New Novel Approaches for Securing VoIP Applications

Chan Yeob Yeun, Kyusuk Han, and Kwangjo Kim

Information and Communications University (ICU)
119,Munjiro,Yuseonggu,Daejeon, 305-732, Korea
{cyeun, hankyusuk, kkj}@icu.ac.kr

Abstract. SIP message authentication and SRTP key agreement are the important issue in the SIP-based VoIP service. Several secure solutions such as HTTP Digest Authentication, SSL/TLS, and S/MIME, are used for the SIP message authentication and key agreement. When the VoIP is used in the wireless environments, the efficiency of security service is one of the important matters in question. For the such efficiency, WPKI is a better substitution than the traditional PKI, while it still requires the effort on the certificate management. Therefore, we would like to propose efficient ID-based cryptosystem for the VoIP in the wireless environments. In this paper, we present the overview of WPKI and the application of ID-based cryptosystem for the SIP message authentication as well as the authenticated one-way key agreement for SRTP. Our novel design reduces delaying for the key generation and provides the explicit mutual authentication.

1 Introduction

Voice over internet protocol (VoIP) is becoming more common and widely used everywhere, where the various security shortcomings are frequently incurring: Session initiation protocol (SIP) [16] message forgery during SIP transaction and eavesdropping Secure real-time transport protocol (SRTP) [3] packet are critical security problems in the SIP based VoIP services.

Currently, HTTP digest authentication between VoIP user and servers, SSL/TLS among servers, and S/MIME for the message authentication are the solutions for the security of VoIP services.

There are several approaches that consist of the SIP message authentication are shown in the VoIP systems as follows. At first, RFC 4474 [14] defines the VoIP server of user side signs the SIP message, when users send their SIP messages to the VoIP server, the server sign the messages. Users do not provide the security of SIP message. However there are too much overhead in the server with the large number of SIP transactions.

The second approach is signing by users themselves. In this case, users ought to posses the enough computational power with the certificate management. In addition, Kong *et al.* [8] proposed the scheme that users create their own public key pairs and the servers share the information of the public key.

Since the construction of traditional PKI [1] has too much communication overhead in the wireless environments, we would like to consider the WPKI (wireless PKI) [11, 17] as the more efficient way to utilize PKI. However, even WPKI gives the significant efficiency, the overhead from the certificate management still remains.

Therefore, we consider the certificate-less environments with the employment of ID-based cryptography. In 2006, Ring *et al.* [15], proposed the authentication and key agreement schemes for the VoIP employing ID-based cryptography. Their design is based on two-pass key agreement protocol with signatures and it takes relatively much time for verifying the signature in ID-based cryptography that may occur the delay in key generation in their design.

In this paper, we present the overview of WPKI and the application of ID-based cryptosystem for the SIP message authentication as well as the authenticated one-way key agreement for SRTP. Our novel design reduces delaying for the key generation and provides the explicit mutual authentication.

2 Related Works

2.1 VoIP security

For the authentication, SIP presently uses *HTTP digest authentication* [7], which does not provide message integrity, end-to-end security, and has lack of scalability to multi-domain because of the shared user password based model.

Secure/Multipurpose Internet Mail Extensions (S/MIME) [2] is a protocol that adds digital signatures and encryption to Internet MIME (Multipurpose Internet Mail Extensions) messages described in RFC 1521 [5]. SIP allows sections of the messages to be encrypted using S/MIME, however S/MIME is dependent upon a Certificate Authority (CA) and accompanying Public Key Infrastructure (PKI), and therefore limited by the adoption of such a system. Also, it is possible that S/MIME is likely to be too heavy for resource constrained handsets.

The model in the RFC 4474 [14] defines the server signs user address binding and contact address with own domain certificate. Please see Figure 1 for more detail. In this model, users do not have to keep their own certificate and allow user's message authentication in the outside of the user domain. In this case, the public key is not used by every user so that the delegation of signature generation is required for the practical solution.

However, the message signing in the environment with the large number of user will be the server's overhead. When a great number of transaction happens, the server might be vulnerable against DoS attack. Furthermore, the computational power of mobile devices are continually being improved.

Kong *et al.* [8] proposed the model that users sign their own SIP messages with their public keys. Users self-generate public key pairs and register them to their registered VoIP server, and sign the SIP message with the private key. In the mobile environments, generating public key pairs and registering them to servers will be the computational overhead.

