전방향 안전성을 갖는 RSA 전자서명 기법에 대한 연구

김대엽[†]·주학수[††]

요약

인터넷을 통해 제공되는 다양한 서비스의 보호를 위해 각각의 시스템들은 Public Key Infrastructure (PKI)를 널리 사용하고 있다. 그러나 PKI의 사용에는 여러 가지 문제점이 여전히 존재한다. 그러한 문제 중 하나가 일부 서비스들은 공개키 인증서의 즉각적인 검증을 필요로 하지만 PKI는 이와 같은 요구를 만족시키지 못한다는 것이다. 이러한 문제를 해결하기 위하여 Boneh를 비롯한 몇몇 연구자들이 중재자를 이용한 RSA 전자 서명기법 (mRSA)이라는 개념을 처음 도입하였다. 또한, Gene Tsudik은 초기 mRSA의 취약점을 개선하여 '약한' 전방향 안전성을 갖는 새로운 mRSA을 제안하였다. 본 논문에서는 약한 전방향 안전성 개념의 실제 적용에 따른 취약성을 분석하고 강한 전방향 안전성을 갖는 새로운 mRSA를 제안한다.

키워드 : 전자서명, 중재자, 전방향 안전성

A Study On Forward Secure Mediated RSA Digital Signature

Kim DaeYoub[†] · Ju HakSoo[††]

ABSTRACT

Many service systems use Public Key Infrastructure (PKI) to protect the service. But there are problems with the use of PKI. One of the problems is that some services would require a function instantaneously to check public key certificate, but PKI does not satisfy such request. To solve the problem, Boneh et al. first proposed the concept of mediated RSA (mRSA). Then Gene Tsudik proposed 'weak' forward secure mRSA. In this paper, we analyze the weakness of these schemes and find the source of the vulnerability. And we propose a new mRSA that is strong forward secure.

Key Words : Digital Signature, Mediator, Forward Security

1. Introduction

When customers use internet services, for example, banking system, Public Key Infrastructure (PKI) always protects the services. However, there are problems with the use of PKI. The biggest problem is checking the revocation status of a public key certificate. In order to check the status, service providers and customers have to check a certificate revocation list (CRL). But CRL is periodically generated, there is a time-gap between a point of time when a public key is revoked and a point of time when CRL include the record of the revoked public key.

To solve the problem of checking the revocation status of the public key certificate, Boneh et al. first proposed an efficient scheme to obtain instantaneous revocation status of signer's public key certificate [1][2]. They called the scheme mediated RSA (mRSA). It consists of four participants: a trusted third party (TTP), a security mediator (SEM), a signer, and a verifier. In their scheme, a TTP first generates a private key for a signer, and divides the key into two partial keys. Then the TTP gives one partial key to the signer and the other partial key to a SEM. Since the signer has only a partial key of the private key, he/she can generate only a partial signature with his/her own partial key. To generate a whole signature, the signer must get the SEM to generate

[†] 종신회원 : 삼성전자 삼성종합기술원 전문연구원
[††] 종신회원 : 삼성전자 디지털미디어총괄 DM 연구소 책임연구원
논문접수 : 2006년 10월 17일, 심사완료 : 2007년 3월 14일

the other part of the signature. At that time, the SEM must check the revocation status of signer's public key certificate. If the certificate has already been revoked, then the SEM should stop generating the other partial signature for the signer. In this scheme, the instantaneous checking of revocation status is achieved by the SEM.

This scheme was a new efficient approach, but it had a weakness. It didn't satisfy forward security. A digital signature scheme is said to be forward secure if an attacker steals signer's private key but he can't forge a signature that appears to have been generated before the key was stolen [3].

Gene Tsudik proposed an improved mRSA scheme, and called the scheme weak forward secure mediated RSA (wfs+RSA)[4]. Tsudik defined 'weak' as an attacker is allowed to compromise only one of two partial keys issued by the TTP through the lifetime of the key. Hence, wfs+RSA can not satisfy forward security if both partial keys are compromised.

The first goal of this paper is to propose some attack scenarios against wfs+RSA and to find the sources of the vulnerability of wfs+RSA. To describe the weakness of wfs+RSA, we suppose a situation that a partial key owner (e.g., a signer or an attacker) colludes with the other partial key owner (e.g., an attacker) to change a signature-time or to forge an illegal signature. Then we describe how they change the signature-time or forge the signature, and why such attack is possible.

The second goal of this paper is to propose a novel scheme that satisfies forward secrecy, even if both partial key are compromised. To construct the scheme that we propose, we use periodic partial keys, periodic signing keys, and Chinese reminder theorem (CRT).

