An Efficient Covert Channel

SATTAR J ABOUD and MOHAMMED AHMED AL-FAYOUMI
Department of Computer Science
The University for Graduate Studies, Faculty of IT
Amman - Jordan

Abstract: - The signature algorithm with a broadband covert channel that does not want the sender to compromise the security of the entity signing key is the Elgamal signature algorithm. But contrary to the common idea, the design of the digital signature scheme does not maximize the covert uses of its signatures, but minimizes them. The suggested scheme illustrates that several discrete logarithm schemes are vulnerable, since they are used in more than one group concurrently, and the key data may reveal by these groups which discrete logarithm are facile, but the digital signature scheme is more secure in this means.

Keywords: - covert channel, digital signature scheme, Elgamal signature scheme, broadband channel, narrowband channel, discrete logarithm problem.

1. Introduction

The specific security requirements of digital signatures are still considered as open research challenges [1,2,3,4,5,6] . However, various digital signature algorithms have the feature that the signer of a document can conceal certain data in the signature that can be detected by a trusted authority, and that the existence of this concealed data can not be recovered by any given example of the signature. This channel is invented by Simmons, who named it subliminal channel [7]. The difficulty initially began in the environment of nuclear weapons defects in international agreement verification. The United State of America and Russia have made a decision to place particular sensors in every other nuclear side in order to share specific agreed sensor data, and required integrity controls to stop data being processed and therefore to stop supply false information that an attempt does or does not succeed [8]. Also, both sides made sure certain that the integrity mechanisms can not be misused to transmit other forbidden data. This will concern with schemes employed to consider not only the occurrence of nuclear tests, but the numbers of fielded nuclear arms. If a Russian sensor designed to transmit just the absence or presence of an American rocket in storage can covertly communicate the storage site, then this data might be employed to ease a first attack. One of the first designs of tools to confirm international agreement compliance had just such a defect, the sensor site might be communicated employing a covert channel in an early authentication protocol relied on discrete logarithms problem [7].

To perceive the operation of these channels, consider the Elgamal signature algorithm [9,10] . Assume that p is a prime number where computing discrete logarithms in z_p^* is difficult. Suppose a is the generator of z_p^* , assume also that x is the entity private signing key less than p . Compute the public signature verification key $d = a^x \bmod p$ .Suppose an integer number less than p where $\gcd(r,\theta) = 1$, with $\theta = p-1$, and m is the message to be signed. So the Elgamal signature on m is (g,s) such that:

$$g = a^r \bmod p \quad (1)$$

$$s = (m - x * g)/r \bmod \theta \quad (2)$$

The two formerly given covert channels in this scheme are:

1. The broadband channel in which the signer shares the entity signing key with the message receiver, permitting r is inconsiderably detected

employing formula (2). We can therefore encrypt a secret message straight on from r.

2. The narrowband channel in which signer attempts various values of r until the signer can forces a number of bits of g to cipher a covert message c, so entity could be required to encrypt a ten bit message in the low order bits of g and tries consecutive values of r until the signer obtained the target. This will take roughly a thousand attempts on average, and typically the covert bandwidth in bits per signature is around the binary logarithm of the number of calculations that signer is eager to achieve.

The narrowband channel may be adequate for a sensor in missile storage to cipher little bits of data, and eventually this data might disclose its physical site. The narrowband covert channel might also be employed to reveal encryption key. Therefore, covert channel is significant in a number of uses. But neither of the mentioned channels is perfect. The signer should either adapt entity signing key or accept serious computational restrictions on the applicable covert bandwidth. This guided the authors to raise the question: is there any different algorithm with a broadband covert channel that does not want the sender to compromise the security of the entity signing key. However, the Elgamal signature scheme has such channel.

2. The Proposed Scheme

Suppose that the modulus $p = q * n + 1$ such that n is smooth and finding discrete logarithms is difficult in subgroup of z_p^* of order q that is calculated by $a^n \bmod p$. If the covert message we want to transmit is c, we can find:

$$r \equiv c \bmod n \tag{3}$$

However, we can compute $r = c + r^- * n$ for certain randomly selected r. Now, when the receiver obtains the signature (g, s) then generates $g^q \bmod p$ and computes i as follows:

$$(a^q)^i \equiv g^q \bmod p \tag{4}$$

This is feasible since the order of the subgroup of z_p^* generated by $a^q \bmod p$ is smooth. By the Pohlig-Hellman scheme [11] combining with Pollard rho algorithm [12], this will require a computation time of $O(\sqrt{B})$ where B is the smoothness bound i.e., the largest prime factor of n. We will then find:

$$c \equiv i \bmod n \tag{5}$$

The covert message can thus be detected. Given i, we can find the signing key by formula (2), thus more messages can be recovered. This channel is a broadcast one, in the sense that any person can find the discrete logarithm computation and detect $x \bmod n$. Though, we can also generate narrowcast channel, in which the covert message c is just available to participants who have certain shared secret. Especially, when $\theta = n * q_1 * q_2 + 1$, and the discrete logarithm problem is difficult in the groups of order q_1 and q_2, then the signer can keep entity signing key secret mod q_1 but disclose its value mod q_2 to the intended receiver of covert messages. Entity can now transmit the covert message c as $r \bmod q_2$.

