国際大学
INTERNATIONAL UNIVERSITY OF JAPAN

Economics & Management Series EMS-2023-08

The Pitfalls of the Certificate-Based User Authentication Scheme on Korean Public Websites: Implications for Cross-Platform and Cross-Browser Compatibility and End-User Computing

Hun Myoung Park
International University of Japan

June 2023

IUJ Research Institute
International University of Japan

The Pitfalls of the Certificate-Based User Authentication Scheme on Korean Public Websites: Implications for Cross-Platform and Cross-Browser Compatibility and End-User Computing

ABSTRACT

The Korean government has employed a certificate-based user authentication scheme powered by Microsoft Internet Explorer and ActiveX plug-ins for the past two decades. Users must obtain accredited digital certificates, install all required plug-ins on their machines, and undergo all user authentication procedures. Public websites lack cross-platform and cross-browser compatibility and discriminate against those who do not use Windows and Internet Explorer. Most stakeholders mistakenly take a series of authentication procedures for granted and endure an inconvenient, burdensome, vulnerable, and fallible user authentication scheme. Given limited awareness of web accessibility and cybersecurity, they unwittingly make electronic copies of security code cards, store accredited digital certificates on a hard disk or flash drive, and mechanically click “Yes” or “OK” whenever a dialog box pops up. This monolithic end-user computing environment, despite its crucial pitfalls, contributed to the early diffusion of online public information and services; indeed, it was a double-edged sword. Although most ActiveX or non-ActiveX plug-ins were removed from public websites by 2021, the troublesome certificate-based authentication scheme remained almost unchanged for a long time (1999-2020). This case study illustrates the influences of the weird user authentication scheme on web accessibility and end-user computing and the importance of international technology standards.

KEYWORDS

E-government, User Authentication, Digital Certificate, Cross-Platform and Cross-Browser Compatibility, Device Independence, Web Accessibility.

INTRODUCTION

Korean e-government was largely led by two former presidents, Kim Dae-Jung (1998-2003) and Roh Moo-Hyun (2003-2008), who took strong initiatives, such as the Digital Signature Act (1999) and Electronic Government Act (2001), after the 1997 Asian financial crisis. In his inaugural speech, President Kim promised to make Korea an information powerhouse that is best able to use computers in the world and aggressively constructed a broadband Internet infrastructure, while the Roh Administration enhanced client-centered online services and online civic participation through government-wide system integration (NIA, 2011, 2017).

These supply-led efforts made a significant difference in a densely populated society where strong senses of belonging, engagement, and connectedness stimulated the demand for information technology services.

According to the International Telecommunication Union, the Internet penetration rate in Korea increased from .8% (41st place in the world) in 1995 to 45% (7th) in 2000, 74% (7th) in 2005, 84% (11th) in 2010, 90% (18th) in 2015, and 97% (10th) in 2020, skyrocketing especially between 1998 (7%) and 2008 (81%).[1] Korea was ranked top or second in the ICT development index from 2007 to 2017 (ITU, 2009-2018). In the United Nations E-Government Survey, Korean e-government development index was ranked 15th in 2001 and 5th in 2005 but received the top ranking in 2010-2014 and 2nd or 3rd in 2016-2020 largely due to high telecommunication infrastructure and online service scores (UN, 2001-2020).[2] A total of 41% of citizens used e-government services in 2007, but this usage rate increased from 62% in 2010 to 77% in 2015 and 89% in 2020, while citizens' satisfaction with e-government information and services increased from 65% and 63% to 94% and 98%, respectively (MIS & NIA, 2012-2020). Based on this unusual success in e-government, Korea exported its online service applications to many developing countries, such as Indonesia, Kenya, Mongolia, Peru, Uzbekistan, and Vietnam. According to the Ministry of Interior and Safety, a total of 124 applications (worth USD 269 million) were exported in 2016 and 324 (worth USD 450 million) in 2020.

Nevertheless, Korean websites suffered from a lack of cross-platform and cross-browser compatibility. They employed a unique certificate-based user authentication scheme that was designed primarily for Microsoft Windows and Internet Explorer (IE) and

[1] The number of fixed broadband subscriptions per 100 inhabitants was .03 in 1998 but soared to 8 in 2000, 25 in 2005, 35 in 2010, 39 in 2015, and 43 in 2020 and mobile subscriptions numbered 73 per 100 inhabitants in 2008, 97 in 2010, 107 in 2015, and 116 in 2020.

[2] It was ranked 47th in 2001 and 86th in 2005 but led the ranking from 2006 through 2008 in West's global e-government studies at Brown University (West, 2001-2008).

implemented by ActiveX plug-ins.[3] This user authentication scheme requires clients to obtain accredited digital certificates from certificate authorities (CAs) and enter a certificate password to login and perform transactions. They must also install all required plug-ins on their Windows machines. This odd authentication system has persisted in the Republic of Korea, unbelievably, over the past twenty years. Interestingly, these problems have been hidden behind the celebration of e-government success and thus have failed to draw noticeable attention from stakeholders until recently. How were Korean public websites isolated from global technology standards for so long that they thus became the so-called Galapagos of e-government?

This case study explores the certificate-based user authentication and the accredited digital certificate systems of Korean public websites over the past two decades (1999-2020). This narrative explains how this user authentication scheme impaired cross-platform and cross-browser compatibility but, despite its pitfalls, remained almost unchanged for such a long time. Then, the policy implications of this case are discussed.

WEB ACCESSIBILITY AND USER AUTHENTICATION

This section provides a basic understanding of web accessibility, cross-platform and cross-browser compatibility, digital certificates, and user authentication before moving on to the case study.

Cross-Platform and Cross-Browser Compatibility

Web accessibility makes web content accessible to a wide range of people with visual, auditory, physical, speech, cognitive, neurological, and other disabilities so that they can perceive, understand, navigate, interact with, and contribute to the web (Thatcher et al.,

[3] ActiveX controls are software frameworks that can be used to develop small applications, which are downloaded and executed by web browsers. Unlike Java applets, ActiveX plug-ins are not executable on a large variety of operating systems and browsers but run mostly on Windows and IE.

