A Method of Risk Assessment for Multi-Factor Authentication

Jae-Jung Kim* and Seng-Phil Hong**

Abstract—User authentication refers to user identification based on something a user knows, something a user has, something a user is or something the user does; it can also take place based on a combination of two or more of such factors. With the increasingly diverse risks in online environments, user authentication methods are also becoming more diversified. This research analyzes user authentication methods being used in various online environments, such as web portals, electronic transactions, financial services and e-government, to identify the characteristics and issues of such authentication methods in order to present a user authentication level system model suitable for different online services. The results of our method are confirmed through a risk assessment and we verify its safety using the testing method presented in OWASP and NIST SP800-63.

Keywords—Multi-factor Authentication, PKI, User Authentication, Biometric Authentication

1. INTRODUCTION

Many different types of online services have become available with the development of the internet. However, because the internet does not enable direct interaction between users, there are no methods of physical authentication for users who access important resources. Thus authentication of lawful users of internet services is paramount. As hacking technologies have become more diversified and advanced, security and authentication have become unable to rely on ID and password-based authentication alone. Single-factor authentication using an ID and password has been found to be vulnerable to malware attacks, replay attacks, offline brute force attacks, key logger Trojans, dictionary attacks and shoulder surfing. In recent times, there has been an increase in multi-factor authentication methods based on human characteristics, such as fingerprint recognition.[1] In addition, the number of government policies demanding mandatory multi-factor authentication is increasing.[2]

1.1 Types of User Authentication

1.1.1 Single-Factor Authentication

Authentication is a process of user identification based on the following elements [3].

※ This research paper is supported by Seoul R&BD Program (JP090988)
Manuscript received August 11, 2010; accepted September 9, 2010.
Corresponding Author: Sengphil Hong
* First Author, Dept. of Computer Science, Sungshin W. University, Seoul, Korea (jajukim@hotmail.com)
** Corresponding Author, Professor of Dept. of Computer Science, Sungshin W. University, Seoul, Korea (philhong @sungshin.ac.kr)

Table 1. Types of Authentication

Authentication	Types
Proof-of-Knowledge (Something you know?)	Passwords, PIN, Mom's Name, Phone# , etc
Proof-of-Possession (Something you have?)	Smartcards, Tokens, Driver's license, PKI certificates
Proof-of-Characteristics (Something you are?) -physiologically or behaviorally	Fingerprints, Hand geometry, Facial image, Iris, Retina, DNA, voice, signature patterns

1.1.2 Multi-Factor Authentication

Multi-factor authentication is a method of user identification that combines a number of single factor authentications. It is used for priority customer information and high-risk financial transactions [4]. The strength of an authentication mechanism can be judged on how many things it depends on [5].

1.2 Types of User Authentication

Various user authentication methods including name verification, mobile phone verification, i-PIN[6], electronic payment (VISA Anshim Click, Internet Secure Payment(ISP)), accredited certificates[7] and fingerprint authentication[8] used in user authentication for web portals, e-transactions, financial institutions (banks) and e-government services are shown in Table 2.

Table 2. User authentication methods for various services

Service	Function		Know
Web portal	Log-in (optional)		ID/PW, OTP
	Registration		Name verification, i-PIN, mobile phone authentication
	ID/password retrieval (one selected)		E-mail notification, Registered mobile phone, User authentication through mobile phone, Accredited certificate, ID card data verification, Credit card verification
E-transaction	Log-in		ID/PW, Accredited certificate
	Electronic payment	Account transfer	Account information + Accredited certificate
		Credit card payment	Credit card information + Accredited certificate - VISA Anshim Click - Internet Secure Payment (ISP)
		Mobile phone payment	Mobile phone information + resident registration number
Financial institution (Internet banking)	Log-in		Accredited certificate, ID/PW
	Account transfers	Type 1	Accredited certificate + OTP generator
			HSM Accredited certificate + security card
			Accredited certificate + security card + 2-channel authentication
		Type 2	Accredited certificate + security card + SMS
		Type 3	Accredited certificate + security card
E-government (Public Procurement Service[9])	Log-in		Accredited certificate
	Electronic bidding		Accredited certificate + fingerprint security token

2. USER AUTHENTICATION AND LEVEL OF ASSURANCE MODEL

2.1 United States

The Office of Management and Budget (OMB 04-04) [10] describes four levels of identity authentication assurance levels. Each assurance level describes the degree of confidence in that the user that presented a credential (e.g. a password) is in fact that user.

