On the Security of Internet Banking in South Korea – a lesson in how not to regulate security

Hyoungshick Kim Jun Ho Huh Ross Anderson

July 4, 2011

Abstract

South Korean Internet banking systems provide an interesting natural experiment. Having been concerned at restrictions on crypto key length during the 1990s, the Korean government set up a closed security system for online banking. Users are obliged to install proprietary security software – ActiveX plugins that implement a bundle of protection mechanisms in the user's browser. In consequence, almost everyone in Korea uses Internet Explorer rather than other browsers.

We conducted a survey of bank customers who use both Korean and other banking services, and found that the Korean mechanisms impose significant usability penalties. Usability here is correlated with compatibility: Korean users have become stuck in an isolated backwater, and have not benefited from all the advances in mainstream browser and security technology. Also, the proprietary mechanisms fail to provide a trustworthy platform. We conclude that Korea should rejoin the mainstream.

1 Introduction

The Internet has changed the way people use banking services: bank customers can now pay bills and transfer funds without having to go to a bank branch. Koreans have been enthusiastic about online banking: the Bank of Korea reported that 57.29 million online accounts[1] had been registered as of September 2009[2] with an average day seeing 29.03 million Internet banking transactions, transferring 30.17 trillion Korean Won (about USD 26 billion).

One curious fact, though, is that Internet banking systems in Korea only support Microsoft Internet Explorer (IE) and only the Windows version. Bank customers cannot use other web browsers like Safari, Firefox, Opera and Chrome. In consequence, IE has become the dominant web browser in Korea. Recent market share trends for web browsers in different parts of the world[3] illustrate the effect; Figure 1 shows that Korean users have been effectively handed over as a captive audience to IE.

The reason is simple enough – regulation. The Korean government introduced a 'Digital Signature Act' which supports a regulated Public Key Infrastructure (PKI) to guarantee the interoperability of digital signature and encryption algorithms for all electronic transactions processed in Korea. As the necessary encryption and signing functions are not supported in existing web browsers, the banks provide these functions as external plugins. As IE is the dominant browser, the banks and security companies implemented these plugins as ActiveX controls, effectively locking the users in to IE.

[1] Some users have multiple accounts; the population is around 49 million.

[2] http://eng.bok.or.kr/

[3] http://gs.statcounter.com/

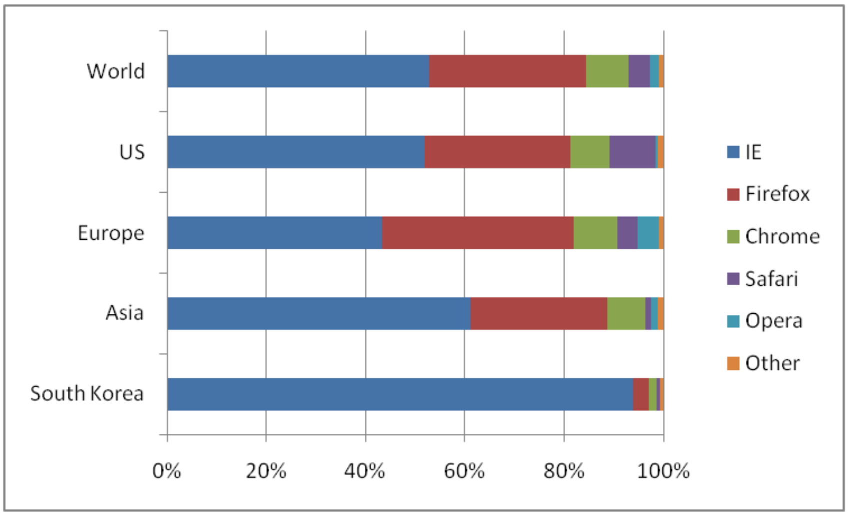


Figure 1: Web Browser Market Share by Geographic Regions (May 2010)

Much debate [7, 1] has raged in Korea around the requirement that users install external security plugins, the lack of effort by the vendor companies to provide better compatibility with other operating systems and browsers, and the usability implications for bank customers. More recently, changes regulations have been contemplated as smartphones (e.g. iPhones) have become popular in Korea; current smartphone users cannot bank or shop online with their smartphones. It is not hard to imagine a similar discussion emerging again and again whenever a new electronic device or service is introduced.