2006). Web accessibility can reduce development and maintenance time, alleviate server load, improve interoperability, and provide financial benefits, including cost savings (Thatcher et al., 2006). *Device independence* refers to making the web accessible to various user agents, such as web browsers, assistive devices (e.g., screen/text readers), and mobile devices (e.g., smartphones). The World Wide Web Consortium (W3C) says that web accessibility ensures access to the web for anyone with or without disabilities, while device independence is intended to make the web accessible at any time and in any way by supporting various devices and access mechanisms. *Cross-platform* and *cross-browser compatibility* means that websites are designed and developed to work across various operating systems (OSs) and web browsers.[4]

W3C has developed the Web Content Accessibility Guidelines (WCAG) since 1998 to enhance the accessibility of websites worldwide. On the basis of the WCAG, many countries introduced their own accessibility regulations, such as Section 508 of the Rehabilitation Act in 1998 (US), Korean WCAG in 2005, and the Directive on the Accessibility of Websites and Mobile Applications of Public Sector Bodies in 2016 (EU). Nevertheless, all countries still have difficulty enforcing their regulations due to a lack of understanding of legal guidelines, outdated standards, inadequate training, insufficient time, and technical/financial/legal challenges (Loiacono, Romano, & McCoy, 2009). For example, Jaeger (2006), Loiacono, Romano, and McCoy (2009), and Olalere and Lazar (2011) studied American public websites, while Gambino, Pirrone, and Di Giorgio (2016) and Hyun and Kim (2008) reported noncompliance with accessibility regulations in Italian and Korean public websites, respectively. Moon and Moon (2009) reported poor cross-browser

[4] Each web browser has its own default settings and rendering engine to interpret web documents. IE employs Microsoft's Trident engine, whereas Google Chrome and Firefox adopt Blink and Gecko, respectively. If web pages are customized to IE, they will not be rendered properly in other web browsers or will not be accessible from some devices.

compatibility on 59 Korean government websites. Yi (2020) examined ten Korean healthcare websites and argued that web-based plug-in errors during the authentication process are significantly challenging to those with disabilities (pp. 54-55).

Authentication and Digital Certificate

A subject (user) must be properly identified, authenticated, and authorized by information systems to access data and computing resources. A *digital certificate* (or public key certificate) is an electronic text file that contains the subject name, signature algorithm, subject's public key, certificate issuer name, issuer's digital signature, validity period, and others, which are arranged according to the X.509 standard (Kahate, 2008). Digital certificates are issued from CAs, such as IdenTrust, DigiCert, and Sectigo.

A server digital certificate is used to prove to a client (web browser) that the web server is exactly what it claims to be (*server authentication*), while a client certificate authenticates the client as the real owner of the public key to the web server (*client authentication*). *User authentication* verifies a subject by means of something the subject knows (e.g., password and security question), something the subject is (e.g., retina and fingerprint), something the subject does (e.g., voice pattern and handwriting), and/or something the subject has (e.g., digital certificate and authentication token) (Stallings, 2017). Password-based authentication is the most common mechanism and asks for a username and password. Certificate-based user authentication in the public key infrastructure (PKI) requires client digital certificates. Multifactor authentication combines more than one authentication means, such as a password and OTP token. The critical issue is how to manage the security risk of passwords and private keys successfully (Whitman & Mattord, 2012).

NATIONAL PUBLIC KEY INFRASTRUCTURE IN KOREA

The Korean government developed the National PKI (NPKI) framework and adopted a certificate-based user authentication scheme. Financial Supervisory Service (FSS), a

government agency to supervise financial affairs, revised its Regulation on the Supervision of Electronic Financial Activities (RSEFA) in 2006 and officially made it mandatory to use accredited digital certificates in electronic financial transactions (Article 7). The government requires each web server (called a "secure server") to encrypt personal and authentication information during transmission using either a secure sockets layer (SSL)/transport layer security (TLS) certificate or encryption application (client software or application).[5]

[Figure 1 about here]

PKI versus NPKI

PKI with SSL/TLS provides secure communication between web servers and clients (web browsers). In the TCP/IP model, HTTP (Hypertext Transfer Protocol) at the application layer is running over SSL/TLS, which is located over transport (TCP), Internet, and network access layers (left in Figure 1). In contrast, NPKI does not use SSL/TLS in web browsers but relies on browser plug-ins (client applications) instead (right in Figure 1); unlike PKI, NPKI does not encrypt all information, including images, but protects only sensitive information between web servers and clients. NPKI uses a proprietary protocol that is developed by individual agencies and service providers, not by international standardization organizations (Table 1). Korean websites allowed unencrypted legacy Internet protocols (i.e., HTTP, Telnet, and FTP) until the 2010s (right in Figure 1). This closed framework suffered from incompatibility problems and could barely adapt to rapidly evolving technologies (Park, 2016).

[Table 1 about here]

[5] Article 5 of the Criteria for Technological and Managerial Measures to Protect Personal Information (2008) and Article 15 of the Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection, etc. (2008).

In PKI, server authentication is mandatory in the handshake phase and uses an extended validation (EV) server certificate, but client authentication is optional (Table 1). Then, password-based user authentication asks the client's username and password. In NPKI, both server and client (user) authentication are mandatory and a certificate-based method is employed (Table 1). Client applications send an accredited digital certificate, digital envelope (session key encrypted using the server's public key), and digital signature to the server as a log-in request; that is, user authentication occurs in the process of establishing a secure session between a server and client (Park, 2016). In PKI, web browsers (user agents) perform user authentication, but browser plug-ins are used in NPKI (Table 1).

Accredited Digital Certificates

PKI allows digital certificates that are issued by a variety of CAs, who compete with each other in the certification market. In NPKI, the market was virtually monopolized sector by sector (Table 1). The Ministry of Information and Communication, pursuant to the Digital Signature Act (1999), licensed six CAs, such as the Korea Internet and Security Agency (KISA), Korea Financial Telecommunications and Clearings Institute (KFTC), and Korea Securities Computing Corporation (KOSCOM), to offer certification services. KFTC's Yeskey (formerly Yessign), for instance, has issued accredited digital certificates for Internet banking since 2002 and KOSCOM's SignKorea for stock trading since 2003.

In PKI, Digital certificates are stored in the certificate store of web browsers. In NPKI, accredited digital certificates and private keys were stored in a file system as text files (`signCert.der` and `signPri.key`) in the same folder (KISA, 2010), specifically, *\Program Files\NPKI* until Windows XP or *\Users\(account)\AppData\LocalLow\NPKI* thereafter (Windows Vista, 7, 8, and 10). Clients are not allowed to change the name and location of these designated folders. These files should be transferred securely according to the personal information exchange standard, PKCS#12 (KISA, 2010), but, in fact, anyone could easily

copy the whole NPKI folder from one device to another. Unfortunately, most clients used to store accredited digital certificates on their hard disk, flash drive, or smartphone, which is more vulnerable to ever-evolving phishing techniques than a security token (Park, Kim, & Lee, 2014). Both PKI and NPKI use passwords (passphrases) to protect private keys (Table 1). As long as passwords can be stolen by keyloggers and deciphered out of a stolen NPKI folder, there is no substantial difference in the security concerns of private key management between PKI and NPKI.

