GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

How safe is my money online?

Introduction

Most people trust their money to banks for several good reasons. Banks are regulated by the various federal and state agencies, and the money deposited is insured by those agencies. But even with the federal regulations and insurance, just how secure is the contemporary online bank? Banks started as secure depositories for currency, legal documents like deeds, bonds and other tangible assets. It was the responsibility of the bank to store the valuables and keep them intact. The bank assumed the responsibility to hold those assets until the customer requested them back. Banks created standards for recognizing who the proper owners are and how and when their assets can be taken in and returned. With the advent of ATMs and branch networks, banks had to take the lead in applying the basic concepts of security to financial data rather than tangible assets. You are paid by direct deposit, pay bills with online payment systems, bank by phone, wire transfer funds, and your student loan is repaid by automatically debiting your account. None of these types of transactions involve cash or even a piece of paper. A contemporary bank's fundamental reason to exist is to secure, transmit and receive data, a new asset.

The concept of financial data security can be broken down into three basic components, namely confidentiality, integrity, and availability. Confidentiality limits access to information only to the parties desired. Integrity adds controls so that no one other than the desired parties can make changes to the information. Availability just means that the owners of the information will have access to their information when needed. Confidentiality is maintained by signature verification, photo ID requirements, PIN selection, and written policy restricting banks from divulging account information. Integrity is maintained through physical security of vaults, cameras, armored cars, security guards etc. and through detailed audits and examinations. Availability of cash and account balances are set by branch and ATM systems. Moving to an online financial institution still requires the same three components of confidentiality, integrity, and availability, but with a different method of securing data and communication.

Securing data in the modern world.

Security is based around establishing a trust relationship between two or more entities. Trust is based on identification, authentication and authorization. Identification is a simple process of providing a basic naming system that sets a unique identity for each party. Authentication is a secondary process that is used as a confirmation of the identity. This confirmation means that each party must know something about the other or depend upon a third party trusted by both parties to verify the identities exchanged in the identification phase. Authorization is the granting of rights from one party to the other based on the identity and authenticity. Privacy is another key component to secure communications. No one other than the two participants should be able to listen to the

© SANS Institute 2000 - 2005 Author retains full rights.

exchange of information.

In the last few years, the Internet has given the bank a new path to the customer and when combined with powerful relational databases, the customer has the availability to bank any time and anywhere. This high availability means that for the first time, critical private data may now be transmitted over a public network. The same security principles that operate in a bank branch must work in the online environment. The bank must authenticate your identity, grant you and only you access to your account information, and have the system functional when advertised. To this end, Microsoft developed a specification and software set under the name "Marble" which later in 1977 became Microsoft Internet Finance Server Toolkit. [1] The MIFST specification is designed to be flexible and reuse as many software components as possible. Microsoft selected OFX/GOLD and some widely accepted software standards and promising tools to incorporate into version 2.0 of MIFST. MIFST 2.0 demonstrated enough improvement that some major bank software providers such as Marshall & Isley and OpenSolutions Inc. adopted it. [2]

The Tools

SSL

Secure Socket Layer defines a private channel of communication over the public network by installing itself over top of a reliable transport protocol, typically TCP/IP.[3] SSL provided the basic encryption technology framework that Netscape introduced in their first browser and that Microsoft incorporated in Internet Explorer starting with version 3.0. Encryption is the process of altering data to obscure it from being read by any other than then the intended parties. It was designed to allow higher layer protocols to enhance the security model by handling the basic components of providing for privacy, identification, and authentication portions of the security model. [4,5]

SSL vulnerabilities

The majority of attacks against SSL stem from the lack of signed certificates at both ends. [6] Also, RSA has documented a potential method to break the SSL session on an Apache web server[7] and similar vulnerability exists in Microsoft popular browsers as well. [8] All of these SSL vulnerabilities are quite difficult to exploit, requiring large amounts of data, greater than 300MB in the Apache case or additional planning and possibly altering DNS records to take advantage of the security holes in Internet Explorer. Still, there are many servers that companies have in production that lack all the security updates. Each of these servers is at risk and it is incumbent upon the administrators of those servers to eliminate the flaws in security. They must make sure that the flawed version 2 of SSL is not in use and that the key size is set to 128 bits. While none of the known vulnerabilities are serious threats, the fact that some have been found mean that in

© SANS Institute 2000 - 2005 Author retains full rights.

the future, more or better methods to break SSL will be found. [9] The basic security of storing a key in the browser presents an opportunity for a break in security. There are long lists of security holes in many of the popular browsers and it might be possible in the future to extract the SSL key form a target computer, and then masquerade as that computer and compromise the session security.

