Developing Security Assessment Models in Web² Mobile Environments

Bong Gyou Lee, Hyunsik Seo, Giseob Byun, Keon Chul Park,
Soo Kyung Park, and Taisiya Kim

Graduate School of Information, Yonsei University,
134 Shinchondong, Seodaemungu, Seoul, Korea
{bglee,seohs,parkkc,tgbgs,sk.park,lucky8619}@yonsei.ac.kr

Abstract. The purpose of this study is to develop and present security assessment models to manage the quality of Web² mobile environments. Web² is an evolved concept of web from Web 1.0 and Web 2.0 which means, diverse services and technologies including Real-time service, Social Network Services, Augmented Reality technology and Location Based Service are realized in mobile environment. However, compared to Web 1.0 and Web 2.0, few studies have been conducted for the security issues of Web² mobile environment. To be prepared for such issues, this paper reviews the characteristics of security in Web² mobile environments and present security assessment models in perspectives of Sensor-generated threats and User-generated threats. This study is significant in that it presents the directionality of the security issues to be discussed later in Web² mobile environments. This study will have implications for businesses and researchers preparing Web² mobile services and marketing.

Keywords: Web² Mobile Environment, Security Assessment, Sensor-generated Threats, User-generated Threats.

1 Introduction

Recently, the development of mobile network infrastructures, mobile communication technologies, and terminal technologies; the advent of diverse applications; and the activation of application markets have led the global increases in the supply and use of smart phones. That is, with the evolution of mobile Internet networks such as WiFi and 3G that enable users to freely access and use the Internet anytime and anywhere; the upgrading of the performance of smart phones into all-in-one devices that enable document works and support replays of diverse multimedia; the advent of diverse applications that satisfy users' needs; the development of an operating system (OS) that supports the applications; and the activation of application markets where those applications can be bought and sold, smart phones are providing new opportunities for businesses and revenue creation in the saturated mobile market, where it has become difficult to create revenues with voice services [1]. However, diverse factors threatening these new opportunities provided by smart phones are also appearing. Of these, the fact that the possibility and areas that are exposed

F. Daniel and F.M. Facca (Eds.): ICWE 2010 Workshops, LNCS 6385, pp. 73–84, 2010.
© Springer-Verlag Berlin Heidelberg 2010

to security threats are increasing is a serious problem [2]. In particular, it is considered that this will be a larger threat in Web² mobile services that enable attribute information collected from various kinds of sensors in real-time to be communicated from device to users and from device to device. Such services will also enable augmented reality technologies utilizing such information and Social Network Services (SNS) between users as information exchanges and access to and opening of networks increase. To review security related studies, a study that analyzed technical trends and the vulnerability of security in Web 1.0 and Web 2.0 environments [3], a study on the trend of security technologies and the direction to standardize the technologies [4], and a study on security issues and efficient measures to inspect the web [5] have been conducted. However, in reality, where as mobile Web² services are constantly evolving, the studies that have been conducted to prepare for the situation are insufficient. Therefore, the purpose of this study is to develop and present security assessment models in Web² mobile environments. To present a model used to prepare for security issues in Web² environments, it is necessary to assess the different types of security and the potential threats to each of them. In order to accomplish this, a framework will be developed through three broad stages. First, the characteristics of Web², which has evolved through Web 1.0 and Web 2.0, will be discussed. Second, based on these characteristics, security issues that might occur will be presented. Third, various threats to security that could occur in mobile environments will be reviewed; these will be mapped onto the security issues presented in the second stage. By illustrating the types, channels of occurrence, and the contents of damage of expected security issues, the security assessment model for Web² will be refined. This study has implications for businesses and related researchers preparing diverse services for Web², where paradigms are rapidly changing.

