**Proceedings of GLOGIFT 08**
June 14-16, 2008
Stevens Institute of Technology
Hoboken, NJ, pp. 196-201

# SECURE E-BANKING

**Nirmalya Chakraborty* and Jayanthi Ranjan****

**ABSTRACT**

*In this paper I have described the current situation, concerning alternative channels in security measures in the e-banking sector. There is a need to examine the business motives for additional safety levels for the offered banking services. Some implementation details of e–Banking (Internet / Phone / Mobile Banking) are also presented and I conclude with a comparison with alternative potential solutions and future technology improvements expected.*

**Keywords:** *security, OTP, Internet Banking, two-factor authentication*

## Introduction

During the last two decades banking industry has adopted new service channels (alternative channels), based on technology progress. The most widely known are ATMs, Internet / Mobile Banking and Phone Banking. With the alternative channels a customer is able to perform banking transaction without his physical presence at the Branch and, very often, while being abroad. As a result, security is the ultimate prerequisite for performing successful operations and establishing confidence to the alternative channels customers. Security measures differ, according to each separate channel and follow certain rules established by each Bank, as a part of its security policy. Very often Banks should comply with regulations defined either from international organizations or from local authorities. Because of the many kinds of threats, which have been recently appeared on alternative channels, Banks are obliged to implement higher security levels. Thus, a security analyst should visualize the access, authentication, authorization, and privacy controls necessary to protect the entire transaction.

## The Scope of Security in e-Banking

The assets in an e-banking sector should be mapped in aligned with the business objectivity of providing secure service. The assets in an e-commerce system can be:

1. Customer names and databases
2. Credit-card numbers
3. Web-server availability

The need for securing each of the following assets should also be categorically understood. The needs in general should be:

* Senior Lecturer, Banarasidas Chandiwala Institute of Information Technology
New Delhi, India, nir_net@yahoo.com

** Associate Professor, Institute of Management and Technology (IMT)
Ghaziabad, India, jranjan@imt.edu

1. Encryption of the network connection
2. Locating data on separate databases and encrypting the data.
3. Firewall with DoS protection capability
4. Redundant servers

The Implementation should also be prioritized according to the architecture implemented. The Priorities can be:

1. Install the firewall
2. Harden the web-server
3. Implement encryption
4. Implement a secure database
5. Live the system

## The Road Map towards Secure Banking

The realistic procedure of implementation of the security controls should be well defined and I am presenting the most logical methods towards implementing it.

- Explicit responsibility should be assigned for establishing and maintaining corporate security policies
- Sufficient physical controls should be established to provide a secure area to house the e-banking systems including armed guards, CCTV with motion sensors, smoke and fire alarm systems, and biometric authentication like fingerprint or retina scan
- Security profiles should be created and specific authorization privileges assigned to all users of e-banking systems including customers, internal users, and system administrators and outsourced service providers. LDAP-based directory solutions or Identity management solutions can be used for an effective implementation of this requirement.
- Storage of sensitive data on organization's desktop and laptop systems should be minimized and properly protected by encryption, access control and data recovery plans
- Preparedness for meeting the credit card companies' requirement takes about a year.
- Staff can start by documenting their intentions in a written security policy.
- Then they can roll out a company-wide process for keeping OS and software up-to date.
- They can segment the network so that systems handling customer information are separated from other systems on the network.
- They can implement 128-bit SSL on their website and separate e-commerce application, customer database, and the web server from each other on separate physical servers protected by network access controls.
- They can decide to use software that did not store the actual credit card numbers on the customer database but instead stored a one-time hash of the same number when supplied by the customer.
- They can implement IDS and hired staff to be responsible for managing and monitoring network security.

Security for a credit card number should also include securing the systems on which it resides, the network attached to that system, the other systems on its network, non-computer

equipments like fax machines and phone switches attached to that network. It should also include securing the processes and procedures that affect that credit card number such as system administration, backup tape rotation and handling, and background checks and hiring and termination procedures. Securing the data means discovering its path throughout the system and protecting it at every point.

### False Sense of Security

Firewalls do not block all unwanted access. All firewalls allow some access into the network from the outside. These can be e-mails, DNS, Java on browsers, and VPN connections.

Many companies use MS Outlook Web Access for mailing that can be compromised through weak passwords bypassing the firewall.

Firewalls can also be bypassed using well-crafted packets that confuse the firewall capability like fragmented packets or ICMP messages tunneling into a working firewall.

Dial-up Modems that dial a user into the internal network are also threat vectors that bypass the firewall totally.

