ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

Efficient Unflaws of Secure Data Transmission Using s-BGP

Nithya.s MSC[1], Babu.T.G MSC., MPHIL.,[1][2]

M. Phil Scholar, Dept. of Computer Science, Arignar Anna Govt Arts College, Cheyyar, India[1]

Assistant Professor, Dept. of Computer Science, Arignar Anna Govt Arts College, Cheyyar, India[2]

ABSTRACT: In current world situation involved many type of attacker to steal your own data for purpose of money, hobby and revenge. In this paper how to secure and transfer the data also found the minimum distance to reach the destination .we use two techniques to prohibit the attacker, 1) RFD (route flap dumping) and 2) MRAI (minimum route advertisement interval) this worked are find who is the hacker and how unaccepted the link furthermore and general things are used to transfer the data is internet protocol, border gateway protocol(BGP), path vector protocol, distance vector protocol, routers, autonomous system(AS), latitude, longitude and MED etc. It consist as AS-PATH, path cost, PID, key .The border gateway protocol is used to transfer the data one AS system to another. It provide the best feature of ibgp (ingress) and ebgp (egress) .RFD and MRAI use routing table and times tamper to calculate the distance of path and path changes, suddenly inform to neighbor AS system.

KEYWORDS: RFD, MRAI, iBGP, eBGP, AS etc.,

I. INTRODUCTION

1.1 NETWORK SECURITY

Network security is protection of the access to files and directories in a computer network against hacking, misuse and unauthorized changes to the system.[11] An example of network security is an anti virus system.

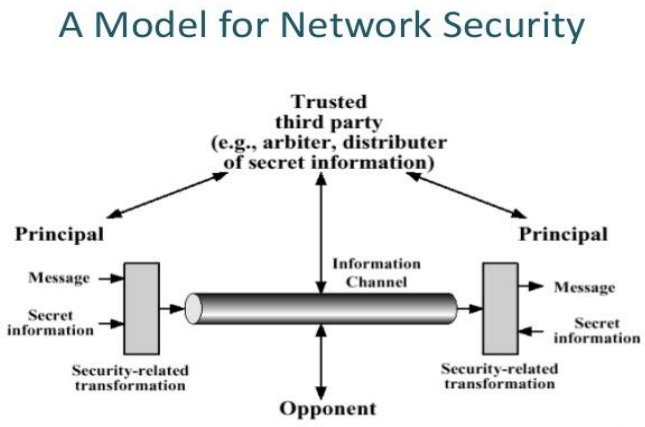

Fig 1.1

1.2 COMPUTER SECURITY:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

1.3 CRYPTOGRAPHY:

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. [11]Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Three types of cryptographic techniques used in general

1. Symmetric-key cryptography
2. Hash functions.
3. Public-key cryptography.

`` The art of protecting information by transforming it (encrypt it) into an unreadable format, called *cipher_text*. Only those who possess a secret *key* can decipher (or *decrypt*) the message *into plain_text*. Encrypted messages can sometimes be broken by cryptanalysis, also called *code breaking*, although modern cryptography techniques are virtually unbreakable.

RSA ALGORTHIM:

- Based on the idea that factorization of integers into their prime factors is hard.
- n=pq, where p and q are distinct primes
- Proposed by Rivest, Shamir, and Adleman in 1977 and a paper was published in The Communications of ACM in 1978
- A public-key cryptosystem

PROOF FOR THE RSA ALGORITHM

- $C^d \equiv (M^e)^d \equiv M^{ed} \equiv M^{1+k\varphi(n)} \equiv M \pmod n$ by Euler's theorem and Exercise 19 on p.192
- p=885320963, q=238855417,
- n=p. q=211463707796206571
- Let e=9007, ∴ d=116402471153538991
- M="cat"=30120, C=113535859035722866

II. LITERATURE REVIEW

2. RPKI ARCHITECTURE:

[1].A architecture for an infrastructure to support improved security for BGP routing [RFC4271] for the Internet. The architecture encompasses three principle elements:

I. Resource Public Key Infrastructure (RPKI).

II. Digitally signed routing objects to support routing security.

III. A distributed repository system to hold the PKI objects and the signed routing objects.

In this article are used to verify the set of IP address or AS system. In addition to this initial application, the infrastructure defined by this architecture also is intended to provide future support for security protocols such as Secure BGP [S-BGP] or Secure Origin BGP [soBGP]. This architecture is applicable to the routing of both IPv4 and IPv6 datagram's. IPv4 and IPv6 are currently the only address families supported by this architecture.