2 The Concept of Web²

2.1 Evolution of the Concept of Web

With the development of information technologies and user demands, the web has evolved from 1.0 to 2.0, and is now developing into Web² [6]. Web 1.0 consisted of text-centered HTML documents, information or services were produced by a few experts, and users had to accept them unilaterally. Later, the web became Web 2.0, thanks to the advent of sites that provided services using diverse data made into platforms through the participation of many people. In addition, technical changes that occurred at this time enabled the supply of web production tools to the public [7]. With these evolutions, the sharing and openness of information content were emphasized. Now, the availability of mobile Internet and smart phones is working as a catalyst for the development web applications. Web², a term coined by Tim O'Reilly (2009), refers to interactions between the web and the world, that is, the cyber world and the real world. In addition, the exponential expansion from Web 2.0 to Web², rather than an arithmetical increase to 3.0, means that the web is now becoming a reality in itself instead of an aggregate of static HTML pages intended to describe reality [3]. In Web², augmented realities, location information, social networks, etc.

are highlighted. Thus, it is becoming possible to obtain useful information on a user's surroundings in real time and manage personal connections [8]. Therefore, more sensors and people are introducing platform data and applications in order to actively induce sharing and participation.

2.2 Features of Web²

2.2.1 Sensor-Generated Information

In Web² environments, unique and diverse services are created and provided through sensor-generated information. Based on the microphones, cameras, motion sensors, proximity sensors, and location sensors that are built into smart phones, applications are appearing that utilize sensor-generated information [6]. Sensor networks such as digital cameras, mobile phones, LBS (Location Based Services) equipment, RFID (Radio-Frequency Identification), etc. are creating the phenomenon of an "Internet of Things" that connects humans with things and things with things. This phenomenon enables consumers to easily obtain historical or geographical information by attaching tags to information [9]. Representative utilizations of sensor-generated information include "augmented reality" (AR) which refers to technologies that combine virtual information with the real world in real time to give the information [10]. Unlike virtual realities, where all environments are produced as 3-dimensional computer images, here virtual information is superimposed on real images. Thus, the sense of reality is improved. In the case of the iPhone's Sekai Camera application, letter information (names, reputations, etc.) called "air tags" are provided along with photos and other information buildings, restaurants, etc. These are shown through the iPhone's camera. These services create added values such as convenience, sympathy in experiences, safety, efficiency, etc., and are actively applied in the mobile broadcasting,· advertising, education, game, and medical manufacturing industries [11]. Large volumes of data in the real world come to meet the web in real time through sensor-generated services.

2.2.2 User-Generated Information

Web² has a feature called "crowd sourcing" that enables large groups of people to create collective works with higher values than the works of individual participants [12]; as it has become possible to share information by exchanging contents and services in real time through smart phones, the web has become much more interactive. The mapping between non-structured data generated by users and structured datasets is becoming a core capability of Web². Examples of this include Twitter, which is a network of micro-blogs; the "information cascades" posted on Twitter spread from Twitter to become fundamental sources of information for many people who want to know what happened. Operations such as adding data points on maps through web mapping applications take the form of collective intelligence through users' searches and responses in real time and information sharing in real time [6]. User-generated services are currently enjoying the limelight, as they provide relation-type services based on the characteristics of speed and novelty.

3 Security Issues in Web² Mobile Phones

3.1 Changes in Security Issues in Relation to the Evolution of the Web

As the web evolves, the technologies and services are rapidly converging and being standardized. However, matters related to security are not keeping pace [13]. As a result of this weakness, there have been attempts to illegally obtain numerous datasets provided in web services [14]. The early Web 1.0, designed to receive the information and services unilaterally provided by portal service businesses, was composed of HTML, URL, and HTTP. It provided the elementary interactions of simple clicks through links. To overcome the early static HTML environments, technologies such as the Java applet, Java script, and ActiveX appeared. However, they were directly related to the vulnerability of security [15] because using Java script, which had many weaknesses in security, or imprudently using ActiveX with unidentifiable providers, was fatal for security. Meanwhile, Web 2.0 services that provided user participation, sharing, and high openness included all the security issues in the existing web while having wider areas that could be attacked than the existing web services. This was due to the additional methods of accessing services and the interactive and asynchronous operation method of Web 2.0 [16]. For instance, in Web 2.0, an XML content feed that uses the RSS and Atom standards is used. This feed not only enables both users and web sites to obtain the headlines and texts of contents, but also basically enables users to see the summaries of relevant web sites. Unfortunately, there is a problem with this: it is not perceived that the applications and added systems used in these processes are vulnerable [3]. It is expected that issues of web security will not go away in the course of evolution into Web². In the case of Web² represented by AR, Real-Time Web, and SNS, it is expected that not only will security issues in the existing Web 2.0 be included, but the scope will also be widened due to the expansion of mobile services, the strengthening of mutual connectivity between users, and the use of sensor networks. Thus, security is becoming more important. This can be identified through recent research such as studies on security vulnerabilities in the mobile web [17]; these analyzed the mobile ubiquitous sensor network (USN) technology and cases of security vulnerabilities [18]; threats to security in SNS environments and related countermeasures, based on Europe ENISA reports [19]; and the sharing and protection of identities in SNS environments [20]. Therefore, it is expected that in Web², along with the security issues that have appeared in Web 2.0, additional security problems resulting from the fusion of diverse technologies and services will occur. In Web² mobile environments, threats to security will exist due to rapid increases in the volume of data communications using mobile sensors such as AR, followed by the volume of data created by users resulting from increased use of SNS. The changes in security issues resulting from the evolution of the web are shown in Table 1.

