4th WSEAS Int. Conf. on E-ACTIVITIES, Miami, Florida, USA, November 17-19, 2005 (pp118-122)

Safety Enhancement Measures for Online Transaction ; Case study of Internet banking in Korea

JAE-SUK YUN, WON-YOUNG KANG
Infrastructure Protection Division
Korea Information Security Agency
78, Garak-Dong, Sonpa-Gu, Seoul
South Korea

Abstract: The rapid development of the Internet and the amount of people who are beginning to gain or already have access to the Internet is phenomenal. As more people are beginning to log on, the range of abilities of the internet is starting to diversify, from online auction sites, shopping at home, and of course, doing banking through the Internet. However, there was an Internet banking hacking incident, which two hacked into the Internet banking system of a local bank by installing a program to find out personal identification numbers (PIN) and electronic certificate information used for Internet banking. The hackers used a hacking program installed at a computer on a PC room, which is very common in Korea, when hackers visited a certain Web site with the computer. The victim used Internet banking without knowing the installed program was sending his PIN number and personal information to the hackers. The program used the 'key stroke' method, which sends hackers whatever the victim types on the keyboard. And also there should be prompt precautions for new type of financial fraud, "phising", a technique whereby the websites of known institutions are entirely or partly copied and e-mails are used to obtain private or confidential data of the customers of those institutions and this fraud affects users' credibility on online banking system. Internet banking seems to be the way of the future, and with the rapid advances of technology and the internet, online banking will continue to grow. Therefore it is very important and imminent issue to build safe and reliable environment. So, in this paper, vulnerabilities in Internet banking system are analyzed and several measures for trust building of internet banking are suggested.

Key-Words: - Internet Banking, Hacking, PIN, OTP, cyber space, information infrastructure

1 Introduction

Numerous factors — including competitive cost, customer service, and demographic considerations — are motivating banks to evaluate their technology and assess their electronic commerce and Internet banking strategies. Many researchers expect rapid growth in customers using online banking products and services. The challenge for national banks is to make sure the savings from Internet banking technology more than offset the costs and risks associated with conducting business in cyberspace.

Internet banking, which was introduced in Korea six years ago, is emerging as the dominant means of online transaction and banking method for customers nowadays. According to the Bank of Korea (BOK), Internet banking, including transactions via mobile phone Internet services, has overtaken transactions via bank tellers. Internet banking has reached 30.5 percent recently and banking with tellers fell to 30.6 percent.

Banking through cyber space continued to surge over the past few years in Korea. After staying at 11.7 percent in June 2002, it rose to 18.8 percent in June 2003 and 25.7 percent in June 2004.

It's quite natural for people to prefer Internet banking, which is more convenient and charges lower fees. Service charges on account transfers and money remittances via bank tellers at branches range between 600 won(app. USD 0.5) and 2,000 won.(app. USD 2) in Korea.

However, there was an Internet banking hacking incident, which two hacked into the Internet banking system of a local bank by installing a program to find out personal identification numbers (PIN) and electronic certificate information used for Internet banking.

The hackers used a hacking program installed at a computer on a PC room, which is very common in Korea, when hackers visited a certain Web site with computer. The victim used Internet banking without knowing the installed program was sending his PIN number and personal information to the hackers. The

program used the `key stroke' method, which sends hackers whatever the victim types on the keyboard.

In this regard, there was a wide spread warning, which some measures have to be taken in government, and public level.

2. Information Infrastructures in Korea

In an effort to grow into a global leader in ICT, Korea has embarked on the two initiatives' "Cyber Korea 21" in 1999 and "e-Korea Vision 2006" in 2002. As a result, it presently has the world's highest broadband penetration rate. With yet another program "Broadband IT Korea Vision 2007," Korea aims to become a world leader in information infrastructure.

Korea ranks second across the world in terms of Internet users, which stand at 35 million as of 2004. The wide spread use of the Internet is attributable to the nationwide deployment of optical cables and a variety of broadband Internet services including wireless LAN. Korea is planning to provide a seamless Internet service through wired, and wireless convergence services such as WiBro(Wireless Broadband), and next generation internet services.

Korea launched the world first commercial service of CDMA in 1996, which was greatly contributing to the expansion of the telecommunications market. At present, Korea has 35 million mobile subscribers with an over 75% penetration rate, and out of which as many as 28 million users are subscribed to CDMA 2000 1x or above. This figure well illustrates that the Korean ICT market is truly "new technology friendly."