The multiplicative ability used in this algorithm can also be employed to attack the signature in some situations [13,14,15]. For instance various tools are available to exclude these attacks, and they are also usable in this algorithm. The proposed scheme is designed to use a combination of an appropriate one way hash function $h(.)$ with which m shell is hashed before signing in order to bind the size of the key in verification. To avoid the potentiality of message collisions, it is preferable that the hash function employed must have a 160 bits product and secure hash algorithm [16,17] which seems to be an appropriate choice.

In summary, when we apply the Elgamal signature algorithm with a as a generator of z_p^*, we are signing at the same time in a number of different groups that correspond to the factors of θ. The proposed signing key can be secure in a few of these, shared with some participants, and will be available to each user mod the smooth part of θ. This smooth

part is at least 2, so that p is a random prime number; it will be around $\log_2 B$ [18].

3. Structure of the Channel

Obviously, the prime p is selected to supply any preferred combination of narrowcast and broadcast channels. The prime that is best for broadcast in Elgamal signature was given in the original design of the digital signature scheme, this have $(p-1)/q = 2^{70} * 3^{45} * 5^{30} * 7^{25} * 11^{20}$ [19], producing a broadcast channel of about 352 bits. The present digital signature scheme [10] proposes a special pair of primes, namely:

p = 11106950485250668473896599553110864943642757210461774008701010238258396788746424481120264311896935333601619506678772919359575477956779496046310058460953487 27 and
q = 1016505658889014629900729618210002584918553821669

The factors of $(p-1)/q$ were found by Paul Leyland and are 2.

q_1 = 4196363948260739557

q_2 = 420810174371644789390718 2873

q_3 = 309382440150971553074910129575307384019243127389783508284907

Employing the prime p for Elgamal signature could give a secure signature, in the groups of order q and q_3, might be weakened to supply a narrowcast covert channel. These will also be a transmit channel of fairly over 160 bits per signature, as the signing key could be obtained in the groups whose orders are 2, q_1 for roughly 2^{34} multiplications and q_2 for roughly 2^{47} multiplications.

It must be explicit from this example the way to choose p for any wished combination of broadcast and narrowcast covert channel size. In the example of an arbitrarily selected prime p, it may be exposed that the expected size in bits v of the result of all prime divisors $\le B$ is just about $\log_2 B$ [18]. So the covert channel needs a computation time of $O(2^{v/2})$ to convey v bits, whereas the formerly known narrowband channel required around 2^v. Furthermore, v has a large difference, for one in 100 1024-bit primes; one finds a result of v which is around four times bigger than the predictable result [18]. Anyhow, the values of p and q in the present digital signature scheme are not acutely out of the standard.

4. Discussion

The proposed channel occurs when a digital signature is carried out in a composite group with the feature that the key in one or more of its subgroups is shared with the receiver. This sharing could be explicit, in the case of the narrowband channel, or implied in the situation where trusted secret can easily calculate the key in the appropriate group or groups. It is obvious that the suggested channel could be avoided by working in a group of prime order. In the instance mentioned, we might substitute a by $a^{(p-1)/2}$ or $a^{(p-1)/q_3}$, and in fact this is the approach used by digital signature scheme [20]. After the digital signature scheme was suggested, it developed to have been designed to increase the secret channel size [21]. This statement was denied at the time by a person in charge in NSA [22], and we can at present notice that he was correct; the digital signature scheme does not increase the secret benefit of a signature, but reduces it by eradicating the suggested channel.

The proposed scheme has suggestions for security and secrecy; a person can find out the message key k as well as the signing key $x \bmod m$, actually in a standard discrete logarithm based cryptography, we can expect to detect the keys mod the smooth element of the order. It could be reckless of a developer to let such server key disclosure, as numerous random number generators illustrate regularities as a result of resonances, or implementation bugs. An Elgamal algorithm employing the p and q originally suggested by the digital signature scheme could be disclosing more than two thirds of every key. In lots of applications, and this would be adequate to raise the attack. However, for now we suggest that developers of Diffie-Hellman and Elgamal sort schemes must apply groups of prime order each time.