In the existing Web 2.0, it is considered that the data created through the participation of a small number of professionals would represent only a small part.

Table 1. Changes in security issues resulting from the evolution of the web

Classification	Web 1.0	Web 2.0	Web²
Characteristics	Information and services unilaterally provided by portal service businesses	User participation, sharing, and high openness	Expansion of mobile services, strengthened mutual connectivity between users, and the use of sensor networks
Representative Technology and Services	HTML, ActiveX	AJAX, FLAX, XML, RSS, Atom, Tagging, LAMP	AR, Real-Time Web, SNS
Security	Weakness due to using ActiveX and dependence on OS/browser	Wider areas that may be attacked compared to Web 1.0 services due to the additional methods of accessing services and the interactive and asynchronous method of operation	Wider areas that may be attacked compared to Web 2.0 services due to the fusion of diverse technologies and services, such as the expansion of mobile services and the use of sensor networks

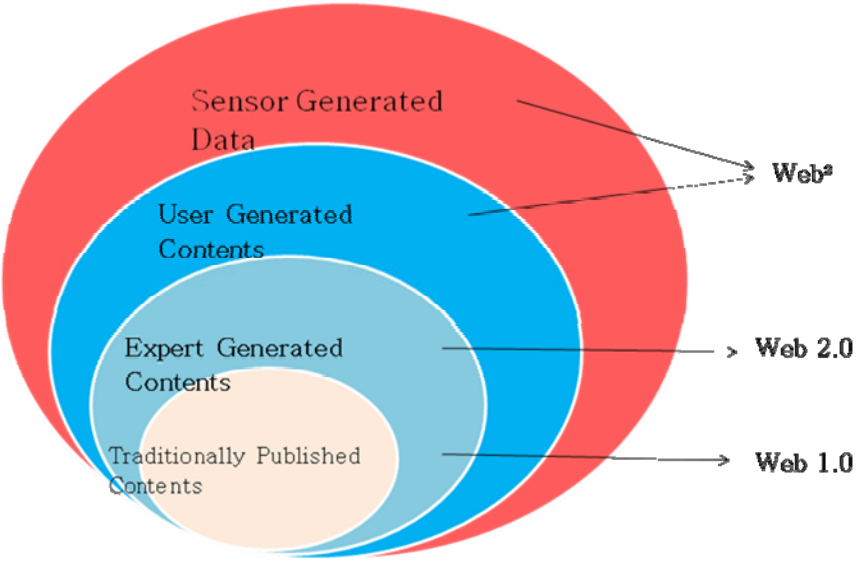

Fig. 1. Data types generated by Web²

3.2 Security Issues in Web²

For Web², it is expected that the security issues related to smart phones will further increased. In this study, the most important characteristics of Web² services were seen as sensor-generated information for the implementation of AR, etc., and user-generated information for the implementation of SNS. Therefore, the security issues that will appear in new forms in these two dimensions will be discussed as the most pertinent issues for Web².