Korean Internet banking is a valuable case study of the implications of mandating proprietary, closed or monopolistic security solutions. This paper aims to contribute: (1) an analysis of the strengths and weaknesses of the proprietary Korean security mechanisms compared with standard technologies and (2) a study of the usability issues raised by employing these proprietary mechanisms.

2 Security Mechanisms Used in South Korea

In Korea, on top of the standard security requirements [6] – user/server authentication, confidentiality data integrity and non-repudiation, the banks seek to ensure that their customers use trustworthy platforms. Although some banks from other countries are also sensitive to this issue and encourage their customers to install anti-virus software, Korea aappears alone in forcing its customers to install specific software.

Table 1 summarizes the security mechanisms being used in the Korean banking systems to fulfil these requirements. We also list the mechanisms that are commonly used in some banks in the UK and the US for comparison.

In most other countries, Secure Sockets Layer/Transport Layer Security (SSL/TLS) is the de facto Internet banking standard for ensuring confidentiality and data integrity. The Korean banking systems, however, use proprietary protocols based on RSA, HMAC, and a block cipher called SEED (see Section 2.1). Elsewhere, some combination of ID, password and one-time password (OTP) is commonly used for authentication; again, the Korean systems are unique in that they also use RSA. In fact, RSA is also used for non-repudiation, a property rarely found in other countries.

Table 1: Security Mechanisms for Online Banking

Requirements	All Korean banks	UK bank A	UK bank B	US bank C
Server authentication	proprietary –	SSL/TLS –	SSL/TLS –	SSL/TLS personal indicator
User authentication	ID/password OTP private key (SW)	ID/password OTP –	ID/password – secret key (HW)	ID/password OTP –
Data integrity	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Non-repudiation	digital signature	–	digital signature	–
Confidentiality	proprietary	SSL/TLS	SSL/TLS	SSL/TLS
Malware detection	anti-virus	anti-virus [O]	anti-virus [O]	anti-virus [O]
Network access control	firewall	firewall [O]	firewall [O]	firewall [O]
Anti-keylogger	keystroke enc.	keystroke enc. [O]	–	–

([O] indicates that the feature is optional.)

2.1 Secure and Authenticated Communication Channel

In 1999, the Korean government launched an Internet banking system based on its regulated PKI. This was adopted rapidly by the banks; by the end of 2000, 20 of them were offering Internet banking services based on this PKI.

A user obtains a digital certificate through a government Certificate Authority, for which they must pass an online authentication test. The process is managed through proprietary software downloaded from a bank's website. The issued certificate is stored either on the user's hard disk or in an external device such as a USB stick.

A secure authenticated channel (SAC) is established between the user and the bank server using digital certificates. The protocols used to generate session keys are not published. The communication traffic is encrypted by the block cipher called SEED [10] – a 128-bit symmetric key block cipher developed by a Korean government agency in 1998, with a 16-round Feistel structure. Since SEED and protocols that use it are not supported by standard web browsers (including IE), a plugin is required.

This is all a by-product of the "Crypto wars" in the 1990s during which the US government tried to restrict strong cryptography. The encryption algorithms supported by the web browsers distributed outside the US had key sizes limited by the US government to 40, or later 56, bits for symmetric encryption algorithms (RC4/DES). Thus the Korean government funded the development SEED as the national standard for secure e-commerce.

2.2 User Authentication

Online banking systems worldwide use a wide range of technologies for authentication, including passwords, Personal Identification Numbers (PINs), digital certificates, physical tokens such as smart cards, One-Time Password (OTP) generators, transaction profile scripts, and biometric identification. Korean systems generally use two or three of these techniques, rather than relying on just one. A common authentication process runs as follows:

1. A customer logs into the website using their ID and password.

2. To carry out a banking transaction, some digits from an indexed Transaction Authentication Number (iTAN) printed on the user's private security card or an OTP (generated by an OTP generator) are entered.

3. Online transaction records are digitally signed with the user's secret key stored in the user's PC or external memory.

Step 2 may involve an "out-of-band" channel, such as postal delivery of a security card or a physical token, or a mobile-phone-based challenge/response process.

A combined authentication mechanism, if carefully designed and implemented, should provide reasonable security. However the designer has to worry about man-in-the-middle attacks, social engineering and malware. The use of digital certificates, for instance, seems reliable in theory, but without strong protection for the user's private keys, it may buy less than you think. To mitigate key-stealing attacks, password-based encryption for the private keys has been legislated: an encryption key, derived from the customer's password alone, is used to protect the private keys. The Korean government proposed a specification in 2004 – derived from the Public Key Cryptography Standard (PKCS) #5 – where "SEED" is the standard encryption algorithm used. Triple DES was added as another standard encryption algorithm in 2007.

