TELKOMNIKA Indonesian Journal of Electrical Engineering
Vol.12, No.4, April 2014, pp. 3200 ~ 3207
DOI: http://dx.doi.org/10.11591/telkomnika.v12i4.4931

Attack the Anycast Signature Scheme

Jinbin Zheng
School of Mathematics and Computer Science, Longyan University
No. 1, Dong Xiao North Road, Longyan 364012, China. +86-0597-2793778
email: jbzheng518@163.com

Abstract

Today, the internet is increasingly being considered to provide services, and not just in order to connect. As this view became more universal, the important factors of providing such services are reliability and availability of the services to meet the needs of a large number of users. Anycast is a communication mode in which the same address is assigned to a group of servers and the router will send the request to the "best" server. Al-Ibrahim and Cerny proposed an authentication scheme of anycast communication. Their scheme is based on El-Gamal type signature scheme. We prove that their preferred scheme, which does not require interaction among the various signers, is insecure.

Keywords: *digital signature, anycast communication, denial attack, forgery attack*

1. Introduction

Al-Ibrahim and Cerny describe an authentication scheme for anycast communication based on El-Gamal type digital signature [1-[2], [11]. They proposed an authentication solution were similarly related to the concept of proxy signatures. The method applied a strong scheme from [3, 4] and obtained by improving the scheme from [5, 15]. There are many approaches for improving the scalability of a service, but the common one is to replicate the servers. Server replication is the key approach for maintaining user-perceived quality of service within a geographically wide-spread network. This is empowered by the underlining network infrastructure known as anycast communication. Each user owns a private key and a public key, and all arithmetic is done in a common group in which the discrete logarithm problem is intractable. In this scheme, the author presents varieties denial attacks. Thus, for this scheme is insecure.

2. Review of Anycast Signature Scheme

In anycast communication, a common IP address(anycast address) is used to define a group of servers that provide the same service. A client sender desiring to communicate with only one of the servers sends datagrams with the IP anycast address [1]. Al-Ibrahim et al. firstly proposed a concast signature in 2002 [11], Stinson pointed out an attack for the concast scheme [12]; later, Liu gave an improvement [13] upoun the concast scheme. On the other hand, Al-Ibrahim and Carny also presented the anycast authentication signature in 2003. The operation conception be described as follow:

a. Initialization. The communication of each server with the group coordinator. A signature delegation algorithm is used in this communication. Each server starts playing the role of the coordinator's proxy.

b. The actual serving. The anycast server uses the delegated signature, together with the proof of his delegation. The concept is described as follow [1].

Notation:

1) p, q : two large primes such that $q \mid (p-1)$.

2) g : a generator with order $q \in Z_p^*$.

3) U_i and V : are denote User's ID.

4) $H(.)$: denote a one way hash function.

Received September 21, 2013; Revised November 19, 2013; Accepted December 10, 2013

2.1. The Scheme of Concept

Definition 1. Discrete logarithm problem is $DLP(p,g,y)$ a problem that on input a prime p and integers g , $y \in Z_p^*$, outputs $y \in Z_{p-1}$ satisfying $g^x \equiv y \pmod q$ if such an x exists. Otherwise, it outputs $\perp$.

The above function, which outputs $\perp$ if there is no solution to the query, should be expressed as DLP [16] and the notation DLP should be used only for a weaker function such that nothing is specified for the behavior of the function in the case when there is no solution to the query [6].

Genaral Work:

The Al-Ibrahim et al.'s scheme consists of two phases: Initialization phase and Verification phase.

Initialization Phase:

User U_i signs a message M in the following way.

Step 1. U_i Computes

$$m_i \equiv H(M_i). \tag{1}$$

Step 2. U_i Selects a random integer k_i, and computes

$$r_i \equiv m_i \cdot g^{-k_i} \pmod p. \tag{2}$$

Step 3. U_i Computes

$$s_i \equiv k_i - r_i \cdot x \pmod q. \tag{3}$$

Step 4. U_i Sends the (M_i, s_i, r_i) with messages to the verifier.

Verification Phase:

After receiving (M_i, s_i, r_i) the signature, Verifier V can verifies the following:

Step 1. V Computes

$$m_i \equiv H(M_i). \tag{4}$$

Step 2. V Computes

$$l_i \equiv g^{s_i} \cdot y_i^{r_i} \cdot r_i \pmod p. \tag{5}$$

Step 3. If it holds, V can be certain that (M_i, s_i, r_i) is indeed the signature generated by U_i when:

$$m_i \equiv l_i. \tag{5}$$

2.2. The Anycast Scheme

The anycast operation will play the role of the signer by group coordinator G, which delegates his signature rights to all the member of the anycast group.

