NUMBER 11 — APRIL 23, 1999

RSA Laboratories' Bulletin

News and advice on data security and cryptography

Recent Results on Signature Forgery

Robert D. Silverman
RSA Laboratories, Bedford, Massachusetts, USA

David Naccache
Gemplus, Issy-les-Moulineax, France

Abstract

A weakness has been found in the ISO 9796 signature standard using RSA™. The padding method proposed by the standard is the origin of the problem and will require probable changes in ISO 9796 parts 1 and 2. This weakness was discovered by Gemplus' cryptography division and the ENS and UCL cryptography groups while implementing the standard. A paper reporting the problem will be presented at Crypto '99 but information can readily be obtained on RSA Data Security's and ISO's web sites. Not all implementations are at risk as some protocol specifics may protect applications from the weakness; no attack has been conducted on real transactions. ISO is actively working on this security issue and should come up soon with a new solution. The attack's authors will provide all necessary assistance to ISO in this task. This process is normal and shows how open security standards are improved day after day by the iterative contribution of all experts around the world. When a weakness is found standards are corrected and improved to become more resistant. Security standards relying on secrecy (security by obscurity) cannot be scrutinized by the open expert community and be improved by this process. It is also important to notice that security is relative regarding time and what is secure today may need to be improved tomorrow.

Robert Silverman is a Senior Research Scientist at RSA Laboratories, and can be reached at rsilverman@rsa.com. David Naccache is Cryptography and Security Group Manager at Gemplus in Issy-les-Moulineax, France.

Introduction

This document discusses a recently discovered attack on several digital signature padding schemes. The attack is applicable in different ways to each of the schemes. We emphasize here that the attack does not threaten the use of the RSA algorithm in digital signatures. It does not recover the private key and is less effective than a factoring attack except in special circumstances. Whether one can recover the private key for Rabin or Williams signatures is still under investigation. Rather, the attack is based upon the way messages are formatted and hashed before they are signed. The attack is particularly potent in certain signature schemes where signature verification also recovers the message.

In a recently released paper [1], J-S. Coron, D. Naccache, and J. Stern announce a practical way of forging signatures that are based upon ISO 9796-2 and a format that differs in only one bit from ISO 9796-1, as well as theoretical observations on PKCS #1 v2.0 (which is the same signature scheme as in PKCS #1 v1.5), ECASH™, SSL-3.02 and ANSI X9.31. We emphasize again that the observations on these four formats are theoretical only and do not threaten in any way the security of products using PKCS #1 v2.0, ECASH, SSL-3.02 and ANSI X9.31 or, in general, signature schemes specified in these standards. Actually, Coron *et. al.* consider that the extremely negligible impact of the new attack on PKCS #1 v2.0, SSL-3.02 and ANSI X9.31 should be regarded as a very positive indicator of their sound design rationale and *increase* the public's confidence in those designs. The attack on PKCS

RSA Laboratories
A Division of RSA Data Security

#1 and SSL-3.02 is less effective than prior attacks based upon finding hash collisions and only applies when the modulus takes on very peculiar forms. The attack on ANSI X9.31 only applies when the modulus takes a very peculiar form and the standard does not permit constructing moduli of this form. The attack that is the most effective essentially gets its effectiveness from the fact that the very slightly modified version of ISO 9796-1 considered by the authors (which is however never used in any specific product) does not use hash functions.

This attack is completely different than the result last year by Daniel Bleichenbacher on RSA encryption [2]. Coron-Naccache-Stern's attack applies only to signature schemes, not encryption schemes (See also the *CryptoBytes* survey on RSA encryption [5].)

The attack is posed within the general framework of a new theoretical attack on all signature schemes based on RSA. This attack shares many mathematical features of Index-Calculus attacks on the discrete logarithm problem and of the Number Field Sieve attack on integer factorization. One attempts to get the legitimate owner of a key to sign a set of chosen messages. The size of this set is sub-exponential in the size of the key being forged. The messages are chosen to have special structure; they are chosen so that the messages when represented as integers are divisible only by small prime numbers. Such integers are commonly called smooth numbers. One uses the smoothness properties to build a database (a set of indices) which can then be used to forge new signatures. This class of attack on RSA signature schemes was first observed by Desmedt and Odlyzko [3] and taken into account in the original design of PKCS #1 v1.5, based on an unpublished observation by Rivest [4].

