RSA-PADDING SIGNATURES WITH ATTACK STUDIES

George Stephanides
Department of Applied Informatics, University of Macedonia
156 Egnatia Street, 540 06 Thessaloniki, GREECE

Nicolae Constantinescu, Mirel Cosulschi, Mihai Gabroveanu
Department of Informatics, University of Craiova
13 A.I. Cuza Street, 200585 Craiova, ROMANIA

Keywords: RSA cryptosystem, digital signature, fixed pattern padding.

Abstract: A fixed-pattern padding consists in concatenating to the message m a fixed pattern P. An RSA signature for the padding P and message m is obtained by raising the message m and the padding P to the private decryption exponent d. In this paper we prove that the security of RSA fixed-pattern padding is insecure for messages at least two-thirds of the size of n, the RSA public modulus.

1 INTRODUCTION

RSA is a cryptosystem invented in 1977 by Rivest, Shamir and Adleman (Rivest et al., 1978). It is now the most widely used cryptosystem because its simple underlying mathematics, based on number theory which was known back at least 150 years ago. Common uses of RSA are: privacy, data protection, digital signatures, authenticity and security of data transferred between web servers.

RSA uses an encryption exponent denoted by e, a decryption exponent denoted by d, and the modulus denoted by n. To sign a message m using RSA a user must first compute its hash value using a hash function and this is due to the slowness in computation when signing the entire message. This is rather a standard procedure recommended by PKCS #1 v. 2.0, RSA Laboratories (Network Working Group, 1998). So, a signature of RSA would be obtained as

$$s = (H(m))^d \pmod{n}$$

Observe the use of d; this exponent is also called the private exponent, which means it is the private key of a user in an RSA cryptosystem. By applying the power d to the hash of the message we obtain a fixed length signature which can be verified by anyone, computing

$$s^e = H'(m)^{d \cdot e} = H'(m) \pmod{n}$$

This way the verifier obtains the hash value contained in the signature, by computing the hash for the message m and comparing H' with H obtained from m he can be certain that the message was truly signed by the right person.

This paper considers RSA signatures without the use of hash functions but with fixed pattern padding. This means that if someone wishes to sign a message m, he adds a padding P to the message and then obtains a signature by computing

$$s = (P \mid m)^d \pmod{n}$$

The more general case is where RSA signatures in which a simple affine redundancy is used. To sign a message m, the signer first computes

$$R(m) = \omega \cdot m + a \tag{1}$$

where

$$\begin{cases} \omega \text{ is the multiplicative redundancy} \\ a \text{ is the additive redundancy} \end{cases} \tag{2}$$

Considering the above representation a message m would be signed as

$$s = R(m)^d \pmod{\text{n}}$$

Stephanides G., Constantinescu N., Cosulschi M. and Gabroveanu M. (2006).
RSA-PADDING SIGNATURES WITH ATTACK STUDIES.
In *Proceedings of WEBIST 2006 - Second International Conference on Web Information Systems and Technologies - Internet Technology / Web Interface and Applications*, pages 97-100
DOI: 10.5220/0001249100970100

A left-padded redundancy scheme $P \mid m$ is obtained by taking $\omega = 1$ and $a = P \cdot 2^l$, whereas a right-padding redundancy scheme $m \mid P$ is obtained by taking $\omega = 2^l$ and $a = P$.

Previous attacks by De Jonge and Chaum (Jonge and Chaum, 1986), and Girault and Misarksy (Girault and Misarksy, 1997) were multiplicative attacks against RSA signatures with affine redundancy (see (Misarsky, 1998) for a complete report) and their attacks were based on the extended Euclidean algorithm. De Jonge and Chaum (Jonge and Chaum, 1986) presented a multiplicative attack for which $\omega = 1$, and the size of the message m was at least two thirds of the RSA modulus n

$$\mid m \mid \succ \frac{2}{3} \mid n \mid$$

The first attack was extended by Girault and Misarksy (Girault and Misarksy, 1997); they succeeded in reducing the size of the message at $\frac{1}{2}$ of the modulus n, and their attack applies to any value ω and a, so

$$\mid m \mid \succ \frac{1}{2} \mid n \mid$$

Girault and Misarsky also extended the multiplicative attacks to RSA signatures with modular redundancy

$$R(m)^d = \omega_1 \cdot m + \omega_2 \cdot (m \bmod b) + a \qquad (3)$$

where ω_1, ω_2 are the multiplicative redundancies, a is the additive redundancy and b is the modular redundancy.