3.2.1 Security Issues Related to Sensor-Generated Data

One of the most important characteristics of Web² is that information can be generated by sensors. In particular, smart phones may create unique services using 3-axis accelerometers, proximity sensors, and ambient light sensors. They may also provide location information services. In addition, as shown in the case of the sport kit combined with Nike, smart phones provide unique services that enable users to access their exercise information and history on the web, along with other sensors. One problem with these sensor-based services is that they can be vulnerable in terms of security. For instance, a small USB receptor module can be produced in order to detect a Nike+iPhone (or iPod) sensor UID. The Nike+iPhone serial communication tool will provide functions such as simultaneous traffic logging for two serial ports, receiver initializations, rink command transmissions, and operation time logging with sensors in operation; thus, when many traffic logs overlap, the protocol between the iPhone and the receiver, as well as the data exchanged, can be accessed by illegitimate users. In addition, embedded modules that log and track of Nike+iPhone sensors can be developed using Intel's iMote2; malicious persons will be able to collect real-time location information from GPS sensors through the embedded modules. In addition, it will become possible to monitor the sensor data transmitted from Nike+iPhone sensors utilizing Linux-based Gumstix and the existing iPod. In this case, it will be possible to track many people with sensors through the above mentioned equipment. Sensor-generated security issues include methods of attacking the above-mentioned smart phones. For instance, with the information disclosure type of attack, users' jogging routes and daily schedules can be stolen and, if similar sensors are systematically used by businesses later, the businesses may infringe customers' privacy by tracking customer information when customers visit stores for the first time. In addition, batteries may be exhausted through continued communications with sensors. Moreover, cross-platform-type attacks that infect computers or induce the deterioration of their performance when users check their personal exercise information will be also become possible.

3.2.2 Security Issues Related to User-Generated Data

Security issues related to user-generated include "social engineering hacking," which is an attack method by which an individual uses people's vulnerable points to get them to act in accordance with the attacker's intention so that he or she can obtain information. As social networks such as Twitter, mini home pages, blogs, and messengers have attracted huge numbers of users, this hacking method take advantage of the fact that hacking using social characteristics is easier than technical methods. As a result, damages such as the spread of malignant codes and phishing are rapidly increasing. The attacker collects information related to not only to family relations but also to friends, workplace lives, or social meetings. Attackers disguise themselves as friends or acquaintance in order to form trust when approaching the subject of attack. Later, when it is judged that trust has been formed, the attackers execute an attack based on the information collected. The subject of attack, that is, the victim, fails to understand the seriousness of the request of the attacker due to compensation or a sense of moral obligation and comes to accept and execute the request of the attacker [21]. Since open-type OS-based smart phones store a lot of confidential and personal information that is pursued by attackers, such as certification keys related to various

kinds of personal information transmitted through SMS, as well as e-payment information, if the information is leaked, the impact of the damage will be serious. The figure on the right side of Fig. 2 shows a case in some countries where the attacker sent SMS to victims and asked them to pay money to protect their information; as a result, many iPhone users suffered financial harm. As such, it is expected that hacking attempts targeting domestic smart phone users will frequently occur; since serious infringements on privacy may occur due to the hacking of malignant attackers, countermeasures are required.

4 Security Assessment Model for Web² Mobile Environments

To be prepared for security issues in Web² environments, the types of security issues and their potential threats should first be assessed. For instance, Kim and Kang (2009) divided the attacks that could be made in mobile environments into six types: wireless attacks, overcharging attacks, viruses and worms, break-in attacks, DoS (Denial of Services) attacks, and loss or theft [22]. Furthermore, Jang (2010) divided such threats into four types: threats of mobile malignant codes, attacks on the vulnerable points of mobile applications, attacks on mobile platforms, and access to networks without considering security [2]. In addition, Guo et al. (2004) divided the types of threats into attacks on smart phones and attacks through smart phones; they divided attacks on smart phones into attacks through the Internet, infections in synchronization with PCs, and attacks or infections from other smart phones through Bluetooth or UWB [23]. Since the security of smart phones is achieved through organic relations that involve the responsibilities of developers, distributors, and users, it is destined to be affected by mobile OS, applications, mobile platforms, and networks. Since this study is assessing the new threats to security that are expected to appear in Web², the threats will be divided according to the characteristics of Web² for review.

4.1 Threats to Sensor-Generated Data

It is expected that information installed in smart phones that is generated by many sensors, such as 3-axis accelerometers, proximity sensors, and ambient light sensors, will mainly be vulnerable to threats through mobile OS and mobile applications as follows.

