JOURNAL OF KOREA MULTIMEDIA SOCIETY, VOL. 7, NO. 12, DECEMBER 2004(pp. 1719-1728)

Development of Security Service for Mobile Internet Banking Using Personal Digital Assistants

Young-yeol Choo[†], Jung-In Kim[††]

ABSTRACT

The fusion of Internet technology and applications with wireless communication provides a new business model and promises to extend the possibilities of commerce to what is popularly called mobile commerce, or *m-commerce*. In mobile Internet banking service through wireless local area network, security is a most important factor to consider. We describe the development of security service for mobile Internet banking on Personal Digital Assistants (PDAs). Banking Server and Authentication Server were developed to simulate banking business and to support certificate management of authorized clients, respectively. To increase security, we took hybrid approach in implementation: symmetric block encryption and public-key encryption. Hash function and random number generation were exploited to generate a secret key. The data regarding banking service were encrypted with symmetric block encryption, RC4, and the random number sequence was done with public-key encryption. PDAs communicate through IEEE 802.11b wireless LAN (Local Area Network) to access banking service. Several banking services and graphic user interfaces, which emulatedthe services of real bank, were developed to verity the working of each security service in PDA, the Banking Server, and the Authentication Server.

Keywords: M-commerce, wireless LAN, symmetric encryption, public-key encryption, PDA.

1. INTRODUCTION

Within the last few years, Internet has changed the way for commerce and offers quick and world-wide access to relevant marketing and business information. At the same time, owing to the technological advance in telecommunication and multimedia services, millions of users enjoy the convenience accrued from Internet, by using their computers or portable devices. With the deployment of new wireless communication technologies and new network devices, the number of users of mobile terminal (cell phones and Personal Digital Assistants (PDAs)) is rapidly increasing. In addition, performance increase in PDA makes it possible for Internet service provider to support various real-time services such as traffic information, location-based service (LBS), electronic commerce and so on. The fusion of Internet technology and applications with wireless communication provides a new business model and promises to extend the possibilities of commerce to what is popularly called mobile commerce, or *m-commerce*. Mobile electronic commerce is defined as any type of transaction of data including economic value and exploiting a mobile terminal at least at one end[1-3].

The mobile banking service, as a type of *m-commerce*, will enable people to access their account and transfer funds anytime, anywhere through their mobile devices such as cell phones and PDAs. The mobile banking service includes mobile payment, Internet billing, account aggregation, stock exchange, Internet shopping mall, and financial portal. Obviously, security and trust

※ Corresponding Author : Young-yeol Choo, Address : (608-711) 535 Yongdang-dong, Nam-gu, Busan, Korea, TEL : +82-51-610-8398, FAX : +82-51-610-8847
E-mail : yychoo@tit.ac.kr
[†] Dept. of Computer Engr., Tongmyong Univ. of Information Technology
[††] Dept. of Computer Engr., Tongmyong Univ. of Information Technology
(E-mail : jikim@tit.ac.kr)
Receipt date : May 4, 2004, Approval date : Aug. 11, 2004
※ This Work was supported by Tongmyong University of Information Technology Research Fund of 2004.

relationships are key issue for the success of mobile banking through mobile telecommunication networks and wired networks. In the telecommunication network, interruption during the roaming process is also one of the obstacles for guaranteeing security in mobile banking service. Mobile banking process includes complex security issues as follows.

- Reliable Communication networks.
- Encryption/decryption algorithm to prevent inappropriate disclosure of information.
- Authentication for the authorized users
- Digital signature to cope with repudiation.

Mobility and security support in Internet is expected to increase according to the deployment of IPv6 network[4,5]. Encryption/decryption can be categorized commonly as two types: symmetric encryption/decryption and asymmetric one[6]. Symmetric encryption is referred to single-key encryption because the same key is used during encryption and decryption processes. Total secrecy of encryption key should be maintained during key lifetime. Hence, key distribution is a problemassociated to these encryption schemes. Numerous algorithms such as Triple Data Encryption Standard (DES), Blowfish, International Data Encryption Algorithm, RC5, CAST-128, etc., belong to this category[6].