2.1SINGLE-HOMED SUBSCRIBERS:

In BGP, a single-homed subscriber with Provider Aggregatable (PA) address space does not need to explicitly authorize routes to be originated for the prefix(es) it is using, since its ISP will already advertise a more general prefix and route traffic for the subscriber's prefix as an internal function.

2.2 MULTI-HOMED SUBSCRIBERS:

Here we consider a subscriber who receives Provider Aggregatable (PA) IP address space from a primary ISP (i.e., the IP addresses used by the subscriber are a subset of ISP A's IP address space allocation) and receives redundant upstream connectivity from one or more secondary ISPs, in addition to the primary ISP.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

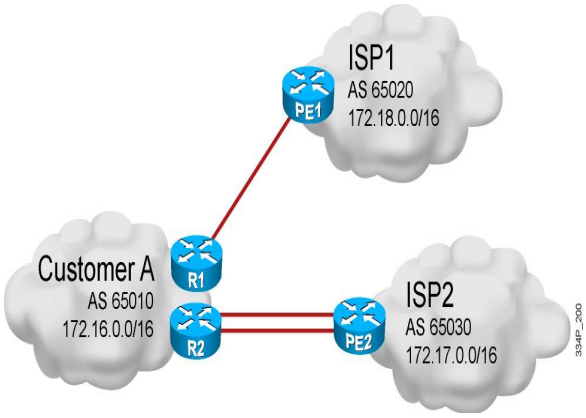

Fig 2.2 multi-homed subscribers

3. BORDER GATEWAY PROTOCOL:

Border Gateway Protocol (BGP) [2], [3] tied together the internet's global routing infrastructure. BGP routers exchange routing updates to adapt to topological connectivity changes caused by either intentional routing policy changes or more commonly unexpected software and hardware failures. Be- because BGP runs in a flat routing space, a single unstable route can cause a ripple effect which results in thousands of update messages propagating throughout the entire network. It is well known that a relatively small percentage of unstable routes exists in the global routing system and contributes an out of proportion number of routing updates [4] [5].

4. ROUTE FLAP DAMPING:

[2]. The original RFD algorithm was developed in the mid 1990s and standardized in RFC 2439. [3] Route Flap Damping (RFD), is designed to detect and suppress perpetual route instabilities. It was once considered an effective means to maintain the overall Internet routing stability.

4.1 Why Revisit RFD?

Recent rises of real-time applications bring new require- ments to the routing system. Compared to conventional non real time data communications, real-time voice and video applications are much less tolerant to delay jitters that are causedbyfrequentroutechanges. Measurement studies show that BGP events are highly correlated with 50% of Skype quality degradation and 90% of call drops [6]. At the same time, network operators gradually lose control over routing instability: not only the flap damping is largely turned off, but also the use of MRAI has been decreasing due to the de- sire for faster routing convergence. We believe that if we can fix RFD's reachability loss problem, it could again play an important role in stabilizing the global routing system.

4.2 RFD+RG: NOTANOTHER ROUTE FLAP DAMPING ALGORITHM:

In addition to route flap damping; we call the combined scheme Route Flap Damp- ing with Reachability Guard (RFD+RG). The basic idea is to suppress a flapping prefix only when one or more alternative routes to exist, i.e., when the reachability to p can be preserved. We emphasize that this work is not another damping algorithm itself, but a complementary addition to any existing rout flap damping scheme.

5. MRAI (Minimum Route Advertisement Interval) TIMER:

The Minimal Route Advertisement Interval (MRAI) [3] is used to pace out BGP updates by introducing a minimal gap between two consecutive up- date messages for the same prefix, with a default value of 30 seconds. Note that MRAI enforces a nondiscriminatory rate limit on all prefixes, regardless their status of (in)stability.

