

Attacking the Diebold Signature Variant – RSA Signatures with Unverified High-order Padding

Ryan W. Gardner^{a,*}, Tadayoshi Kohno^b, Alec Yasinsac^c

^a*Department of Computer Science, Johns Hopkins University, Baltimore, MD 21218, USA*

^b*Department of Computer Science and Engineering, University of Washington, Seattle, WA 98195, USA*

^c*Department of Computer Science, Florida State University, Tallahassee, FL 32306, USA*

Abstract

We examine a natural but improper implementation of RSA signature verification deployed on the widely used Diebold Touch Screen and Optical Scan voting machines. In the implemented scheme, the verifier fails to examine a large number of the high-order bits of signature padding and the public exponent is three. We present an very mathematically simple attack that enables an adversary to forge signatures on arbitrary messages in a negligible amount of time.

Keywords: Cryptography, RSA signature, Padding, Voting, Cryptanalysis

1. Background

Standard signatures using the RSA primitive are generally computed in two steps: 1) A one-way transformation T is applied to a message m to produce an encoded message M . 2) The RSA primitive using the private exponent is applied to M to generate the signature σ . Given a signature σ' on a message m' , verification generally proceeds similarly: 1) Again, the transformation T is applied to m' to obtain the encoded message $M' = T(m')$, and 2) the RSA primitive using the public exponent is applied to the signature σ' to produce M'' . 3) Finally, M' and M'' are checked for equality, and the signature verifies if and only if they are equivalent.

In this paper, we examine an improperly implemented RSA signature scheme, which uses a public exponent of three, where the verifier fails to com-

pare a large number of the high-order bits of the encoded messages M' and M'' . We briefly present an simple attack against such implementations that enables an adversary to forge signatures on arbitrary messages in a negligible amount of time. Specifically, the attack works for any transformation function T and for all messages when $b < \frac{1}{3}\ell_n - 3$, where b is the number of low-order bits of M' and M'' that are examined, and ℓ_n is the bit-length of the RSA modulus.

This flawed signature scheme has become relevant in practice as we observe multiple instantiations of it in recent (May 2007) versions of the widely used Diebold voting machine firmware.¹ We find that the Diebold Touch Screen bootloader 1.3.6 and Optical Scan 1.96.8 employ a natural, yet flawed, implementation of “text-book” RSA where a transformation function $T = \text{SHA-1}$ is used, and the least significant 160 bits (i.e. the SHA-1 hash) of M' and M'' are exclusively examined when verifying their equal-

* Corresponding author.

Email addresses: ryan@cs.jhu.edu (Ryan W. Gardner), yoshi@cs.washington.edu (Tadayoshi Kohno), yasinsac@cs.fsu.edu (Alec Yasinsac).

¹ The code was examined under a charter from the Florida Department of State in June 2007 [8].

ity. The verified signatures cover data [8] that, if unauthenticated, has been publicly reported to enable simple arbitrary software installation [11], vote pre-loading (and pre-removing) [10], arbitrary code execution [15], and a mass spreading, vote stealing virus [6] on the voting machines.

Several other research papers have analyzed variants and flawed constructions of RSA authentication systems and their padding and redundancy schemes. Recently, Bleichenbacher describes an attack under conditions similar to those we examine, where a public exponent of three is used and erroneously implemented signature verification code fails to appropriately verify most of the *low-order* bits of a PKCS-1 padded message [1]. Examining another standard, Coron, Naccache, and Stern extend a chosen plaintext attack on the RSA cryptosystem by Desmedt and Odlyzko [5] to develop a signature forgery strategy that is effective on a scheme that uses a padding format differing from ISO 9796-1 by only one bit [3]. In addition to these more common modes for RSA, several studies have discovered weaknesses, under varying conditions, in a number of schemes that do not hash messages before signing, but instead apply redundancy bits to them [2, 4, 9, 12–14].

2. Construction

We now describe the construction of the flawed RSA signature scheme we examine.

Let $n = pq$ be an ℓ_n -bit standard RSA modulus equal to the product of two primes, and let d denote the private exponent such that $3d \equiv 1 \pmod{\phi(n)}$. Let 3 be the public exponent. We use the notation $[x]_{:a-b}$ to refer to the value obtained by writing bits $a - b$ of x as a binary number, where bit 0 is the least significant bit of x . Furthermore, in the general scheme we find, a message m is transformed into an encoded message M using a transformation T before it is signed. In practice, the function T usually involves hashing and padding the message m or applying redundancy to it. However, for the sake of this analysis, we let T be any function $T : \{0, 1\}^* \rightarrow \mathbb{Z}_n^*$ (where $\mathbb{Z}_n^*$ may be approximated as all integers inclusively between 0 and $n - 1$).

