International Journal on Applications in Engineering and Technology
Volume 2: Issue 2: February 2016, pp 1-4 www.aetsjournal.com ISSN (Online) : 2455-0523

BORDER GATEWAY PROTOCOL TO PREVENT ROUTING ATTACKS FOR IMPROVED SECURITY MEASURES

Bala vignesh.P, Harish.AG, Suresh.S
Guided byK.Arun patrick
(NehruInstitute ofTechnology,Coimbatore,India)

Keywords—*RC4 Algorithm – Anti Tiger Algorithm – Shortest Path calculation for data transmission- Attainment of data privacy through Enhanced technique – Encryption using RC4 algorithm – Key Generator for specific node- Prevention of Routing Attacks*

***Abstract*—Border Gateway Protocol (BGP) is vulnerable to routing attacks because of the lack of inherent verification mechanism. Several secure BGP schemes have been proposed to prevent routing attacks by leveraging cryptographic verification of BGP routing updates.TIGER, which aims to invalidate the "proven" security of these secure BGP schemes and allow ASes to announce forged routes even under full deployment of any existing secure BGP proposal.By launching TIGER attacks, malicious ASes can easily generate and announce forged routes which can be successfully verified by the existing secure BGP schemes. TIGER attacks can evade existing routing anomaly detection schemes by guaranteeing routing data-plane availability and consistency of control- and data-plane. Toward a new securing BGP scheme, we propose Anti-TIGER to detect and defend against TIGER attacks.Anti-TIGER enables robust TIGER detection by collaborations between ASes.Spread Spectrum Communication technique to watermark certain special probing packets, which manifest the existence of TIGER attacks. Anti-TIGER does not require any modifications in routing data-plane, therefore it is easy to deploy and incrementally deployable.**

1.INTRODUCTION

BORDER Gateway Protocol (BGP) is the de-facto protocol to ensure the inter-AS connectivity of the Internet. However, since BGP does not have built-in mechanisms to verify if a route is genuine, it suffers severe security plagues. Any AS (or BGP router) can announce a fake route, and its neighbors cannot verify if the route is valid. For example, on Feb. 24th, 2008, Pakistan Telecom (AS17557) started an unauthorized announcement of the prefix 208.65.153.0/24. One of Pakistan Telecom's upstream providers, PCCW Global (AS3491), forwarded this announcement to the rest of the Internet, resulting in the hijacking of YouTube traffic on a global scale for more than two hours. Many similar traffic back holes and interceptions with active routing attacks and mis-configurations have been reported.

In order to effectively eliminate false routing updates, a wide array of secure BGP schemes have been proposed. For example, Secure BGP (S-BGP) provides route attestation by leveraging heavy cryptographic operations. Researchers recently have theoretically "proven" the security of S-BGP. To reduce the complexity of route attestations, many variants have been proposed. Among these, BGPsec is recently proposed by IETF, where route attestation overhead is reduced while retaining the same security of S-BGP.

In this paper we propose TIGER attacks, which aims to launch routing attacks even with fully deployment of these "proven secure" BGP proposals. In TIGER, two Ases equipped with the existing BGP security mechanisms collude to generate forged routing paths, whose signatures can be successfully verified by other ASes. That is, with TIGER, any pair of colluding ASes can invalidate the existing idealized BGP security proposals and launch routing attacks at will, e.g., generating routing blackholes or attracting traffic.

TIGER can be easily launched by ISPs or ASes because it does not require modification to BGP protocol. Instead, TIGER can be launched by configuring commercial offthe-shelf (COTS) routers deployed with or without BGP security mechanisms. Specifically, two COTS BGP routers in two different ASes build BGP sessions by tunneling, such that these two ASes can collude to generate forged routing paths without being detected by other ASes. We call these two routers TIGER routers. With TIGER routers, network operators can configure BGP filtering to launch attacks for specific destinations, while not impacting traffic to other destinations. For example, in Fig. 1, TIGER routers in AS3 and AS6 collude to build a tunnel session between them and generate a fake BGP link AS3-AS6 over the tunnel. In the meanwhile, they encapsulate the traffic from AS1 to AS7. Thus, AS1 cannot perceive the existence of the tunneled ASes, i.e., AS4, AS8, and AS7, in the traffic forwarding path to AS7. Through the tunnel session, AS3 and AS6 also can obtain the signatures of the routing updates from each other, which allow them to re-announce the routing updates with the "correct" signatures generated by S-BGP or BGPsec. In this

way, colluding TIGER Ases can generate fake and shorter routes to hijack traffic even under the full deployment of S-BGP or BGPsec.