They showed their model is efficient because of the overhead from the message signing is distributed to each user. However, their model still have the overhead from the public key registration to all servers. Since the public key pairs are self-generated by each user, the cost to register the public key pairs to all servers should not be ignored.

Generic public key cryptosystem requires the verification of the publc key in the certificate, and the communication with the trusted third party (TTP), whom the servers role in [8].

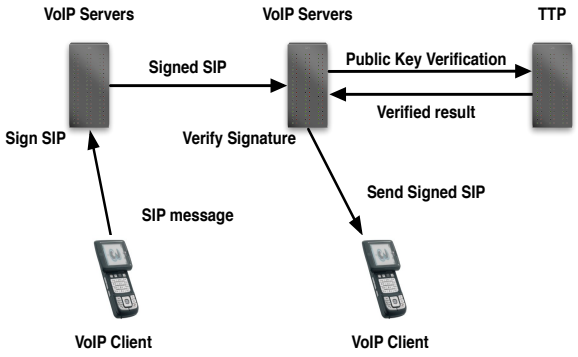

Fig. 1. Server signs SIP message (in RFC 4474)

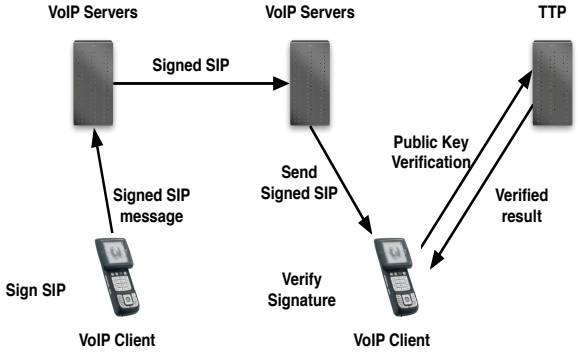

Fig. 2. User signs own SIP message (Generic PKI)

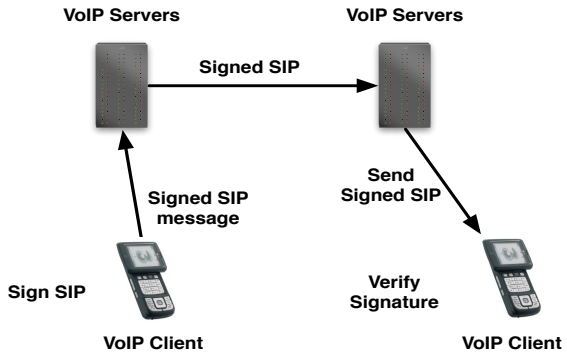

Fig. 3. User signs own SIP message (ID-based cryptography)

Also, each user has to manage other user's public key.

In this paper, we propose an efficient and practical secure VoIP service with applying ID-based cryptography. We address the combination of the signature scheme in [6] and the key agreement scheme in [10]. With such combination, we achieve the one way authenticated key agreement for the SRTP as well as the message integrity and authentication for the SIP. Using ID-based cryptosystem, user has the benefit from the removing of public key verification. Also we would like to discuss Ring *et al.* [15]'s design with our proposed protocol.

2.2 WPKI

Generally, WPKI is known to be more efficient than traditional PKI. [9] showed the implementation result of RSA and ECDSA in the mobile phone. From their results, the performance of ECDSA showed about 5 times faster than RSA. The key size was 163 bits for ECDSA, while 1024 bits required for RSA to achieve the same security level. Thus the following section describe briefly about wireless PKI. Please refer [17] for more details.

TCP/IP and PKI are computationally intensive solutions, also incur a large communication overhead, which are undesirable in wireless environments. Nevertheless, the basic elements of PKI and certificate remain the same. Also, it is trivial that most VoIP applications will be employed in the wireless environments, which brings the requirements of more efficient way.

The wireless PKI (WPKI) can be used for the same applications as those with PKI. However, the characteristics of the wireless environment can give rise to the development of a whole new set of revolutionary applications including banking, payments, ticketing and receipt, stock trading, gambling and public administration. Compared to a PKI, WPKI applications have to work in an environment with less powerful CPUs, less memory, restricted power consumption, smaller displays, and diverse input devices [11–13]. Figure 4 shows the WPKI architecture [9]. The enhancements of WPKI are described as follows.