2.2.1. Initialization Ready Stage

User U_i signs a message M in the following way.

Step 1. Coordinator chooses the secret key $x \in Z_p$ and computes the public key

$$y \equiv g^x \pmod p). \tag{7}$$

The key y is the identifier of the group.

Step 2. Coordinator randomly chooses a value $z_i \in Z_p$ and computes

$$U_i \equiv g^{z_i} \pmod p). \tag{8}$$

Where $1 \le i \le n$, then it sends t_i to i th server.

Step 3. Server A_i selects a randomly value $\alpha_i \in Z_p$ and computes

$$t_i \equiv g^{\alpha_i} \cdot u_i \pmod p). \tag{9}$$

belong to Z_p^*, then it sends t_i to the coordinator.

Step 4. Coordinator computes

$$v_i \equiv t_i \cdot x + z_i \pmod p). \tag{10}$$

Step 5. Server A_i received v_i from Coordinator and computes

$$x_i \equiv v_i + \alpha_i \pmod p). \tag{11}$$

Then checks:

$$g^{x_i} \equiv y^{t_i} \cdot t_i \pmod p). \tag{12}$$

if it is equality. If it is correct, then accepts x_i as secret key legal.

2.2.2. Actual Serving Stage

Sever A_i node:

Step 1. Computes

$$m_i \equiv H(M_i). \tag{13}$$

Step 2. Chooses a random number k_i and computes

$$r_i \equiv m_i \cdot g^{-k_i} \pmod p). \tag{14}$$

Step 3. Computes

$$s_i \equiv k_i - r_i \cdot x_i \pmod q). \tag{15}$$

Step 4. Sends (M_i, s_i, r_i, t_i) to the client.

2.2.3. Client node:

Step 1. Fetches the key y_i from the registry.

Step 2. Computes

$$h \equiv H(M_i). \tag{16}$$

Step 3. Computes

$$l_i \equiv g^{s_i} \cdot (y_i^{t_i} \cdot t_i)^{r_i} \cdot r_i \pmod p. \tag{17}$$

Step 4. Accepts the signature if:

$$h \equiv l. \tag{18}$$

With the recent interest in securing group and broadcast communication and multicast communication, there has been a great demand for designing a new class of fast signature schemes that can handle a vast number of signature from broadcast communication and multicast communication or group-based application efficiently, rather than using typical signature schemes. Based on the threshold proxy one-time signature scheme, a specific case is when $t = 1$, which depicts the anycast model. The anycast authentication problem was discussed in [1] and a solution was proposed based on a conventional digital signature. Briefly, the anycast model represents the situation where any of a group of n servers (signers) may provide the same (equivalent) service to a client (verifier) [14].

3. Weaknesses of Anycast Scheme

Anycast is a network addressing and routing scheme whereby data is routed to the 'nearest' or 'best' destination as viewed by the routing topology [10]. For anycast scheme, the group coordinator will play the role of the signer, which delegates his signature rights to all the members of the anycast group. The term is intended to echo the terms unicast, broadcast and multicast.

a) In unicast, there is a one-to-one association between network address and network endpoint: each destination address uniquely identifies a single receiver endpoint Figure 1. In computer networking, unicast transmission is the sending of messages to a single network destination identified by a unique address [7].

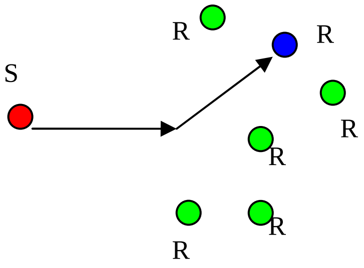


Figure 1. Unicast Services [7].

b) In broadcast, there is a one-to-many association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, to which all information is replicated Figure 2. Broadcasting can be performed as a high level operation in a program, for example broadcasting Message Passing Interface, or it may be a low level networking operation, for example broadcasting on Ethernet [8].