MRAI timer reduce a frequently route changes. It is the minimum amount of time that must pass between consecutive announcements of a route. It limits the frequency of route announcements sent to neighbor. If MRAI time enable in source router, the source will accept one request in MRAI time. If the attacker announces a route to source

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 7, July 2017

and immediately withdraw, the source will accept a request in first MRAI time and next MRAI time the source will accept a second request. The attacker receives a first request and decides this route is most prefer route and sends a data. The data will be dropped by attacker. The attacker will be found in policy changes. The Autonomous System changes its policy it sends a message to its neighbor. The neighbor compares a previous message then find a attacker. Note that MRAI enforces a nondiscriminatory rate limit on all prefixes, regardless their status of instability. Find a attacker then generate a route and transmit a data to reach a destination satisfy the two properties.[7].

III. ADVANTAGES AND DISADVANTAGES

The various advantages of BGP protocol are

- **Fast convergence and fault tolerance:** When BGP add path is enabled, more than one path to a destination is advertised. If one of the paths goes down, connectivity is easily restored due to the availability of backup paths. If the next hop for the prefix becomes unreachable, the device can switch to the backup route immediately without having to wait for BGP control plane messages.
- **Enhanced load balancing capabilities:** Traditionally with RRs in an iBGP domain, only the best path is given to the clients even if ECMP paths exists. This affects load balancing. With additional paths advertised by RRs, the clients have more effective load balance.
- In use two mechanism are very useful RFD and MRAI timer.
  Besides the advantages of BGP, it is also have some of demerits which are as follows:
- Load balancing is achieved for the BGP IPv4 and IPv6 address family neighbors only and not for EVPN neighbors. For more information on BGP EVPN, refer to the BGP EVPN chapter.
- BGP add path does not provide any advantage for ARP and MAC routes supported by EVPN peers. L2 ECMP is not currently supported.
- BGP multipath must be configured to choose ECMP paths. Only the best path and the first 5 ECMP paths are chosen as additional paths for basic functionality support and advertised to neighbors with path IDs.

IV. CONCLUSION

The two techniques are more useful to solve the instability of route changes and also secure the data from hackers. It contains the routing table to update the current changes, in routing table are very helpful to inform the changes on near autonomous system with help identifying and addressing protocol. In system security purpose use firewall, it like as use BGP (border gateway protocol) are used for transfer the data in one routing system to another.

REFERENCES

[1] M. Lepinski and S. Kent, “An infrastructure to support secure Internet Routing,” 2012 [Online]. Available: https://tools.ietf.org/html/rfc6480.
[2].Lixia Zhang lixia@cs.ucla.edu”Route Flap Damping with Assured Reachability”2010[Online]. Available: https://tools.ietf.org/html/rfC7800.
[3]. C. Villamizar, R. Chandra, and R. Govindan. BGP Route Flap Damping. RFC 2439 (Proposed Standard), Nov. 1998
[4]. G.Huston, “The BGP Instability Report “ , http://bgpupdates.potaroo.net/instability/bgpupd.html. , 2010.
[5]. R. Oliveira, R. Izhak-Ratzin, B. Zhang, and L. Zhang. “Measurement of highly active prefixes in BGP”. In GLOBECOM’05.
[6]. P. Jakma. “Revisions to the BGP ’Minimum Route Advertisement Interval”. http://tools.ietf.org/html/draft-ietf-idr-mrai-dep-02. , 2010.
[7]. Lixin Goa ”On inferring autonomous system relationships in the Internet”
2000. ISBN: 0-7803-6451-1.
1)[8]. RFC 7196 - IETF Datatracker ,
https://datatracker.ietf.org/doc/rfc7196/.
2)[9]. “Stealth Probing: Efficient Data-Plane Security for IP Routing”.
https://www.cs.princeton.edu/~jrex/papers/stealth06.pdf
3)[10] RFC 7730 – “Resource Public Key Infrastructure (RPKI) Trust Anchor”.
https://tools.ietf.org/html/rfc7730.
[11]. www.cs.columbia.edu/~hgs/teaching/security/slides/crypto2.pdf.
[12] http://www.webopedia.com/TERM/C/cryptography.html
[13]. www.idc-. online.com/technical_references/.../A_Model_for_Network_Security.pdf