### Online Banking Fraud Schemes

Most online banking fraud schemes involve two steps. First, the criminal obtains the customer's account access data, i.e. logon name and password. Second, the criminal uses this information to transfer money to other accounts and withdrawals the funds. For the first step, criminals have employed different schemes in the past:

The "over the shoulder looking" scheme occurs when a customer performs financial transactions while being observed by a criminal. A fair number of cases have been reported where the criminal obtained customer's account access data just by observing customers at a public Internet access point.

The "phishing" scheme involves using fake emails and/or fake websites. The word "phishing" stems from combining the words "password" and "fishing". Criminals send emails that appear to be from the customer's bank that direct customers to a fake website. This website impersonates the bank's website and prompts customers for their account access data. Over the past months, most banks have executed customer education programs, thereby reducing the effectiveness of this scheme. It will, however, take awhile before all customers are smart enough to extinct phishing.

The "Trojan horse" scheme is based on embedding a computer virus type software program onto the customer's PC. Trojans often tie themselves into the keyboard driver and record keystrokes. Once a Trojan detects that the customer opens an online banking website, it captures login name and password, and sends it to the criminal.

In the year 2003, phishing was the dominant fraud scheme. In the year 2004, banks experienced a sharp rise in Trojan fraud scheme attacks.

### One Time Passwords

To improve security, some banks use "one time passwords", also called OTP. Upon activation of the customer's account for online banking, the bank mails a list of OTPs to the customer. Each time the customer perform a transaction, he enters one OTP for verification. Once used, the OTP becomes invalid. If the customer runs out of OTPs, he is sent a new list.

While this approach effectively prevents "over the shoulder looking", it generally fails to

prevent other fraud schemes. Phishing emails also ask for OTPs, and a customer naive enough to give out his logon name and password will likely also provide OTPs.

Trojans simply also capture the OTP once entered. At the same time, they falsify the customer's input in the browser software (e.g. by adding an invisible character) or cause the browser software to crash. This causes the customer's transaction to be intercepted and the OTP to still be valid. The criminal can then use this valid OTP to perform a fraudulent transaction.

### Hardware Tokens

The high-tech alternative to paper OTP lists is "hardware tokens". These devices have the form factor of a key chain attachment, featuring a crypto processor and a display. A hardware token displays a new OTP every 60 seconds. Because each OTP is only valid for a limited period of time, they provide significant protection against "over the shoulder looking" and phishing schemes.

Hardware tokens can, however, not protect the customer against Trojans. The fact that the OTP is only valid for a short time just reduces the amount of time the criminal has to exploit the data obtained by the Trojan. Because many criminals already use automated scripts on their servers to perform fraudulent transactions once the access data is received from the Trojan, the time limit proves no significant barrier to the criminal.

In addition, some banks have discovered Trojans that perform the fraudulent transaction right from the customer's PC. As this involves next to no delay, the hardware token approach fails to prevent Trojan fraud schemes.

### Transaction Specific OTPs

The shortcoming of both paper OTP lists and hardware tokens lies in the fact that each OTP is not transaction specific. That is, the same OTP can be used to verify either a genuine or a fraudulent transaction. One possible way to come by this flaw is to use a "key generator" device that generates an OTP based on primary transaction parameters.

A key generator looks similar to a pocket calculator. It has a keypad that lets the customer enter the source account, target account, transaction amount, and a PIN. Based on these parameters, the key generator generates a transaction specific OTP. The customer now enters the transaction parameters into the online banking application including the generated OTP. When the bank's server receives the online transaction, it performs the same calculations as the key generator and thus verifies the OTP.

If a criminal captures such an OTP, he cannot use it for a fraudulent transaction, since this OTP can only be used to verify a transaction with the same parameters as entered on the key generator. Because the key generator is a separate hardware device with no connection to the Internet, it is immune to getting attacked by malicious software.

For these reasons, key generators can be considered a highly effective fraud prevention measure for online banking capable of preventing all known fraud schemes. The disadvantages of key generators are, however, the cost of the device, the fact that the device must be physically present to perform online banking, and the fact that the customer basically has to enter each transaction two times.

### OTP by SMS

Some of the disadvantages of using key generators are avoided by sending OTPs to the customer using SMS. With this approach, the customer first sends the complete transaction to the bank's server. The bank's server then creates a random number as OTP and sends it to the

customer's mobile phone as text message. The customer now enters this transaction specific OTP into the online banking application, and sends it also to the bank's server. If the generated OTP matches the one transmitted by the customer, the transaction is verified.