Asymmetric encryption/decryption is called generally as public-key algorithm and uses a pair of keys. That is, either of the two related keys can be used for encryption, with the other used for decryption. A key, which is called as *public key*, is published openly by placing it in a public register or file. On the other hand, the companion key is kept private, which is called as *private key*. In this paper, the key used in symmetric encryption is named as *secret key*in order to differentiate to the keys used in public-key encryption. Processing overhead in public-key encryption is larger than that of symmetric one. Public-key encryption also can be used in secret key distribution, authentication, and digital signature. There have been proposed many public-key encryption algorithms such as RSA algorithm, Elliptic Curve Cryptography (ECC), ElGamal, and so on. Authentication process is also needed to decide whether a client logged in is authorized or not.

In this paper, we describe the development of security system for Internet banking using PDA via wireless LAN. The security service was implemented over Windows CE Operating System. Authentication is also implemented for authorization of a user access to the banking system. This type of encryption in the application layer does not require any change in the infrastructure or protocols of the network. Due to the processing overhead, both of the public-key encryption and symmetric encryption were adopted. We used RC4 encryption to the data exchanged between PDA and Banking Server. The secret key of RC4 at source node is generated at each login session. Because the secret key is changed at every session, it can be called as *session key*. When a client is to log in, a private key was generated from a random number sequence and hash function defined previously. Insteadof the direct distribution of secret key, the random number sequence is encrypted with the public key of the destination node and transferred to the destination for generation of the private key. Because RC4 is simple and fast and requires a low memory, it is suitable for hardware or software implementation[6]. In addition, it adopt variable-length key. Hence, there is a tradeoff between speed and security. Although the export approval process by U.S.A government is simplified, a product must limit the RC4key size to 40 bits. An additional 40-bit string, called a salt, can be used to thwart attackers. RC4 seems to be potentially vulnerable due to simple operation such as XOR during encryption process. However, it incorporates rotations whose amount is data dependent and can use long key size. These strengthen the algorithm against cryptanalysis.

The sequence mentioned above also happens when a message is exchanged between the Banking Server and the Authentication Server. Therandom number sequence to produce private key is encrypted with public key and exchanged between Banking Server and Authentication Server. Because private key is not transmitted directly, an attacker cannot extract private key if an attacker don't know the hashing function. This may increase the strength of data encryption/ decryption.

The remainder of the paper is organized as follows. The configuration of mobile banking systems is described in section 2. In section 3, we present the implementation for the secure banking service and encryption/decryption flow in detail along with communication sequence. Section 4 contains concluding remarks.

2. RELATED WORKS

There are various types of mobile platforms proposed to support secure mobile Internet commerce. They can be categorized as two types: mobile platforms based on wireless Internet and ones based on mobile devices[13]. The former includes J2ME (Java 2 Micro Edition), WIPI (Wireless Internet Platform for Interoperability), BREW (Binary Run-time Environment for Wireless), and so on. The later contains Windows Mobile for Smartphone, Mocha (Modular & Configurable Handset S/W Architecture), EMP (Ericsson Mobile Platforms), PalmOS, and so on. While some applications are implemented over former architecture, others operate on later platform. On the other hand, the former architectures may be implemented over later ones. Each of platform architectures has merit and demerit. So, it is not supposed that one platform may sweep over the whole market of mobile devices in the near future. This increases the complexity in guaranteeing interoperability among various applications.

For secure wireless communication, a mobile device can adopt WAP (Wireless Application Protocol) or TCP/IP. They provide communication security using SSL (Secure Socket Layer) and WTLS (Wireless Transport Layer Security), respectively. WAP requires a proxy or gateway in its architecture to perform protocol conversion. This proxy-based architecture causes potential performance bottleneck. In addition, it doesn't provide end-to-end security[14,15]. In WAP 2.0 specification[16], WAP gateway is not used at all by adding support for the standard Internet communication protocols such as IP, TCP, and HTTP. Hence, WAP-based mobile phones are turned into Internet devices. However, to upgrade to WAP 2.0, mobile phones and wireless networks should be changed[17]. Another solution to support end-to-end security is to use SSL/TLS and TCP/IP.

However, current Internet based on TCP/IP (Transmission Control Protocol/Internet Protocol) does not provide confidentiality and availability during communication process and especially weak to worm virus attack and eavesdropping. So, it reveal weakness in interception and interruption [6,7]. As a standard for Web security solution, SSL is located between Transport layer and Application layer of OSI (Open System Interconnection) 7-layer model and uses TCP port 443. Before data exchange between WEB browser and server using SSL, all the data on the WEB is encrypted and MAC (Message Authentication Code) is calculated to append it to the message. However, because SSL is located over Transport layer, a user cannot select a data in a HTML (Hyper Text Markup Language) page to encrypt[6,12]. It encrypts all the data and transmits to server. This increases processing burden and reduces the communication speed. It is also memory-intensive for wireless devices[14,17]. Hence, plug-in type of solution is preferred.