2.3 Trustworthy User Platforms

The user is the ultimate "client" of the system, not the web browser. The user connects to the bank server through the interfaces available on the web browser. The browser collects the user input, makes requests to the bank server to perform transactions, receives the server response/data, and displays the output to the user. A trustworthy user platform, therefore, must secure the communication channel between the user and the browser.

This channel is frequently attacked by malware that tries to steal sensitive information, such as credit card details and other banking credentials. Some attacks are technical, involving zero-day exploits or other engineering tricks that install malware regardless of anything the user can do; others use social engineering tricks. For example, websites often ask users to download a special codec, which actually turns out to be malware.

To mitigate such attacks, the Korean banks oblige the users to install new (or upgrade existing) security plugins when they access the banking service.

- An anti-virus program is installed to provide real-time protection against known malware. It detects malware by going through the files on the customer's disk and removing all the files that match the signatures in a blacklist. Therefore, it relies on timely updates and on the integrity of the blacklist. The Korean banks require the blacklist to be updated in real time.

- A personal firewall is designed to prevent the malware communicating with an external adversary. It monitors all incoming and outgoing traffic and permits only authorized connections while the user is doing banking. Its goal is to prevent man-in-the-middle or man-in-the-browser attacks being executed by malware.

- A keystroke encryption routine protects sensitive information from the moment it is typed into the keyboard until it reaches the browser. This is intended to prevent the information from being read or tampered with en route to the browser.

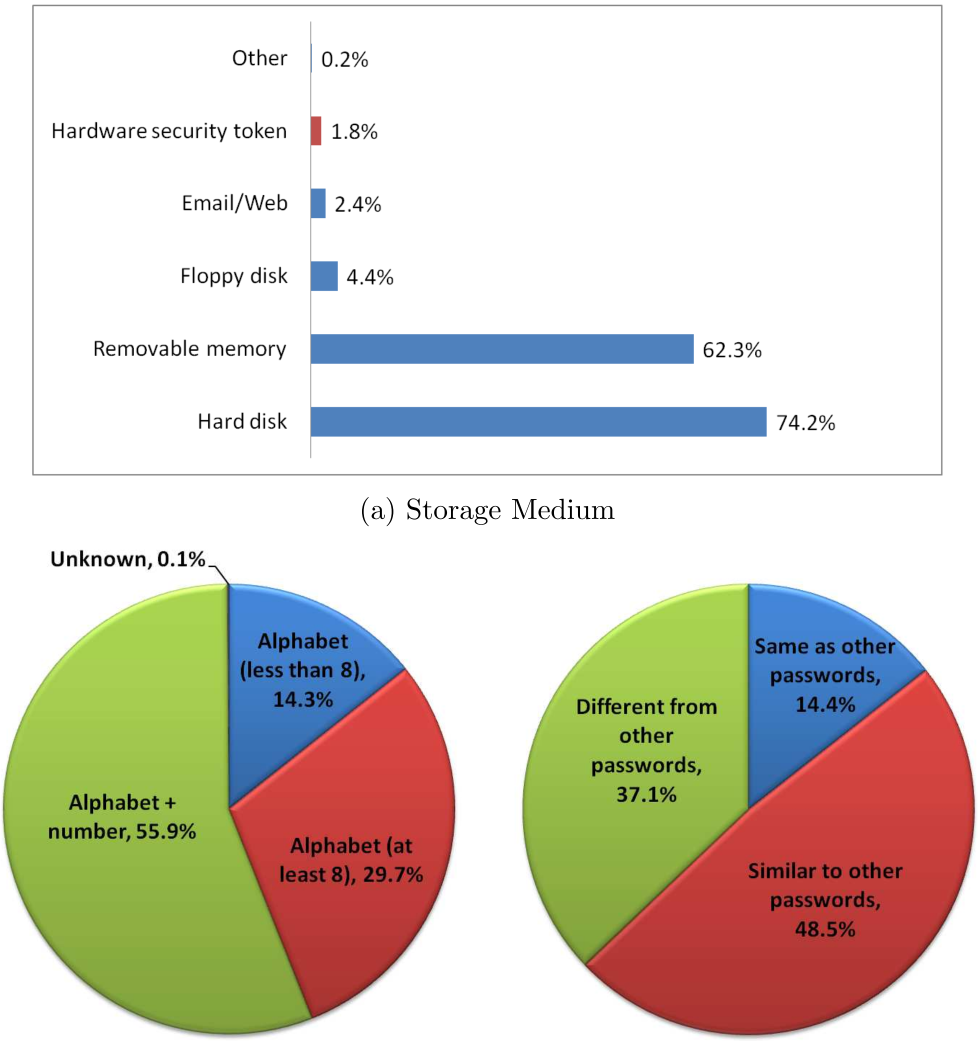
3 Why are These Security Mechanisms Not So Effective?

