2010 2nd International Conference on Industrial and Information Systems

Research on the Improved Security Mechanism of BGP

Junchun Ma[1,2], Yongjun Wang[1]
[1]School of Computer Science, NUDT
Changsha 410073, China

Jiyin Sun[2]
[2]Research Inst. of High-tech Hongqing Town
Xi'an 710025, China

***Abstract*—This paper has a thorough study and improvement to the SE-BGP security mechanism based on analyzing the merit and shortcoming of many kinds of BGP security mechanism proposed in recent years. The improvement project makes up the insufficiency of original project, has a good extendibility and easy deploying, enabling the SE-BGP security mechanism to have a better guarding ability.**

***Keywords*—inter-domain routing, security, SE-BGP, TTM trust model**

I. INTRODUCTION

BGP is the key constituent of the Internet routing foundation structure, the main function of which is presiding over the inter-domain routing selection with non-ring circuit among the autonomous system. Because the initial design of BGP didn't consider the security content and it lacks the authorization and authentication mechanism with basic elements, BGP is facing many latent security threats with the expansion of network. Moreover recently none of BGP security mechanisms is effectively applied also there are many kinds of BGP security mechanisms.

S-BGP is proposed by Kent of BBN Corporation in 2000[1], which is the most complete and representative solution in the current research. It can solve most security problem by combining with PKI, the confirmation route attribute and IPSec security mechanism. But during concrete realizing, S-BGP must use two patulous PKIs based on X.509 (v3), and each PKI must comply with the real world AS number, address allocation level, etc., so S-BGP has great barrier in the aspect of deployment.

SoBGP is proposed by White of Cisco Corporation in 2003[2], which adopts source address certificate to attest. But it doesn't protect the BGP connection relation between ASs, and doesn't attest the BGP attribute, so it can't guarantee the AS-PATH isn't tampered during route transmitting.

In view of the insufficiency of these two kinds of security mechanism, many scholars propose improvement security mechanism, such as OA (origin authentication) service proposed by Aiello in 2003[3], SPV (security path vector) proposed by Hu in 2004[4], psBGP (pretty security BGP) proposed by Wan in 2005[5], ect..

However, these security mechanisms may introduce new problem with obtaining some improvement. Especially all of them don't solve the key problem – certificate management. In view of this problem, HU Xiangjiang et al. proposed a kind of SE-BGP security mechanism in 2008[6], which greatly simplified the certificate management and had good scale extendibility.

This paper proposes an improved BGP security mechanism based on the thorough analysis to the SE-BGP security mechanism.

II. SE-BGP SECURITY MECHANISM

SE-BGP is proposed based on analysis to the Internet topology characteristic, which establishes the PKI authentication center with AS alliance as the unit. It uses a new trust model – TTM, which guarantees the conversation security between Ass by IPSec. Like S-BGP, SE-BGP also needs PKI's support.

PKI AS alliance is called 'security AS alliance', marked as *SA*, and mark the key node as *T*. In the local area of security AS alliance, the manner of source authentication and address authentication is like S-BGP. An example in Fig.1 shows a possibility AS alliance connection chart, in which there are 4 security AS alliance.

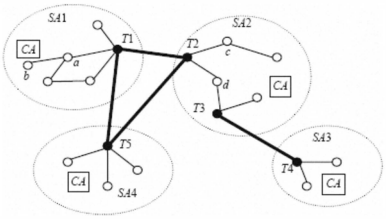

Figure 1. A chart of AS alliance connection

A. Certificate authority of alliance

The certificate authority of AS alliance can be organized and managed by 'authority' department (e.g. government, large-scale ISP, etc.). Each node in security AS alliance needs to propose certificate application to certificate authority, the content of which includes address allocation unit and AS number. After checking the application, certificate authority releases certificate to AS nodes, the content of which includes ASN, address allocation unit and corresponding public key.

A special point of SE-BGP is that the key nodes in other security AS alliance connected with the key nodes in the security AS alliance also need to be authenticated in the security AS alliance. As shown in Fig.1, SA1 is connected with SA2, the key node T1 in SA1 wants to apply for certificate in SA2, and similarly, T2 in SA2 also wants to apply for certificate in SA1.

CA needs to release a 'key nodes connection table', in which there records the key nodes in security area and the key nodes in other security area connecting with the key

978-1-4244-8217-7/10/$26.00 ©2010 IEEE

node. Any node in security alliance needs to gain this table.

B. TTM model

TTM is a distributional PKI structure, which is shown as Fig.1. Key nodes *T1* and *T2* simultaneously have two set of public key certificates, namely *T1* and *T2* both have the public key certificate of *SA1* and *SA2*. Firstly, two function is defined: $S_k(m)$ stands for the signature of node k to its releasing message m, $V_k(s)$ stands for the validation of node k's public key to signature S. To node k, the condition that accepting release message m is $V_k(S_k(m)) = m$.