In [17], a prototype solution for secure communication over the wirelessnetwork is presented using J2ME wireless toolkit 1.0.4 of Sun Micro-

systems. The solution makes use of the WAP stack tp perform HTTP. It requires WAP gateway and there is no end-to-end connection between the client and the bank server. Hence, bank should have its own trusted and secure gatewaywithin its security boundary.

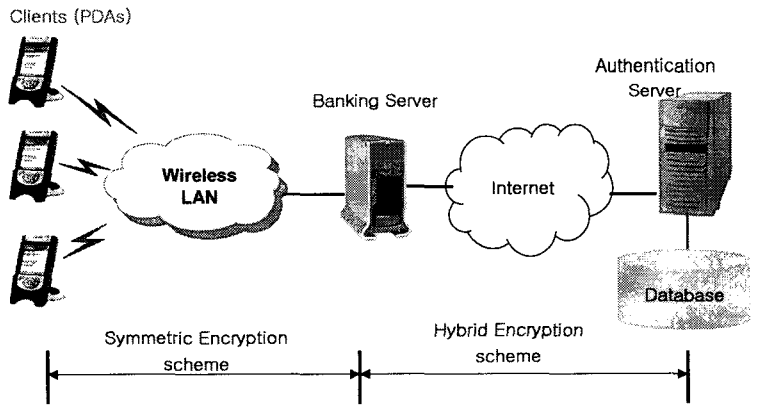
In [18], implementation of e-Payment was proposed by simplifying public key computing based on J2ME. However, the function is limited to payment and authentication should depend on offline to reduce communication load. The requirements for supporting mobile Internet banking is well summarized in [1] and [15].

3. CONFIGURATION OF MOBILE BANKING SYSTEM FOR PDA

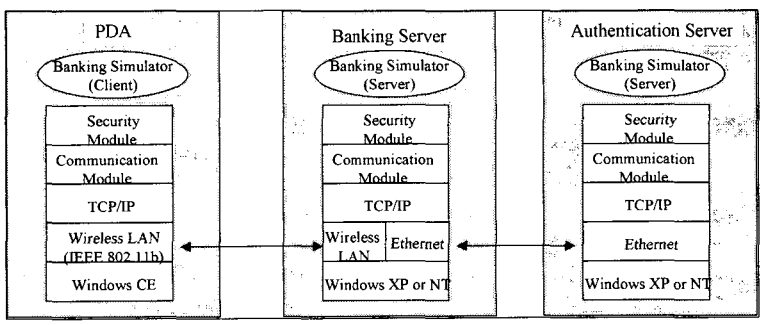
The developed mobile banking system for PDA consists of PDA, Banking Server, and Authentication Server with communication network among them, which is shown in Fig. 1(a). Fig. 1 (b) shows the system environment and the components of each system. We assumed that user authentication between different wireless network domains was provided by Network Layer service of OSI (Open Systems Interconnection) 7 layer model. When handover occurs, IP should manage it using macro-mobility protocols such as Mobile IP[19] with micro-mobility protocol[20] such as Fast Handoff, Hierarchical Mobile IP, Proactive Handoff, and so on.

3.1 PDA

Client program on PDA consists of three modules: user interface module, security module, and communication module. Atfirst, user interface



(a) System configuration.



(b) Architecture of each system.

Fig. 1. Configuration and architecture of developed mobile banking system.

module displays a window for a user to enter his/her ID and password for login process. After successful login, it provides the main window for various banking services such as payment, deposit, money transfer, account information, and so on. The security module encrypts the data entered by a user for registration, login, and service request and decrypts the response data from Banking Server. All the data is encrypted with RC4 algorithm using a secret key. The secret key is generated from a random number sequence that is used as input of the hash function promised initially. This key is maintained until the login session is closed

Instead of direct distribution of secret key, the random number sequence is encrypted with public key from the Banking Server and transmitted to the Banking Server for the key generation. Although an attacker captures the message on the communication link, he/she may not analyze the key if he/she doesn't know the hash function. This will increase the strengthof security. Communication module takes charge of data exchange between PDA and Banking Server using wireless LAN (Local Area Network).