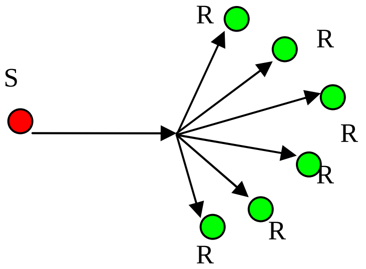
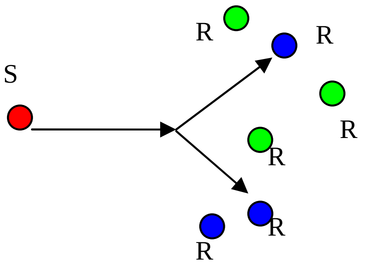


Figure 2. Broadcast Services [8].

c) In multicast, there is also a one-to-many association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, to which all information is replicated Figure 3. Multicast is most commonly implemented in IP multicast, which is often employed in Internet Protocol (IP) applications of streaming media and Internet television [9].

d) In anycast, there is also a one-to-many association between network addresses and network endpoints: each destination address identifies a set of receiver endpoints, but only one of them is chosen at any given time to receive information from any given sender Figure 4. On the Internet, anycast is usually implemented by using Border Gateway Protocol to simultaneously announce the same destination IP address range from many different places on the Internet [10].



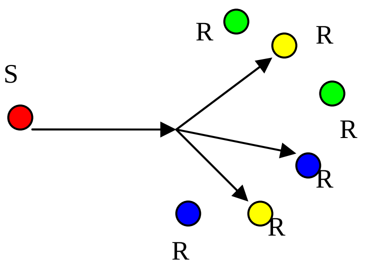


Figure 3. Multicast Services [9] Figure 4. Anycast Services [10]

As known for a forgery attack in following [6].

Step 1. Eve randomly chooses a number s_i'.

Step 2. Eve calculates:

$$r_i' \equiv H(M_i') \cdot g^{-s_i'} \cdot (p-1)^2 \pmod{q}. \tag{19}$$

Step 3. Eve forged signature on the message M_i when she use (M_i', s_i', r_i').

A signature forged using upon-described method is valid, because the following equations hold:

Proof.

$$\begin{aligned} g^{s_i'} \cdot y^{r_i'} \cdot r_i' &\equiv y^{H(M_i') \cdot g^{-s_i'} \cdot (p-1)^2} \cdot H(M_i') \pmod{p} \\ &\equiv H(M_i') \pmod{p}. \end{aligned} \tag{20}$$

To actual serving of their scheme, even for:

$$l_i \equiv g^{s_i} \cdot (y^{t_i} \cdot t_i)^{r_i} \cdot r_i \pmod{p}. \tag{21}$$

Eve compute:

$$\begin{aligned} l_i &\equiv g^{s_i''} \cdot (y_i^{t_i} \cdot t_i)^{r_i''} \cdot r_i'' \pmod{p} \\ &\equiv (y_i^{t_i} \cdot t_i)^{H(M_i'')\cdot g^{-s_i''}\cdot (p-1)^2} \cdot H(M_i'') \pmod{p} \\ &\equiv H(M_i'') \pmod{p}. \end{aligned} \tag{22}$$

3.1. Denial Attack I

Eve lets secret key $x = 0$ and $k_i = 1$ in first.

Step 1. Eve computes:

$$y_i \equiv g^x \equiv g^0 \equiv 1 \pmod{p}. \tag{23}$$

Step 2. Eve computes:

$$m_i' \equiv H(M_i'). \tag{24}$$

Step 3. Eve computes:

$$\begin{aligned} r_i' &\equiv m_i' \cdot g^{-k_i} \pmod{p} \\ &\equiv m_i' \cdot g^{-1} \pmod{p}. \end{aligned} \tag{25}$$

Step 4. Eve computes:

$$\begin{aligned} s_i' &\equiv k_i - r_i' \cdot x \pmod{q} \\ &\equiv 1 - 0 \pmod{q} \\ &\equiv 1 \pmod{q}. \end{aligned} \tag{26}$$

After Eve finished the four steps, she had denied the valid signature (M_i', s_i', r_i') of user U_i. Eve computes:

$$\begin{aligned} m_i' &\equiv g^{s_i'} \cdot y_i^{r_i'} \cdot r_i' \pmod{p} \\ &\equiv g^1 \cdot 1^{m_i' \cdot g^{-1}} \cdot m_i' \cdot g^{-1} \pmod{p} \\ &\equiv m_i' \pmod{p}. \end{aligned} \tag{27}$$

3.2. Denial Attack II

Eve sets secret key $x = p - 1$ and $k_i = -p + 2$.