Inconvenient User Authentication

User authentication in NPKI is inconvenient and burdensome. Websites required users to sign in first, but a username and password alone was not sufficient.[6] Clients had to obtain accredited digital certificates from licensed CAs; store them on a hard disk, flash memory, or security token; and renew and register them every year. They had to install all required ActiveX plug-ins on their Windows machines and upgrade them whenever requested. Otherwise, the web server triggered a pop-up message, "Some security programs were not installed," and then redirected to the software download page. Clients could not move forward until all plug-ins were completely deployed; their access was denied even before logging in. These tasks were overwhelming to computer novices and those with disabilities and irritating to most clients, including experts. Then, clients had to enter a certificate password (not username password) to obtain their private key. Users had to carry security code cards or OTP tokens that were issued by banks or securities firms (Figure 2).[7] They had to have their own mobile phone to receive a six-digit verification number sent from

[6] In PKI, clients just need to provide their username and password for login. Some websites additionally ask a security question (e.g., "What is your hometown?") or require a one-time password (OTP) to validate their identity, and others require a reCAPTCHA test to ensure that they are not a machine (e.g., web bot).
[7] Approximately 30 or 35 four-digit random numbers are printed on a security code card. In general, a client is asked to type in the first two digits of a randomly selected number and the last two digits of another randomly selected number from the card.

a financial institution; e-mail was not allowed for verification. Even after logging in, clients needed to provide a certificate password, security code, or verification number when conducting financial transactions.

[Figure 2 about here]

It is time-consuming and even challenging to provide a digital certificate password, security code, or verification number without any mistake. An accredited digital certificate password must contain special characters (e.g., @ and *), alphabetic characters, and numbers. It is bothersome to click correct characters and numbers using a virtual keyboard (plug-in) since character and number keys are often randomly arranged in a dialog box to prevent keystroke logging (Figure 3). This cumbersome requirement often induces human errors. A simple mistake at any step will revert to the first step of an electronic transaction. To make the situation worse, five consecutive mistakes in password or code input automatically lock further access and put clients in an awkward position. It was almost impossible, especially for the blind, to understand and navigate virtual keyboards and certificate entry dialog boxes devoid of software accessibility (Hong, Choi, & Kim, 2011). In short, a series of almost acrobatic moves are required to access and use public websites in wonderland.

[Figure 3 about here]

According to the Annual Survey on E-Government Services Use, the main reasons for not using e-government services are unfamiliarity with PCs and the Internet (50-60%) and complicated authentication procedures (30-50%) (MIS & NIA, 2012-2020). Approximately two percent of e-government users wanted to stop using online information and services largely due to burdensome and complicated procedures for identification and authentication (40-80%) and concerns about personal information loss (20-70%). Approximately 30-50 percent of the users requested primarily that authentication procedures be improved and information protection/security be enhanced. Although the majority of citizens were satisfied

with e-government services, they thought that the certificate-based user authentication scheme was not as convenient and safe as expected.

PITFALLS OF ACTIVEX PLUG-INS

In NPKI, the encryption application approach (as opposed to SSL/TLS) was employed to establish secure connections and perform user authentication. Web browsers available in Korea, such as Netscape Navigator and Microsoft IE, supported SSL/TLS but not 128-bit encryption until the 1990s. Web browser plug-ins on the client side were introduced as a feasible solution to ensure safe transactions at the targeted 128-bit level. The plug-ins began to be developed coincidentally using Microsoft ActiveX controls, which were the *de facto* technology at that time. Although most web browsers began to support 128-bit and even 256-bit encryption in the early 2000s,[8] Korean websites did not switch to the SSL/TLS approach. Instead, plug-ins were continuously used by service providers, but their quality and safety were not properly validated by CAs and FSS (Kim, 2009). This authentication scheme powered by ActiveX plug-ins was far from the international standard and technological neutrality principle (Song, 2015). It was not, however, dictated by related laws and guidelines *per se*, but rather resulted from administrative failures to implementation them appropriately (Park, 2012).

Accredited digital certificates were required not only for financial transactions but also for nonfinancial ones, such as issuance of birth certificates and application of Visa renewal. Clients must install various plug-ins on their Windows machines even for browsing web pages, viewing PDF files, uploading/downloading files, playing video/audio clips, and printing documents. This pervasive use of ActiveX plug-ins brought about problems with vulnerability, fallibility, incompatibility, and bad end-user practice.

[8] Microsoft began to support SSL in 1995 (IE2), 128-bit encryption and TLS 1.0 in 1997 (IE4), 128-bit encryption worldwide in 2000 (IE5.5), and 256-bit encryption in 2006 (Vista version of IE7).

First, ActiveX controls are known to have security flaws. Java applets may not access system resources, but ActiveX plug-ins are able to access Windows systems and thus change programs and data. Some plug-ins required administrator privileges for installation (MIS, 2019). Most clients tend to reduce the security level and enable plug-ins and pop-ups because they do not know exact technical details about IE's security options; they themselves disarm their Windows systems (Kim, 2009; MIS, 2019). This computing practice is vulnerable to malicious attacks. Some plug-ins appear to infringe on privacy by collecting clients' information on IP addresses, MAC addresses, hard disks, and other devices (against Article 24 of the Digital Signature Act). Microsoft stopped technical support for ActiveX controls as of April 2014, but Korean public websites continuously adhered to their use until the end of the 2010s. The certificate-based user authentication scheme plastered with ActiveX plug-ins or equivalents in NPKI has not shown security advantages over password-based authentication in PKI with SSL/TLS implemented; instead, it cultivated a "hacker-friendly" computing environment.[9]

Second, each website requires approximately five plug-ins for keylogging prevention, firewalls, computer virus scanning, device information collection, and others. This is because licensed CAs did not provide subscribers (clients) with necessary computer software packages for licensed certification practices (against Article 2 of the Enforcement Decree of the Digital Signature Act); instead, individual service providers arbitrarily provided their own plug-ins (as opposed to client applications officially reviewed and approved by CAs and FSS) that software vendors developed (Kim, 2009). The more clients access websites, the more plug-ins stacked up in Windows machines. Hence, Windows became slow, unstable, and

[9] For example, Korean Airline employed certificate-based user authentication for flight booking if a flight departs from Korea, otherwise (e.g., departing from Japan) it applied a typical password-based authentication over SSL/TLS, which is widely used in the globe.

vulnerable to attack. For instance, some infamous virus scanning and anti-keylogger plug-ins slowed the processing speed substantially so that users must endure a long wait before completing online services. Furthermore, it was laborious, if not impossible, to remove them completely. It is a nightmare to restart frozen Windows and IE or rebuild the Windows machine in case of system crash.