2. Weak forward secure mRSA

2.1 Gene Tsudik's scheme

In this section, we briefly introduce Gene Tsudik's scheme. The main idea of this scheme is that both a signer and a SEM evolve their partial keys in parallel.

2.1.1 Generating key phase

Let (t, T) be the length of the update period and the maximum number of update period, respectively. Let k be an even integer. If a signer applies for registration to a TTP, the TTP first chooses a pair (p, q) of prime numbers with $\frac{k}{2}$bit size. Then the TTP calculates

$$n = p \times q.$$

Next, to generate a public key e, a private key d, and a pair (d_u, d_s) of partial keys of d for the signer, the TTP chooses or computes these keys such that

$$gcd(e, \phi(n)) = 1,$$
$$d \times e \equiv 1 \mod \phi(n),$$
$$d \equiv d_u + d_s \mod \phi(n),$$

where $\phi(n)$ is Euler's phi-function. Next, to compute a pair $(d_{0,u}, d_{0,s})$ of the initial periodic partial key of the partial keys, the TTP calculates both $d_{0,u}$ and $d_{0,s}$ as follows:

$$d_{0,u} \equiv d_u \times e^{-T} \mod \phi(n),$$
$$d_{0,s} \equiv d_s \times e^{-T} \mod \phi(n).$$

Finally, the TTP sends $d_{0,u}$ to the signer and $d_{0,s}$ to a SEM, and publishes (t, T, n, e).

Let i be the index of a current period. A periodic private key that is used to generate a signature at the period i is computed as follows:

$$d_i = d_0 \times e^i = (d \times e^{-T}) \times e^i.$$

To generate a signature, both the signer and the SEM respectively compute each periodic partial key as follows:

$$d_{i,u} = d_{0,u} \times e^i,$$
$$d_{i,s} = d_{0,s} \times e^i.$$

2.1.2 Singing phase

Let i be the index of a current period and m be a message. Let H be a secure one-way hash function taking a period index i and a message m as its input parameters. First, the signer computes $h = H(m, i)$ and sends h to the SEM. Then, the SEM and the signer do the follows in parallel:

- After the SEM receives h from the signer, the SEM must check the revocation status of signer's public key certificate. If signer's certificate is already revoked, the SEM must stop generating a partial signature for the signer. Otherwise, the SEM generates a partial signature

$$PS_{i,s}(m) \equiv h^{d_{i,s}} \bmod n.$$

Finally, the SEM sends the partial signature $PS_{i,s}(m)$ to the signer.

- The signer calculates the other partial signature

$$PS_{i,u}(m) \equiv h^{d_{i,u}} \bmod n.$$

After the signer receives the partial signature from the SEM, the signer calculates

$$h_1 \equiv (PS_{i,s}(m) \times PS_{i,u}(m))^{e^{T-i+1}} \bmod n.$$

Then the signer checks whether $h = h_1$. If two values are same, the signer finally generates a whole signature

$$S_i(m) \equiv PS_{i,s}(m) \times PS_{i,u}(m) \bmod n.$$

2.1.3 Verifying phase

To verify the signature $S_i(m)$, a verifier first computes $h_1 = H(m,i)$. Then the verifier calculates

$$h_2 = (S_i(m))^{e \times e^{T-i}}.$$

Finally, the verifier compares h_1 with h_2. If two values are same, the verifier accepts $S_i(m)$ as valid.

2.2 The weakness of Tsudik's scheme

In this section, we propose two attack scenarios describing why Tsudik's assumption about 'weak' is not appropriate for a security system. The first scenario is that a signer whose certificate is revoked colludes with an attacker who discovers a periodic partial key $d_{i,s}$ to change a signature-time or to forge an illegal signature that appears to have been generated before the certificate was revoked. Since the signer can generate a periodic partial key $d_{i,u}$, we assume that these attackers have both periodic partial keys of same period i. The second scenario is more general than the first scenario. We suppose that attackers discover two periodic partial keys of different period. That is, let $j < i$, then they discover $d_{i,s}$ and $d_{j,u}$, and they collude together to forge an illegal signature that appears to have been generated before the period i, for example, at the period $i-1$. They can compute both d_s and d_u as follows:

$$d_s = d_{0,s} \times e^T = (d_{0,s} \times e^i) \times e^{T-i} = d_{i,s} \times e^{T-i},$$
$$d_u = d_{j,u} \times e^{T-j}.$$