3.2 Banking Server

Banking Server simulates the service provided by conventional bank in real world. At the same timeit plays a role of service agent for registration and authentication between PDA and the Authentication Server. If the Banking Server receives a message from PDA, it extracts the random number sequence and decrypts it with matched private key. Then, it generates the secret key using the random number sequence as input of promised hash function. The Banking Server decrypts the message with the secret key and decides the service requested by the client. Then it prepares a query to the database in the Authentication Server. DB access is achieved with ADO (ActiveX Data Object) and ODBC (Open Data Base Connectivity)[9,10]. This message is encrypted before transmission.

The Banking Server also has a function to emulate a real banking service.

3.3 Authentication Server

Authentication Server includes database for registered clients and security module for message encryption/decryption. If the Authentication Server receivesa request from a user to open an account, it saves user's ID and password. Then, it transfer authentication certificate to PDA. The certificate includes public key with matching private key. In encryption/decryption procedure, messages are encrypted/decrypted by secret key that is encrypted/decrypted with public-key algorithm.

3.4 Security Service Flow for Mobile Internet Banking

To support securityfor mobile Internet banking service, security modules on PDA, Banking Server, and Authentication Server cooperate with each other along with communicating messages. Information flow during security service is shown in Fig. 2.

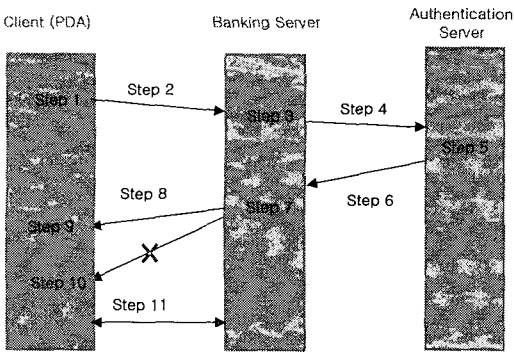


Fig. 2. Information flow for the developed mobile banking system.

The operation that happens at each step is as follows.

(1) step 1: When a user logs in to the mobile

banking system, a secret key is generated using random number sequence and the login string (user's identifier and password) is encrypted with the secret key.

(2) step 2: The login string encrypted with private key along with random number sequence encrypted with public key is transmitted to Banking Server through a socket.

(3) step 3: Banking Server decrypts the received random number sequence with its private key and generates secret key by hashing the random number sequence.

(4) step 4: Banking Server sends the received message from PDA without encryption.

(5) step 5: Authentication Server repeat the process at step (3) to generate the private key. With this private key, user ID and password are recovered.

(6) step 6: The Authentication Server compare the identifier and password of the login string with records of database, and returns the authentication result (true or false) with a certificate to the Banking Server.

(7) step 7: If the response from the Authentication Server is true, the Banking Server confirms the service request from the client on PDA. Otherwise, it rejects.

(8) step 8: The client performs step (9) when the request is confirmed. Otherwise, step (10) is performed.

(9) step 9: The client can advance to step (11) for the Internet banking service through PDA.

(10) step 10: Because the access is denied, the client may be requested to enter a new ID and password or do registration process.

(11) step 11: The client can go on doing the next step for the mobile Internet banking service. However, it does not imply that the client can access the remote database of a bank. Instead of the direct accessing, the client encrypts each query with secret key and sends it to the Banking Server through socket interface. Upon receiving the encrypted query, the Banking Server executes the query as a proxy after decrypting it with the secret key, and it returns the result after encrypting it with the secret key.

4. IMPLEMENTATION OF SECURITY SERVICE

We developed programs for PDA in Windows CE 3.0, and implemented those for the Banking Server and the Authentication Server in Windows XP[8,11]. We aimed that the exploitation of the security service cannot be restricted to specific hardware or software architecture. The specification of PDA used for implementation test is as follows.

- CPU: Intel StrongARM 1110 (206 MHz)
- Memory: 128 MB
- Communication: IEEE 802.11b, RS-232C
- OS: Microsoft Windows CE version 3.0.9348

SQL Serverof Microsoft is chosen as the database management system in Authentication Server. To connect with the SQL Server, the security module sends a query using ADO and ODBC. Message exchange between a PDA and the Banking Server is achieved using TCP/IP socket over campus mobile network the protocol of which is IEEE 802.11b. The Banking Server communicates with the Authentication Server through wired Internet. RC4 and public-key encryption is used for encryption of message and random number sequence, respectively.