Our contributions are summarized as follows:

_ We present TIGER attacks where colluding Ases generate fake routing paths even under full deployment of secure BGP proposals, e.g., S-BGP and BGPsec, and therefore invalidate the "proven" security of these mechanisms.

_ We propose Anti-TIGER that accurately and robustly detects TIGER attacks through AS collaborations, by designing mechanisms of identifying possible victim ASes with neighbor AS graphs. In particular, Anti- TIGER builds covert channels between intermediate ASes and victim ASes with Spread Spectrum Technique to effectively evade interference in attack detection.

_ We evaluate the capability of TIGER and Anti-TIGER by simulations with real AS topologies of the Internet. We confirm that TIGER attacks can hijack a considerable number of prefixes. We further demonstrate that these attacks can be successfully detected by Anti-TIGER even in the presence of sophisticated attacks to interfere in TIGER detection .

2.RC4 - ALGORITHM

Encryption is the process of transforming plaintext data into ciphertext in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data. Hence, encryption is mainly used to ensure secrecy. Companies usually encrypt their data before transmission to ensure that the data is secure during transit. The encrypted data is sent over the public network and is decrypted by the intended recipient. Encryption works by running the data (represented as numbers) through a special encryption formula (called a key). Both the sender and the receiver know this key which may be used to encrypt and decrypt the data classification) or the object property value (for k-NN regression) is known. This can be thought of as the training set for the algorithm, though no explicit training step is required.

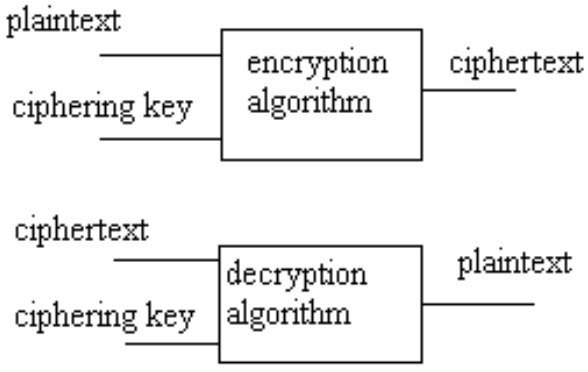


Fig.1 Encryption/Decryption Block Diagram

Cryptography is a tool that can be used to keep information confidential and to ensure its integrity and authenticity [2]. All modern cryptographic systems are based on Kerckhoff's principle of having a publicly-known algorithm and a secret key. Many cryptographic algorithms use complex transformations involving substitutions and permutations to transform the plaintext into the ciphertext. However, if quantum cryptography can be made practical, the use of one-time pads may provide truly unbreakable cryptosystems [3].

Cryptographic algorithms can be divided into symmetric-key algorithms and public-key algorithms. Symmetric-key algorithms mangle the bits in a series of rounds parameterized by the key to turn the plaintext into the ciphertext. Triple DES and Rijndael (AES) are the most popular symmetric-key algorithms at present. These algorithms can be used in electronic code book mode, cipher block chaining mode, stream cipher mode, counter mode, and others [3].

Public-key algorithms have the property that different keys are used for encryption and decryption and that the decryption key cannot be derived from the encryption key. These properties make it possible to publish the public key. The main public-key algorithm is RSA, which derives its strength from the fact that it is very difficult to factor large numbers [4].

Legal, commercial, and other documents need to be signed. Accordingly, various schemes have been devised for digital signatures, using both symmetric-key and public-key algorithms. Commonly, messages to be signed are hashed using algorithms such as MD5 or SHA-1, and then the hashes are signed rather than the original messages [3].

