will operate on NetWare, Windows 2000, Windows NT, Sun Solaris, and Linux, thus ensuring compatibility with current and future systems.

5.3 Other Security Issues

- Many policies and procedures were developed or updated and placed on the Bank's Intranet for prompt distribution and referral
- All modems and dial-up lines were removed from all PCs within the company
- Internet access is now restricted and controlled with NDS security behind a firewall
- Security review guidelines were created to receive weekly reports from the Human Resources Department and reconcile current employees with active users on the network. Additionally, the updated security standards address who, what, and when security reviews will be done on the various applications
- Password unauthorized disclosure, modification, and removal was address with user awareness and protecting the password on the local workstations. Stopping the use of PWL files protected the password. We then implemented a registry setting on all computers across the Bank's network that prevents the PC from creating a PWL file, and forces the users to have a screen saver password. Lastly we force the screen saver password to be the same as the Novell password.
- We installed an automated software inventory program to assist with license issues and deter illegal software installations.
- We developed a company-wide virus protection program with automatic updates and scans on all servers and workstations.

6. **Conclusion**

In conclusion the project to automate and consolidate 85 locations into one wide-area-network had many challenges. Some challenges were technical, some economical, some were human related. We were able to increase operational efficiencies, enhance the security (confidentiality, integrity, and availability) of all bank data, and decrease monthly expenses once the capital equipment was amortized by only 50%.

References:

1. King, Christopher; Dalton, Curtis; Osmanoglu, Ertem, Security Architecture: Design, Deployment and Operations. Berkeley:Osborne/McGraw-Hill, 2001. 240 – 242.

2. Borisov, Nikita; Goldberg, Ian; Wagner, David: “Security of the WEP Algorithm.” URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

3. Borisov, Nikita; Goldberg, Ian; Wagner, David: “Intercepting Mobile Communications: The Insecurity of 802.11”. URL: http://students.cec.wustl.edu/~cs673/WEP.ppt, Slide 4

4. “CISCO 1700 SERIES MODULAR ACCESS ROUTERS”: URL:http://www.cisco.com/en/US/products/hw/routers/ps221/prod_configuration_guide09186a008007cfa7.html

5. Atkinson, Randall. “IP Encapsulating Security Payload (ESP).” August 1995. http://www.faqs.org/rfcs/rfc1827.html

6. Oehler, Michael; Glenn, Robert, “HMAC-MD5 IP Authentication with Replay Prevention.” February 1997. http://www.faqs.org/rfcs/rfc2085.html

7. Krawczyk, Hugo; Bellare, Mihir; Canetti, Ran: “HMAC: Keyed-Hashing for Message Authentication.” February 1997. URL: http://www.faqs.org/rfcs/rfc2104.html

8. Kaufman, Charlie; Perlman, Radia; Speciner, Mike, Network Security: Private Communication in a Public World. Prentice Hall, 1995. 205 – 222.

9. Federal Financial Institutions Examination Council, Information Technology Examiniation Handbook. URL: http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html

10. Department of Energy Intelligence and Security Directives and Instructions. “Password Management.” URL: http://www.fas.org/irp/doddir/doe/m5639_6a-1/m5639_6a-1_a-9-2.htm