At first glance, the Korean Internet banking systems seem more secure than the systems used in Britain or the USA (see Table 1). Certainly the feature count is higher: more security mechanisms have been sold to the banks and are distributed by them. In this section, we identify the fundamental problems with these mechanisms and show why they offer at best a modest improvement.

3.1 Poorly-Protected Private Keys

In theory, public key cryptography may provide a neat solution for user authentication. In practice, however, PKI has proved to be difficult to deploy; it's expensive, and protecting the user's private key is hard.

In the Korean banking system, password-based encryption is the main mechanism used to protect user private keys. According to a government survey in 2008 [9], only 1.8% of 849 respondents used a hardware security token such as a smartcard (see Figure 2 (a)). As for the other 98.2%, key is kept in the hard disk and/or in removable memory such as a USB stick; in consequence their security is only as good as their password. This password can be compromised by malware through password-guessing or key-logging attacks.



(a) Storage Medium

(b) Password Type

(c) Comparison

Figure 2: Private Key Usage for Korean Online Banking

A recent criminal case illustrates the problem [4]: two Chinese hackers stole 450 million Korean Won (about USD 386,000) from 86 online accounts of 32 financial services by intercepting the victims' passwords with keyloggers. We argue that while digital signatures might provide good protection in theory, they provided no additional protection here in practice; using the captured user passwords, the hackers obtained the victims' private keys.

The Korean system does supply plugins that try to stop keyloggers. But even if these worked infallibly, only 56% of the total 849 respondents used a combination of alphabetic, numeric and special characters as their passwords to encrypt the private keys (see Figure 2 (b)). To make matters worse, around 63% of the respondents used passwords which are same as or similar to the passwords used in other services (see Figure 2 (c)). So maybe half the users might still have their passwords guessed offline by malware.

3.2 Untrustworthy User Interface

It's not enough just to protect the private key. A trustworthy user interface is also required, or a man-in-the-browser attack can defeat the signing process. For example, after a user enters destination account details and transfer amount, malware could modify the details sent to the token for signature, while continuing to display the intended transaction. Also, unless the token has an external keypad, an attacker can steal the PIN to access the private key stored in the security and do transactions without the user's participation at all. So a trustworthy signature creation device must have both a trustworthy display and a trustworthy keypad. But most hardware security tokens used in Korean Internet banking do not provide trustworthy I/O.

Where the principal threat to a system comes from malware, digital signatures are not an appropriate response. In fact, the main reason many banks have introduced OTP mechanisms or SMS transaction confirmation instead is to limit the exposure to keyloggers.

3.3 Limitations of the External Plugins

In Section 2.3, we discussed how customers are obliged to install four external plugins – in addition to the protocol crypto plugin, there's an anti-virus product, a firewall, and keystroke encryption software.

First, as malware writers get more organised, the proportion of malware that's detected is falling steadily. The low success rates (from 5% to 46%)[4] of early (near 0-day) detections by top anti-virus products show the limitations of this technology. Malware is no longer written by kids for fun, but by criminal firms for profit; these firms appear to have proper test departments which verify that their products aren't detected by the main AV products.

Second, the firewall software shipped by Korean banks runs only while the user is using the Internet banking service. So malware that wants to bypass it can just wait until the user logs off to send sensitive information back home. The product may provide some protection against session-stealing and real-time man-in-the-browser attacks. But perhaps this is the most that can be done; if banking software interfered with the user's online activities when she was not engaged in banking, it would be unacceptable.

Third, the keystroke encryption software has limitations too. It is hard to guarantee that a keystroke encryption scheme hooks lower than any potential malware; and if it's not designed carefully, it could prevent normal key inputs from being read by installed, benign programs.