5. Conclusions

We have solved Simmons difficulty by proving that the Elgamal signature scheme has a broadband covert

channel; the proposed channel, which does not require the sender to compromise the security of the entity signing key. However, Simmons assumption that such mechanisms did not exits is not completely wrong, since the bandwidth of the suggested channel in bits for each signature is precisely equivalent to the number of bits that the signer is set to compromise of entity signing key. Thus, it may clearly be that Simmons assumption holds with a more exact formulation.

We have also perceived that the design of the DSS does not maximize the covert usefulness of its signatures, but minimizes them. The proposed scheme also demonstrates that numerous discrete logarithm based schemes are vulnerable, whilst the DSS is not susceptible in this means.

References

[1] Sattar J Aboud and Asim El Sheikh, "A New Method for Public Key Cryptosystem and Digital Signature Scheme Based on both Integer Factorizations and Discrete Logarithms", Asian Journal of Information Technology, Vol. 3, Number 4, 2004, pp. 284-289.

[2] Sattar J Aboud and Mohammed Ahmed Al-Fayoumi, "Two Efficient Digital and Multisignature Schemes", Proceeding of the IASTED International Conference on Computational Intelligence, Calgary, Canada, 2005, pp. 457-362

[3] M Musbah, Aqel and M. Ammar, "Function Structure and Operation of a Modern System for Authentication of Signatures of Bank Checks", Pak. Information Technology Journal 4(1), 2005, pp. 96-105.

[4] M Ammar, and M. Musbah, "Verification of Signatures of Bank Checks at very Low Resolutions and Noisy Images", Applied Science University Journal, Jordan, 2003.

[5] M Ammar, and M. Mousbah, "A High Efficiency Method for Automatic Signature Verification", Patent No. 09/453730, 2/12/1999, USA, 2002.

[6] Douglas R Stinson, "*Cryptography Theory and Practice*," CRC 3rd 2006, pp. 281-317.

[7] G Simmons, "*Subliminal Channels Past and Present"*, European Transactions on Tele-communications v 5 no 4 1994, pp. 459-473.

[8] G Simmons, "*How to Insure That Data Acquired to Verify Treaty Compliance are Trustworthy*", Contemporary Cryptology, IEEE 1992, pp. 617-630

[9] T. Elgamal, "*A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*", IEEE Transactions on Information Theory, v 31, no 4, pp. 469-472, 1985.

[10]Federal Information Processing Standards, "*Digital Signature Standard*", National Institute of Standards and Technology, US Department of Commerce, (FIPS) Publication 186, Washington D.C., May 1994.

[11]S Pohlig, and M Hellman, "*An Improved Algorithm for Computing Logarithms over GF(p) and its Cryptographic Signature*", IEEE Transactions on Information Theory, v 24, no 1 1978, pp. 106-110.

[12]J Pollard, "*Monte Carlo Methods for Index Computation mod p*", Mathematics of Computation, v 32 no 149 July 1978, pp. 918-924

[13]Sattar J Aboud and Evon M Abu-Taieh, "*A New Deterministic RSA-Factoring Algorithm*", Jordan Journal of Applied Science, Volume 8, No. 1, pp. 54-66, Amman-Jordan, 2006.

[14]Sattar Aboud, "*Baghdad Method for Calculating Multiplicative Inverse*" international Conference on Information Technology, Las Vegas, Nevada, USA, 2004, pp. 816-819.

[15]Sattar Aboud "*Fraction – Integer Method (FIM) for Calculating Multiplicative Inverse*", Journal of Systemics, Cybernetics and Informatics, Volume 2, Number 5, 2005, USA

[16]FIPA 180-1, "*Secure Hash Standard*", US Department of Commerce/NIST, 1995

[17]FIPA 180-1, "*Secure Hash Standard*", US Department of Commerce/NIST, 1994

[18]P van Oorschot and M Wiener, "*On Diffie-Hellman Key Agreement with Short Exponents*", Advances in Cryptology, EUROCRYPT 96, Springer LNCS, v1070 pp, 332-343

[19] R Anderson, "*A Practical RSA Trapdoor*", Electronics Letters v 29 no 11 pp. 993-995

[20] B Schneier, "*Applied Cryptography*", 2nd edition, Wiley 1995.

[21]G Simmons, "*Subliminal Communication is easy using the DSS*", Advances in Cryptology, EUROCRYPT 93, Springer LNCS, v 765, pp. 218-232.

[22]B Snow, Comment made from the floor at Eurocrypt, 1993.