A Security Flaw in the X.509 Standard

Santosh Chokhani
CygnaCom Solutions, Inc.

Abstract

The CCITT X.509 standard for public key certificates is used to for public key management, including distributing them with a high degree of confidence in binding between the users and their public keys. The two locations where the public key parameters of certificate signer (also called certificate issuer or certification authority) can be placed in a X.509 certificate are vulnerable to parameter substitution attack. The Department of Defense FORTEZZA card and the Multilevel Information Systems Security Infrastructure (MISSI) are **NOT** vulnerable to the attack described in this paper.

1.0 Introduction

The CCITT and ISO have developed a X.509 public key certificate standard to provide high integrity, authenticated binding between entities and their public keys. This standard is being adopted worldwide including the United States Federal Government, Government of Canada, American National Standards Institute (ANSI), and the U.S. banking industry for public key management and public key infrastructures. While there may be some minor differences in these standards, the security area analyzed in this paper is common to all of them. Hence, the findings of this paper are applicable to all known standards and implementations of public key certificates.

In Section 2, we provide a background on the X.509 certificate and certificate revocation list (CRL) standards. In Section 3, we describe the potential flaw the standard is vulnerable to. In Section 4, we describe the risk of the flaw based on various cryptosystems used to sign the certificates and CRLs. In Section 5, we provide some recommendations. Finally, an appendix provides some implications for the Digital Signature Standard (DSS).

2.0 X.509 Background

The joint ISO CCITT X.509 standard and its amendments describe the formats for public key certificate and CRLs issued by trusted authorities [4, 5]. These trusted authorities are also called Certification Authority or CA. The certificate and CRL are Abstract Syntax Notation.1 (ASN.1) encoded objects using the Distinguished Encoding Rules (DER). The entire content of the certificate and the ASN.1, DER concepts are not critical to understanding the flaw we describe. Thus, we will concentrate only on the aspect of the certificates and CRL that relate to the flaw. Figure 1 below describes the format of the X.509 certificate. For the details of the contents of the certificate, please read the X.509

standards and related draft and balloted amendments. A public key certificate is a signed (by a CA) object that binds an entity (e.g., an user) to his/her public key. The certificate contents relevant to this paper are: certificate issuer (signer) distinguished name, subject distinguished name, and subject public key. This information is within the signed envelop of the certificate. The signed envelop may optionally contain issuer public key parameters and/or the subject public key parameters. In addition, as Figure 1 illustrates, the signature (termed signed macro in the X.509 standard) may optionally contain the issuer public key parameters. The signed macro always contains the digital signature. The inclusion of public key parameters in the signed macro allows efficient signature verification based on these parameters without having to decode the certificate and then extract the parameters from the issuer public key parameters field. The issuer public key parameters are included in the signed envelop and/or the signed macro to allow the CAs in a trust chain to have different public key parameters. The subject public key parameters field allows the subjects to have different parameters from their certificate issuers.