These external plugins may be effective against simple malware. But the commercialisation of malware is making it rapidly more sophisticated; it could modify the standard Korean plugins or prevent them being installed in the first place. And even though these security mechanisms are mandated, Korea accounts for a massive 31.1% of the world's malware [12] and remains one of the top hosts for phishing attacks [15]. These facts lead us to ask how much the government's security plugins actually help.

[4] http://winnow.oitc.com/malewarestats.php

3.4 Security Features Available in Modern Web Browsers

Modern web browsers provide a number of security features that try to make Internet bank fraud harder. These range from alarms when a user tries to navigate to a suspect web site, through extended validation certificates, to browser-specific features. For example, Google's Chrome is to run each tab in a separate process, to limit the scope of malicious code. There are also research browser projects such as OP [5]. It's nice to see competition and innovation among browser products; but Korean users are unable to use them.

3.5 Lack of Security Proof

Korean Internet banking systems use proprietary authentication protocols. Yet protocols are notoriously difficult to get right, and most go through several iterations before the bugs are tweaked. The most widely-used protocols nowadays, such as Kerberos and SSL/TLS, are not merely the result of an iterative process of improvement, but have security proofs. SSL/TLS in particular has been studied for a long time, and formally verified [14] – its end-to-end security is equivalent to the cryptographic strength of the underlying algorithms if implemented properly. Security proofs are no panacea, as the implementation can have bugs; but SSL/TLS has also been subjected to of comprehensive analysis [11, 13, 3]; if and when flaws are found, they are generally fixed rapidly by the community.

4 What the Users Think About the South Korean Services

To investigate the usability implications of the security mechanisms discussed here, we conducted an anonymous online survey (see Table 2) to study (1) how users feel about using Korean services compared to those from other countries; and (2) why users prefer, or do not prefer, using Korean services over services from other countries. We made the assumption that services from other countries do not require their users to install extra security software (which is generally the case).

We invited volunteers interested in Korean online banking to participate, and got a total of 401 participants. 80 of these participants had experience of using banking services from Korea as well as from other countries (see Q2), out of a total of 379 people who had experience of Korean services (see Q1). The participants' IP addresses were checked to prevent multiple responses.

The results for Q3 show that 70% of those who have had experience in using both services prefer to use the services from other countries. Q5 reveals that the two most common reasons are simplicity and standards. The results for Q8 and Q9 indicate that 68.9% of those who have used Korean services felt uncomfortable, mainly due to their complexity and lack of compatibility with web standards.

For Q4, Q5, and Q9, some participants offered other interesting reasons. In particular, for Q9, 25 participants commented about the system crashes that result from installing the ActiveX plugins. 4 participants commented about the inconvenience of having to carry around digital certificates to use Internet banking.

It must be said, though, that none of the users were impressed with the security of other countries' banks (Q5) while 58.3% said that the most important reason they prefer Korean services was "It feels more secure" (Q4). We argue in this paper that Korean services are not actually more secure, but perhaps unsophisticated users assume that services which are complex and difficult to use must also be complex and difficult to defraud. Perhaps this is another example of "security theatre", which tackles the feeling but not the reality.

In addition, we compared the network traffic of two Korean banking services (banks A and B) against a UK banking service (bank C) to analyse the relative performance (see Table 3).

Table 2: Usability Survey Results

Q1. Do you have experience in using a Korean Internet banking service?	
Yes	94.5% (379)
No	5.5% (22)
Q2. Do you have experience using an Internet banking service from another country?	
Yes	21.1% (80)
No	78.9% (299)
Q3. If you had to select one service for Internet banking, which country's service would you prefer to use? (For those who have answered "Yes" to Q2)	
Internet banking service from Korea	30.0% (24)
Internet banking service from another country	70.0% (56)
Q4. What is the most important reason you prefer the Korean service?	
It's simpler	25.0% (6)
It's faster	8.3% (2)
It's more compatible with the Web standards	0.0% (0)
It feels more secure	58.3% (14)
Other	8.3% (2)
Q5. What is the most important reason you prefer the service from another country?	
It's simpler	50.0% (28)
It's faster	1.8% (1)
It's more compatible with the web standards	39.3% (22)
It feels more secure	0.0% (0)
Other	8.9% (5)
Q6. If all of the services provide the same level of security, which country's service would you prefer to use? (For those who have answered "Yes" to Q2)	
Internet banking service from Korea	15.0% (12)
Internet banking service from another country	63.8% (51)
I don't mind using either	21.3% (17)
Q7. Do you know why ActiveX controls are installed on your machine when you use the Korean banking service? (For those who have answered "Yes" to Q1)	
I know exactly	32.2% (122)
I know briefly	49.1% (186)
I have no idea	18.7% (71)
Q8. How often have you felt uncomfortable using the Korean banking service?	
All the time	41.7% (158)
Most of the time	26.9% (102)
Sometimes	27.2% (103)
Never	4.2% (16)
Q9. Why did you feel uncomfortable using the Korean banking service?	
It was complicated	20.9% (76)
It was slow	11.6% (42)
It had compatibility issues with the web standards	45.5% (165)
It felt insecure	7.7% (28)
Other	14.3% (52)