Signature generation on a message $m \in \{0, 1\}^*$ then consists of the following two classic computations:

$$M = T(m) \quad (1)$$

$$\sigma = M^d \pmod{n} \quad (2)$$

and the resulting signature is then $\sigma \in \mathbb{Z}_n^*$.

Verification proceeds similarly given a signature σ' and a message m' . The verifier computes:

$$M' = T(m') \quad (1)$$

$$M'' = \sigma'^3 \pmod{n} \quad (2)$$

Then, although an appropriate algorithm would verify that $M' = M''$, in the faulty construction we find, the verifier checks

$$[M']_{:0-(b-1)} = [M'']_{:0-(b-1)}$$

for a $b < \frac{1}{3}\ell_n - 3$. The signature is considered valid if and only if the two values are equivalent.

3. Attack

Assuming the verification scheme described above, we now describe a very simple method for forging signatures on arbitrary messages.

Let m be any message and $M = T(m)$. It follows from the construction that if we can find a value σ , such that

$$\sigma^3 \equiv M + 2^b z \pmod{n}$$

for any integer z where $2^b z < n$, then σ is a valid signature. (Notice that if $2^b z > n$, its value is likely to alter the lower b bits of the modular reduction, in which case they will no longer match those of M .)

In the case where M is odd, a solution is almost immediate when we consider the problem in $\mathbb{Z}_{2^b}^*$. Since we know the order of $\mathbb{Z}_{2^b}^* = 2^{b-1}$, we can find the cube root of $M \pmod{2^b}$. First, using Euclid's extended algorithm, we find r such that $3r \equiv 1 \pmod{2^{b-1}}$.

Claim 1 $\sigma \equiv M^r \pmod{2^b}$ is a valid signature on m when M is odd.

Proof. $\sigma^3 \equiv M^{3r} \equiv M^{1+y\phi(2^b)} \equiv M \pmod{2^b}$ by Euler's theorem. Since σ was generated as an element of $\mathbb{Z}_{2^b}^*$, we know it can be written as an integer less than 2^b . Thus, $\sigma^3 \leq 2^{3b} \leq 2^{\ell_n-9} < n$ and $\sigma^3 \equiv M + 2^b z \pmod{n}$ for some z where $2^b z < n$. $\square$

In the case where M is even, the same attack does not apply since $M \notin \mathbb{Z}_{2^b}^*$. Instead, we use a slightly modified approach to obtain a member from that group.

Choose c to be the least integer such that $(2^b c)^3 > n$, and let r be defined as above.

Claim 2 $\sigma = 2^b c + ((M + n)^r \pmod{2^b})$ is a valid signature on m when M is even.

Proof. Let $\tau = ((M+n)^r \bmod 2^b)$. We will first find an upper bound on σ^3 . Since $\tau < 2^b$,

$$\sigma^3 = (2^b c + \tau)^3 < (2^b(c+1))^3.$$

Further, $(2^b(c-1))^3 < n$ by our choice of c , which we can rewrite

$$c+1 < \frac{\sqrt[3]{n}}{2^b} + 2.$$

Combining these two inequalities yields

$$\sigma^3 < \left(2^b \left(\frac{\sqrt[3]{n}}{2^b} + 2\right)\right)^3 = (\sqrt[3]{n} + 2^{b+1})^3,$$

or, by our bound on b ,

$$\sigma^3 < \left(\sqrt[3]{n} + 2^{(\frac{1}{3}\ell_n - 3) + 1}\right)^3 = (\sqrt[3]{n} + 2^{-2} \sqrt[3]{n})^3.$$

Thus,

$$\sigma^3 < \frac{125}{64}n.$$

Now, with the above bound, and the fact that $\sigma^3 > n$, by our choice of c . We can conclude $(\sigma^3 \bmod n) = \sigma^3 - n$. Hence, σ is a successful forgery iff $\sigma^3 - n \equiv M \bmod 2^b$. Indeed,

$$\begin{aligned} \sigma^3 - n &\equiv (2^b c)^3 + 3(2^b c)^2 \tau + 3(2^b c) \tau^2 \\ &\quad + \tau^3 - n \bmod 2^b \\ &\equiv \tau^3 - n \bmod 2^b. \end{aligned}$$