Third, ActiveX plug-ins are often error-prone and incompatible with other add-on and stand-alone applications (MIS, 2019). Some fallible websites continuously asked clients to reinstall plug-ins even after they were successfully installed, and others continued requesting certificate password input even after a correct password was provided; thus, users must restart IE or Windows. Some plug-ins in a virtual machine could not recognize some special characters; that is, there was no way to provide a correct password in the virtual machine.[10] This situation became even worse and more embarrassing for those with disabilities. Some stand-alone firewall and antivirus programs often conflicted with corresponding ActiveX plug-ins and thus must be disabled or uninstalled first. In some cases, two websites required different versions of a plug-in, one of which had to be removed to avoid version conflict.

Finally, ordinary users accustomed themselves to bad computing practices. Clients unwittingly tended to store accredited digital certificates on their hard disk/flash memory and make electronic copies of their certificate passwords and security code cards for the sake of convenience. Some clients, who were overwhelmed by acrobatic user authentication procedures, illegally asked family members or friends to obtain accredited digital certificates and conduct various transactions for themselves (against Article 23 of the Digital Signature Act). These practices imply a serious password management problem in the certificate-based

[10] When the author inquired about this fatal malfunction of ActiveX plug-ins, technical support representatives of a licensed CA could not find the source of this problem. After a long fruitless conversation, they simply recommended the latest Windows as an easy and realistic solution.

user authentication. Websites and CAs warned about this risk through plug-ins, emails, and campaigns, but most users rarely changed their habits. Since ActiveX plug-ins or equivalents (.exe and .dmg applications) were mandatory, citizens must install all of them and go through all hassling procedures one by one or give up using online information and services. Not only ordinary citizens but also professional experts could hardly distinguish required plug-ins from malicious ones. Accordingly, most users were inclined to mechanically click the "Yes" or "OK" button whenever a dialog box popped up without knowing what they were (Kim, 2009; MIS, 2019). This user experience (UX) was inconvenient and increased the risk of losing confidential information and infecting the computer with malware (Kim, 2014). According to KISA, digital certificate theft increased from 9 thousand in 2013 to 42 thousand in 2014, decreased to 23 thousand in 2015 and 7 thousand in 2016, and then soared to 46 thousand in 2020.

MONOLITHIC DESKTOP SOFTWARE MARKET

Despite the various problems associated with ActiveX plug-ins, Korean public websites were locked into the certificate-based user authentication ecosystem mainly supported by Microsoft Windows, IE, and ActiveX controls. Accordingly, Linux and Firefox users were often denied access and received a ludicrous pop-up message: "This website is customized to Internet Explorer" or "Netscape 6.0 is not supported." This means that web servers checked whether a client was using Windows and IE, and if not, they refused to provide information and services, implicitly urging him or her to become a Microsoft customer (Kim, 2009). This situation was nothing else but Procrustes who compelled victims to lie on his iron bed and then stretched or cut off their legs to fit the bed's length. Most clients became habituated to the monolithic certificate-based user authentication scheme.

A consequence of this Procrustean computing environment is the monopoly in the desktop web browser and OS markets (Park, 2012). The average IE market share in Korea

reached and stayed above 99% from 2004 through 2008 and then dropped to 94% in 2010, 68% in 2015, and 13% in 2020, whereas the corresponding American market share dropped steeply from 91% in 2004 to 73%, 52%, 28%, and 6% during the same period (Figure 4). The decline in the IE share is largely due to the advent of Google Chrome and Firefox. Chrome has grown rapidly in the American market from 9% in 2010 to 42% in 2015 and 59% in 2020, while its corresponding market share in Korea soared recently from 2% to 28% and 70%, respectively. Firefox accounted for 28% of the American market in 2010, and its proportion then gradually declined to 16% in 2015 and 8% in 2020, while its Korean market share remained negligible.

[Figure 4 about here]

Windows has held landslide domination over the Korean desktop OS market. Windows accounted for almost 100% of OSs until 2010 in Korea, and its share declined slowly to 96% in 2015 and 90% in 2020, while the corresponding American figure declined sharply from 96% in 2004 to 85% in 2010, 77% in 2015, and 65% in 2020 (Figure 5). The American market share of macOS gradually increased from 3% in 2004 to 13% in 2010, 18% in 2015, and 20% in 2020, whereas the corresponding figure in Korea was almost negligible until 2015 and then increased slowly to 8% in 2020. The global desktop OS and web browser markets are similar to those of corresponding American markets on the whole.

[Figure 5 about here]

LACK OF PUBLIC ATTENTION

Most stakeholders, including the government, FSS, CAs, service providers, and software vendors, were barely aware of the cross-platform and cross-browser compatibility and cybersecurity problems in the certificate-based user authentication scheme used in NPKI. Once clients were caught up in this weird authentication scheme, they rarely doubted its quality and safety, recognized its hassle in end-user computing, or sought alternatives.

The term “accredited digital certificate” in Korean gave the wrong impression that the government officially authorizes clients’ digital certificates and guarantees their safety (Oh, 2017). Clients mistakenly perceived this certificate-based user authentication as an inevitable due process for secure transactions. They unconsciously took a series of bothersome user authentication procedures for granted and endured all troubles associated with accredited digital certificates and ActiveX plug-ins. As a consequence, the inconvenient, vulnerable, and fallible certificate-based user authentication scheme remained almost unchanged over the past two decades.

There were technological and methodological problems in evaluating web accessibility and device independence. Web accessibility guidelines, such as the WCAG and Section 508, focus mainly on the syntax, design, and style of web documents. Since many guidelines are neither formally specified nor accurately testable, each automated evaluation tool interprets checkpoints in its own way; accordingly, fully automated web accessibility evaluation is not feasible (Centeno, Kloos, Fisteus, & Alvarez, 2006; Harper & Yesilada, 2008). Web accessibility scores and rankings are often inconsistent and vary depending on the methods and samples used (Lazar, Beere, Greenidge, & Nagappa, 2003; Centeno et al., 2006). Manual assessment with human judgment is inevitable, but a visual rendering check is flawed because web browsers generously interpret HTML (Hypertext Markup Language) and CSS (Cascading Style Sheets) and then display the result with syntax errors corrected (Harper & Yesilada, 2008). The cross-platform and cross-browser compatibility (device independence) of websites is more difficult than other types of web accessibility to evaluate appropriately. This problem is even worse when web browsers rely on plug-ins because not only web documents but also add-on programs must be examined to understand how they go

wrong. The calculated web accessibility scores hardly reflect device independence and compatibility correctly.[11]

Despite the lack of public attention, civil society continuously raised this issue, but its voices were rarely heard in policy processes. For instance, the Open Web, a nonprofit organization for enhancing web accessibility, requested that KFTC, a dominant CA, support not only IE but also other web browsers, such as Firefox and Chrome. In 2007, this advocacy group sued KFTC for violating Article 7 (prohibition of subscriber discrimination) of the Digital Signature Act but eventually lost the case in 2009. The Supreme Court held that it was not illegal for the licensed CA to refuse to provide certification services to Firefox users because they represented a portion of less than 1% of users (Kim, 2009). This case illustrated how major players (i.e., government, CAs, and service providers) viewed web accessibility, specifically cross-platform and cross-browser compatibility issues in NPKI.

