A New Variant for an Attack Against RSA Signature Verification Using Parameter Field

Yutaka Oiwa, Kazukuni Kobara, and Hajime Watanabe

Research Center for Information Security (RCIS),
National Institute of Advanced Industrial Science and Technology (AIST),
1-18-13-1102 Sotokanda, Chiyoda-ku, Tokyo, Japan

Abstract. We present a method to create a forged signature which will be verified to a syntactically well-formed ASN.1 datum, when certificate authorities use small RSA public exponents such as 3. Our attack is related to the technique which Daniel Bleichenbacher reported recently, but our forged signature is well-formed ASN.1 datum, unlike Bleichenbacher's original attack: thus our new attack is still applicable to certain implementations even if these are immune to the Bleichenbacher's attack. We have also analyzed the parameters which enable our attack and Bleichenbacher's, and found that both attacks are possible with the combination of existing public keys of widely-trusted certificate authorities and existing real-world implementations. We have already reported the vulnerability to developers of both GNUTLS and Mozilla NSS to fix their implementations.

List of Keywords: vulnerability, attacks, certificate verification.

1 Introduction

In this paper we present an attack against some implementations of RSA signature verification for small public exponents. More precisely, given (n, e) an RSA public key of a certificate authority (CA), and given h a digest value of a certificate, we present a method to generate a forged signature which, after verified by the public key, will be accepted as a "correct" RSA signature data by several RSA implementations.

The attack is a variant of the attack which Daniel Bleichenbacher presented at the rump session of CRYPTO2006 [1]. His attack generates a syntactically ill-formed signature with some garbage data at the tail of decoded data. Our version of the attack, instead, generates at least syntactically well-formed data, enclosing similar "garbage" data inside the DER data packet. Therefore, some software (e.g. GNUTLS) is vulnerable to our attack, although it is not vulnerable for Bleichenbacher's attack.

The possibility of exploits using such garbage data seems to be understood by several independent parties: at least OpenSSL has added a check routine for those garbage data before we reported a specific attack [8]. Our contributions are (1) we found similar misimplementation in other two SSL implementations

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 143–153, 2007.

(GNUTLS [4] and Mozilla NSS), and (2) we constructed a practical attack and give an analysis on it.

In October 2006, NIST has published a technical notice [6] about the vulnerability which Bleichenbacher has discovered. However, the notice urges implementors to ensure that they checks the non-existence of garbages at the tail of signature messages, which Bleichenbacher has used for constructing the attack, but it overlooks about other possibilities for attacks, like one presented in this paper. Thus, for example, the notice cannot address the issue on GNUTLS (which is not vulnerable for Bleichenbacher's original attack). We believe that it is important to share the technical backgrounds of such vulnerabilities with researchers and implementors by putting it into the form which can be easily referred, so that they can not only fix their implementations but also avoid resurrecting the bugs in future software.

The rest of the paper is organized as follows: we describe Bleichenbacher's original attack in Section 2. In Section 3 we present our new attack and the precise way of generating forged signatures. The next section analyzes the conditions and possible extensions for our attack. A real case of misimplementations and measures we have taken are described in Section 5. Section 6 discusses about possibilities of similar vulnerabilities caused by other misimplementations. In Section 7 we conclude this paper and gives some suggestions for implementors of RSA signature verification.

2 The Bleichenbacher's Attack

In this section we describe the original attack which Bleichenbacher presented at the rump session of CRYPTO2006. It uses the fact that some TLS implementations do not check whether there are any excess data after the ASN.1 packet in the decoded message datum. A correct RSASSA-PKCS1-v1_5 signature message (see [10] for details) with MD5 digest, after RSA verification primitive (*RSAVP1*) is applied, looks like the following (shown in hexadecimal representation):

```
0x0001FF.....................FF
003020300c06082A864886F70D020505000410[ h ],
```

where [h] is the 128-bit MD5 digest value of the certificate signed. A DER-encoded DigestInfo block for signature data containing h, which is shown in the second line, is padded with the PKCS #1 block type 1 padding in the first line. The length of the whole data is adjusted to the length of CA's public key before applying the signing primitive using the CA's secret key.

Bleichenbacher's attack generates a forged signature which will be decoded by the verification primitive to the message

```
0x0001FF......FF
003020300C06082A864886F70D020505000410[ h ]
garbage
```