Table 3. Authentication levels of assurance (OMB 04-04)

Level	Description
Level 1	Little or no confidence exists in the asserted identity; usually self-asserted; essentially a persistent identifier
Level 2	Confidence exists that the asserted identity is accurate; used frequently for self service applications
Level 3	High confidence in the asserted identity's accuracy; used to access restricted data
Level 4	Very high confidence in the asserted identity's accuracy; used to access highly restricted data

NIST 800-63 Electronic Authentication Guideline [11] provides technical requirements for each of the authentication levels of assurance defined in OMB 04-04. Each assurance level has defined controls for identity proofing, token (secret) requirements and authentication/assertion protection mechanisms as summarized in the table below.

Table 4. Technical Requirements of NIST 800-63

Level	Identity Proofing	Token (Secret)	Authentication Protection Mechanisms
1	Requires no identity proofing	Allows any type of token including a simple PIN	Little effort to protect sessions from off line attacks or eavesdroppers, only one token is required.
2	Requires some identity proofing	Allows single-factor authentication. Passwords are the norm at this level	On-line guessing, replay and eavesdropping attacks are prevented using FIPS 140-2 approved cryptographic techniques.
3	Requires stringent identity proofing	Multi-factor authentication, typically a password or biometric factor used in combination with a 1) software token, 2) hardware token, or 3) OTP device token	On-line guessing, replay, eavesdropper, impersonation and man-in-the-middle attack are prevented. Cryptography must be validated at FIPS 140-2 Level 1 overall with Level 2 validation for physical security.
4	Requires in-person registration	Multi-factor authentication with a hardware crypto token.	On-line guessing, replay, eavesdropper, impersonation, man-in-the-middle, and session hijacking attacks are prevented. Cryptography in the hardware token must be validated at FIPS 140-2 level 2 overall, with level 3 validation for physical security

2.2 Canada, Province of British Columbia (BC)

The Electronic Credential and Authentication Standards [12] published by the Province of BC in Canada have the following levels.

Table 5. Authentication levels of assurance in Canada

Level		Description
1	Low	Credential validated or provision of shared secret/file knowledge is a match
2	Medium	Possession of single-factor credential validated by successful log on, in-person presentation or telephone verification with shared secret
3	High	Owner of multi-factor credentials substantiated by successful log on or in person presentation(e.g. software certificate or OTP; multi-factor physical ID card)
4	Very High	Owner of hard multi-factor credentials corroborated by successful log on or biometric match (e.g. PKI and/or high quality biometric)

3. UALS (USER AUTHENTICATION LEVEL SYSTEM) MODEL

3.1 Types and Characteristics of User Authentication

Table 6 shows categorization of user authentication methods used in Korea by the characteristics [13].

Table 6. Categorization of user authentication methods

Authentication Factors: Something You ___				
Know	***Have***			***Are***
Text PIN	IP Address	Accredited certificate	Scratch-off/Bingo card	Fingerprint
Visual PIN	Browser Type	Credit card Information	Phone/PDA, w/OTP	Hand Geometry
Text Password	Cookie	Bank Account Information	OTP Generator	Face Recognition
Life Questions	Email Address	Security Card(Grid card)	USB Device	Iris Recognition
SMS Message	Toolbar/Agent	Mobile Phone Authentication	Proximity/Smartcard	Retina Recognition
	Identification card	i-PIN(ID/PW)	Secure HSM	

3.2 User Authentication Level System

As many diverse user authentication methods are provided by different services, a standard definition of levels in user authentication has come to be required. Accordingly, a 5-level user authentication system is presented as follows.

3.2.1 Level 1

Level 1 uses registered information of offline identification such as credit card information, bank account information, i-PIN, OTP, etc.