"NO PLUG-INS" INITIATIVE

The government established the Korean WCAG (2005, 2010, and 2015), Anti-Discrimination Act for Persons with Disabilities (2008), E-Government Web Standards Guidelines (2008), and E-Government Web Compatibility Guidelines (2009) to improve web accessibility in the public sector. FSS revised RSEFA in 2010 to allow alternative user authentication methods other than the existing certificate-based approach (Article 7). These attempts were not properly put into practice. Starting in 2009, public websites were supposed to support at least three web browsers, but 84% of 200 major websites were reported to still use ActiveX plug-

[11] NIA (2011, 2017) reported that the web accessibility score of Korean government departments and agencies increased from 72 out of 100 in 2005 to 95 in 2010 and 98 in 2015. These scores were surprisingly high but rarely represented the problem with cross-platform and cross-browser compatibility of NPKI. The Ministry of Science and ICT surveyed a random sample of 1,000 websites in Korea and found that the average web accessibility score was 53.7 in 2019, 60.7 in 2020, and 60.8 in 2021 (MSICT, 2019-2021). This survey, however, simply checked the accessibility of web applications (plug-ins) but did not take this checkpoint into account when calculating web accessibility scores.

ins in 2012.[12] The government, CAs, and service providers were not attentive to citizens' complaints and instead fretfully kept a watchful eye on whether new versions of Windows (XP–10) continued to support ActiveX controls.

In 2014, "Cheon Song Yi's coat" happened to become a wedge issue and drew public attention to chronic problems with certificate-based user authentication and ActiveX plug-ins.[13] Under pressure from annoyed citizens and foreigners, the government amended the Electronic Financial Transaction Act in 2014 (Article 21) to prohibit forcing the use of particular technologies and amended RSEFA in 2015 (Article 37) to abolish the mandatory use of accredited digital certificates in electronic transactions. In 2015, Microsoft Edge was introduced in Windows 10 but officially did not support ActiveX controls, and Google Chrome (version 45) ended its support of NPAPI (Netscape Plugin Application Programming Interface), such as ActiveX plug-ins. That is, ActiveX plug-ins were technologically deprecated. Faced with this dead end, the government had no choice but to hurriedly remove ActiveX plug-ins from public websites.

However, most government departments and agencies, who were proud of their top-ranked e-government status since 2006, lacked clear awareness of web accessibility, cross-platform and cross-browser compatibility, and ActiveX problems. They were not ready to follow new recommendations and abide by related laws, guidelines, and international web standards. Instead, they simply replaced ActiveX plug-ins with equivalent applications (.exe and .dmg without ActiveX) and recommended HTML5 over HTML4 under the same authentication scheme. Despite their political rhetoric, conservative regimes (2008-2017) clung to the status quo and rarely made any significant change to the cross-platform and

[12] https://www.korea.kr/news/pressReleaseView.do?newsId=155820220.
[13] Cheon Song Yi is a heroin's name in a Korean drama, *My Love from the Star*, which was very popular, especially in China. Many Chinese fans wanted to purchase her coats from Korean online shopping malls but had difficulty obtaining accredited digital certificates and successfully installing required ActiveX plug-ins.

cross-browser compatibility problem. Consequently, the accumulated number of accredited digital certificates issued by licensed CAs continuously increased from 30 thousand in 2000 to 11 million in 2005, 24 million in 2010, 34 million in 2015, and 47 million in 2020 (NIS et al., 2021, p. 83).

In 2018, the Moon Jae-In Administration took a strong "No plug-ins" initiative to eliminate ActiveX plug-ins from all public websites and announced in early 2021 that 99% of ActiveX and .exe plug-ins were removed. The Digital Signature Act was eventually amended in 2020 to abolish the accredited digital certificate framework. Now, former licensed CAs and private certification companies can compete with each other to improve certification services and meet clients' various demands.

In fact, banks and securities firms began to partially provide non-ActiveX plug-ins even before Microsoft ended its support for Windows XP and developed alternative add-ons for macOS and Linux. Licensed CAs did not provide necessary client applications for subscribers, while FSS failed to ensure that CAs and service providers performed certification services pursuant to related laws and guidelines. Recently, CAs renamed the accredited digital certificate "common digital certificate" and introduced a new concept of "financial digital certificate," which is stored in CA's cloud storage. Nevertheless, it is still challenging, if not impossible, to fully use public websites without Windows; Macintosh and Firefox users, for example, could not fully use online information and services.[14] Due to institutional, perceptual, and behavioral inertia, it will take a longer time to make websites fully accessible in Korea regardless of OS and browser type.

DISCUSSION

[14] Some browser extensions (.exe) do not work properly on Linux and MacOS. Some websites (e.g., the court's online services) still do not support many web browsers other than IE and Chrome and/or still require installing various plug-ins.

Korean websites relied on certificate-based user authentication powered by ActiveX controls. While computer security technologies have rapidly evolved over time, this authentication scheme, which was isolated from global technology standards, remained almost unchanged for the past two decades. This "Galapagos e-government" illustrates a fatal lock-in effect of information technologies. Once institutionalized, a technology is difficult to alter even if it turns out inefficient and inconvenient.[15] The government eliminated most ActiveX plug-ins by 2021, but most citizens still stay with the path-dependent authentication scheme even though alternative methods are now legally available.

The digital certification industry was dominated by monopolistic licensed CAs, to which the accreditation of certification practices for digital signature was granted by the government. They did not actually compete with each other because each licensed CA had its own business domain. Clients were forced to use the authentication method, OS, web browser, and plug-ins that licensed CAs and service providers favored. Without competition, there was no incentive for licensed CAs to provide convenient and trustworthy certification services. Despite a long history of digital signatures and widespread use of accredited digital certificates, none of the six Korean CAs are on the list of trusted CAs in web browsers.