As shown in Fig.1, suppose node c in *SA2* need to release message m to node b in *SA1*. When *T2* receives the message of c and passes authentication, it signs signature to m with the key in CA of *SA1* with the content m_{c-T2}. When *T1* receives the message from *T2*, it validates m with public key in CA of *SA2* and validate $m = m_{c-T2}$ with private key in *T1*. If pass the validation, it signs signature m_{c-T1} to m with private key of *SA1*. Therefore, the message node b receives is m' and two signature -- $ST1(m_{c-T1})$ and $ST2(m_{c-T2})$. The condition Node b accepts the message m is as follows.

$$m' = V_{T1}(ST1(m_{c-T1})) = V_{T2}(ST2(m_{c-T2}))$$

Suppose 1. There is no 'unite' between two key nodes, namely there doesn't exist the signature and transmission to the same false message between two key nodes. Because node b has public key of *T1* and *T2*, b can validate $m' = V_{T1}(ST1(m_{c-T1})) = V_{T2}(ST2(m_{c-T2}))$, namely $m' = m_{c-T1} = m_{c-T2}$. Because *T1* already validate $V_{T2}(ST2(m_{c-T2})) = m$, namely $m_{c-T2} = m$, it can be seen from suppose 1 that there doesn't exist $m_{c-T1} = m_{c-T2} \neq m$.

In synthesis above, if b pass the validation $m' = m_{c-T1} = m_{c-T2}$, then there has $m' = m$.

By analyzing the work principle of TTM, it is easy to gain the theorem as follows.

Theorem 1. When two security AS alliance directly connect, if there is no unite between the key nodes, then the message from the node of one security AS alliance to the other is able to validating, and the validation method is just validating the partial certificate of security AS alliance.

Theorem 2. When two security AS alliance connect by another security AS alliance, if there is no unite between any two connection key node, then the message from the node of one security AS alliance to the other is able to validating, and the validation method is just validating the partial certificate of security AS alliance.

In one word, TTM trust model make the most of AS topology characteristic and trust relationship characteristic, which simplifies the management of certificate by the key nodes signature transformation. In other words, this authentication way is similar to the queue. When people stand in the queue, they judge the straight line by the two people in front of them instead of from the beginning of line. If every person in the queue can do this well, the queue do be a straight line finally. TTM uses this 'linear superimposition' characteristic to validate overall message by validating partial message.

III. IMPROVED SE-BGP SECURITY MECHANISM

Although BGP security mechanism can't keep away the unite attack between nodes, it limits the scope of nodes between the key nodes or nodes in the same AS alliance. This paper improves TTM model by analyzing SE-BGP security mechanism and digital signature project, enabling to resisting the unite attack between nodes.

Still take that above as an example, in which node c in *SA2* needs release message m to node b in *SA1*. The particular realization steps are as follows.

(1) node c firstly passes the message m to *T2* with private key encryption;

(2) *T2* deciphers the message when receiving from c with c's public key. After authentication, it signs a signature to m with *CA1* public key, whose content is m_{c-T2}, then passes the signing message to *CA1*;

(3) When *CA1* receives the message from *T2*, it deciphers with *CA1* private key and confirms whether $m = m_{c-T2}$. If through the confirmation, it signs a signature to m with *T1* public key with the content m_{c-CA1}, and passes the signing message to *T1*;

(4) When *T1* receives the message from *CA1*, it deciphers with *T1* private key and confirms weather $m_{c-T2} = m_{c-CA1}$. If through the confirmation, it signs a signature to m with *T1* private key with the content m_{c-T1}.

Therefore, the message received by node b is three signatures, $ST1(m_{c-T1})$、$ST2(m_{c-T2})$ and $S_{CA1}(m_{c-CA1})$. The condition node b accepts releasing message m is as follows.

$$V_{T1}(ST1(m_{c-T1})) = V_{T2}(ST2(m_{c-T2})) = V_{CA1}(S_{CA1}(m_{c-CA1}))$$

Because in the SE-BGP security mechanism, the authentication center CA in AS alliance is the government, large-scale ISP, etc., which is has more 'authority', therefore based on original plan, the message transmission between nodes is supervised by CA. For example, node a needs release message m to node b, it firstly releases the message with signature to the authoritative organization CA of SA in which node b is, after passing CA's confirmation, it is passed to node b with signature. This method can prevent effectively the unite deceit with node a and node b for CA can validate a's signature information, which can improve the guard ability of security mechanism and has higher security.

IV. CONCLUSION

Because the SE-BGP safety mechanism uses Internet's analysis topology connection rule, uses partial PKI the authentication mechanism, has avoided the certificate overall situation dissemination, thus may achieve "the local control, the overall situation is most superior", and in the scale, the performance and the management aspect has the good extendibility, this article has made the improvement to this plan's TTM trust model, causes the improvement program not only to have the original plan above merit, simultaneously enabled the original plan to have the better guard ability.

ACKNOWLEDGMENT

This research is supported by the National 863Plan Project of China, under Grant No.2009AA01Z432

REFERENCES

[1] Kent S, Lynn C, Seo K. *Secure border gateway protocol (S-BGP)*. IEEE Journal on Selected Areas in Communications, 2000,18(4):582−592.

[2] White R. *Architecture and deployment considerations for secure origin bgp (soBGP)*. IETF Internet draft: draft-whitesobgp-architecture-01, 2006.

[3] Aiello W, Ioannidis J, McDaniel P. *Origin authentication in Interdomain routing*. In: Proc. of the 10th ACM Conf. on Computer and Communications Security. Washington: ACM, 2003. 165−178.

[4] Hu YC, Perrig A, Sirbu M. *SPV: Secure path vector routing for securing BGP*. ACM SIGCOMM Computer CommunicationReview, 2004,34(4):179−192.

[5] Wan T, Kranakis E, van Oorschot PC. *Pretty secure BGP (psBGP)*. Technical Report, TR-04-07, SCS, 2004..

[6] Hu XJ, Zhu PD, Gong ZH. *SE-BGP:An Approach for BGP Security*. Journal of Software, 2008,19(1),167-176