WPKI Protocols. The traditional method used to handle PKI service requests relies on the

ASN.1 Basic Encoding Rules (BER) and Distinguished Encoding Rules (DER). BER/DER require more processing resources than a WAP device should effectively have to handle. WPKI protocols are implemented using WML 2.0 and WMLSCrypt. WML 2.0 and SignText function in WMLSCrypt provide for significant savings when encoding and submitting PKI service requests as compared to the methods used in traditional PKI.

WPKI Certificate Format. The WPKI certificate format specification sought to reduce the amount storage required for a public key certificate. One of the mechanisms was to define a new certificate format for server side certificates, which significantly reduces the size as compared to a standard X.509 certificate. Another significant reduction in the WPKI certificate can be attributed to Elliptic Curve Cryptography (ECC). With ECC, the saving in the overall size of the certificate is typically more than 100 bytes due to the smaller keys needed for ECC vs. other signature schemes. WPKI has also limited the size of some of the data fields of the IETF PKIX certificate format. Because the WPKI certificate format is sub-profile of the PKIX certificate format, it is possible to maintain interoperability between standard PKIs.

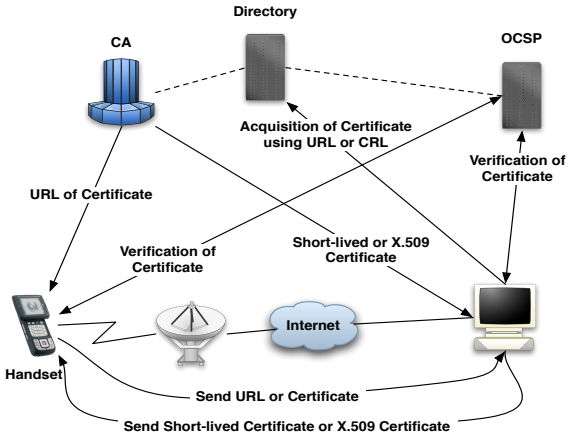

Fig. 4. Wireless PKI Architecture [9]

WPKI Cryptographic Algorithms and Keys. While traditional signature schemes are optionally supported by the WAP security standards, they are viewed as impractical to implement in the wireless environment from a performance and resource viewpoint. Traditional signature schemes demand much more processing, memory, and storage resources in the WAP device when compared to the resource requirements of more efficient cryptographic-ECC. ECC techniques are recognized as the most optimized, and therefore the best suited for supporting security in the wireless environment. The keys for elliptic curve are typically of the order of six times smaller than equivalent keys in other signature schemes, for example 164 bits vs. 1024 bits. This creates great efficiencies in key storage, certificate size, memory usage

and digital signature processing. ECC is fully supported by the WAP security standards and has been widely accepted by WAP device manufacturers. However, one must carefully choose good Elliptic Curves otherwise it might be prone to various attacks.

WPKI is an extension of, and includes most of the technologies and concepts that are present in traditional PKI. WPKI must be optimized using more efficient cryptography such as ECC but one must carefully select the good curves in order to prevent known attacks. One of the issues with getting WPKI widely accepted is the management of certificates via CA's.

By using WPKI with VoIP applications, we are able to provide swift key agreement protocol with signing and verifying.

2.3 ID-based signature scheme

In this section, we describe the signature scheme used for our model, which is based on the scheme 1 in [6].

At first, we define $h : \{0,1\}^* \times V \rightarrow (Z/lZ)^\times$, $H : \{0,1\}^* \rightarrow G^*$, where $G^* := G \setminus \{0\}$. ID-based signature scheme consists of 4 algorithms, *Setup*, *Extract*, *Sign*, and *Verify*, and 3 entities, the trusted authority (TA), the signer, and the verifier.

Setup: TA select a random integer $t \in (Z/lZ)^\times$, computes $Q_{TA} = tP$, where t remains secret. And then, TA publishes Q_{TA}.

Extract: The signers request own private keys $S_{ID} = tH(ID)$ to TA, where ID is signers' identities.