This problem became fatal when Firefox (version 51 in 2017) and Chrome (68 in 2018) began to mark unencrypted websites without proper SSL/TLS certificates as "Not Secure" in the address bar. This is because most Korean websites shunned SSL/TLS and instead used client applications (plug-ins), independent of web browsers, to authenticate the server; web browsers could not know the authentication result and accordingly displayed the "Not Secure" warning (Park, 2016). As of 2020, 48% of 1,210 public websites were reported to still be using HTTP (Kim, 2020). The Ministry of Interior and Safety has provided

[15] Despite its disadvantages, QWERTY won over Dvorak and became a dominant keyboard layout due to its technical interrelatedness, economies of scale, and quasi-irreversibility (David, 1985).

government SSL (G-SSL) certificates for departments and agencies since 2015, but G-SSL works on Windows but is not compatible with mobile OSs (Lim, 2018). The ministry failed to get recognized as a trusted CA and thus stopped G-SSL issuance in 2019. The Moon administration introduced the "HTTPS-Only" policy in 2020 and required all public websites to use SSL/TLS certificates. Public websites had to obtain extended validation (EV) SSL/TLS certificates from foreign trusted CAs to avoid being labeled "Not Secure."[16]

The Korean government appeared to pay less attention to the institutional environment for online transactions in favor of a technological solution for cybersecurity. Once a user's username, account number, password (4-digit number), and security code card are acquired through online/offline phishing or hacking, anyone can obtain an accredited digital certificate for the account issued (Park, Lee, & Park, 2017). The ease of reissuing certificates with verification of digital identity is convenient but vulnerable to fraud, implying problems in institutional rules and end-user computing rather than technological flaws.

The Korean certificate-based user authentication scheme imposed an asymmetrically heavy burden and responsibility on clients. Clients must carry digital certificates, security code cards, and their cell phones and get various plug-ins installed on their machines. If someone steals and misuses clients' accredited digital certificates, licensed CAs and website owners will disclaim liability for illegal transactions on the basis of the Electronic Financial Transaction Act (Article 9), and clients with limited IT competence and legal capacity are likely to bear the primary responsibility for security breaches (Kim, 2013). Related laws and industry practices should be altered appropriately so that client-centric service providers assume primary responsibility and are eager to take preventive cybersecurity measures (e.g.,

[16] As of 2021, the Korean government portal gets its server certificate from DigiCert, the Prime Minister's Office from Sectigo, and Seoul Metropolitan Government from GlobalSign. Even KISA, who was a root CA, uses a server certificate issued by DigiCert. Surprisingly, the President's Office (Blue House) and KFTC still stay with HTTP.

fraud detection systems) proactively. Otherwise, any technological fix alone, such as the elimination of ActiveX plug-ins from websites, will not be sufficient.

CONCLUSION

Korean e-government employed a certificate-based user authentication scheme and rarely provided cross-platform and cross-browser compatibility before the 2020s. Internet users had to obtain and renew accredited digital certificates, install all ActiveX plug-ins that websites required, get a security code card or OTP token ready, and undergo all troublesome authentication procedures; otherwise, they were locked out of online information and services. Public websites discriminated against those who did not use Windows, IE, and ActiveX controls. This uniform computing environment contributed to the early diffusion of online transactions across the nation and enabled Korea to lead the global e-government ranking over the past 15 years.

Nevertheless, this Procrustean homogeneity in turn worsened the web accessibility problem and end-user computing environment. Microsoft Windows accounted for almost 99 percent of the desktop OS market in Korea during the 2000s. Most clients unconsciously took a series of bothersome user authentication procedures for granted and endured all troubles associated with digital certificates and ActiveX plug-ins. They unwittingly made electronic copies of security code cards, stored accredited digital certificates on hard disks, and mechanically clicked on the “Yes” or “OK” button whenever a dialog box popped up. Once clients accustomed themselves to the complicated hassle of authentication, they were not aware of the risk of such computing practices. Hence, the inconvenient, vulnerable, and fallible certificate-based user authentication system remained almost unaltered over the past two decades.

Recently, the Korean government eliminated most ActiveX plug-ins from public websites and required them to use SSL/TLS certificates. The current certificate-based user

authentication needs to be replaced by a typical password-based authentication or token-based authentication that is supplemented by other authentication factors. It will be a long time before an appropriate user authentication system, which neither requires all clients to study cybersecurity nor takes undue responsibility for online transactions, is institutionalized in Korea. Regardless of which authentication scheme is employed, clients must not be discriminated against on the basis of their operating systems and user agents.

REFERENCES

Centeno, V.L., Kloos, C.D., Fisteus, J.A., & Alvarez, L.A. (2006). Web accessibility evaluation tools: A survey and some improvement. *Electronic Notes in Theoretical Computer Science*, 157(2), 87-100. doi: 10.1016/j.entcs.2005.12.048.

David, P.A. (1985). Clio and the economics of QWERTY. *American Economic Review*, 75(2), 332-337. Retrieved from http://www.jstor.org/stable/1805621.

Gambino, O., Pirrone, R., & Di Giorgio, F. (2016). Accessibility of the Italian institutional web pages: A survey on the compliance of the Italian public administration web pages to the Stanca Act and its 22 technical requirements for web accessibility. *Universal Access in the Information Society*, 15(2), 305-312. doi: 10.1007/s10209-014-0381-0.

Harper, S., & Yesilada, Y. (2008). Web accessibility and guidelines. In S. Harper & Y. Yesilada (Eds.), *Web accessibility: A foundation for research* (pp. 61-78). Springer-Verlag London.

Hong, K.S., Choi, S.E., & Kim, S.I. (2011). Accessibility evaluation of accredited certificate subscriber software [in Korean]. *Journal of the Korea Contents Association*, 11(2), 40-53. doi: 10.5392/jkca.2011.11.2.040.

Hyun, J.H., & Kim, B.C. (2008). Web accessibility compliance of Internet banking in Korea [in Korean]. *Journal of Information Technology Services*, 7(2), 77-93.

International Telecommunication Union (ITU). (2009-2018). *Measuring the information society report*. Geneva, Switzerland.

Jaeger, P.T. (2006). Assessing Section 508 compliance on federal e-government websites. *Government Information Quarterly*, 23(2), 169-190. doi: 10.1016/j.giq.2006.03.002.

Kahate, A. (2008). *Cryptography and network security* (2nd ed.). New Delhi: Tata McGraw Hill Education.

Kim, K.C. (2009). *The uncomfortable truth of Korean web* [in Korean], Seoul, Korea: Digital Media Research.