Step 1. Eve computes:

$$\begin{aligned} y_i &\equiv g^x \pmod{p} \\ &\equiv g^{p-1} \pmod{p} \\ &\equiv 1 \pmod{p}. \end{aligned} \tag{28}$$

Step 2. Eve computes:

$$m_i' \equiv H(M_i'). \tag{29}$$

Step 3. Eve computes:

$$\begin{aligned} r_i' &\equiv m_i' \cdot g^{-k_i} \pmod{p} \\ &\equiv m_i' \cdot g^{-(-p+2)} \pmod{p} \\ &\equiv m_i' \cdot g^{p-1} \cdot g^{-1} \pmod{p} \\ &\equiv m_i' \cdot g^{-1} \pmod{p}. \end{aligned} \tag{30}$$

Step 4. Eve computes:

$$\begin{aligned} s_i' &\equiv k_i - r_i' \cdot x \pmod{q} \\ &\equiv 1 - 0 \pmod{q} \\ &\equiv 1 \pmod{q}. \end{aligned} \tag{31}$$

After Eve finished the four steps, she had denied the valid signature (M_i', s_i', r_i') of user U_i. Eve computes:

$$\begin{aligned} m_i' &\equiv g^{s_i'} \cdot y_i^{r_i'} \cdot r_i' \pmod{p} \\ &\equiv g^1 \cdot 1^{m_i' \cdot g^{-(-p+2)}} \cdot m_i' \cdot g^{-1} \pmod{p} \\ &\equiv m_i' \pmod{p}. \end{aligned} \tag{32}$$

4. Conclusion

In the past, Al-Ibrahim et al. decribed an authentication scheme for concast and anycast communication based on El-Gamal type digital signature. They proposed an authentication solution were similarly related to the concept of proxy signature. For anycast scheme, the group coordinator will play the role of the signer, which delegates his signature rights to all the members of the anycast group.We already know how to deny and forge signature so that anycast is effected. For forged attack, we can make a set of forgery signature which succeed the anycast communication of authentication. Thus, for this scheme is insecure.

Acknowledgements

The authorswould like to thank Chenglian Liu for his comments that help to improve themanuscript. This paper partially supported from college funding under the information security research team project.

References

[1] M Al-Ibrahim, A Cerny. Authentication of anycast communication. *MMM-ACNS*. 2003; LNCS 2776: 419-423.

[2] CP Schnorr. Efficient signature generation by smart cards. *Journal of Cryptology*. 1991; 4(3): 161-174.

[3] K Zhang. Threshold proxy signature schemes. *Information security, Lecture Notes in Computer Science*. 1998; 1396: 282-290.

[4] H Ghodosi, J Pieprzyk. Repudiation of cheating and non-repudiation of zhang proxy signature schemes. *Information Security and Privacy, Lecture Notes in Computer Science*. 1999; 1587: 129-134.

[5] M Mambo, K Usuda, E Okamoto. Proxy signature: delegation of the power to sign message. *IEICE Transaction on Fundamentals.* 1996; E79-A: 1338-1354.

[6] Chenglian Liu, Yongning Gou. Security analysis of concast and anycast digital signature. *Applied Mechanics and Materials.* 2012; 121(126): 1177-1182.

[7] Wikipedia. Unicast scheme. *Wikipedia website, http://en.wikipedia.org/wiki/Unicast.* 2012.

[8] Wikipedia. Broadcast scheme. *Wikipedia website, http://en.wikipedia.org/wiki/Broadcasting.* 2012.

[9] Wikipedia. Multicast scheme. *Wikipedia website, http://en.wikipedia.org/wiki/Multicast.* 2012.

[10] Wikipedia. Anycast scheme. *Wikipedia website, http://en.wikipedia.org/wiki/Anycas.* 2012.

[11] M Al-Ibrahim, H Ghodosi, J Pieprzyk. Authentication of concast communication. *Progress in Cryptology INDOCRYPT. Lecture Notes in Computer Science.* 2002; 2551: 185-198.

[12] DR Stinson. Attack on a concast signature scheme. *Information Processing Letters.* 2004; 91(1): 39-41.
[13] C Liu. Improvement of authentication of anycast communication. *International Conference for Internet Technology and Secured Transactions (ICITST'09).* 2009; 1-3.
[14] Mohamed Al-Brahim, Anton Cerny. *Proxy and threshold one-time signature.* First International Conference on Applied Cryptography and Network Security, Lecture Notes in Computer Science*.* 2003; 2846: 123-136.
[15] Z Yan, F Zhang. Cryptanalysis to a Certificateless Threshold Signature Scheme. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1496-1502.
[16] L Ma. More Efficient VLR Group Signature Based on DTDH Assumption. *TELKOMNIKA Indonesian Journal of Electrical Engineering*. 2012; 10(6): 1470-1476.