Sign: To sign the SIP message m The signer selects arbitrary length $P_1 \in G^*$ and a random integer $k \in (Z/lZ)^\times$, and computes followings;

1. $r = e(P_1, P)^k$
2. $v = h(m, r)$
3. $u = vS_{ID} + kP_1$

Verify: The verifier receives the message m and the signature (u, v), computes followings;

1. $r = e(u, P) \cdot e(H(ID), -Q_{TA})^v$
2. Accepts if and only if $v = h(m, r)$

2.4 ID-based Key Agreement Scheme

Assume two entities A, and B who exchange the key, where A requests the key exchange. Key agreement methods are defined as the following forms. *Non-interactive* is the method that A pre-shares the key for each entity. A encrypts the self-generated session key using the pre-shared key with B and sends the encrypted session key to B. However, there is claim that the session key is controlled by A and at least one communication is required, which is no more *non-interactive*.

The other way is *Two-pass* method, which A and B mutually exchange key generating information. [15] is based on the two-pass key agreement protocol.

Another way is *One-way* method, which A sends key generating information and encrypted message using the session key to B at the same time. In this model, the communication is required only once. We concludes the one-way method is practical considering the cost and security.

In 2006, Ring *et al.* [15] showed the two-pass key agreement model, which is shown in Figure 5.

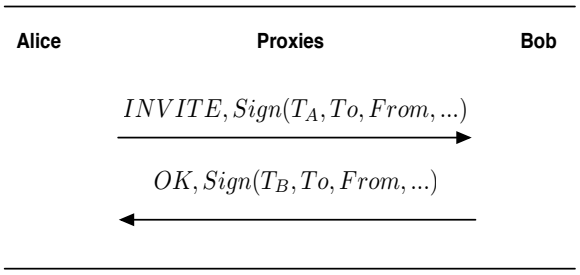

Fig. 5. Ring *et al.*'s Key Agreement Model for SIP [15]

To reduce the delay from computing the session key used for SRTP encryption, we propose the one-way key agreement model. The example is shown in Figure 6.

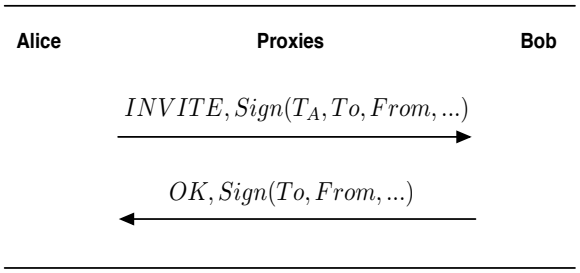

Fig. 6. Our proposed Key Agreement Model for SIP

Figure 7 shows the comparison of our one-way key agreement and two-pass key agreement [15] employing in VoIP.

As shown in Figure 7, Alice can pre-compute the session key when she send the **INVITE** message to Bob. When Alice and Bob agreed to the session key and send SRTP transaction, they can reduce the delay, which is shown in two-pass model. In two-pass key agreement model, Alice can compute the session key after Bob responds with **OK** message. In practical

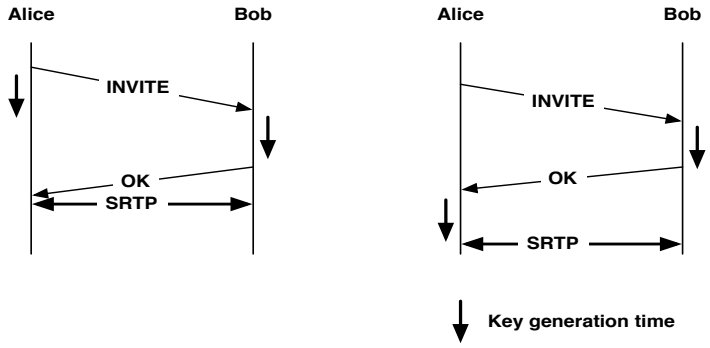

Fig. 7. Comparison of one-way and two-pass key agreement

VoIP application, employing our model, the delay is reduced.

For the one-way key agreement protocol, we apply the scheme 1 in [10], which is one-way method. The protocol is as following.

We assume two entities A and B in the protocol. S_A denote the private key of A, which is $sH(ID_A)$, where s is the master secret of KGC. $H(ID_A)$ is A's public key, where H is the hash function, $H : \{0,1\}^* \rightarrow G_1$, G_1 is additive cyclic group. ID_A is the identity of A. Please refer to [4] for the bilinear maps from elliptic curve pairings.

Parameter Distribution: A selects a random integer $r \in Z_q^*$ and computes $X_A = rH(ID_A)$. A sends X_A to B via the public channel.