Public-key management can be done using certificates, which are documents that bind a principal to a public key. Certificates are signed by a trusted authority or by someone (recursively) approved by a trusted authority. The root of the chain has to be obtained in advance, but browsers generally have many root certificates built into them

.

y = -7E-06x6 + 0.0002x5 - 0.0027x4 + 0.0164x3 -0.0506x2 +0.077x +0.6707 (1)

y = 0.0003x2 - 0.0058x + 0.2621 (2)

y = 3E-06x3 - 0.0005x2 + 0.0594x - 1.4331 (3)

y = -9E-08x3 +0.0018x2 -0.0645x +0.3796 (4)

y = -3E-07x3 +0.0019x2 -0.064x +0.3722 (5)

y = 1E-06x6 -4E-05x5 +0.0005x4 -0.0031x3 +0.0088x2 - 0.007x +0.7721 (6)

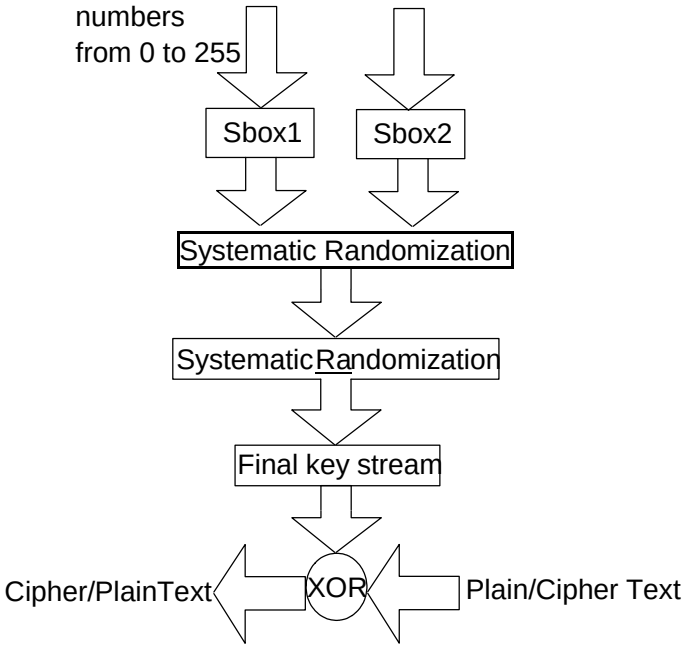
y = -8E-07x6 + 2E-05x5 - 0.0003x4 + 0.0013x3 - 0.0015x2 + 0.0009x + 0.7763 (7)

y = 0.0003x2 - 0.0053x + 0.2669 (8)

y = 3E-06x3 - 0.0005x2 + 0.0603x - 1.4542 (9)

y = -4E-07x3 + 0.0018x2 -0.0675x +0.4091 (10)

y = -8E-09x3 -0.0018x2 -0.0609x –0.3625 (11)



2.1 RC4 Steps

The steps for RC4 encryption algorithm is as follows:
1- Get the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate one array with numbers from 0 to 255.
4- Fill the other array with the selected key.
5- Randomize the first array depending on the array of the key.
6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text.

3. ENCRYPTION WORKS

HOW ENCRYPTION WORKS

The encryption process involves taking each character of data and comparing it against a key. For example, one could encrypt the string "THE SKY IS HIGH" of data in any number of ways, for example, one may use a simple letter-number method. In this method, each letter in the alphabet corresponds to a particular number. If one uses a straight alphabetic to number encryption (i.e., A=1, B=2, C=3, and so on), this data is translated into the following numbers: 20 8 5 19 11 25 9 19 8 9 7 8. This series of numbers is then transmitted over a network, and the receiver can decrypt the string using the same key in reverse. From left to right, the number 20 translates to the letter T, 8 to H, 5 to E, and so on. Eventually, the receiver gets the entire message: "THE SKY IS HIGH".