4.1 Implementation of Security Service between PDA and Banking Server

We will describe the implementation of security service and communication between PDAand Banking Server in detail. Fig. 3 shows the security service flow and the functions of security modules at a server (Banking Server) and a client (PDA).

Before a client logs in using a PDA, the PDA receives a public key from the Banking Server to encrypt a secret key and define hash function to

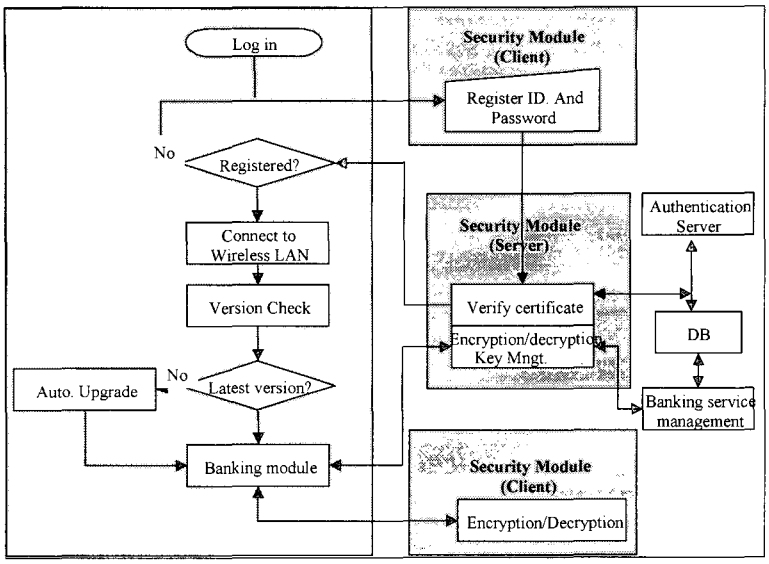


Fig. 3. Security service flow and functions of security modules at a server (Banking Server) and a client (PDA).

generate the secret key at initialization phase. When a user logs in to the mobile banking system using PDA, a security module in PDA chooses a random number sequence. This random number sequence M is used as the input of hash function $H(M)$to generate a secret key. That is, secret key is fixed-length hash value given as $H(M)$, where M is random number sequence of variable length. This procedure is shown at Fig. 4.

At this phase, thesecurity module in PDA encrypts a login string of the user's identification and password with the RC4 algorithm and sends it to the Authentication Server via the Banking Server. The login string is attached to the message with the random number sequence and transmitted for authentication of the client. The message format is shown Fig. 5.

The service mode represents the type of service requested by a client. At this instance, requested service is authentication. The service index includes the data relevant to the service mode. Token is used to separate each field in the message. At login phase, the service index contains encrypted login sting in the form of "client's identification+<token>+password+<token>".

Upon receiving the string received from the

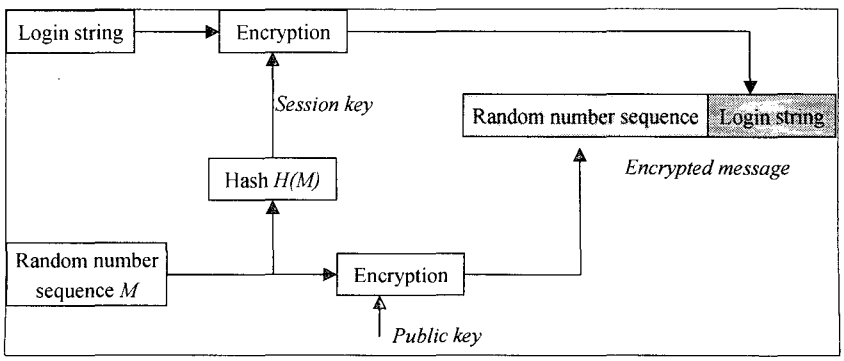


Fig. 4. Private key generation scheme at login state.

Service mode	T	Random no. sequence	T	Service index	T

T : Token

a) Message format from PDA to Banking Server.

Service mode	T	Response message	T

b) Response message from Banking Server to PDA.