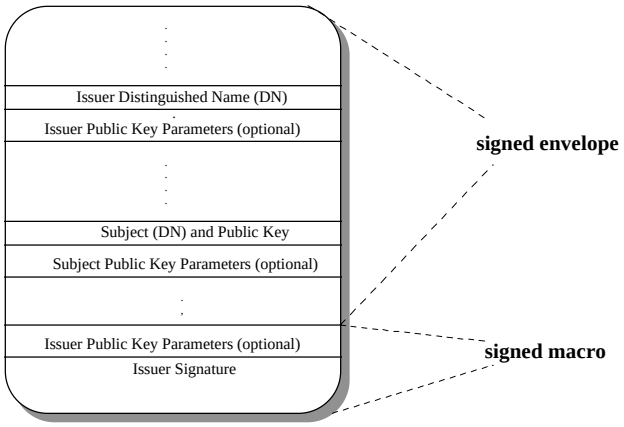

Figure 1: X.509 Public Key Certificate Format

Figure 2 below describes the format of the CRL. For the details of the contents of the CRL, please read the X.509 standards and related draft and balloted amendments. A CRL is a signed (by a CA) object that lists the revoked certificates. In order to maintain trust, public keys corresponding to revoked certificates should not be used since the CA no longer vouches for the binding between the users and their public keys as published in original certificates. The CRL content relevant to this paper is: certificate issuer (signer) distinguished name. This information is within the signed envelop of the CRL. The signed envelop may optionally contain issuer public key parameters. In addition, as Figure 2 illustrates, the signature (termed signed macro in the X.509 standard) may optionally contain the issuer public key parameters. The signed macro always contains the digital signature. The inclusion of public key parameters in the signed macro allows efficient signature verification based on these parameters without having to decode the CRL and then extract the parameters from the issuer public key parameters field. The issuer public

key parameters are included in the signed envelop and/or the signed macro to allow the CAs in a trust chain to have different public key parameters.

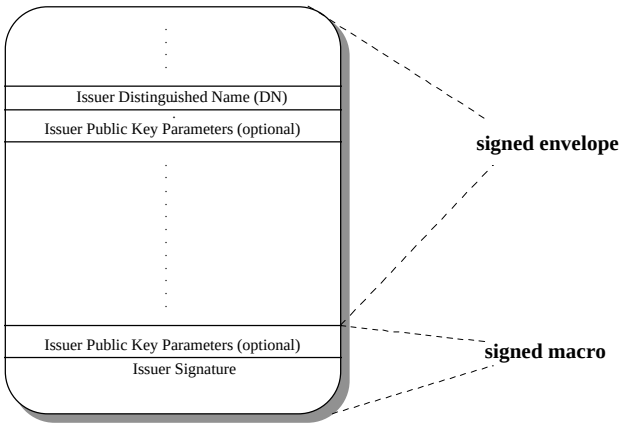

Figure 2: X.509 Certificate Revocation List Format

3.0 Basic Flaw -- Public Key Parameters Substitution

The use of issuer public key parameters fields (both in the signed envelop and in the signed macro) are vulnerable to substitution attack. The detailed scenario is as follows.

We need issuer public key and public key parameters to verify the signatures on the certificate and CRL. The issuer public key is expected to be obtained through a trusted and authenticated means. It is not available in the signed object (certificate and CRL).

A public key digital signature cryptosystem offer a certain degree of security. The degree of security is defined as the computational complexity of forging signatures or computing the private key for a public key and public key parameters of certain quality and size. For example, we know that in the Digital Signature Standard, the size of the large modulus p, size of the small modulus q, and the properties of p, p-1, and q are critical to security. The properties include ensuring that p and q are primes of appropriate size and that q divided evenly into p-1.

If the issuer public key parameters are used from the signed envelop or the signed macro, an attacker who wants to replace, modify or create bogus certificates and CRL, can substitute these values in the objects (certificate and CRL) and resign the objects (certificate and CRL). This allows the attacker to translate a hard public key cryptography problem into one of finding a new set of parameters and private key that are consistent with the trusted public key. Finding this may be easier, as hard or harder. This all depends on the mathematical properties of the cryptosystem.

For example in the DSS, the public key is y, private key is x, and public key parameters are p (large modulus), q (small modulus), and g (generator). We know that if the parameters are generated according to the standard, given y, p, q, g, it is hard discrete logarithm problem to find the private key x. What has not been analyzed in the literature is given y, could one find parameters p', q', and g' such that find a new key x' would be easier than the hard discrete logarithm problem. If this was possible, an attacker could substitute p, q, g in the issuer public key parameters in a certificate and/or CRL with p', q, g' and then use x' to sign the certificate and or CRL. The user of the certificate will use y, p', q', and g' to verify the signature.

In summary, our basic claim is that the two locations where the issuer public key parameters appear, are unauthenticated. This is true even if one of these parameter set is within the signed envelop. This is due to that fact that the parameters values in the certificate itself are used to validate the signatures on the same certificate. Thus, an attacker can always substitute the parameters and resign. The ease of finding a private key and parameter set consistent with the authenticated public key depend on the cryptosystem chosen. The cryptosystem specific issues are analyzed in Section 4 below.