Most encryption methods use much more complex formulas and methods. The sample key was about 8 bits long; some keys are extremely complex and can be as large as 128 bits. The larger the key (in bits), the more complex the encryption and the more difficult it is to be cracked [4].

3.1. Encryption Keys

To encode a message and decode an encrypted message, one needs the proper encryption key or keys. The *encryption key* is the table or formula that defines which character in the data translates to which encoded character. Here, encryption keys fall into two categories: public and private key encryption [5].

3.2. Private Key Encryption

Private keys are also known as *symmetrical keys.* In private key encryption technology, both the sender and receiver have the same key and use it to encrypt and decrypt all messages. This makes it difficult to initiate communication for the first time. How does one securely transmit the single key to each user? However, public keys encryption is used [5].

3.3. Public Key Encryption

Public key encryption, or a Diffie-Hellman algorithm, uses two keys to encrypt anddecrypt data: a public key and a private key. Public keys are also known as *asymmetrical keys*.The receiver's public key is used to encrypt a message then this message is sent to the receiver who can decrypt it using its own private key. This is a one-way (the original sender is now going to be the receiver of this new message) and can only be decrypted with his or her private key. If the original sender does not have a public key, a message can still be sent with a digital certificate (also sometimes referred to as a digital ID). The digital ID verifies the sender of the message.communication. If the receiver wants to send a return message, the same principle is used. The y = -4E-07x3 + 0.0018x2 -0.0675x +0.4091 (10)
y = -8E-09x3 -0.0018x2 -0.0609x –0.3625 (11)message is encrypted with the original sender's public key

4. EXISTINGSYSTEM

Inter-AS connectivity of the Internet. BGP does not have built-in mechanisms to verify if a route is genuine, it suffers severe security plagues.Hijacking of YouTube traffic on a global scale for more than two hours.Many similar traffic backholes and interceptions with active routing attacks and mis-configurations Many similar traffic backholes and interceptions with active routing attacks.

5. DESIGN OF ANTI-TIGER

Anti-TIGER is consisted of four phases:(1) NAG construction for each AS, (2) suspicious traffic detection, (3) collaborative TIGER attack detection, and (4) TIGER defense. This section first presents detailed design and implementation of these procedures, and then analyzes possible threats for Anti-TIGER.

6. PROPOSED SYSTEM

TIGER, which aims to invalidate the "proven" security of these secure BGP schemes and allow ASes to announce forged routes even under full deployment of any existing secure BGP proposal. Anti-TIGER enables robust TIGER detection by collaborations between ASes. In particular, we leverage Spread Spectrum Communication technique to watermark certain special probing packets, which manifest the existence of TIGER attacks.

7.References

[1] China's 18-minute mystery. [Online]. Available:http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml, 2010.

[2] Defending against BGP man-in-the-middle attacks. [Online]. Available: http://www.renesys.com/tech/presentations/pdf/ blackhat-09.pdf, 2009.

[3] Detecting IPv6 tunnels in an enterprise network. [Online]. Available: http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6553 /white_p aper_c11-629391.html, 2013.

[4] The route view project. [Online]. Available: http://www.routeviews.org/, 2013.

[5] Stealing the internet: An internet-scale man in the middle attack. [Online]. Available: http://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov- kapela.pdf, 2008

[6] TEAM CYMRU BGP/ASN analysis report. [Online]. Available: http://www.cymru.com/BGP/summary.html, 2013

[7] Youtube hijacking: A RIPE NCC RIS case study. [Online]. Available: http://www.ripe.net/news/study-youtube-hijacking.html,2008

[8] H. Ballani, P. Francis, and X. Zhang, "A study of prefix hijacking and interception in the internet," in Proc. Conf. Appl., Technol., Archit., Protocols Comput. Commun., 2007, pp. 265–276.

[9] O. Bonaventure, C. Filsfils, and P. Francois, "Achieving sub-50 milliseconds recovery upon BGP peering link failures," IEEE/ ACM Trans. Netw., vol. 15, no. 5, pp. 1123–1135, Oct. 2007.