SET

Secure Electronic Transaction is a one of the newer standards dating back to 1997. Visa and MasterCard authored it as a way to "facilitate secure payment card transactions over the Internet."[10] It is based on a third party key authority to verify credit card and merchant validity. SET is broken into a series of 28 protocol messages that are accepted by a merchant server, cardholder software set, payment gateway, and certificate authority. A merchant server is a package to process debit or credit card transactions. A payment gateway is run by a third party that processes and obtains the merchant authorization to charge the customers account. The cardholder application or digital wallet is stored on the consumers computer or internet access device that stores the card holder identity, digital key, and reference information from the card to be charged for the transaction. The certificate authority is a trusted third party and verifies the digital certificates when requested by the other components of a SET message chain. It provides the customer added protection since their card numbers are never transmitted over the public network and protects the merchant by adding a feature of repudiation through the use of digital certificates. SET does not address the privacy issue since encryption is not directly addressed by the specification. SET must depend upon a secure transport provided by another product like SSL. SET duplicates and extends identification and authentication, while it adds authorization and repudiation. [10]

SET Vulnerabilities

Even though SET is very thorough at verifying identities and authorizations, a potential exists for compromising the transaction. The cardholder's computer with the certificate information could be stolen or duplicated. Employees at the merchant's location could redirect the transaction to a different merchant server and collect the funds from there. The key software components are all stored on the computers used in transactions creating opportunities to steal or copy certificate information and forge the identity of one or more of the protocol messages. [11]

OFX

Open Financial Exchange is a specification for exchanging financial information online. Checkfree, Microsoft, and Intuit developed the specification in 1997 to enable traditional financial service companies to use the Internet to conduct business between themselves and their customers. The goal was to give a common interface for all the disparate systems used by banks, brokerages, and service bureaus. Microsoft used it as

© SANS Institute 2000 - 2005 Author retains full rights.

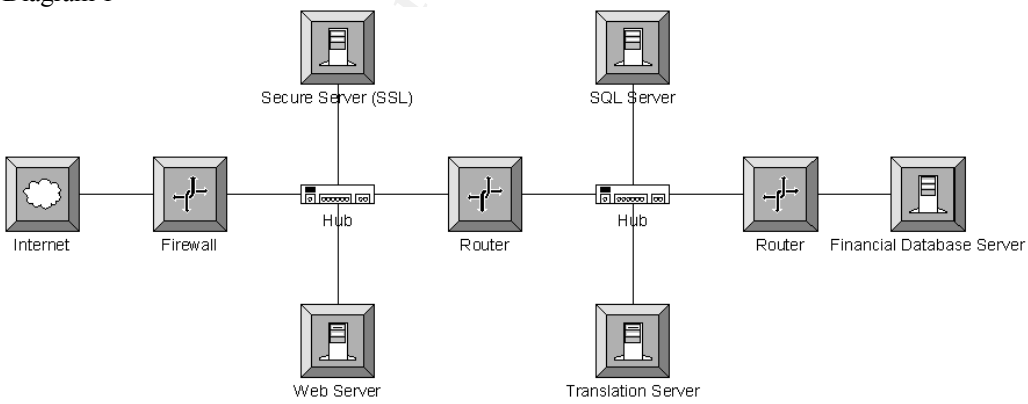
the basis for their Marble platform for electronic banking. Intuit also adopted OFX as the interface for their popular Quicken line of personal finance managers. OFX depends upon SSL for the basic message security, server authentication, and encryption of data. [12] OFX uses several security measures of its own. In the Microsoft implementation, the user name and password are included in each message to the OFX server.

OFX Vulnerabilities

There is a potential weakness in this implementation. The OFX server listens to all properly formed OFX messages. The MIFST specification does not include a test for failed signon attempts and depends upon the financial institution's application developer to check for invalid usernames and passwords. This lack of a valid ID check allows for a "denial of service" style attack by flooding the OFX server with invalid user name and passwords. There is a second, more insidious attack theoretically possible if the hacker is able to gain a valid user name by social engineering. Since the default specification for OFX does not track failed logon attempts, the hacker can than launch a dictionary crack against the valid user name and can watch for an accepted message from the OFX gateway server. If the application developer has not added some type of user name security to lock that system on failed attempts, the hacker would have a very long window of opportunity to attempt the dictionary crack of that valid user's password.