#	Authentication method	
	Something You Have	**Something You Know**
①	Credit card information (RRN, credit card number, expiry date, CVC number)	+ Credit card password
	⇨ Stringent ID verification required in credit card issuance and delivery in an offline environment	
②	Bank account information (name, RRN, account number, bank name)	+ Account password
	⇨ Keyboard protection and security channels must be activated when entering or transmitting account information and password	
③	Mobile phone verification (RRN, mobile phone#)	+ SMS verification
	⇨ RRN is referenced to check the name in which a mobile phone is registered and possession of mobile phone is checked via SMS	
④	i-PIN	(ID/PW)
	⇨ User authentication issue still remains as ID and password issued through identification using accredited certificates, credit cards and mobile phones	
⑤	OTP generator	(single-use password)
	⇨ OTP can be used instead of an ID and password	

3.2.2 Level 2: Soft Token + Password

Level 2 uses an accredited certificate issued by a CA after a CA identifies the user with a reliable certificate issued by the government such as an NID card, driver's license, passport, etc.

#	Authentication method	
	Something You Have	**Something You Know**
①	Accredited certificate	+ Certificate password
	⇨ Certificates issued through in-person ID verification can achieve reliable online user authentication	

3.2.3 Level 3

Level 3 uses an accredited certificate with another security measure such as security card, mobile phone (some form of storage media), security token, etc.

#	Authentication method	
	Something You Have	**Something You Know**
①	Accredited certificate + security card	+ Certificate password
	⇨ Issues can arise if a security card issued through in-person identification is lost or scanned	
②	Accredited certificate + security card	+ Certificate password + mobile phone SMS
	⇨ Transaction details are sent to user's mobile phone via SMS to ensure that a transaction made is correct	
③	Accredited certificate + mobile phone (storage device)	+ Certificate password
	⇨ Accredited certificate is saved in a mobile device for use anytime; wired/wireless transmission of certificate information must be performed in a safe manner	
④	Accredited certificate + security token	+ Certificate password + PIN
	⇨ A security token controls passwords and is protected by a PIN; it is a safe portable storage device that stores Accredited certificates and enable s electronic signatures to prevent the exposure of personal keys ⇨ Security tokens used to store Accredited certificates must be quality-approved by a recognized organization, e.g., Root CA	

3.2.4 Level 4

Level 4 uses an accredited certificate with other hardware devices such as an OTP, security token, 2-channel authentication, etc.

#	Authentication method	
	Something You Have	**Something You Know**
①	Accredited certificate + security card + security token	+ Certificate password + PIN
	⇨ Accredited certificate is saved in a security token for protection and use with a security card	
②	Accredited certificate + OTP generator	+ Certificate password
	⇨ Accredited certificate is used together with a safe OTP generator instead of a security card; additional costs for OTP generator use are incurred	
③	Accredited certificate + security card + 2-channel authentication	+ Certificate password
	⇨ A method of using an Accredited certificate and security card for verification followed by a final confirmation using the internet, phone or fax ⇨ 2-channel verification involves user authentication using 2 different communication channels, e.g. internet and phone or phone and fax	

3.2.5 Level 5: Hard Token + Biometric

Level 5 uses an accredited certificate with biometric information such as a fingerprint, etc.

#	Authentication method		
	Something You Have	**Something You Know**	**Something You Are**
①	Accredited certificate + security token	+ Certificate password + PIN	+ Fingerprint
	⇨ Accredited certificate and fingerprint are saved in a security token and authentication is performed using a PIN and certificate password		
②	Accredited certificate + security token	+ PIN	+ Fingerprint(=certificate password)
	⇨ Accredited certificate and fingerprint are saved in a security token; the security token is accessed using a PIN and the fingerprint is used for verification instead of a certificate password for user convenience		
③	Accredited certificate + security token	+ Certificate password + PIN	+ Biometric
	⇨ Accredited certificate is stored in a security token and accessed using a PIN and certificate password; authentication is performed using the user's biological information (palm, iris, face, retina)		

3.3 Selection of User Authentication Methods

The process of user authentication method selection is as follows.

1) Transaction types, risk levels, user authentication methods and additional security measures used in the concerned service are examined.
2) Threats and vulnerabilities in user authentication are analyzed.
3) Influences on various transactions are analyzed and risk assessment is performed to identify the frequency and severity of such threats and vulnerabilities.
4) A user authentication method is selected based on a suggested user authentication level system.
5) After applying the user authentication, a test is performed to ensure that the risk has been eliminated.