In all the signature schemes, an encoding operation (e.g., hashing and formatting, or just formatting in the ISO 9796-1 case) is applied to a message to produce a message representative , to which the RSA signature primitive is applied. The RSA verification primitive recovers the message representative and either a decoding operation is applied to recover the message, or a verification is applied to the message and the message representative to determine whether they are consistent.

The different schemes all use the RSA primitive, but vary in their encoding operation. An attacker does not have direct access to the RSA primitive but can influence the message representative. The degree of influence determines the effectiveness of the attack. In PKCS #1, ANSI X9.31 and SSL-3.02 there is extremely little influence because the message representative is highly structured and a hash value is included. But in the very slightly modified version of ISO 9796-1 the message representative directly includes portions of the message and bit positions can therefore be influenced individually.

Attacks on ISO 9796-2 and Slightly Modified ISO 9796-1

In theory, against random message representatives whose length is comparable to the RSA modulus length, the attack is no more effective than a Number Field Sieve attack on the RSA modulus. However, the way ISO 9796-1 constructs its messages before signing is very close to providing a special structure that can be exploited. This standard only signs messages which are at most one-half the length of the RSA modulus. The message is then expanded to the full length of the modulus by interleaving bytes together. No hash of the message is taken before the signature is applied. This special structure could have been effectively attacked by the smoothness attack outlined above if the standard's specifictions would have differed by one single bit. The attack is such that thousands of signatures on a 1024-bit modulus (formatted with this quasi-ISO 9796-1 format) can be forged in a single day using only a single computer of moderate power. Forged messages have the curious property of not depending on the attacked system's modulus and could therefore be potentially recycled from system to system. ISO WG2 SC27 will post an informative communication on the its website in the coming days.

The ISO 9796-2 standard does use a hash function, but again messages are formulated with a special padding that can be exploited. This time the attack is not nearly as effective as for the quasi-ISO 9796-1 format, but nevertheless the attack still takes considerably less time than a standard birthday/collision attack. For a 160-bit hash function and a 1024-bit key a birthday attack can be expected to take 2^{80} operations, whereas this new attack takes only 2^{60} operations and 2^{40} space.

ECASH uses a somewhat similar structure to ISO 9796-2, but the differences are enough so that an attack on ECASH is effective only when the length

of the message being signed plus the length of the hash output is close to the length of the RSA modulus. The attack is similar to that on ISO 9796-2, but applies in fewer situations. ECASH padding can be vulnerable if used with long, non-random messages.

The attack on ISO 9796-2 can be expected to take a few weeks to forge a very small number of signatures on a single PC.

Theoretical Observations on PKCS #1 v2.0, SSL-3.02 and ANSI X9.31

In the cases of PKCS #1, SSL-3.02 and ANSI X9.31 the attack should be regarded as a mere theoretical observation and not a concrete threat. The attack's authors heavily insist on underlining that in these three cases the attack "applies" in only extremely limited circumstances and does not endanger current implementations of these standards. The observation only applies when the RSA modulus is of the form $2^k \pm c$ for small c and for a very limited number of more specialized cases. The phenomenon, even when applicable, on all three standards actually takes more time than it does to factor the modulus and must be regarded as a theoretical curiosity. Further, such moduli are generally avoided because they may be amenable (depending on c) to the special form of the Number Field Sieve and can be factored much faster than general integers of the same size. This is especially true in the case where c has low Hamming weight.

Further, these moduli are explicitly prohibited by the ANSI X9.31 standard. It should be noted that ISO 9796 does allow the use of these special moduli. The paper by Coron, Naccache and Stern also suggests one additional form of the modulus that should be avoided if using ANSI X9.31. However, such a modulus can not occur if the standard is followed. It would be required to have an odd bit length and the standard requires a bit length which is a multiple of 256.