However, this also has consequences of issues regarding data protection, privacy and consumer rights which are the topics of recent legislation in Korea.

3 Security in Internet banking

Security is paramount. International experience suggests that Internet banking customers tend to be more price-sensitive and hence more likely to move their deposits from one bank to another. This tendency is reinforced by the convenience of conducting Internet transaction. Technology failures that disrupt or impair services may trigger abnormal transactions by customers.[2] Commentators have argued that it is not the electronic component of banking that is raising problems for regulators and legislators, but the digital aspect of this technology, which is being used as backbone of the Internet banking, which is core problem. This is because, when text, sound or images are in digital form, they can be altered, revised, transformed and transmitted in myriad ways. In short, the 'digital' bridge between bankers and customers can be easily breached. Furthermore, since money is involved, there is great incentive to breach this bridge.[3]

The threats to the security of Internet banking systems and the consequent losses could derive many sources such as international, external or internal attacks-mainly with the aim of financial gain-malfunctions and technical problems of the system, customer misuse or inadequate design and improper implementation of electronic banking and money systems in the part of the banks.[4]

According to the 1996 report of the Task Force on Security of Electronic Money, the security risks of the system and the proposed respective measures were grouped mainly into three categories as follows;

1. Prevention measures, including tamper-resistance of devices, cryptography, online authorization, additional verifications during transactions, supervision and monitoring by a central operator.
2. Detection measures, such as transaction traceability and monitoring, interaction with a central system, limits on transferability of electronic money and statistical analysis of payment flows.
3. Containment measures, including among others, limits on the value stored, expiration dates on devices and on value, registration of the identity of the users with the issuer or a central authority.

The multitude and variety of the solutions and the rapid evolution of technology have made the Task Force conclude that, 'It is the combination of measures, together with the rigors with which they are implemented, that will serve to reduce risk most effectively. Thus, it is more important to focus on the overall security risk management approach for a particular product, rather than use of individual measures.

4 Current status of Internet banking in Korea

Korea has led the online banking trend, including both Internet banking and mobile banking, thanks to its

tech-savvy citizens and state-of-the-art infrastructure for both the Internet and Web-capable cell phones.

Fixed-line access to the Internet is ubiquitous across the country with about 12 million out of 15.5 million households hooked up to the always-on Internet. More than 30 million people out of Korea's 48 million carry mobile phones that can be connected to Internet-on-the-move services. Korea's world-envied infrastructures enabled online banking, and tech-aware Koreans braced for the burgeoning new online banking offerings. According to the Bank of Korea (BOK), the number of transactions on the Internet almost doubled in two years from 4.8 million in 2002 to 8.7 million last year.

As of the end of 2004, Internet banking users amounted to 24.3 million compared to just 4.1 million in 2000. Everyday up to 10 million banking transactions are performed in cyberspace. The central bank also said the number of mobile banking transactions jumped about six-fold in two years from 1.1 million in 2002 to 6.3 million in 2004. Online banking, including transactions through the Internet and cell phones, is expected to soon emerge as the primary means of banking. Nineteen domestic banks in June saw their online banking usage continue to surge, rising to 30.5 percent while banking with tellers fell to 30.6 percent.

Internet banking is expected to rise above traditional banking with tellers soon because Internet banking is more convenient and economical with lower service fees. Service charges on account transfers and money remittance via tellers at bank branches range between 600 won and 3,000 won. By contrast, Internet banking charges only 300-600 won for the same service.

In addition, with the introduction of a cheaper Internet platform of wireless broadband, named WiBro, in 2006, the country's dependence on online banking is expected to further increase. Primary fixed-line operator KT plans to embark on a commercial service of the homegrown mobility-specific Internet next April at an affordable price. WiBro, also known as the 2.3-gigahertz portable Internet due to its bandwidth, enables people on the road to remain connected to the Internet at the speed of current fixed-line broadband.