Fig. 5. The format of message between PDA and Banking Server.

client, the Banking Server determines the service mode requested by the client. Then, it decrypts a random number sequence with its private key and generates secret key using hash function defined at initialization phase. Next, the Banking Server sends a query with the identifier and password to the Authentication Server. If the authentication is confirmed, the Authentication Server sends a certificate to the Banking Server. The certificate contains a public key and the matching private key for the client on PDA. When the response message arrives from the Authentication Server, the Banking Server forwards the certificate to the PDA. After the authentication succeeds, it checks the software version and upgrades if it is not latest version. Then, the user can use the mobile banking service, and all the data are exchanged via the Banking Server using the certificate. The key pair in the certificate and the private key is maintained until the client logs out.

When a client sends login string at initial state, an attacker may capture a login string from PDA and copy it to replay later. To cope with replay attack, secret key is re-generated at every session. After successful login, security module in PDA appends encrypted data of current time to each transaction message. Fig. 6 illustrates several interface windows implemented in PDA, the Banking Server, and the Authentication Server in order to provide the security service mentioned above.

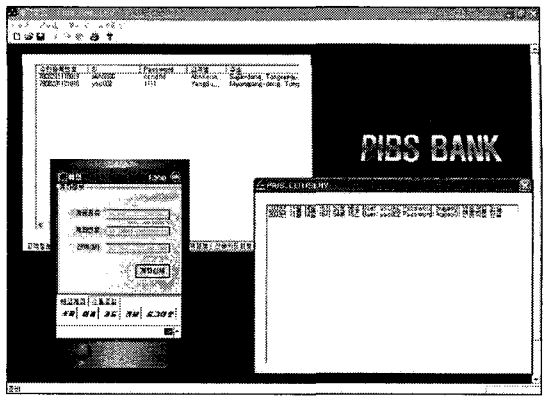


Fig. 6. An illustrative window of PDA, Banking Server, and Authentication Server.

4.2 Performance of Proposed Implementation in a PDA

Performance of proposed implementation was tested to evaluate computational overhead of RC4 and hash function. Under Windows Operating System, clock resolution is larger than a millisecond. Hence, without real-time clock, precise measurement of execution time is not available. In this test, ten thousand of executions have been done and the resulting time was averaged. The execution time includes the time elapsed for RC4 encryption. As shown in Table 1, the processing time was less than a millisecond when the data size is less than 1 Kb. The processing time for secret key generation using hash function along with random number generation, which are proposed in this paper, was also less than a millisecond.As a result, proposed scheme is feasible for implementation in PDA.

Table 1. Test result of execution time of RC4

data size	Execution time of RC4	
	encryption (msec.)	decryption (msec.)
1 KB	0.18248	0.56678
10 KB	0.64997	1.11925

5. CONCLUSION

In this paper, we described the implementation

of security service for mobile Internet banking using PDA. Due to the processing burden of SSL, security service in a PDA took plug-in type of implementation. In order to increase security of the message, which was encrypted with RC4 algorithm, the secret key was generated using hash function and random number sequence. Moreover, the random number sequence was encrypted exploiting public key and exchangedbetween the PDA and the Banking Server. The security service was implemented using hybrid encryption scheme. That is, a client's data was encrypted with symmetric block encryption, RC4, and the random number sequence to generate the secret key of RC4 was done with public-key algorithm. For authentication of a client, the Authentication Server was developed to create and transmit a certificate for an authorized client. The communication between PDAs and the Banking Server and between the Banking Server and the Authentication Server was realized through IEE802.11b wireless LAN and wired Internet, respectively. Several banking services and graphic user interfaces, which emulated the services of real bank, were developed to verity the working of each security service in PDA, the Banking Server, and the Authentication Server. The implemented security service may easily extend to other encryption algorithms such as triple DES (Data Encryption Standard), SEED, and so on.

The implementation over various platforms such as WIPI, WAP, and so on is remained as future works. When a client sends login string at initial state, an attacker may capture a login string from PDA and copy it to replay later.

6. REFERENCES

[1] J. Felix Hampe, Paula M.C Swatman, and Paul A. Swatman, "Mobile Electronic Commerce: Reintermediation in the Payment System," Proc. Of 13th International Bled Electronic Commerce Conference, pp. 693-706, June, 2000.

[2] Aphrodite Tsalgatidou and Jari Veijalainen, "Mobile Electronic Commerce: Emerging Issues," Lecture Notes in Computer Science 1875, pp. 477-486, 2000.