In this paper we extend Girault and Misarsky's attack against RSA signatures with affine redundancy to messages of size as small as one third of the size of the modulus, thus

$$\mid m \mid \succ \frac{1}{3} \mid n \mid$$

2 THE PROPOSED ATTACK

This section concentrates on extending the attack of Girault and Misarsky's multiplicative attack on RSA signatures with affine redundancy to a level where we have the size of the message equal to one third of the RSA modulus n. A multiplicative attack is an attack in which the redundancy function of a message can be expressed as a multiplicative combination of the redundancy functions of other messages. With respect to this we search for four messages, m_1, m_2, m_3, m_4, which are at least one third of the size of the modulus n, and verify the following equation

$$R(m_1) \cdot R(m_2) = R(m_3) \cdot R(m_4) \pmod{n} \qquad (4)$$

Message m_1, is the message whose signature will be forged, this can be done by computing

$$R(m_1)^d = \frac{R(m_3)^d \cdot R(m_4)^d}{R(m_2)^d} \pmod{n}$$

From (4) we obtain:

$$(\omega \cdot m_1 + a).(\omega \cdot m_2 + a) = (\omega \cdot m_3 + a).(\omega \cdot m_4 + a) \pmod{n}$$

Denoting $P = a/\omega \pmod{n}$, we obtain:

$$(P + m_1).(P + m_2) = (P + m_3).(P + m_4) \pmod{n}$$

For the following substitutions

$$\begin{aligned} t &= m_3 \\ y &= m_2 - m_3 \\ x &= m_1 - m_3 \\ z &= m_4 - m_1 - m_2 + m_3 \end{aligned} \qquad (5)$$

the following equation holds

$$((P + t) + x) \cdot ((P + t) + y) = (P + t) \cdot ((P + t) + x + y + z) \pmod{n}$$

which simplifies into

$$x \cdot y = (P + t) \cdot z \pmod{n} \qquad (6)$$

Next we need to determine the values x, y, z and t with respect to (6). First, we obtain two integers *z* and *u* such that

$$P \cdot z = u \pmod{n}$$

with

$$\begin{cases} -n^{\frac{1}{2}} < z < n^{\frac{1}{3}} \\ 0 < u < 2 \cdot n^{\frac{2}{3}} \end{cases}$$

One solution is suggested by Girault, Toffin and Vallee (Girault et al., 1988). Finding a good approximation to the fraction $\frac{P}{n}$ can be done efficiently by developing it in continued fractions. This implies using the extended Euclidean algorithm to P and n. A solution is found such that $\mid z \mid < Z$ and $0 < u < U$ if $Z \cdot U > n$, which is the case here with $Z = n^{\frac{1}{3}}$ and $U = 2 \cdot n^{\frac{2}{3}}$.

We then select an integer y such that

$$n^{\frac{1}{3}} \leq y \leq 2 \cdot n^{\frac{1}{3}}$$

and $gcd(y, z) = 1$. We find the non-negative integer $t < y$ such that:

$$t \cdot z = -u \pmod{y}$$

which is possible since $gcd(y, z) = 1$. Then we take

$$x = \frac{u + t \cdot z}{y} \leq 4n^{\frac{1}{3}}$$

and obtain:

$$P \cdot z = u = x \cdot y - t \cdot z \pmod{n}$$

which gives equation (6), with x, y, z and t being all smaller than $4 \cdot n^{\frac{1}{3}}$. From x, y, z, t we derive, using (5), four messages m_1, m_2, m_3 and m_4, each of size one third the size of n:

$$\begin{aligned} m_1 &= x + t \\ m_2 &= y + t \\ m_3 &= t \\ m_4 &= x + y + z + t \end{aligned} \tag{7}$$