Established Key: A and B computes followings;

- A: $k_{AB} = e(S_A, H(ID_B))^r \oplus e(S_A, H(ID_B))$,
- B: $k_{BA} = e(X_A, S_B) \oplus e(H(ID_A), S_B)$.

$\oplus$ denotes XOR operation.

3 Proposed Scheme

We assume a sender A, a receiver B, and a server in a certain VoIP service. The sender and the receiver generate messages for VoIP service, as clients, while the server provides VoIP service.

To generate SIP message, the sender (denote A) generates followings;

- $r = e(P_1, P)^k$
- $t = H^*(r) \cdot H(ID_A)$
- $v = h(m, t)$
- $u = vd_A + kP_1$

Here, $h : \{0,1\}^* \times G_1 \rightarrow (Z/lZ)^\times$, $H : \{0,1\}^* \rightarrow G_1$, and others follow [6]. To generates t, r should be transformed from elliptic curve to finite fields. H^* is a *map-to-point* hash function, which $H^* : G_2 \rightarrow \{0,1\}$. To compute with $H(ID_A)$, the transformation is necessary.

$e : G_1 \times G_1 \rightarrow G_2$. G_1 is cyclic additive group, generated by P with order q. G_2 is cyclic multiplicative group with the same prime order q. d_A denotes A's private key, $d_A = sH(ID_A)$. m is the SIP message, which includes the sender's address, the receiver's address, message generated time, Session Description Protocol (SDP) and other necessary information.

Then, A sends $(u, v) \in (G, (Z/lZ)^{\times})$ to the receiver B.

After receiving (u, v), B generates the following.
$t = H^*(r) \cdot H(ID_A) = H^*(e(u, P) \cdot e(H(ID_A), -sP)^v) \cdot H(ID_A)$.

After that, A and B generate the session key simultaneously.
- $A : k_{AB} = e(d_A, H(ID_B))^{H^*(r)} \oplus e(d_A, H(ID_B))$.
- $B : k_{BA} = e(t, d_B) \oplus e(H(ID_A), d_B)$.

The correctness of $k_{AB} = k_{BA}$ follows,
$k_{AB} = e(d_A, H(ID_B))^{H^*(r)} \oplus e(d_A, H(ID_B))$
$= e(H(ID_A), H(ID_B))^{H^*(r)s} \oplus e(H(ID_A), H(ID_B))^s$
$= e(t_{d_B}) \oplus e(H(ID_A)), d_B)$
$= k_{BA}$

Therefore, r can be used for both SIP message signature and the key generation, which reduces the additional communication only for the key generation.

$\oplus$ is the additive operation in G_2. When the hash function $H^{'} : G_2 \rightarrow \{0, 1\}$ is used, $\oplus$ can be XOR operation in $k_{BA} = H^{'}(e(t, d_B)) \oplus H^{'}(e(H(ID_A), d_B)$.

4 Security Analysis

We describe the security analysis for our secure VoIP design as follows.

4.1 Security in SIP message authentication

The security in SIP message authentication is the same as the security in [6]. When the attack is succeed, the Diffie-Hellman problem is solved. However, the DH problem is known as the mathematical hard problem. It is also secure against Man-in-the-middle attack due to the explicit digital signature scheme is applied. Therefore, we also achieve the authenticated one-way key agreement.

4.2 Security in SRTP key generation

For the key generation protocol in [10] is followings.
- **Known-key security** The session key in each session should be independent. When the session key is leaked, it should not threat the other session keys.
- **Unknown key share** When A and B exchange the session key, The other entity C is not exchanging the key.
- **Key control** No entity should not use the previous parameter for the session key.
- **Sender's key-compromise impersonation** When the private key of A is leaked, the attacker can impersonate A, but not other entities.
- **Sender's forward security** When A's private key is leaked, the security of previous session has guaranteed.
- **Random number compromise security** The leakage of the certain parameters selected by A doesn't affect to the leakage of A's private key or session key.

Known-key security To generate r, where $r = e(P_1, P)^k$, the sender randomly choose P_1 and k in each session. The leakage of P_1 or k doesn't affects the previous session.

Unknown key-share To generate to key the receiver B verifies the signature of the sender A first. Also, the sender self-generates the session key without any information from the receiver. Therefore, Any other entities except A and B cannot exchange the key. To succeed the attack, the adversary should be able to generate the signature of A or know the private key of B.