- ***Threats through mobile OS*** use the characteristics of OS. Whereas the iPhone and Blackberry have closed-type platforms, the Symbian, Android, and Windows mobiles have open type platforms. Functions that block untrusted information are limited or lacking; in particular, iPhones show serious security problems due to Jail Break. Although the security of iPhones is considered better that those of other OS, Jail Break phones are vulnerable to attacks by hackers and can be remotely controlled by others. These are called zombie phones. In addition, the user will not only suffer monetary damage, but his/her privacy will also be infringed on because his/her current location can be grasped through information generated by sensors such as GPS.
- ***Threats through mobile applications*** can be divided into two types. The first inserts viruses, worms, malignant codes, etc. into applications downloaded by smart

phone users from the App Store. These interfere with the smart phone users' control over information or seize personal information. This type may falsify files internal to smart phones or exhaust batteries. The second type attacks the vulnerable points of mobile applications and applications that have not been carefully verified in relation to security have many vulnerable points. Abusing this, the attackers cause problems such as illegally accessing networks or obtaining the authority to control mobile devices [2].

4.2 Threats Involving User-Generated Data

Threats involving user-generated data are security issues arising from human relations in connection with the provision of SNS among the characteristic services of Web². It is considered that the services will be vulnerable mainly to threats made through access to mobile platforms and networks, as follows.

- ***Threats through mobile platforms*** exist in the App Store. In the case of Google's Android Market, separate processes to examine the registrations of applications have not been put in place; thus, it is difficult to block the registration of illegal applications and, in the case of iPhone, due to the closed OS operation, some users refuse the operation. In case the phones go through Jail Breaking, which refers to arbitrary device transformations or modifications, applications that have not gone through security checks can be easily downloaded so that the phones will have serious vulnerable points. Serious problems may result such as the rapid reduction of the life of batteries, controlling the devices remotely, and the leakage of personal information.
- ***Threats through access to networks*** occur in the representative networks used by smart phones such as mobile communication company networks (3G), WiFi, and Bluetooth. Recently, with the development of wireless interfaces such as Bluetooth and wireless LAN, free access to networks is guaranteed anytime and anywhere. However, due to careless management, cases of malignant uses such as leaking or monitoring personal information by abusing social closeness occur frequently. Through smart phones, which have limited functions compared to PCs, networks can be contaminated with viruses or malignant codes. The risk that smart phones will be exposed to attacks such as packet sniffing and phishing will be larger in future. Based on the issues mentioned so far, the routes and contents of damage are organized by the type of security issue in Table 2. As reviewed so far, it is expected that threats to sensor-generated data will mainly arise through the characteristics of smart phones, and threats to user-generated data by the users participating in the relevant network. In Web 1.0, although there were no sensor-based services, there were system-centered services provided that involved many vulnerable points, mainly in OS and applications. In Web 2.0, since participation and openness-centered services were provided, in addition to the existing problems in mobile OS and applications, security problems in terms of access to mobile platforms and networks were larger. Since systems have become more sophisticated though the use sensors, and because the active role of participants is emphasized, it is considered that for Web², there will be problems at higher levels than those in Web 1.0 and 2.0; furthermore, sensor- and user-based issues should also be emphasized. Therefore, as shown in Fig. 2, all security issues will be taken into account and a framework to develop security assessment models for Web² will be presented.

Table 2. Web² mobile security threats

	Type of threat	Threatened route	Result of threat	
Sensor Generated Threat	Threats through mobile OS	• Identify theft program • Permission system • Signature authentication system • Jail Break	• Remote controls • Acquisition of authority to control mobile devices • Reduction in the life of batteries • Zombification of contaminated smart phones	• Leads to monetary damage • Seizing personal information • Privacy infringement • Illegal marketing resource
	Threats through mobile applications	• Virus worm, applications downloaded with malignant codes • Application attack of vulnerable points		
User Generated Threat	Threats through mobile platforms	• Malignant access by careless management of wireless interface • Network contamination		
	Threats through access to networks	• Illegal remodeling and transformation • Application market's weak security		