Kim, K.C. (2013). Liability for unauthorized online financial transactions: The meaning of "forged or falsified means of access" [in Korean]. *Journal of Korea Information Law*, 17(3), 145-174.

Kim, Y.D. (2014, May 27). Accredited digital certificate, PKI, and safe certification technology [in Korean]. *IT World*. Retrieved from https://www.itworld.co.kr/news/87711.

Kim, Y.H. (2020, October 27). Introducing HTTPS in public websites [in Korean]. *ZD Net Korea*. Retrieved from https://zdnet.co.kr/view/?no=20201027155427.

Korea Internet and Security Agency (KISA). (2010). *User interface specification for the interoperability between accredited certification authorities* [in Korean]. Seoul, Korea.

Lazar, J., Beere, P., Greenidge, K., & Nagappa, Y. (2003). Web accessibility in the Mid-Atlantic United States: A study of 50 homepages. *Universal Access in the Information Society*, 2(4): 331-341. doi: 10.1007/s10209-003-0060-z.

Lim, M.C. (2018, December 27). G-SSL certificates failed to remove the "Not Secure" warning on public websites [in Korean]. *ZD Net Korea*. Retrieved from https://zdnet.co.kr/view/?no=20181227003039.

Loiacono, E.T., Romano, N.C., Jr., & McCoy, S. (2009). The state of corporate website accessibility. *Communications of the ACM*, 52(9), 128-132. doi: 10.1145/1562164.1562197.

Ministry of Interior and Safety (MIS) & National Information Society Agency (NIA). (2012-2020). *Annual survey of e-government service use* [in Korean]. Seoul, Korea.

Ministry of Interior and Safety (MIS). 2019. *Guidelines for removing plug-ins on public websites* [in Korean]. Seoul, Korea.

Ministry of Science and ICT (MSICT). (2019-2021). *Annual report on web accessibility* [in Korean]. Kyunggi Province, Korea.

Moon, T.E., & Moon, H.N. (2009). A study on the evaluation and improvement methods of web accessibility and usability of Korean government department websites [in Korean]. *Korean Journal of Business Administration*, 22(3), 1511-1535.

National Information Society Agency (NIA). (2011, 2017). *National informatization white paper* [in Korean]. Daegu, Korea.

National Intelligence Service (NIS), Ministry of Science and ICT, Ministry of Interior and Safety, Korean Communications Commission, Financial Services Commission, Ministry of Foreign Affairs. (2021). *White paper on national information protection* [in Korean]. Seoul, Korea.

Oh, D.I. (2017, June 13). The summary of debates on accredited digital certificates [in Korean]. *Security News*. Retrieved from https://www.boannews.com/media/view.asp?idx=55255.

Olalere, A., & Lazar, J. (2011). Accessibility of U.S. federal government home pages. *Government Information Quarterly*, 28(3), 303-309. doi: 10.1016/j.giq.2011.02.002.

Park, H.M. (2012). The web accessibility crisis of Korea's electronic government. *Proceedings of the 45th Hawaii International Conference on System Sciences*, Maui, HI, 2319-2328. doi: 10.1109/HICSS.2012.591.

Park, H.S., Lee, J.H., & Park, S.C. (2017). Implementation, security, and usability analysis of accredited certificate-based Internet banking [in Korean]. *Journal of Internet Computing and Services*, 18(4), 69-78. doi: 10.7472/jksii.2017.18.4.69.

Park, S.C. (2016). A comparative analysis of NPKI and SSL/TLS for secure Internet transactions [in Korean]. *Journal of the Korea Institute of Information and Communication Engineering*, 20(2), 289-298. doi: 10.6109/jkiice.2016.20.2.289.

Park, Y.J., Kim, S.J., & Lee, D.H. (2014). The secure key store to prevent leakage accident of a private key and a certificate [in Korean]. *Journal of the Korea Institute of Information Security & Cryptology*, 24(1), 31-40.

Song, Y.K. (2015). Technology standardization, government intervention, and public electronic certificate in Korea [in Korean]. *KDI Journal of Economic Policy*, 37(Supplementary), 1-32.

Stallings, W. (2017). *Cryptography and network security: Principles and practice* (7th ed.). Pearson Education Limited.

Thatcher, J., Burks, M.R., Heilmann, C., Henry, S.L., Kirkpatrick, A., Lauke, P.H., Lawson, B., Regan, B., Rutter, R., Urban, M., & Waddell, C.D. (Eds.). (2006). *Web accessibility: Web standards and regulatory compliance*. New York: Friends of Ed.

United Nations. (2001-2020). *E-government survey*. New York.

West, D.M. (2001-2008). *Global e-government*. Center for Public Policy, Brown University.

Whitman, M.E., & Mattord, H.J. (2012). *Principles of information security* (4th ed.). Course Technology & Cengage Learning.

Yi, Y.J. (2020). Web accessibility of healthcare websites of Korean government and public agencies. *Universal Access in the Information Society*, 19 (1), 41-56. doi: 10.1007/s10209-018-0625-5.

Table 1. Comparison of PKI with SSL/TLS and National PKI in Korea

PKI with SSL/TLS		National PKI (Korea)
SSL/TLS (International Standard)	Security Protocol	Proprietary protocol
EV server certificate	Server Authentication	NPKI server certificate
Optional	Client Authentication	Certificate-based (Accredited digital certificate + digital signature)
Password-based	User Authentication	
Password-based	Private Key Protection	Password-based
Web browsers	Client Application	ActiveX plug-in or equivalent
Certificate store in web browsers	Certificate storage	Storage units (e.g., hard disk and security token)
Competitive market (e.g., DigiCert and Sectigo)	Certificate Authority (CA)	Sector-by-sector monopoly (e.g., Yessign and SignKorea)
N/A N/A Smartphone/e-mail to receive OTP	Objects to Carry	Accredited digital certificate Security code card or security token Smartphone to receive OTP
N/A	Applications to Be Installed	Plug-ins for keystroke logging prevention, firewall, computer virus scanning, and others
Username, password, reCAPTCHA or OTP	Information for login	Username, digital certificate password