Because the OTP transmitted can only be used to verify the transaction that is already received by the bank's server and cannot be altered from the outside, this OTP is of no use to a criminal. In theory, sending OTPs by SMS should hence be as effective a fraud prevention measure as a key generator. In reality, banks have experienced that the weak point is the mobile phone identification. Effective fraud prevention is only provided if any change of mobile phone number is performed only after thorough identity checking.

Another disadvantage of this approach is that banks need to tie in their infrastructure with the infrastructure of a wireless operator. Wireless operators all over the world are investigating ways to leverage their existing infrastructure into new sources of profit. Most operators hence look into providing financial transaction services of various kinds. Banks hence may soon find themselves in a situation, where wireless operators offer their customers financial transactions using just the mobile phone and nothing else. The bank's offering would involve using first an Internet browser, than wait for an SMS, read it, go back to the Internet browser, type in the OTP and erase the SMS. For a customer, the bank's offering appeals to be a lot more complex than the wireless operator's offering.

### Smart Cards and USB Tokens

Smart cards and USB tokens implement a different approach to authentication. Smart cards contain crypto processors without a display. They must be electrically connected to the customer's PC using a card reader device. USB tokens are essentially the same, only that they render card readers unnecessary by plugging directly into the customer PC's USB port.

By exchanging crypto keys with the bank's server, the bank's server can be sufficiently sure that the online transactions secured with this approach stem from the genuine customer. While smart cards have been hacked in the past, the latest generation smart cards will likely provide a high level of fraud protection for many years.

The disadvantages of the smart card approach lie in its need to by electrically connected to the customer's PC. This connection requires the installation and configuration of specific hardware drivers. In many pilot rollouts of smart cards, this turned out to be a frequent source of customer support needs.

The other disadvantage is that the need for the electrical connection limits the use of online banking. Many customers perform online banking from their office. Installing card reader hardware and drivers is often not possible for managed office PCs. Also, recent electronic organizers and smart phones provide Internet browsers that are well capable to perform online banking, but offer no capabilities to connect a smart card reader or an USB token.

### Transaction Monitoring

A completely different approach to secure online banking comes from the adaptation of fraud prevention systems used with credit and debit card processing. In payment card processing, fraud is a known phenomenon since many years. Technical security measures introduced to payment cards, such as magnetic stripes or chips, have only provided temporary relief from fraud losses.

The only measure that has proved to limit fraud losses permanently was the deployment of transaction monitoring software. This has become the de-facto standard for fraud prevention

with payment card processing worldwide.

Transaction monitoring occurs in the bank's data centre. For each transaction, the transaction monitoring software scrutinizes the current transaction's parameters, and compares it with the previous transaction of both the customer and the counterparty of the transaction histories. By comparing the current transaction pattern to stored known fraud patterns, the software can flag suspicious transactions "on the fly". Such transactions are then referred to a call centre for manual verification.

There are multiple advantages to this approach when compared to the others discussed before. There is no new device to be used by the customer, no dependency on mobile phones and no customer support problem with hardware driver installation. There are also no one-time costs per customer for a card reader or an USB token, and no per-transaction cost for sending SMS.

## Comparison

But what are the disadvantages of transaction monitoring? One problem arises when a new fraud pattern emerges, which is not stored in the transaction monitoring software. Another problem arises when by accident the current genuine transaction patterns resemble a known fraud pattern so much that the transaction monitoring system refers the genuine transaction to the call centre.

The first problem exists with any fraud prevention measure. Once criminals find a way to circumvent the measure, the door to fraud is open. The question becomes what can be done in this case. If the fraud prevention measure involves devices that are distributed to the customers, fixing the security problem becomes difficult. When the French credit card chip system was hacked, retrofitting point of sales terminals to patch up security was estimated to cost 5 billion U.S. dollars. Transaction monitoring provides a significant advantage in this case because it is centralized. By adding the new fraud pattern to the fraud detection logic in the bank's data centre, the entire system becomes instantly "immunized".

The second problem also occurs with any fraud prevention measure. Any measure will impose a certain customer disturbance. Smart cards and USB tokens may cause trouble when their hardware driver becomes incompatible with any change of the customer's PC. And like hardware tokens and key generators, all extra electronic devices have certain likelihood to fail or get lost. OTPs send by SMS may get lost or delayed, in particular with International roaming. Transaction monitoring software will inevitable generate a certain rate of false alarms. Banks must carefully determine which level of customer disturbance they consider acceptable for the security level needed.

## References

1. http://www.netproactiveservices.com/content/article11.htm
2. http://pci2007.upatras.gr/proceedings/PCI2007_volB/B_559-570_Marinakis.pdf
3. http://www.securitysearch.com/