Impact of the Flaw

The flaw is extremely severe. It can destroy trust in an entire Public Key Infrastructure (PKI) since the attacker can modify or create bogus certificates and CRL for intermediate CAs in a chain and for end entities. The trust in a PKI and in a CA depends on the authenticity of certificates and CRLs.

4.0 Implications for Various Cryptosystems

RSA

The parameter substitution attack can not be used in X.509 certificates with RSA since the two public values required for RSA (e - encryption exponent, n - composite number) are both part of the public key. RSA has no public key parameters.

DSS

While the DSS is very clear on the requirement for the public parameters (p - large prime modulus, q - small prime modulus, g - generator) to be authenticated [1], some organizations have registered the DSS algorithms with ISO that provide for p, q, g to be parameters in X.509 sense. Thus, these parameters can be included in the two issuer parameters field discussed previously. Based on the analysis in Section 3 above, these values will be naturally unauthenticated. This leads to X.509 DSS based certificate implementations that are inconsistent with and are in contradiction with the specific requirement of the DSS, namely the need to use authenticated parameters. Appendix provides further details on how an attacker can substitute p, q, and g. The detailed mathematical analysis is beyond the scope of this paper.

MISSI
The attack described here can not materialize in the Department of Defense FORTEZZA card and MISSI due to the fact that MISSI always uses authenticated public key parameters and due to the cryptographic checks in the FORTEZZA card. MISSI uses the authenticated parameters for an initial trusted authority public key and only uses the parameters from the subject public key parameters in the certificates which are always authenticated due to the digital signatures on the certificate.

Different Meanings of the term "Public Key Parameters"
The term public key parameters in a cryptosystem generally means that they could be public and could be common to a group of users. For example, the term DSS parameters in the DSS standard are meant to convey elements of keying material that can be public and be common to a group of users. The DSS standard still requires these parameters to be provided in an authenticated manner and the cryptosystem security depends on their quality, size, and the users obtaining them in an authenticated manner.

The implication of the term "parameters" in the X.509 standard is bigger than the one in the DSS standard or potentially other cryptosystems. The implication in the X.509 standard is that the substitution of the parameter values (in issuer public key parameters fields) may not reduce the security of the cryptosystem. If the parameters are used in these fields, the security of the base cryptosystem can be changed to that of computing a private key that maps to the registered public key under the substituted parameters.

5.0 Recommendations

Analysis Based Parameter Definition
The X.509 certificates provide a flexible mechanism for registering public key and public key parameter syntax for various cryptosystems. When interested parties register a cryptosystem, the parameter substitution problem must be fully analyzed. If it can be shown that the substitution problem is at least as hard as the base cryptosystem, only then the parameters should be registered as part of public key parameters. If the analysis shows that the problem may be simplified or the answer is unknown, the parameters must be registered with the public key. The public key syntax must provide for optional inclusion of the parameters, in order to keep the certificate and CRL size small.

Ignore the Issuer Public Key Parameters Field in Registered Cryptosystem
For cryptosystems like DSS, where the parameters have been already registered and a preliminary analysis shows that the substitution attack is simpler than computing discrete logarithms for cryptosystems as defined in DSS, the parameters in issuer public key parameters fields must be ignored.

Change Cryptosystem Registry

For cryptosystems like DSS, where the parameters have been already registered and a preliminary analysis shows that the substitution attack is simpler than computing discrete logarithms for cryptosystem as defined in DSS, the registry should be modified to carry no parameters in the parameters field, but to carry them optionally in the subject public key information field only.

Use Parameters in Subject Public Key Parameters Field

Our previous recommendations do not reduce the flexibility of different users having different parameters. In a chain of certificates and CRL of arbitrary length, as long as one starts with authenticated public key and public key parameters of a trusted CA, and uses the values in the subject public key parameters field, the substitution attack will not materialize.

Check the Quality and Size of Parameters

One option is that during the use of a certificate or CRL (i.e., their verification) crypto engine checks the quality and size of unauthenticated parameters. We don't recommend this due its performance impact and since these checks may not be a sufficient substitute for authenticated parameters. For example, it will be take prohibitively long (at least minutes on a desktop workstation) to verify the primality of p and q in DSS.