The SSL-3.02 format is a special signature format employed within SSL for signing short-term keys, which involves two hash functions. SSL-3.02 also employs PKCS #1 signatures for many purposes.

Practical Implications

Since the new attack does not apply to the full-fledged ISO 9796-1 format, ISO 9796-1 applications are not in imminent danger. The alert appears however serious enough to motivate a complete in-depth review of the standard. RSA Laboratories and Gemplus are currently assessing the size of the community that would be concerned by this result. ISO 9796-1 was designed specifically for processing short messages in such way that the message can be recovered from a signature. As such, its application is limited to those environments where the message to be signed is short (although the "message" in this case may in fact be a hash value). The prevailing use of RSA signatures in industry is based on PKCS #1, which allows messages of any length, and which is not impacted by the attack at all.

Suggestions

We suggest that ISO 9796 be modified by using FDH (Full Domain Hashing) [6] or PSS (Probabilistic Signature Scheme) [7]. RSA Laboratories and Gemplus intend to propose such alternatives to standards bodies. PKCS #1 or ANSI X9.31 would also be very acceptable as an alternative. Such hashing provides theoretical protection as described by the work of Bellare and Rogaway. Except for the message recovery variant of PSS, however, these alternatives will not help in the case where the signature scheme provides message recovery. Although there are no immediate implications to PKCS #1, SSL-3.02, or ANSI X9.31, we recommend that FDH or a similar format be considered there also, as a precaution against future developments.

References:

1. J.-S Coron, D. Naccache, and J. P. Stern, A New Signature Forgery Strategy, To appear, Crypto '99
2. D. Bleichenbacher, Chosen Ciphertext Attacks Against Protocols Based on the RSA Encryption Standard PKCS #1, Advances in Cryptology, Crypto '98, pp. 1-12
3. Y. Desmedt and A. Odlyzko, A Chosen Text Attack on the RSA Cryptosystem and Some Discrete Logarithm Schemes, Advances in Cryptology, Crypto '85, pp. 516-522
4. R. Rivest, Personal Communication to RSA Laboratories, email 1991
5. B. Kaliski and M. Robshaw, The Secure Use of RSA, RSA Laboratories' CryptoBytes, vol. 1 no. 3, Autumn 1995, pp. 7-13
6. M. Bellare and P. Rogaway, Random Oracles are Practical: A Paradigm for Designing Efficient Protocols, Proc. 1st Annual Conf. on Computer and Communication Security 1993

7. M. Bellare and P. Rogaway, The Exact Security of Digital Signatures: How to Sign with RSA and Rabin, Advances in Cryptology, Eurocrypt '96, pp. 399-416

Standards:

ANSI X9.31-1998, Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), Accredited Standards Committee X9, American Bankers Association

IEEE P1363, Standard Specifications for Public Key Cryptography, draft D9, February 1999. Available from http://grouper.ieee.org/groups/1363/.

PKCS #1 v2.0: RSA Cryptography Standard, RSA Laboratories, 1998. Available from http://www.rsa.com/rsalabs/pubs/PKCS/.

ISO/IEC 9796, Information Technology – Digital Signature Scheme Giving Message Recovery; Part 1 – Mechanisms using Redundancy, 1997.

ISO/IEC 9796, Information Technology – Digital Signature Scheme Giving Message Recovery; Part 2 – Mechanisms using a Hash Function, 1997.

ECASH ™ is a trademark of DigiCash. RSA is a trademark of RSA Data Security, Inc.

For more information on this and other recent security developments, contact RSA Laboratories at one of the addresses below.

RSA Laboratories
20 Crosby Drive
Bedford, MA 01730 USA
781/687-7000
781/687-7213 (fax)
rsa-labs@rsa.com
http://www.rsa.com/rsalabs/

Copyright © 1999 RSA Laboratories, a division of RSA Data Security, Inc., a Security Dynamics Company. All rights reserved.