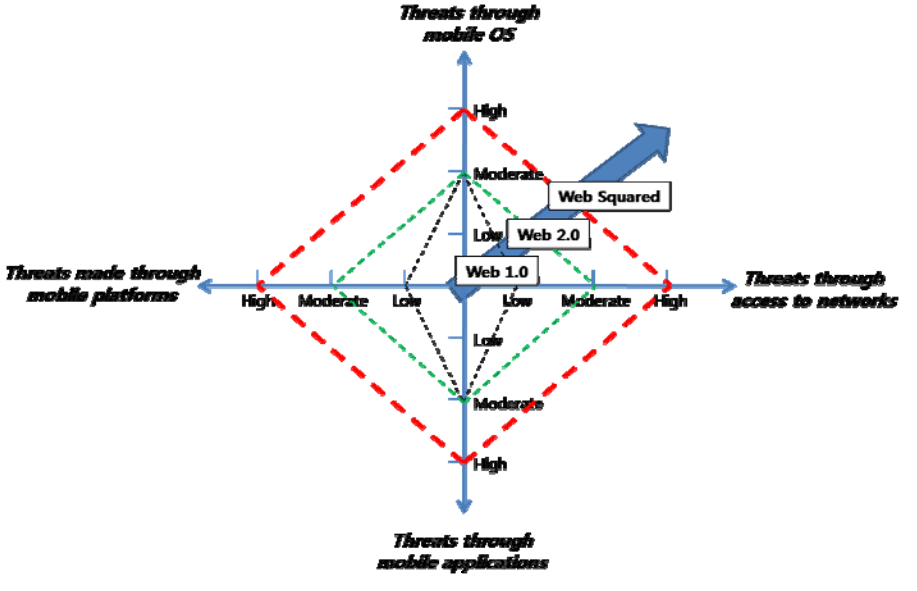

Fig. 2. Security assessment model for web² mobile environment

5 Conclusion and Implications

Unlike security in general information communication technologies, security issues in mobile environments are thought to be relatively less important; thus, research on them has remained at a conceptual level. However, in reality, smart phones are being supplied as a result of the rapid development of mobile environments; thus, it is expected that Web² mobile security issues will be intensively examined when monetary losses occur or when the profitability of new business models in Web² are emphasized. The goal of this study was to prepare for this very issue; its major purpose was to analyze security assessment models for Web² mobiles. To draw the model, along with defining Web² as interactions between the web and the world, the characteristics of services provided in Web² environments were identified as sensor-and user-generated services. Then, the security issues of Web² mobile phones were reviewed based on the characteristics of Web² already delineated. Various types of threats to security related to mobile environments were reviewed by type; these were organized and presented as threats related to sensor- and user-generated data in the context of Web². This review also included the types of security issues, the routes of damage, and the contents of damage. As an outcome of the study, a security assessment model for Web² mobiles was presented. It was argued that threats related to sensor-generated data mainly involved mobile OS and mobile applications; threats related to user-generated data mainly occurred through mobile platforms and access to networks. In this framework, it is judged that, in Web 1.0, importance was attached to systems and sensors; in Web 2.0, the threats to security in Web 1.0 remained, while threats involving user-generated data appeared as new vulnerable points. It is expected that, for Web² mobiles, all these levels of threats to security will be included, while threats related to sensor- and user-generated data will become larger. This study has implications for businesses and related researchers that provide diverse services, and can help them to prepare themselves for Web². First, potential threats to security in mobile environments such as threats made through mobile OS, mobile applications, mobile platforms, access to networks were reviewed. Thus, discussions from diverse viewpoints related to smart-phone security are possible, including those of developers, distributors, mobile communication businesses, vaccine businesses, the government, and research institutions. For instance, users should pay attention to autonomous security such as safety rules in relation to the use of smart phones. Mobile communication businesses should develop and apply technologies that would fundamentally block and eradicate malignant codes that are transmitted as SMS. Manufacturers should apply security technologies when sending/receiving financial or personal information, and should support the encoding of personal information stored in terminals. Mobile platform businesses should establish criteria and systems for the verification of security of the S/W registered in the market and support environments for the development of safe application programs. Vaccine businesses should develop vaccines optimized by considering the storing devices and battery capacities of terminals, which are different from those in general PC environments; they should research and develop vaccines for different OS, which vary with their terminals. The government and research institutions should establish systems of response and cooperation with related organizations; they should also make efforts to develop procedures to respond to smart phone security accidents. In this study, it is suggested that security issues in

Web² cannot be completely solved by simple countermeasures and preventive measures for the devices themselves. For instance, not only threats by sensors, but also threats by users of Web² where participation is emphasized have been presented. Therefore, if threats to mobile security are ignored and attention is concentrated only on the growth of the market and the visible growth of smart phones, technical and political issues that can be solved now may be missed; thus, great social costs may have to be paid later. There is a concept called "techno science" that refers to the idea that revolutions in digital information communications will affect all parts of our daily lives, forming a new culture. This means that new technologies such as smart phones will penetrate into our daily lives and change our cultures accordingly. To establish safe mobile ecosystems for Web² mobiles where the paradigms have changed, we should continuously prepare and develop our mobile cultures.