However, such cutting-edge infrastructures and high usage rates of online banking are not all a bed of roses. Thorns have emerged. In May, two hackers installed a key-logger, which logs every stroke to harvest private information like user names or passwords, at a computer in an Internet cafe and obtained a female user's data, necessary for Internet banking. They then drew out 50 million won ($48,000) from her bank account after transferring the money to five different local banks. The accident surprised the nation because Korea's Internet banking systems were believed to be 100 percent secure because of their requirement of multiple authentication processes. Indeed, the banks shelled out big bucks to create a system impenetrable to outside attacks but they paid little attention to the possibility that customers' information can be leaked from the outside.

After the Internet cafe incident, The Bank made anti-key logger programs mandatory for Internet banking service subscribers and also overhauled its security card system. Experts point out that the incident shows how the nation should react to the emerging strain of Internet banking hacking and identity fraud.

Internet banking system were found some vulnerabilities. First, insufficiency of using security program on internet banking site. Seconds, insufficiency of security cards management & administration on internet banking. Third, vulnerable for identifying method of issuing accredited certificate online. And fourth, Vulnerability of management program for accredited certificate.

Recently, Most Korean banks have invested heavily in making their Internet banking systems invulnerable to invasion. But hackers managed to outfox the banks because they targeted unsuspecting customers instead. So there was warning the two incidents should serve as a wake-up call for banks since they have left the security of customer information to the customer themselves outside banks.

With the advent of the Internet and mobile phones, changes were made in the way people undertook transactions and payment. Instead of visiting bank branches in person, they could check their balances, view transaction records and perform transactions via the Internet or Internet-enabled mobile handsets.

Korean banks have an advanced Internet banking system with multiple layers of security. In the United States, most online banking systems still use single password protection. Such a complicated authentication system helps prevent online fraud attempts or identity theft. But swindlers look to invade customers' computers rather than banks' central systems. The really vulnerable point is the client.

5 Security status of Internet banking in several regions

In Europe, phishing, keystroke logging and other types of scams are increasingly worrying users of online banking services while scaring others away. To retain online customers and win new ones, banks will need to change many consumers' belief that online banking isn't safe. That means banks can't rely solely on governments or ISPs (Internet service providers) to make the Internet a safe place to do business but must deploy or strengthen two-factor authentication -- such as PIN (personal identification number) and TAN (transaction authorization number) -- and educate Net users about security precautions, such as firewalls.

European consumers are losing trust in the Internet as a channel for doing business as computer attacks on them and the companies they do business with mount. Just 30 percent of the 22,907 Europeans polled by Forrester said they are confident of the security of personal financial information, such as credit and debit card numbers, when used to make transactions online. Two-fifths of the interviewed Net users who don't use online banking said they have no plans to do so in the future because of security concerns.

Equally troubling, security fears don't just keep some consumers from signing up for online banking services, they cause some existing online banking users to stop. In the U.K., for instance, 1 million Net users tried online banking and gave it up by 2002, according to Forrester. Nearly 30 percent cited security worries. Similarly, in the U.S., around 3 million Net users have stopped using online banking services, with a third of them also citing security concerns, the market researcher said.

A recent study by analyst Forrester Research has unearthed conflicting views about the safety or otherwise of online banking. The survey of 11,300 UK net users found that while many online banking consumers are complacent about security, a large minority have given up online banking as a direct result of security fears.[1]

Most UK net users are aware of security threats like phishing and keystroke logging but are unfazed by these risks and expect their banks to deal with the problem - even though these attacks are thrown against consumer's PCs rather than a bank's own systems. Ideally users want banks to supply a blanket guarantee against fraud.

Based on responses to its survey, Forrester concludes that an estimated 600,000 from a total of 15m subscribers have ditched online banking as a direct result of security fears. Forrester reckons that users are confused and banks need to step up their efforts to educate customers about online fraud. Measures to restrict the functionality of some accounts (for example controlling how much money can be transferred on any day), stronger internet banking authentication and improved customer profiling are also needed to defend against security threats, it advises.

In addition to people who plan to drop net banking accounts as a result of security fears, another fifth of net users say that security fears will stop them ever banking online. Net users don't know what to think about online banking security. Without the technical knowledge to judge the severity of security threats like keystroke logging and phishing or, frankly, much interest in acquiring that knowledge people struggle to reach a balanced judgment. The result is that about half of the UK's Net users are either complacent or paranoid about online banking security. So UK banks are still facing with communication and security problems.