Table 3: Traffic Comparison

Metrics	Korean bank A	Korean bank B	UK bank C
Packet types	TCP, HTTP, SSL/TLS	TCP, HTTP	TCP, HTTP, SSL/TLS
Number of packets sent/received	8,669	8,961	1,301
Total bytes used	3,653,648	7,787,551	801,297
Number of communicating servers	9	5	1

The network packets were collected and analysed during user login and authentication.

The results show that the number of packets sent/received using the Korean services A and B is roughly 6-7 times higher than that of the UK service C. Similarly, the total byte count is 5-10 times higher in the Korean services, illustrating a relatively high communication cost and low performance. This is because the external plugins have to be downloaded each time. In Korea, this may not a big issue since high-speed Internet access is widespread. However, when a user living outside Korea tries to access the services, these slow transactions may be a burden. It is also interesting to see that using Korean services involves communicating with multiple web servers: these extra web servers usually serve to distribute the mandatory external plugins. This may indicate possible service-denial attacks or other additional failure modes.

Following our initial survey, which was conducted in January 2010 and published as a technical report [8], we submitted this paper and were asked by referees about the user demographic of our survey, and whether it was representative of Korean bank customers. As our initial survey had been anonymous we could not recontact the same subjects; however we used the same methodology to recruit 261 participants who had used Korean online banking services (we ignored 9 partial responses). Their responses to substantive questions on usability were consistent with the first survey: for example, the numbers who have felt uncomfortable about using Korean banking services were as shown in 4.

Table 4: What the users think about Korean services

How often have you felt uncomfortable using Korean services?	September	January
All the time	33.7%	(41.7%)
Most of the time	26.2%	(26.9%)
Sometimes	33.7%	(27.2%)
Never	6.3%	(4.2%)

It does turn out, however, that our sample of users who were able to compare Korean with foreign banking services was both younger and better-educated than the norm. 67.5% of them were aged 25–34, with 10.7% younger and the rest older. Only 4% had not completed college; 67.5% had completed college or university, while the remaining 28.6% had some graduate education. They were also more tech-savvy: about half used a browser other than IE for non-banking web browsing, which is about the norm for the USA and Europe but quite different from the over 90% IE use in Korea. This was despite the fact that about 90% use Windows as their main operating system. In effect, half our survey respondents were switching to IE for banking, or even rebooting from Linux to Windows or running a Windows virtual machine. These young and bright respondents to our second survey were also security-savvy: 88.5% were using their own anti-virus software, while 63.1% used their own firewall. Yet a clear majority of them (68.7%) think security plugins should be made optional, and an even larger majority (83.7%) have experienced an installation failure with them. In short, Koreans who have been exposed to the more liberal online environment of the rest of the world have adopted it, and most of them prefer it.

5 Conclusion

Korean banking offers an interesting natural experiment. While most banks worldwide offer online services to their retail mass market via web browsers, banks in Korea have for ten years insisted that customers use proprietary encryption software that is based on ActiveX controls, together with antivirus, firewall and keylogging countermeasures.

The effects have been rather mixed. On the one hand, Microsoft's IE has an almost complete monopoly in Korea, as customers can't do banking using Firefox or Opera. Recently, web compatibility is becoming serious as new web browsers have emerged for smart-phones, tablets and IPTV. And the Korean strategy is unpopular: we surveyed people who have used both Korean and other banking services, and found that over two-thirds of them felt uncomfortable using Korean services. What's more, those of our respondents who use both Korean and foreign banking services – a young, highly-educated, tech-savvy demographic – have shifted to the same web-browser usage habits as the rest of the world to the extent that they can; about half of them use browsers other than IE, and use IE only for operating their bank accounts.