Since $-n^{1/3} < z < n^{1/3}$ and $y \geq n^{1/3}$, we have $y + z > 0$, which gives using $u \geq 0$

$$x + t = \frac{u + t \cdot (y + z)}{y} \geq 0$$

which shows that the four integers m_1, m_2, m_3 and m_4 are non-negative, and we have

$$R(m_1).R(m_2) = R(m_3).R(m_4) \pmod{n}$$

The complexity of our attack is polynomial in the size of n.

3 EXISTENCE OF SELECTIVE FORGERY

The attack discussed in the previous section is existential, which means that the attacker needs to find the four messages required for forgery. This section deals with the possibility of a selective forgery attack, but in this case the attack no longer runs in polynomial time. Let m_3 be the message whose signature must be forged. Letting x, y, z and t as in Lenstra A., Lenstra H. and Lovasz L. (Lenstra et al., 1982), we compute two integers z and u such that

$$(P + t) \cdot z = u \pmod{n}$$

with

$$\begin{cases} -n^{\frac{1}{2}} < z < n^{\frac{1}{3}} \\ 0 < u < 2 \cdot n^{\frac{2}{3}} \end{cases}$$

We then factor u, and try to write u as the product $x \cdot y$ of two integers of roughly the same size, so that eventually we have four integers x, y, z, t of size roughly one third of the size of the modulus, with:

$$x \cdot y = (P + t) \cdot z \pmod{n}$$

which gives again

$$R(m_1).R(m_2) = R(m_3).R(m_4) \pmod{n}$$

The signature of m_3 can now be forged using the signatures of m_1, m_2 and m_4. For a 512-bit modulus the selective forgery attack is truly practical. For a 1024-bit modulus the attack is more demanding but was still implemented with success.

4 CONCLUSIONS

We have extended Girault and Misarsky's attack on RSA signatures with affine redundancy: we described a chosen message attack against RSA signatures with affine redundancy for messages as small as one third of the size of the modulus. Consequently, when using a fixed padding $P \mid m$ or $m \mid P$, the size of P must be at least two-thirds of the size of n. Our attack is polynomial in the length of the modulus. It remains an open problem to extend this attack to even smaller messages (or, equivalently, to bigger fixed-pattern constants): we do not know if there exists a polynomial time attack against RSA signatures with affine redundancy for messages shorter than one third of the size of the modulus. However, we think that exploring to what extent affine padding is malleable

increases our understanding of RSA's properties and limitations.

REFERENCES

Girault, M. and Misarksy, J. (1997). Selective forgery of rsa signatures using redundancy. In Springer-Verlag, editor, *Proceedings of Eurocrypt '97*, volume 1233 of *LNCS*, pages 495–507.

Girault, M., Toffin, P., and Vallee, B. (1988). Computation of approximation l-th roots modulo n and application to cryptography. In Springer-Verlag, editor, *Proceedings of Crypto '88*, volume 403 of *LNCS*, pages 100–117.

Jonge, W. D. and Chaum, D. (1986). Attacks on some rsa signatures. In Springer-Verlag, editor, *Proceedings of Crypto '85*, volume 218 of *LNCS*, pages 18–27.

Lenstra, A., Lenstra, H., and Lovasz, L. (1982). Factoring polynomials with rational coefficients. In *Mathematische Annalen*, volume 261, no. 4, pages 515–534.

Misarsky, J.-F. (1998). How (not) to design rsa signature schemes. In Springer-Verlag, editor, *Public-key cryptography (PKC)*, volume 1431 of *LNCS*, pages 14–28.

Rivest, R., Shamir, A., and Adleman, L. (1978). A method for obtaining digital signatures and public key cryptosystems. In *Communications of the ACM*, volume 21, no. 2, pages 120–126.

Network Working Group (1998). Rsa cryptography specifications, version 2.0. In *RSA Laboratories, PKCS # 1*.