Since $d = d_u + d_s$, they can compute

$$K = h^d = H(m, i-1)^d.$$

To forge the signature $S_{i-1}(m)$ of a message m at the period $i-1$, they first calculate signer's periodic partial key of the period i as follows:

$$d_{i,u} = d_{j,u} \times e^{i-j}.$$

Then they calculate

$$S = K^{d_{i,s} + d_{i,u}}.$$

Since

$$\begin{aligned} S &= K^{d_{i,s} + d_{i,u}} \\ &= (H(m,i-1)^d)^{(d_s + d_u) \times e^{i-T}} \\ &= (H(m,i-1)^d)^{d \times e \times e^{i-1-T}} \\ &= (H(m,i-1)^d)^{e^{i-1-T}} \\ &= S_{i-1}(m) \end{aligned}$$

, the forged signature S must be accepted as a valid signature $S_{i-1}(m)$ by verifiers. In the first scenario, the signer and the attacker are able to change the signature-time using the similar method to be used in the second scenario.

We found the reason why these attack scenarios were possible. The source of such vulnerability are as follows:

- An attacker is able easily to calculate (d_u, d_s) from $(d_{i,u}, d_{i,s})$.
- Then, the attacker can simply forge the signature of the period $i-1$ from the compromised (d_u, d_s).

In addition, Tsudik asserted that if a period index i be used as one of the input parameters of a hash function, then it is possible that his scheme satisfies weak forward security without any key evolution schemes. But if a signer colludes with an attacker who discovers a periodic partial key of the SEM, as we previously described, they can compute both partial keys d_u and d_s. Hence, it does not satisfy forward security only to take the period index i as an input parameter of the hash function. Therefore, to design forward secure mRSA, a key evolution function must be adopted.

3. A novel scheme

In this section, we propose a novel mRSA that is forward secure even if the both periodic partial keys are compromised. As we described in the section 2.2, Tsudik's scheme is vulnerable because an attacker discovering $d_{i,s}$ is able easily to computes d_s. To reinforce the vulnerability, our scheme adopts an additional periodic signing keys used by a SEM.

3.1 Key generation phase

If a signer applies for registration to a TTP, the TTP first generates a key set $\{p, q, n, e, d, d_u, d_s, d_{0,u}, d_{0,s}\}$ for the signer as section 2.1.1. Next, the TTP generates the T pairs (p_i, q_i) of prime numbers such that $2T$ primes are distinct each other and both p and q are not elements of a set $\{p_i, q_i | 1 \leqq i \leqq T\}$. Then, the TTP generates $2T$ key sets $\{w_i, v_i, n_i\}$ such that

$$n_i = p_i \times q_i,$$
$$gcd(w_i, \phi(n_i)) = 1,$$
$$v_i \equiv w_i^{-1} \bmod \phi(n).$$

(w_i, v_i) is a public/private key pair that is used at the period i by a SEM. Finally, the TTP send $d_{0,u}$ to the signer and $\{d_{0,s}, \{v_i | 1 \leqq i \leqq T\}\}$ to the SEM in secure way.

The storage overhead of our scheme is heavier than it of wfs+RSA. Table 1 describes the kind of key that SEM, a singer, and a verifier have to save, respectively.

Table 1. Comparison of Storage Overhead

	Gene Tsudik's scheme	Our scheme
SEM	$d_{0,s}$	$\{d_{0,s}, \{v_i \| 1 \leqq i \leqq T\}\}$
Signer	$d_{0.u}$	$d_{0,u}$
Verifier	e	$\{e, \{w_i \| 1 \leqq i \leqq T\}\}$

Both the signer and the SEM calculate their periodic partial keys $d_{i,u}$ and $d_{i,s}$ according to the same way described in section 2.1.1.

3.2 Singing phase

Let i $(1 \leqq i \leqq T)$ be the index of a current period and m be a message. To generate a signature $S_i(m)$, the signer first computes $h = H(m, i)$ and sends h to the SEM. Then the SEM and the signer do the following in parallel:

- After receiving h, the SEM checks the revocation status of signer's public key certificate. If the certificate has been revoked, the SEM stops generating a partial signature for the signer. Otherwise, the SEM calculates a periodic key $d_{i,s}$. Then the SEM computes both a partial signature $PS_{i,s}(m)$ and an additional signature $PT_i(m)$ as follows:

$$PS_{i,s}(m) \equiv h^{d_{i,s}} \bmod n,$$
$$PT_i(m) \equiv h^{v_i} \bmod n_i.$$

Then the SEM sends $(PS_{i,s}(m), PT_i(m))$ to the signer.