Table 7. Risk Assessment Criteria [14]

Criteria	Description
Service outline	Outline of customers, customer types, data flow, etc.
Transaction analysis	Analysis of various risk levels for various transaction types (e.g. transaction types, risk levels (high, med, low), authentication methods, additional security measures)
Transaction range	Verification of transaction types and range that require additional authentication
Promotions	Verification of provision of information to customers who use the service in preparation for possible threats (password management, transaction verification, etc.)
Customer categorization	Verification of appropriate authentication methods being used by different customer types
Influence on transactions	How many high-risk transactions take place per day? How will the application of multi-factor authentication influence customer service?

6) Regular ongoing risk assessment and management are performed.

3.4 Evaluation of Stability

Each of the authentication levels of assurance defined in the UALS model added and evaluated items based on technical requirements in the NIST SP800-63.

Table 8. Token types allowed at each assurance level

Token Type	Level 1	Level 2	Level 3	Level 4	Level 5
Bio-Hard crypto token	√	√	√	√	√
Hard crypto token	√	√	√	√	
One-time password device	√	√			
Soft crypto token	√	√			
Passwords & PINs	√				

Table 9. Required Protections

Protect against	Level 1	Level 2	Level 3	Level 4	Level 5
On-line guessing	√	√	√	√	√
Replay	√	√	√	√	√
Eavesdroppers		√	√	√	√
Verifier impersonation			√	√	√
Man-in-the-middle			√	√	√
Session hijacking				√	√
Signer impersonation					√

Table 10. Authentication Protocol Types

Protect against	Level 1	Level 2	Level 3	Level 4	Level 5
Private key PoP	√	√	√	√	√
Symmetric key PoP	√	√	√	√	√
Tunneled or Zero knowledge password	√				
Challenge-response password	√				

Table 11. Additional Required Properties

Protect against	Level 1	Level 2	Level 3	Level 4	Level 5
Shared secrets not revealed to third parties by verifiers or CSPs		√	√	√	√
Multi-factor authentication	√	√	√	√	√
Sensitive data transfer authenticated		√	√	√	√

Table 12. OWASP Testing Item

Classification	Vulnerabilities
T1	Credential Theft (Phishing, Eavesdropping, MITM)
T2	Weak Credentials (Credentials Password guessing and Password Brute force attacks)
T3	Session based attacks(Session Riding, Session Fixation)
T4	Trojan and Malware attacks
T5	Password Reuse (Using the same password for different purposes or operations)

Stability in various user authentication levels can be verified using the multi-factor authentication testing method (OWASP-AT-009) provided by the OWASP (Open Web Application Security Project). [15]

3.5 User Authentication Scheme for Level 5

We propose a user authentication scheme for Level 5. This scheme uses public key infrastructure(PKI) with biometric information(Fingerprints) in order to provide more secure

Table 13. Roles of each entity

Entity	Description
User	The user is the owner of the device and has a unique ID such as a SSN (Social Security Number) issued by the government.
Device	The Device stores the device's certificate, user's certificate, and biometric information (Fingerprint) and has a unique serial number (SN) issued by its manufacturer.
SP	The Service Provider (SP) provides various internet services and these services require user authentication. The SP has a unique ID such as a business registration number (BRN) from the government.
CA	The Certification Authority (CA) identifies each entity such as a user, SP, and device, and issues a certificate.
BA	Biometric Authority (BA) identifies the user and manages the user's biometric information such as fingerprint etc.

Table 14. Notations in the authentication scheme

Symbol	Description	Symbol	Description
R_1, R_2, R_3	Random number	H()	Hash function
$\|\|$	concatenation	CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol	CMP	Certificate Management Protocol
S	RSA Signature	V	Verify RSA signature
E	RSA Encryption	D	RSA Decryption

and reliable user authentication.

We use the double-hashed value that hashes a secret random number with an ID such as a SSN, BRN, etc. This method refers to the subject identification method in RFC 4683 [16].