Since n is odd, $M+n$ is a member of $\mathbb{Z}_{2^b}^*$, and $\tau^3 \equiv M+n \bmod 2^b$ just as we saw in the M odd case. Therefore, $\sigma^3 \equiv M \bmod n \bmod 2^b$. $\square$

4. Conclusion

We have found a natural, but improper implementation of an RSA signature scheme in a highly sensitive application, electronic voting. We present an extremely mathematically simple attack against it, which is also very practical.² We hope this subtle, but real flaw emphasizes the challenges of properly securing systems and also stresses the importance of approaching such tasks diligently.³

² We verified the attack for the odd case on an optical scan machine provided by the state of Florida.

³ After being notified of the flaw, the vendor improved the signature verification code in new versions of their firmware [7] although existing machines that are not updated remain vulnerable, of course.

Acknowledgments

This research was supported by NSF grant CNS-0524252 and by a grant from the Florida Department of State. We also thank Avi Rubin for his comments and support.

References

- [1] D. Bleichenbacher. RSA signature forgery based on implementation error. *Advances in Cryptology – CRYPTO ’06*, Rump session, August 2006. Available at <http://www.imc.org/ietf-openpgp/mail-archive/msg14307.html>.
- [2] E. Brier, C. Clavier, J.-S. Coron, and D. Naccache. Cryptanalysis of RSA signatures with fixed-pattern padding. In *Advances in Cryptology – CRYPTO ’01*, volume 2139, pages 433–439. Springer-Verlag, 2001.
- [3] J.-S. Coron, D. Naccache, and J. P. Stern. On the security of RSA padding. In *Advances in Cryptology – CRYPTO ’99*, volume 1666, pages 1–18. Springer-Verlag, 1999.
- [4] W. de Jonge and D. Chaum. Attacks on some RSA signatures. In *Advances in Cryptology – CRYPTO ’85*, volume 218, pages 18–27. Springer-Verlag, 1986.
- [5] Y. Desmedt and A. M. Odlyzko. A chosen text attack on the RSA cryptosystem and some discrete logarithm schemes. In *Advances in Cryptology – CRYPTO ’85*, volume 218, pages 516–522. Springer-Verlag, 1986.
- [6] A. J. Feldman, J. A. Halderman, and E. W. Felten. Security analysis of the diebold accuvote-ts voting machine. In *USENIX/ACCURATE Electronic Voting Technology Workshop – EVT ’07*, 2007.
- [7] D. Gainey, M. Gerke, and A. Yasinsac. Software review and security analysis of the diebold voting machine software, supplemental report. Technical report, Florida Department of State, August 2007.
- [8] R. Gardner, A. Yasinsac, M. Bishop, T. Kohno, Z. Hartley, J. Kerski, D. Gainey, R. Walega, E. Hollander, and M. Gerke. Software review and security analysis of the diebold voting machine software. Technical report, Florida Department of State, July 2007.
- [9] M. Girault and J.-F. Misarsky. Selective forgery of RSA signatures using redundancy. In *Advances in Cryptology – EUROCRYPT ’97*, volume 1233, pages 495–508. Springer-Verlag, 1997.
- [10] H. Hursti. Critical security issues the diebold optical scan design, July 2005. Available at <http://www.blackboxvoting.org/BBVreport.pdf>.
- [11] H. Hursti. Diebold tsx evaluation: Critical security issues with diebold tsx, May 2006. Available at <http://www.blackboxvoting.org/BBVreportIIunredacted.pdf>.
- [12] A. K. Lenstra and I. Shparlinski. Selective forgery of RSA signatures with fixed-pattern padding. In *Practice and Theory in Public Key Cryptosystems – PKC ’02*, volume 2274, pages 228–236. Springer-Verlag, 2002.
- [13] M. Michels, M. Stadler, and H.-M. Sun. On the security of some variants of the RSA signature scheme. In

- European Symposium on Research in Computer Security*
– *ESORICS '98*, volume 1485, pages 85–96. Springer-Verlag, 1998.
- [14] J.-F. Misarsky. A multiplicative attack using LLL algorithm on RSA signatures with redundancy. In *Advances in Cryptology – CRYPTO '97*, volume 1294, pages 221–234. Springer-Verlag, 1997.
- [15] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, and N. Sastry. Security analysis of the diebold accubasic interpreter. Technical report, Voting Systems Technology Assessment Advisory Board, Office of the Secretary of State of California, February 2006.