Key control Since the key generating parameter t is selected by A, and the process is done in one-way, B cannot control the session key, also it is difficult for A to pre-compute the random integer r and the generator P_1 to control t.

Random number compromise The random integer r is easily known from (u, v). However it is difficult know A and B's private keys or session key from public parameters P, sP, and r. To attack the session key, The knowledge of A or B's private key is necessary. The success of attack with P, sP and r is the same as the success of attack on the signature.

Attacks on sender When A's private key is leaked, the adversary can impersonate A, since r is known to A, while it is not possible to impersonate other entity. However, sender's forward security is not guaranteed unlike [10], since r is sent with the signature.

4.3 Efficiency

Signature generation requires one exponentiation operation in G_2, two hash operations, two multiplication in G_1. Verification requires one exponentiation operation in G_2, two pairing operations, and one multiplication operation. When the several messages are sent by the same identity, the sender pre-compute $e(H(ID), -sP)$ to reduce one pairing operation. For the key generation, one pairing operation of the sender, one multiplication over elliptic curve, one exponentiation operation, and two pairing operation of the receiver.

When we apply to SIP message, two exponentiation, three multiplication, two pairing in the sender side, three pairing and two exponentiation operation in the receiver side.

Using one-way key agreement with signature, we can reduce the delay using two-pass key agreement.

5 Conclusion

In this paper, we suggested new approaches by using WPKI and proposed the efficient and practical method for the SIP message authentication with signature and authenticated one-way key agreement for SIP-based VoIP service with ID-based cryptosystem. In conclusion, our new approaches can reduce the cost for the public key management, and additional process for the key generation with re-using the parameter for the signature verification.

References

1. Public-key infrastructure (x.509) pkix. http://www.ietf.org/html.charters/pkix-charter.html.
2. S/mime mail security (smime). http://www.ietf.org/html.charters/smime-charter.html.
3. M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The secure real-time transport protocol (srtp), March 2004.
4. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *SIAM Journal on Computing*, volume 32, pages 585–615, 2003.
5. N. Borenstein and N. Freed. Mime (multipurpose internet mail extensions) part one: Mechanisms for specifying and describing the format of internet message bodies. RFC 1521, September 1993.
6. Florian Hess. Efficient identity based signature schemes based on pairings. *9th Annual International Workshop, SAC 2002*, 2595/2003:310–324, Jan 2003.
7. J.Frank, P Hallam-Baker, J Hostetler, S Lawrence, P Leach, A Loutonen, and L Stewart. Http authentication: Basic and digest access authentication. RFC 2617, 1999.
8. Lei Kong, Vijay Arvind Balasubramaniyan, and Mustaque Ahamad. A lightweight scheme for securely and reliably locating sip users. *The 1st IEEE Workshop on VoIP Management and Security (VoIP MaSe 2006)*, 2006.
9. Yong Lee, Jeail Lee, and JooSeok Song. Design and implementation of wireless pki technology suitable for mobile phone in mobile-commerce. *Comput. Commun.*, 30(4):893–903, 2007.
10. Takeshi Okamoto, Raylin Tso, and Eiji Okamoto. One-way and two-party authenticated id-based key agreement protocols using pairing. *Modeling Decisions for Artificial Intelligence, Second International Conference, MDAI 2005, Tsukuba, Japan, July 25-27, 2005. Proceedings*, 3558/2005:122–133, 2005.
11. OMA. Wireless application protocol - wireless public key infrastructure. WAP-217-WPKI, April 2001.
12. OMA. Wireless application protocol architecture specification. WAP-210-WAPArch, July 2001.
13. OMA. Wireless transport layer security. WAP-261-WTLS, April 2001.
14. J. Peterson and C. Jennings. Enhancements for authenticated identity management in the session initiation protocol (sip). RFC4474, August 2006.
15. J Ring, KR Choo, E Foo, and M Looi. A new authentication mechanism and key agreement protocol for sip using identity-based cryptography. Proceedings AusCERT Asia Pacific Information Technology Security Conference 2006.
16. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. Rfc 3261, "sip: Session initiation protocol", June 2002.
17. Chan Yeob Yeun and Tim Farnham. Secure m-commerce with wpki. In *In Proceedings of IWAP'01*, pages 171–183, Daejeon, Korea, October 2001.