[3] Markus Jakobsson and Susanne Wetzel, "Security Weakness in Bluetooth," Lecture Notes in Computer Science 2020, pp. 176-191, 2002.

[4] J. P. Hubaux, L. Butty´an, and S. Capkun, "The quest for security in mobile ad hoc networks," in Proc. Of MobiHoc'01, 2001, pp. 146-155.

[5] S. Nesargi and R. Prakash, "MANETconf: configuration of hosts in a mobile ad hoc network," Proc. of INFOCOM'02, pp. 1059-1068, 2002.

[6] William Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd Edition, Prentice Hall, New Jersey, 1999.

[7] Andrew S. Tanenbaum, *Computer Networks*, 4th edition, Prentice Hall, New Jersey, 2003.

[8] Ypyo Lee, *Microsoft Visual C++ Bible 6.0*, Samyang Press, Seoul, Korea, 2000.

[9] Christina M. Anderson, *Microsoft SQL server 2000 resource kit*, Microsoft Press, 2001.

[10] Rebecca Riodan, *Step by step Microsoft SQL server 2000 Programming*, Microsoft Press, 2001.

[11] Bondi,Richard, *Cryptograghy for Visual Basic : A Programmer's Guide to the Microsoft CryptoAPI* John Wiley & Sons, 2000.

[12] INITECH, *INIPluginCE Technical Manual*, INITECH, 2002.

[13] Joon Sung Hong, "Mobile device S/W Platform Trend," Communications of the Korea Information Science Society," vol. 22 no. 1, pp. 8-15, Jan. 2004.

[14] Vipul Gupta and Sumit Gupta, "Securing the Wireless Internet," IEEE Communications Magazine, pp. 68 74, Dec. 2001

[15] J. Claessens, V. Dem, D. De Cock, B. Preneel, and J. Vandewalle, "On the Security of Today's Online Electronic Banking Systems," Computers & Security, vol. 21, no. 3, pp. 253 265, Jun. 2002.

[16] WAP Forum, "WAP 2.0 Technical White Paper," http://www.sapforum.org/

[17] Wassim Itani and Ayman I. Kayssi, "J2ME End-to-End Security for M-Commerce," IEEE Wireless Communications and Networking, vol. 3, pp. 2015 2020, Mar. 2003.

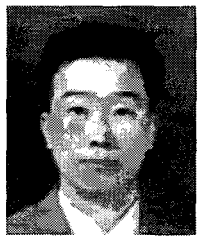
[18] Mi-AeKim, Han-Ki Lee, Seong-Whan Kim, Won-Hyoung Lee, and Eung-Kwan Kang, Implementation of Anonymity-Based e-Payment System for M-Commerce," IEEE International Conf. On Communications, Circuits and Systems, vol. 1, pp. 363-366, Jun. 2002.

[19] Charles E. Perkins, "Mobile IP," IEEE Communications Magazine, pp. 84-99, May 1997.

[20] Andrew T. Campbell, Javier Gomez, Sanghyo Kim, and Chieh-Yih Wan, "Comparison of IP Micromobility Protocols," IEEE Wireless Communications, pp. 2-12, Feb. 2002.

Young-yeol Choo

He received a B.S. and an M.S. degree in Control and Instrumentation Engineering from Seoul National University, Seoul, Korea in 1986 and 1988, respectively and a Ph. D. from the Pohang University of Science and Technology, Pohang, Korea, in 2002. He is currently a full-time lecturer in Dept. of Computer Engineering of Tongmyong University of Information Technology, Busan, Korea since 2002. From 1988 to 2002, he has worked for Posco as a senior researcher. His research interests include computer network, real-time system design and network security.



Jung-In Kim

He received the B.S. in statistics from the Keimyung University, Korea in 1986, and the M.S. and Ph.D. degrees in computer science from Keio university in 1993 and 1996, respectively in Japan. After graduation, he spent 2 years as a researcher at POSTECH, participating in the Posco project for Japanese to Korean MT system. Since 1998, he has been working for the Department of Computer Engineering at TIT(Tongmyong University of Information Technology), Korea, and currently he is assistant professor. His research interests include the core technology for Korean language processing and its applications to machine translation, information retrieval, and text summarization. He is a member of the editorial board of Korea Information Process Society Review, and also a member of KISS, IPJS and IEICE.