The Microsoft Marble specification also lacks some key security elements that should be added before it is used in a production environment. The initial implementation only uses one firewall to protect the financial web site from the Internet, but little protection from users inside the financial institution's network. (Diagram 1)

Diagram 1

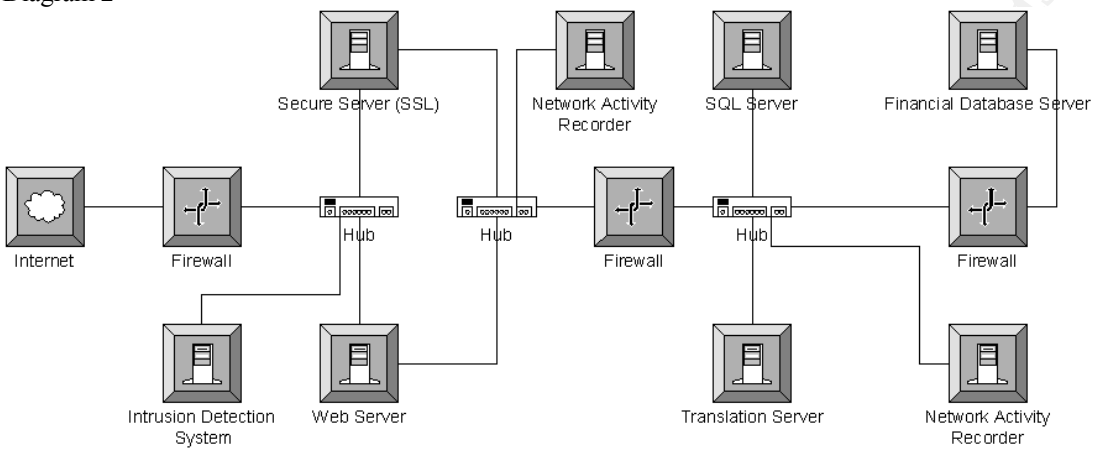


A better configuration would increase the security by adding more layers or depth to the system. Here, only the firewall will control network traffic. The routers can be used for basic traffic filtering, but they do not protect as well as a firewall system could.

© SANS Institute 2000 - 2005 Author retains full rights.

Forensic analysis and apprehension of the hackers would be difficult since there are few ways to monitor and record what happened in the event of a break in. (Diagram 2)

Diagram 2



Security is improved in this diagram since there are no more layers of separation between the Internet and the financial database server. Placing two network cards in the web and secure servers adds one layer, while the substitution of firewalls for routers adds more control to the traffic passed between layers. The intrusion detection computer monitors the activity at the firewall and the Internet connected servers to flag any suspicious activity from the Internet. The network activity recorders are servers running a network monitoring package like "Sniffer" or "tcpdump" and act like the flight recorders of a jetliner. Should something happen, they contain all the traffic that would permit experts to reconstruct the events prior to whatever goes wrong.

IFX

Interactive Financial eXchange (IFX) is a 1999 specification that adds on to the OFX standards and extends what OFX could do. [13] IFX still relies on a protocol for data encryption like SSL. It is similar to OFX in that its main function is authentication, identification, and authorization. It differs from OFX by increasing interoperability with XML. [14]

IFX Vulnerabilities

IFX is still a new standard and has no wide application to date. Since it is not in use, there have been no attempts from the hacker community to compromise the standard, at least for now. IFX is undergoing more intense scrutiny than most of the

© SANS Institute 2000 - 2005 Author retains full rights.

earlier standards. Only testing in the real world will determine if it is sufficiently secure. Its dependence upon SSL and XML mean that there may be ways to compromise IFX in the future. There may also be the typical exploits by passing invalid messages or messages out of sequence in an attempt to find implementations that do not perform integrity checks. Often the responses to these bad messages will yield useable results for the hacker.

Conclusions

One component often overlooked in all the various security models, methods, and protocols, is the end user's computer. No matter what financial service providers or certificate authorities do in software, hardware, or policies, they have no control over the end users' computer. That computer has stored all the digital certificates, most of the consumers' personal information, and quite often, usernames and passwords. People will use the password cache and auto complete features in their browsers which stores information in some very basic forms, even plain text. This use means the consumers' financial and banking data is only as secure as that computer. To further complicate matters, there are an increasing number of lap top computers used in home and in business. The theft of a portable computer means that they no longer have any security, and only the thief may have access to their data.