$$V = Hash\ (Hash\ (SSN||R)),\ R=512bits$$

3.5.1 The process of certificate issuance and sign up site

1) Issue SP's Certificate
   ① SP generates RSA key pairs, random number (R_3).
   ② SP requests certificate with R_3 from the CA using CMP.
   ③ CA generates V_3=H (H (BRN||R_3) and issues certificate.
   ④ SP saves the certificate (V_3) and encrypted private (R_3).
2) Issue User's Certificate
   ① Device generates User's RSA key pairs.
   ② User generates random number (R_2).
   ③ User requests certificate with R_2 from the CA using CMP.
   ④ CA generates V_2=H (H (SSN||R_2) and issues certificate.
   ⑤ User saves the certificate (V_2) and encrypted private key (R_2) into the Device.
3) Issue Device's Certificate
   ① Device generates RSA key pairs.
   ② User sends SSN to Device by secure channel
   ③ Device generates random number (R_1).
   ④ Device requests certificate with R_1 from CA using CMP.
   ⑤ CA generates V_1=H (H (SN||SSN||R_1) and issues certificate.
   ⑥ Device saves certificate (V_1) and encrypted private key (R_1) into Device
4) Register Biometric Information (e.g. Fingerprint)

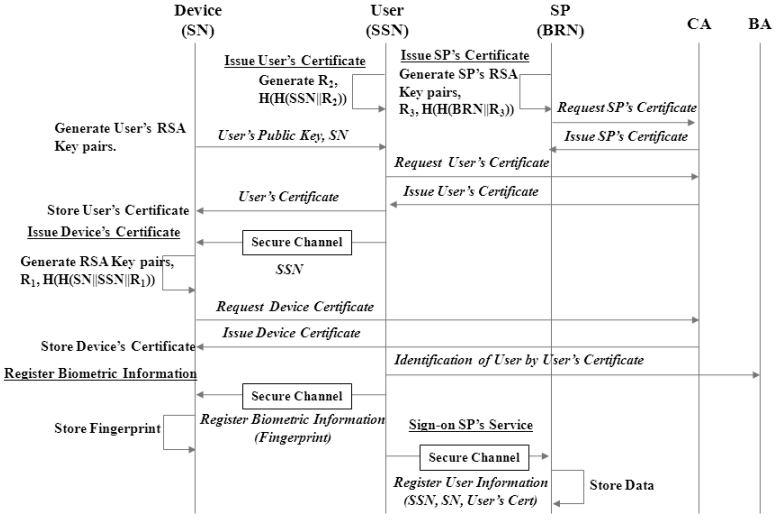

Fig. 1. The procedure of initial setup

① BA identifies User by User's certificate.
② User registers user's fingerprint information into Device.

5) Sign up for SP's service
① User registers User's information via secure channel.
② SP stores the received data from User securely.

3.5.2 The process of authentication among entities.

1) SP Authentication
① SP sends SP's certificate to User. This certificate will be used to encrypt the user's information.
② User verifies SP's certificate by CA's revocation information (CRL, OCSP etc.)

2) Device Authentication
① Device sends R_1, Device's Certificate (V_1), and SN to User by secure channel.
② User verifies Device's certificate by CA's revocation information (CRL, OCSP etc)
③ User generates T_1=H (H (SN||SSN||R_1) with SN, SSN, R_1 and compares them with T_1 and V_1 in Device's Certificate.

3) Biometric Authentication
① Device reads User's Biometric information (e.g. fingerprint) by secure channel.
② Device compares an inputted data with the stored data in the Device.

4) User Authentication
① User generates a digital signature that is encrypted by the SP's public Key.

$$E_{SP\text{-}pub}(S_{USER\text{-}pri}(R_1, R_2)), \text{ User's cert, Device's cert}$$

② User sends the signed and encrypted data to the SP.
③ SP decrypts the received data using the SP's private key.

$$V_{USER\text{-}pub}(D_{SP\text{-}pri}(E_{SP\text{-}pub}(S_{USER\text{-}pri}(R_1, R_2)))=(R_1,R_2)$$

④ SP verifies User's certificate and Device's certificate by CA's revocation information

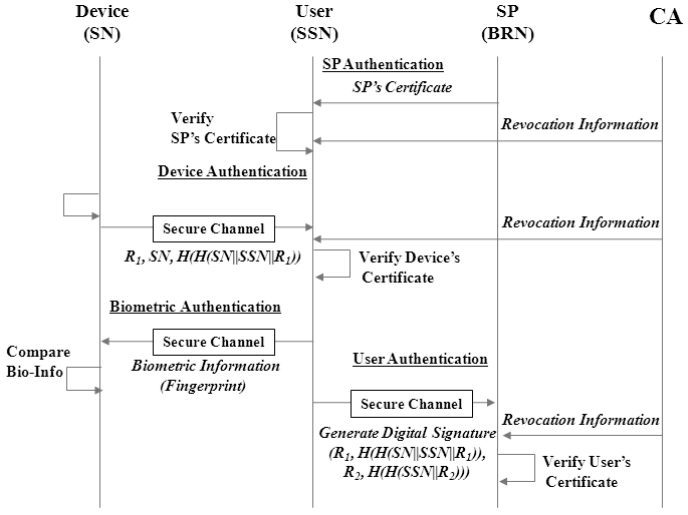

Fig. 2. The procedure of user authentication

(CRL, OCSP etc.)