Cross-fertilize

We stumbled into this flaw while developing rules for public key parameters inheritance in a certificate chain. One lesson we have learned is that the implementors need to pay greater attention to the security and mathematics of cryptosystems and the mathematicians need to be exposed to how the systems are being implemented. Otherwise, problems like this may go undetected.

References

1. FIPS PUB 186, May 19, 1994, page 7, Section 6.

2. Responses to NIST DSS Proposal, Ron Rivest, Communication of the ACM, July 1992, Page 43.

3. A Course in Number Theory and Cryptography, Neal Koblitz, Springer-Verlag, Second Edition.

4. Recommendation X.509 and ISO 9594-8, Information Processing System - Open Systems Interconnection - The Directory - Authentication Framework, 1988.

5. Final Text of Draft Amendment DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions, April 1996.

Appendix - DSS Analysis

In this appendix, we offer some observations on the properties of the DSS in light of the X.509 flaw. A comprehensive mathematical analysis of the DSS cryptosystem is beyond the scope of this paper.

Some of the security aspects of p, q, and g in DSS are:

1. p to be a prime of appropriate size (i.e., $2^{511+64j} < p < 2^{512+64j}$) where j = 0,1,2,..,8.
2. q to be a prime of appropriate size (i.e., $2^{159} < q < 2^{160}$)
3. q evenly divides in p-1
4. g to be a power of (p-1)/q

It is anticipated that the digital signature verification software will not check any of the parameter properties. The primality tests for p, q are definitely out of question due to the time it takes to perform these checks. The security properties will be tested, if at all, during the key generation process. Furthermore, review of the standard shows that in order to generate valid signatures (i.e., the ones that can be verified) one only needs to ensure that p is prime and the property 4 above holds. Property 4 is trivial to meet if q need not be prime. It can be achieved by setting q = p-1 and making all generator satisfying the property since (p-1)/q = 1 and every integer's power of 1 is the integer itself. The rest of the requirements are not critical to mathematics of DSS; they are critical to the security of DSS.

A Simple Attack

The following is a simple attack. An attacker takes a trusted public key y and computes a new large prime modulus p > y. This is easy to do. The attacker sets q = p-1, h = g = y, and x = 1. Now, the attacker can masquerade as the public key "y" holder. This simple attack will change the digital signature components r, s from 160 bits each to the size of q (which is p-1) each.

Other Considerations

While one could develop simple parameters and public key test to prevent the above attack, there are other values the attacker can choose to simplify the discrete logarithm problem.

The following factors help an attacker create a realistic parameters substitution attack:

- weak and trap door prime p [2]
- q not being prime
- p-1 having all small prime factors, simplifying the discrete logarithm problem
- reducing the size of p to that of y, thus reducing the discrete log problem for smaller p
- x need not be constrained since only the attacker keeps x (private key).

According to [2], the DSS crypto problem is a variation of the classic discrete logarithm problem. We lack operational experience with ease of defeating the security of DSS.

The odds of getting a generator by random guess depend heavily on the factorization of p-1 [see page 35 in 3]. The probability that a random number is a generator is $\prod$ (1-1/l) over all l, where l's are the prime factors of p-1. Computing discrete logs is easy if all the primes dividing p-1 are small [see page 103 in 3]. That is one of the reasons for q to be a prime in DSS, guaranteeing that at least one of the prime factors of p-1 is large (160 bits in case of DSS). Since an attacker is generating new p, he may be able to control the probability of guessing a generator and simplifying the discrete logarithm problem. But, these two requirement (namely the ability to find a generator and the ability to compute discrete logarithms) seem to work against each other since too many small primes will make probability product defined above (for a random number to be a generator) small.

Acknowledgments

We found this flaw while developing algorithms for parameter inheritance in a certificate chain for the National Security Agency under contract. We appreciate the review of the drafts of this material by the National Security Agency, and Miles Smid and Jim Nechvatal of the National Institute of Standards and Technology. Miles Smid provided several insights for the organization of the paper and for the presentation of the findings.