The advent of home broadband Internet connections has increased the risk of financial loss to the consumer. The banks' and the FDIC's insurance do not cover loss to a person from theft of the consumers user name and PIN or password. A home computer that is connected to an "always on" Internet connection is at risk from Internet hackers. The majority of consumers use one of the Microsoft Windows Operating System family to access the internet. There are many documented vulnerabilities on the Microsoft web site and patches are available for those. Most people do not take the time to apply the patches and even then, there are still risks. Some notable cases are the remote control applications like the Sub 7 and Back Orifice servers. Both of these remote access servers can be installed on a user's computer through an email attachment or hidden inside a seemingly innocuous program. Once installed, the hacker has full access to that computer and can copy any file or capture the user names and passwords. They can then remotely control that computer and easily assume the identity of the victim.

The best way to improve the consumers' online financial security is through education. The current collection of online financial transaction protocols is fairly secure. Any one alone is probably insufficient, but the combination of two or more makes the users' session information very secure. The financial institutions must educate their customers on the ways to minimize security risks on the customers' personal computers. Start with policy and instructions on the web site. Tell the users about the importance of keeping their computers physically secure. Make sure they understand the importance of protecting their user names and passwords. That unique name and password is the single weakest component of most security models, at least until some form of biometrics or other equally unique identifiable characteristic can be used. Show the customer how to test their systems security as on Steve Gibson's Shields up site [15] and how to download

© SANS Institute 2000 - 2005 Author retains full rights.

patches and updates from Microsoft. [16] Broadband customers must take added care and protect their systems because of the greater threat from the "always on" Internet connection. Give the customer links to common vendors of personal firewalls and also give links to the ISPs that offer the filtering or security gateways.

Financial institutions are vulnerable to some extent as well. It does not matter how good the systems in place are if there is a break in the security of the internal audit procedures. This would be a traditional case of bank embezzlement or employee fraud complicated only by the speed of online processing. The financial institution must trust the bank employees and enforce that trust with policy, procedure, and audit. Background checks for all key personal at the financial institutions and the certificate authorities should be required and that requirement should be listed as part of the institutions security policy statement. The financial institutions must maintain the separation of duties and have two separate reviews of these policies and work procedures. Chartered banks are required to have safety and soundness audits performed on a regular basis. Consumers should only use banks with the FDIC insurance and a published security policy.

Financial data security is not a single step or goal, but an ongoing process. It requires constant vigilance from the consumer, financial service provider, and online merchant to protect themselves. If any of the parties fails to maintain a secure system, all may be at risk. Just because a system is secure today does not imply that it will be secure tomorrow or the next day.

1. Newsbytes: Microsoft Delivers Internet Financial Technology Kit
   http://www.nbnn.com/pubnews/97/104432.html
2. Microsoft Charts Course for Version 2.0 of Internet Finance Server Toolkit
   http://www.microsoft.com/PressPass/press/1998/Apr98/MIFSTpr.asp
3. SSL Protocol 3.0
   http://home.netscape.com/eng/ssl3/draft302.txt
4. How SSL works
   http://developer.netscape.com/docs/manuals/index.html?content=security.html
5. Analysis of the SSL 3.0 protocol
   http://www.counterpane.com/ssl.html
6. Attacks against SSH 1 and SSL
   http://slashdot.org/articles/00/12/18/0759236.shtml
7. SSL Vulnerability in Apache
   http://www.lists.aldigital.co.uk/apache-ssl/msg00422.html
8. Microsoft IE "SSL Certificate Validation" vulnerability
   http://www.ciac.org/ciac/bulletins/k-049.shtml
9. SSL Security Server Survey
   http://www.meer.net/~ericm/papers/ssl_servers.html
10. Secure Electronic Transaction LLC. What is SET?
    http://www.setco.org/set.html
11. Vulnerabilities in the SET specification

© SANS Institute 2000 - 2005 Author retains full rights.

http://home.pacbell.net/panero/crypto/set.html
12. Open Financial Exchange Security Document
http://www.ofx.net/ofx/ab_sec.asp
13. Introduction to the Interactive Financial Exchange Specification
http:// http://www.ifxforum.org/ifxforum.org/ifx_right_main.htm
14. The Oasis XML Cover Pages – Interactive Financial Exchange
http://www.oasis-open.org/cover/ifx.html
15. Gibson Research Center Shields Up!
http://www.grc.com/default.html
16. Welcome to Windows Update and Product Updates
http://windowsupdate.microsoft.com

© SANS Institute 2000 - 2005, Author retains full rights.

Last Updated: July 28th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
Community SANS Indianapolis SEC401	Indianapolis, IN	Oct 09, 2017 - Oct 14, 2017	Community SANS
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event