Many European consumers think online banking is less safe than paying by card in a restaurant. However, online banking security fears are noticeably lower in countries, such as Germany, the Netherlands and Sweden, where banks have introduced two-factor authentication policies. In Germany, for instance, most banks require online banking customers to have their own confidential PIN and a list of TANs to make money transactions online. Some, in fact, now require a third identification number.

6 Safety enhancement measures of Internet banking in Korea

Next December, the Korean government plans to adopt a strengthened personal identity authentication system for Internet banking called the one-time password (OTP) formula. Although the system is not mandatory, banks and individuals are likely to embrace it because those who use the format will be given incentives, such as a higher daily transactions ceiling, on top of better security.

The Ministry of Information and Communication (MIC) recently revealed a policy package aimed at thwarting identity theft in online transactions including the OTP. OTP verification refers to a security system that requires a new password every time a user authenticates him or herself, thus

protecting against an intruder attempting to use an intercepted password.

A small terminal generates a series of passwords six to eight digits long used to log on to an Internet banking site. It changes the OTP every minute so that hackers cannot use stolen OTPs. Up until now, banks resorted to security cards with 30-35 passwords and the system led to the country's first Internet banking crime in which individuals captured passwords with a key-logger program. Korean government expects OTP to become mainstream because it could set higher transaction ceilings for OTP users than security card users.

People using OTP and digital signature certificates will be allowed to transfer 500 million won a day on the Internet beginning next December, 10 times more than users of traditional security cards. Also in time with the full-fledged launch of the OTP, small-sized OTP terminals to be developed that they can be embedded into cell phones or a key ring. In addition to that, over the long haul, a single OTP terminal will be able to provide passwords for multiple banks by integrating servers of the banks.

Internet banking has caught on as the number of Internet banking trading stood at 9.24 million cases during the second quarter of 2005, accounting for 75.5 percent of total financial transactions in cyberspace. Along with the OTP system, the MIC looks to build and distribute new anti-hacking software with stronger security capability this year by teaming up with the Financial Supervisory Service.

In addition, Internet users will have to install firewall program for all kinds of online financial transactions, such as stock trading and insurance, to prevent hackers from stealing personal information starting in December. Thus far, only Internet baking users have been required to install the firewall software.

7 Conclusion

Internet banking has come to age as an arms race between financial institutions and public network attackers. Although the accident in Korea was conducted through an Internet cafe computer, in the future hackers are likely to gain access to vulnerable home computers and intercept the password as it is typed in. In this regard, the most important thing is that people should be cautious about Internet banking. Most of all, Internet banking users need to abandon the belief that Internet baking is safe. Customers must take various measures to make it even tougher for hackers. There are many people who are very cautious in managing bank accounts and passwords in the real world but become careless in performing Internet banking. It will be a good example switching passwords regularly as a good way to discourage fraudsters.

Banks also need to educate their online banking customers about security precautions. Many customers have only a vague understanding of the complex range of security risks they face, such as phishing and keystroke logging. Banks need their customers to help fight these attacks because they are more difficult to spot and defend against than direct attacks on the banks' own systems. Also efforts such as the installation of firewalls and periodic upgrades of anti-virus software would be helpful. However, Internet banking users need to stay alert because hackers can bypass the shields.

Security in Internet banking is not guaranteed by just bank, customer or government's effort but holistic and concerted cooperation with participants in this area should be made together.

References:

[1] http://www.theregister.co.uk/2005/09/07/forrester_ebanking_survey/

[2] Ramin Cooper Maysami, "Financial E-Regulation in Singapore: Global Issues un Supervision of Internet Banking", 2000, J.B.I. 225, 229.

[3] D. Johnston, S. Handa and C. Morgan, *Cyberlaw*, 1998

[4] Sofia Gainnakoudi, "Internet Banking: The Digital Voyage of Banking and Money in Cyberspace", Information & Communication Technology Law, Vol 8, no. 3. 1999. 205, 208

[5] http://www.thestandard.com/movabletype/datadigest/archives/003209.php

[6] Anti-Phishing Working Group. http://www.antiphishing.org

[7] M-Card smart. Migrosbank Switzerland. http://www.migrosbank.ch/de/Private/KartenZahlungsverkehr/MCardMCardSmart.htm.

[8] Bruce Schneier. Two-Factor Authentication: Too Little, Too Late. Communications of the ACM, vol 48, no.4, April 2005.