⑤ SP selects user information (SSN, SN) from their database by subject dn in the user's certificate.

⑥ SP generates T_2=H (H (SSN||R_2) with SSN, R_2 and compares them with T_2 and V_2 in the User's Certificate.

⑦ SP generates T_1=H (H(SN||SSN||R_1) with SN, SSN, R_1 and compares them with T_1 and V_1 in the Device's Certificate.

4. CONCLUSION AND FUTURE WORK

In this paper, we improved the UALS (user authentication level system) model into a 5 level user authentication system. We proposed the user authentication scheme using public key infrastructure (PKI) with biometric in level 5, and we proposed how to select user authentication methods and how to evaluate them with a risk assessment procedure.

Our research makes three contributions. First, we showed and evaluated the improved UALS model using multi-factor authentication compared to other models using United States and Canadian methods. This model is more specific and safer than others. Second, we showed highly secure user authentication schemes using PKI and biometric in level 5. This scheme can be used for high-risk financial transactions or applications for which very high confidence is required in the identity assertion. Third, we showed the risk assessment for multi-factor authentication. Providers of online products and services can provide the customer with safe and reliable authentication measures by carrying out regular risk assessments to analyze the types and levels of risks involved in their products or services.

REFERENCES

[1] Dale Vile, Freeform Dynamic, "*User convenience versus system security*", 2006.
[2] Roger Elrod, "*Two-factor Authentication*", East Carolina University, 2005, July.
[3] [Definition] Wikipedia, Definition of Two Factor Authentication.
[4] Smart Card Alliance (Randy Vanderhoof), "*Smart Card Technology Roadmap for secure ID applications"*, 2003.
[5] Tim Hastings, *Multi-factor Authentication and the Cloud*, 2010.
[6] Korea Internet Security Agency, Introduction of i-PIN (http://i-pin.kisa.or.kr), 2010.
[7] Accredited Certificate: http://www.rootca.or.kr
[8] Public Procurement Service: http://www.g2b.go.kr
[9] Public Procurement Service(PPS), *Bidder Identification and Fingerprint Registration Process*, 2010, April.
[10] OMB M-04-04, *E-Authentication Guidance for Federal agencies*, 2003, December, 16.
[11] NIST, *Special Publication 800-63, Electronic Authentication Guideline*, 2006, April.
[12] Ministry of Citizens' Services, *Electronic Credential and Authentication Standard*, 2010, April.
[13] Bret Hartman, "*From Identity Management to Authentication: Technology Evolution to Meet Cyber Threats"*, ITAA IdentEvent 2008.
[14] Fidelity National Information Services, *Multi -Factor Authentication Risk Assessment*, 2006.
[15] OWASP foundation, *OWASP Testing Guide*, 2008 v3.0, pp.140-143.
[16] IETF RFC 4683, *Internet X.509 Public Key Infrastructure Subject Identification Method (SIM)*, 2006.10.

Jae-Jung Kim

He received his BS degree in Computer Science from Chungnam University in 1997 and MS degree in Information Security from Korea University in 2003, respectively. Since 1997, he stayed in LGCNS and Korea Information Certification Authority Inc. to develop PKI solutions. And now he is undertaking a doctorate course as a member of the information security lab at Sungshin University. His research interests include Public Key Infrastructure (PKI), cross certification, anonymous authentication, and device authentication.

Seng-Phil Hong

Professor Seng-Phil Hong received his BS degree in computer science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched information security for his PhD at the Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received a Ph.D. degree in computer science from Information and Communications University in Korea. He is actively involved in teaching and research in information security at The Sungshin Women's University, Korea. His research papers appeared in a number of journals such as ACM Computing and Springer-Verlag's Lecture Notes in Computer Science, etc. His research interests include access control, security architecture, Privacy, and e-business security.