Acknowledgement

"This research was supported by the KCC(Korea Communications Commission), Korea and KISA(Korea Internet & Security Agency) under the Security System Development for New IT Service program."

References

1. Ji, S.J., Jung, S.Y., Lee, J.H.: Opportunities and Threats of Smart-phone. In: Internet & Security Issues, Korea Information Security Agency, Seoul, Korea (2010)
2. Jang, S.K.: Security Threats in Smart-phone environment. Korea Information Processing Society Review 17, 64–69 (2010)
3. Park, J.H.: Web 2.0 Technical Trend and Web Security Threat Analysis. In: Korea Information Security Agency (2006)
4. Youm, H.Y., Lee, J.S.: Web 2.0 Security Technology Trends and Promoting Standardization. Journal of Telecommunications Technology Association 117, 21–29 (2008)
5. Lee, C.Y., Kim, C.H., Lee, J.H.: Security Problems and Effective Measures of Inspecting Web in Web 2.0. Korea Institute of Information Security and Cryptology 18, 25–33 (2008)
6. O'Reilly, T., Battelle, J.: Web Squared: Web 2.0 Five Years on. O'Reilly Media, Inc., Sebastopol (2009)
7. Kim, S.H., Kim, H.D.: A Study of Web 2.0 Trend & Service View. Research on Digital Policy 5 (2007)
8. Salomon, M.: Would you consider using online virtual worlds for meetings. Telecommunications Journal of Australia 59 (2009)
9. Graham, M.: Transparency and Development: Ethical Consumption and Economic Development through Web 2.0 and the Internet of Things (2010)
10. Wagner, D., Schmalstieg, D.: First Steps Towards Handheld Augmented Reality. In: Proceedings of the 7th IEEE International Symposium on Wearable Computers (2003)
11. Jung, D.Y.: The changes of future that the augmented reality will bring, Samsung Economic Research Institute, Seoul, Korea (2010)
12. Geser, H.: Augmenting things, establishments and human beings (2010)

13. Hong, K.Y., Hong, K.W., Park, J.W., Lee, K.H.: Web Service Security Technology Standardization Trends. Korea Institute of Information Security and Cryptology 14 (2004)
14. Lim, C.G., Ahn, D.S., Kim, K.H., Lee, K.Y.: A Study on the Web Service-Hacking Pattern Recognition System. Webcasting Internet and Telecommunication Review 9 (2009)
15. Lee, W.T., Lee, J.E., Yang, S.C., Hwang, Y.S.: The Changes of Citizens' E-participation and Political Implication in the Age of Convergence between Broadcasting and Telecommunication. Korea Information Society Development Institute (2008)
16. Ritchie, P.: The Security Risks of AJAX/Web 2.0 Application. Network Security 200, 4–8 (2007)
17. Kim, W.J., Moon, Y.J., Lee, S.J.: A Study on the Security Vulnerability and Countermeasure in the Mobile Web 2.0 Environments. Journal of Electrical Engineering and Information Science 34 (2007)
18. Lee, H.D., Park, N.J., Choi, D.H., Chung, K.I.: A Case Study on Mobile USN Technology and Weakness. Korea Institute of Information Security and Cryptology 18 (2008)
19. Korea Information Security Agency, Threats and Countermeasures on Social Network Environment. Information Security Issue Report, Korea Information Security Agency, Seoul, Korea (2007)
20. Lee, H.H., Choi, H.C., Kim, J.H., Cho, S.R., Jin, S.H.: A Study of Sharing Identity and Protect on SNS Environments. Korea Institute of Information Security and Cryptology 19 (2009)
21. Ahn Lab, `http://kr.ahnlab.com/info/securityinfo`
22. Kim, K.Y., Kang, D.H.: Smart-phone Security Solutions in Open-mobile Environment. KIISC Review 19, 21–28 (2009)
23. Guo, C., Wang, H.J., Zhu, W.: Smart-phone Attacks and Defenses. In: Third Workshop on Hot Topics in Networks HotNets-III, San Diego, CA, USA (2004)