Figure 1. TCP/IP models with and without SSL/TLS

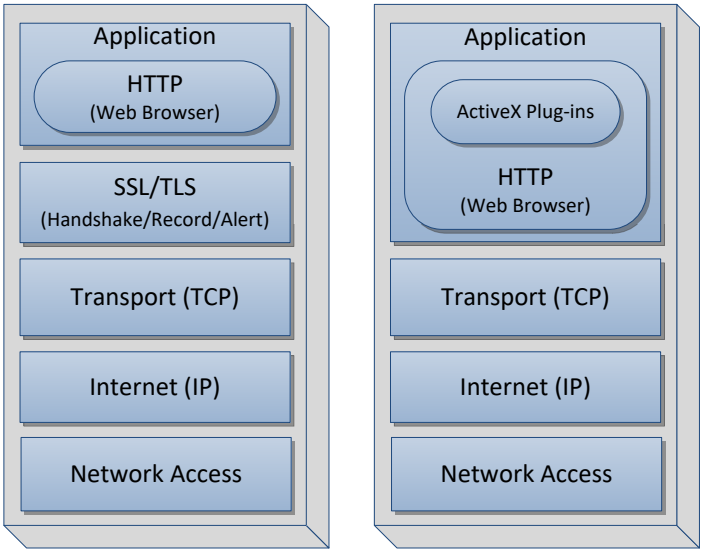
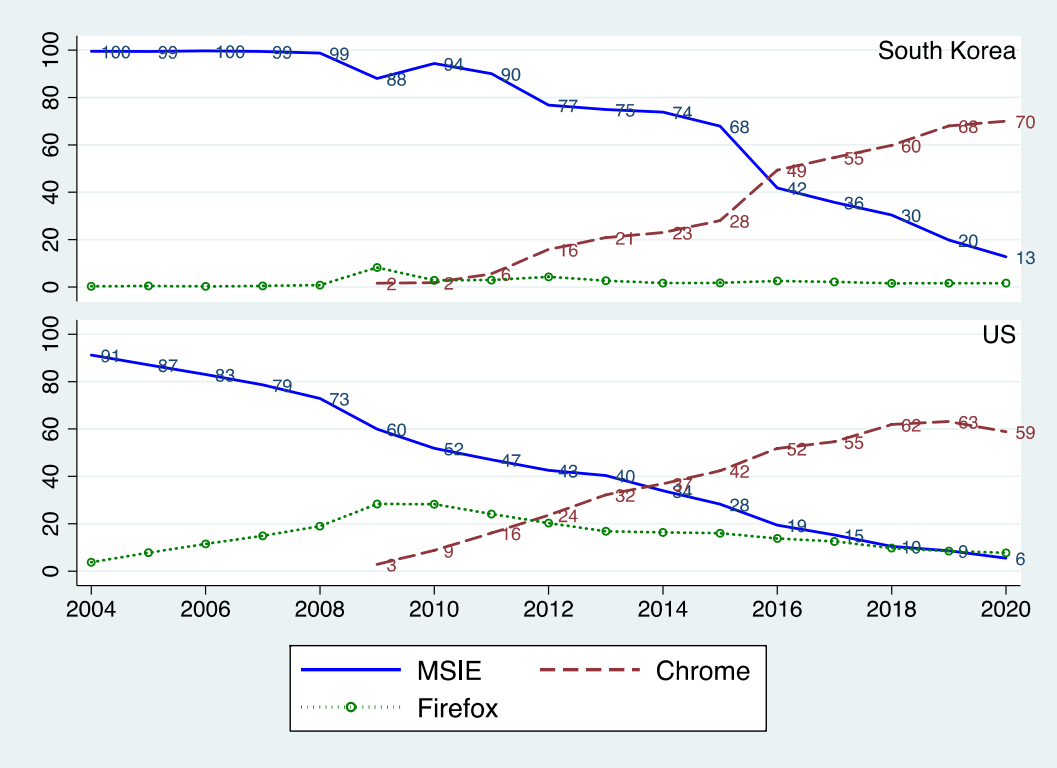


Figure 2. A security code card sample

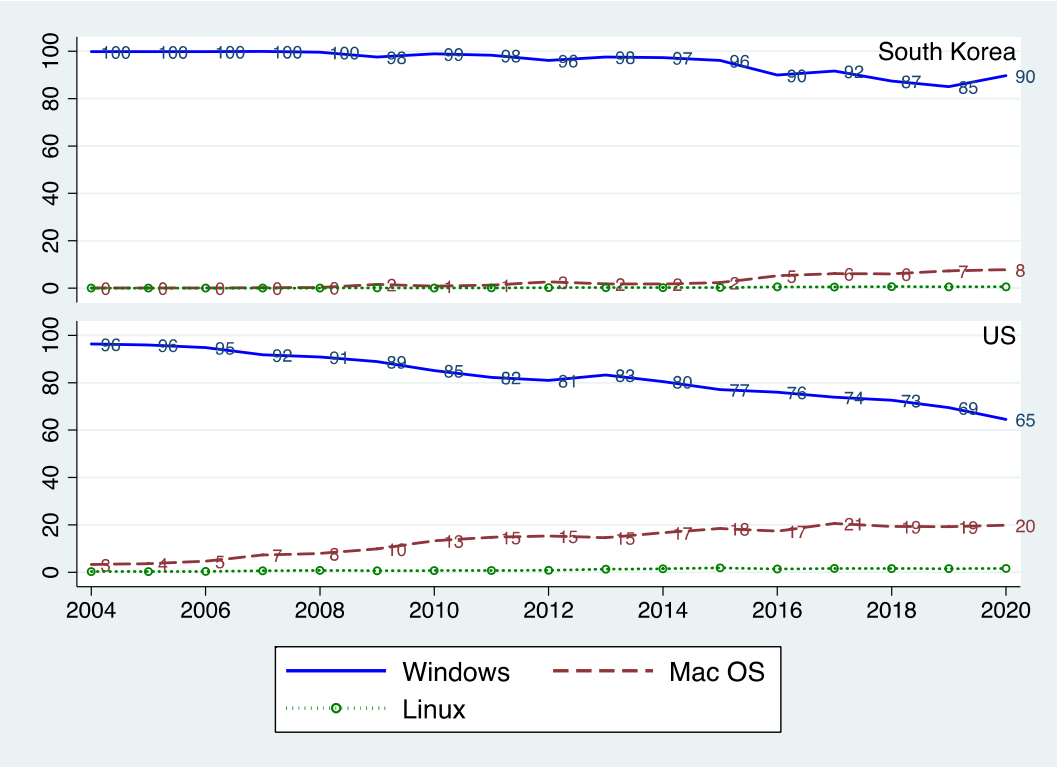
Figure 3. A virtual keyboard sample

Figure 4. Desktop web browser market share in the U.S. and Korea (2004-2020)



Source: Internet Trend/NetMarketShare (2004-2008) and StatCounter (2009-2020).

Figure 5. Desktop operating system market share in the U.S. and Korea (2004-2020)



Source: Internet Trend/NetMarketShare (2004-2008) and StatCounter (2009-2020).