At the technical level, the proprietary security software deployed in Korea offers at best a modest improvement, and certainly cannot provide the Holy Grail of a trustworthy platform. Indeed, by providing a state-sponsored and standardised 'solution' has isolated local electronic banking and commerce from the global mainstream, turning it into a backwater from which its users would escape given the choice.

The lessons learned in Korea may have much wider application. First, when security researchers discuss what options there might be if online bank fraud gets much worse, one of the possibilities is the use of proprietary systems – from variants on the 'trusted computing' theme to virtualization and proprietary bank client software. The Korean experience suggests that these should be treated with caution: the usability and compatibility costs they impose on users are likely to be nontrivial, and they may indeed be unusable in competitive markets because of their adverse effects on innovation.

Second, these lessons go to the role of governments in information security. A number of governments have been tempted to intervene in the technical aspects of security design, usually with effects that damage industry and lead government agencies to lose face. Technical research and development work should be left to industry and academia, who are better at it. The proper role of government is regulation. In the case of banking, that means first and foremost consumer protection: bank regulators should decree the outcome (that customers will not lose money as a result of fraud) rather than the mechanism (so long as defrauded customers are reimbursed, the technical countermeasures used by banks can be left to the market). Government does also have a useful supporting role, for example in the collection and dissemination of dependable statistics. Very few countries publish full bank fraud figures (in Europe, only Britain, France, Spain and the Netherlands do); Korea is not there yet. We recommend that the government publish robust electronic crime statistics, as was for example recommended in a 2008 report to ENISA for the case of European banks [2]. In the meantime, perhaps a crime victim survey can compare customers' experiences across countries. We believe that inter-country comparisons are important to define the security requirements and determine whether in fact it is necessary to invest in a next generation of online banking security technology.

References

[1] Open Web. `http://openweb.or.kr/?page_id=22`.

[2] Ross Anderson, Rainer Böehme, Richard Clayton, and Tyler Moore. Security Economics and the Internal Market. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec, 2008.

[3] Karthikeyan Bhargavan, Cédric Fournet, Ricardo Corin, and Eugen Zalinescu. Cryptographically verified implementations for TLS. In *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*, pages 459–468, New York, NY, USA, 2008. ACM.

[4] China Daily. China detains 2 hackers for stealing deposits at ROK banks. http://www.chinadaily.com.cn/business/2009-08/08/content_8545826.htm, 2007.

[5] Chris Grier, Shuo Tang, and Samuel T. King. Secure Web Browsing with the OP Web Browser. In *IEEE Symposium on Security and Privacy*, pages 402–416, Washington, DC, USA, 2008.

[6] Alain Hiltgen, Thorsten Kramp, and Thomas Weigold. Secure Internet Banking Authentication. *IEEE Security and Privacy*, 4(2):21–29, 2006.

[7] Gen Kanai. the cost of monoculture. http://blog.mozilla.com/gen/2007/02/27/the-cost-of-monoculture/, 2007.

[8] Hyoungshick Kim, Jun Ho Huh, and Ross Anderson. On the security of internet banking in south korea. Technical Report RR-10-01, March 2010.

[9] Korea Information Security Agency. Digital Signature Usage Annual Report. http://www.kisa.or.kr/jsp/public/library/report_list.jsp, 2008.

[10] H.J. Lee, S.J. Lee, J.H. Yoon, D.H. Cheon, and J.I. Lee. The SEED Encryption Algorithm. RFC 4269 (Informational), December 2005.

[11] John C. Mitchell, Vitaly Shmatikov, and Ulrich Stern. Finite-state analysis of SSL 3.0. In *SSYM'98: Proceedings of the 7th conference on USENIX Security Symposium*, pages 16–16, Berkeley, CA, USA, 1998. USENIX Association.

[12] Network Box. Korea becomes world's biggest producer of internet viruses. http://www.network-box.co.uk/aboutus/news/korea-becomes-world%E2%80%99s-biggest-producer-internet-viruses, 2010.

[13] R. Oppliger, R. Hauser, and D. Basin. SSL/TLS Session-Aware User Authentication. *Computer*, 41(3):59–65, 2008.

[14] Lawrence C. Paulson. Inductive analysis of the internet protocol tls. *ACM Transactions on Information and System Security (TISSEC)*, 2(3):332–351, 1999.

[15] RSA Laboratories. RSA Online Fraud Report. http://www.rsa.com/solutions/consumer_authentication/intelreport/10947_Online_Fraud_report_0510.pdf, May 2010.