- The signer calculates the other partial signature

$$PS_{i,u}(m) \equiv h^{d_{i,u}} \bmod n.$$

After receiving a signature pair $(PS_{i,s}(m), PT_i(m))$ from the SEM, the signer calculates

$$PS_i(m) \equiv PS_{i,s}(m) \times PS_{i,u}(m) \bmod n.$$

Then the signer verifies both $PS_i(m)$ and $PT_i(m)$. If two signatures are valid, the signer calculate a solution x of the following system of linear congruence using the Chinese remainder theorem:

$$x \equiv PS_i(m) \bmod n,$$
$$x \equiv PT_i(m) \bmod n_i.$$

$S_i(m) = x$ is signer's signature for the message m at the period i.

3.3 Verifying phase

To verify a signature $S_i(m)$ for the message m at the period i, a verifier first calculates $h = H(m, i)$. Then the verifier computes

$$h_1 = S_i(m)^{w_i} \bmod n_i.$$

If $h \neq h_1$, the verifier stops verifying the signature and reports this result. Otherwise, the verifier computes

$$h_2 \equiv S_i(m)^{e \times e^{T}\,'} \bmod n.$$

If $h = h_2$, the verifier accepts $S_i(m)$ as valid.

3.4 Security analysis

Let i be the index of a current period. Assume that an attacker discovers both periodic keys $d_{i.u}$ and $d_{i,s}$. Suppose that he attacker also compromises a periodic signing key v_i, and tries forging a signature for a message m at the period $i-1$. To generate an illegal $S_{i-1}(m)$, the attacker must compute both $PS_{i-1}(m)$ and $PT_{i-1}(m)$. That is, it is necessary to compute three keys $d_{i-1,u}$, $d_{i-1,s}$, and v_{i-1}. Because there is no any relationship between v_i and v_{i-1}, it is too difficult for the attacker to guess v_{i-1} from given v_i. So the attacker can not generate $PT_{i-1}(m)$. Therefore, the attacker can not forge $S_{i-1}(m)$ even if the attacker can calculate $PS_{i-1}(m)$.

4. Conclusion

This research proposes two general principles are needed to design forward secure mRSA. First, the evolution scheme to generate the periodic partial keys must be carefully designed so that the scheme is not invertible. Second, it must be difficult to calculate signer's private key with given periodic partial keys of both the signer and the SEM. The new scheme that we propose is designed on these principles. To achieve these principles, we do not improve the evolution scheme for the generation of periodic partial keys but adopt the additional periodic signing keys used by the SEM. In our scheme, the forward security is guaranteed by the signature $PT_i(m)$ with the periodic signing keys v_i. Therefore, our scheme is forward secure even if both periodic partial keys $d_{i,u}$ and $d_{i,s}$ are compromised. But in order to generate periodic signs and to verify them, SEM and verifiers of our scheme have to save additional private keys and public keys, respectively. As a result, our scheme is appropriate for service systems such as Internet banking that need security function (e.g., authentication, non-repudiation), even though the systems do not have time-stamp servers to verify signature-times.

References

[1] D.Boneh, X.Ding, G.Tsudik and C.Wong, "A Method for Fast Revocation of Public Key Certificates and Security Capabilities", Procedding of USENIX Security Symposium 2001.

[2] D.Boneh, X.Ding, G.Tsudik, "Fine-grained control of security capabilities", ACM Transactions on Internet Technology (TOIT) Volume 4, Issue 1. 2004.

[3] Mihir Bellare, Sara K. Miner, "A Forward-Secure Digital Signature Scheme", Advance in Cryptology-CRYPTO'99, LNCS vol. 1666, Springer-Verlag, pp.431-448, 1999.

[4] Gene Tsudik, "Weak Forward Security in Mediated RSA", Security in Communication Networks: Third International Conference, SCN 2002, LNCS vol. 2576, Springer-Verlag, pp.45-54, 2002.

김 대 엽

e-mail : daeyoub69@paran.com

1997년 고려대학교 대학원 수학과 (이학석사)

2000년 고려대학교 대학원 수학과 (이학박사)

1997년~1999년 (주)텔리맨 위성통신연구소 책임연구원

2000년~2001년 (주)시큐아이닷컴 정보보호연구소 책임연구원

2002년~현재 삼성종합기술원 CNL. 전문연구원

관심분야 : CAS, DRM, 스마트카드 보안, 보안 프로토콜

주 학 수

e-mail: haksoo.ju@samsung.com

1999년 고려대학교 대학원 수학과 (이학석사)

2005년 고려대학교 대학원 수학과 (이학박사)

2001년~2005년 한국정보보호진흥원 연구원

2006년~현재 삼성전자 DM연구소 책임연구원

관심분야 : DRM, 보안 프로토콜