International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 5, May - 2014

Survey Paper on BGP Prefix Hijacking

Anand K.Patel[1], Nisha V.Shah[2], Jignesh B.Maheta [3] Jaydipsinh B.Jadeja [4]
[1] PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University
[2] Assistant Professor *at* Sardar Vallabhbhai Patel Institute of Technology ,Vasad
[3] PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University
[4]PG-ITSNS Student, Department of Computer Engineering, Gujarat Technological University

***Abstract*—In this paper, we showed various techniques for BGP prefix hijacking. Many researchers has came up with interesting techniques to prevent BGP prefix hijacking. It is important to understand multiple techniques to research about BGP prefix hijacking. So we gone through many papers which demonstrates about BGP prefix hijacking. In "Prefix Hijacking Alert System" by M. Lad et al. showed a novel technique for BGP prefix hijacking. Apart from this we presented many techniques which are suggested by the various researchers.**

Keywords—Network, BGP, Prefix hijacking, interdomain and intradomain.

I. INTRODUCTION

Cloud computing is seen as a trend in the present day scenario with almost all the organizations trying to make an entry into it. The users can access their data from anywhere. Resources in cloud system can be shared among a large number of users. Cloud computing isa technology that uses the internet & central remote server maintained data and application. A simple example of cloud computing yahoo, Gmail, Hotmail. Users don't need a software or server to use them. All consumer would need is just an internet connection and they can start sending emails.

The National Institute of Standards and Technology (NIST) has defined cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources, e.g. networks, servers, storage, applications, and services, that can be rapidly provisioned and released with minimal management effort or service provider interaction.[1]

The several numbers of definitions have been given explaining the cloud computing. **Cloud Computing has been defined as** the new state of the art technique that is capable of providing a flexible infrastructure, such that user need not own the infrastructure supporting services. This integrates the features supporting **high scalability** and **multi-tenancy.**

The main advantage of using cloud computing are :-

- Reduction in the cost of hardware and maintenance cost
- Global Accessibility
- Flexibility and highly automated process where in the customer need not worry about software up-gradation which tends to be a daily matter.

II. INTRADOMAIN AND INTERDOMAIN ROUTING

Today internet is so large that one routing protocol will not be able to handle the task of updating the routing tables at regular intervals of all the routers. To overcome this scenario an internet is divided into various autonomous systems. Autonomous system is a group of network routers under the control of single administration. Routing inside an autonomous system is called an intradomain routing. Routing between autonomous systems is called as interdomain routing. Each autonomous system can choose one or more than one intradomain routing protocols to handle routinf inside the autonomous system but it can choose only one interdomain routing protocol to handle routing between autonomous systems. There are several intradomain and interdomain routing protocols in use.

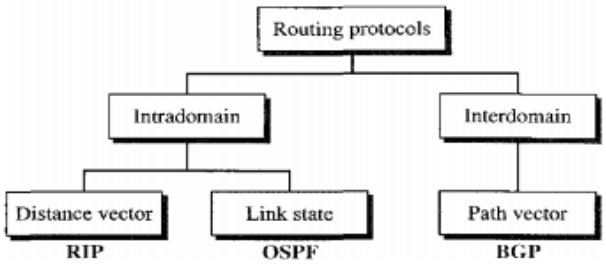

Figure 1 Routing Protocols

Different routing protocols are as follows:-

- **RIP(Routing Information Protocol):-**
  The Routing Information Protocol(RIP) is and intradomain routing protocol used inside an autonomous system. It is a very simple protocol based on distance vector routing. Using RIP, a gateway host (with a router) sends its entire routing table to its closest neighbor host every 30 seconds.
- **OSPF(Open Shortest Path First):-**

OSPF protocol is an intradomain routing protocol based on link state routing. Using OSPF, a host that obtains a change to a routing table or detects a change in the network immediately multicasts the information to all other hosts in the network so that all will have the same routing table information. OSPF multicasts the updated information only when a change has

taken place. RIP is supported within OSPF for router-to-end station communication.

- **BGP(Border Gateway Potocol):-**

The routing protocol that connects large IP networks to form a single internet is the Border Gateway Protocol. It is the standart inter-domain routing protocol used today. It ensures that each participating network(autonomous system) has route for reaching every block of IP addresses known as prefixes. It is a path-vector protocol in which information about network topology is spread only by local contact.

III. RELATED WORK

Techniques from literature	Abstract	Conclusion
Beyond ligntning: A survey on security challenges in cloud computing	Introduction to the cloud computing and security challenges	Cloud Computing is a very good technology for an organization which reduces costs and increases efficiency.
Autonomous Security for autonomous systems	A Pretty Good BGP, a system that protects against various types of attacks on AS	PGBGP is an effective in stopping attacks made against AS& also has very low overhead. But it is vulnerable to DOS attack
Prefix Hijack Alert System 15th USENIX Security Symposium	A Prefix Hijacking Alert System is introduced which alerts prefix owners when any BGP origin changes	Prefox hijacking problem is categorized into cryptography based on non-crypto based.
Broder Gateway Protocol	Commands for setting up BGP basic configuration is defined	BGP configuration done using done using neighbor and network commands.
IP prefix hijacking detection using the collection of AS characteristics	A Prefix hijacking detection algorithm based on network reachability is designed	A BGP prefix hijack is a network attack in which false aouncement is made that causes network reachability problem and communication failure
A Survey on Security Issues in Cloud Computing	Introduction to Cloud Computing and various threat to it.	Attacks in Cloud Computing is categorized into different types at various level.

Prefix hijacking is a type of network attack in which a wrong announcement related to the IP addresses associated with an Autonomous System(AS) is made and hence malicious parties get access to the untraceable IP addresses. On the internet, IP space is associated in blocks and remains under the control of AS's. Am autonomous system can broadcast information of an IP contained in its regime to allits neighbors. These AS's communicate using the Border Gateway Protocol(BGP) model. Sometimes, due to some error, a faculty AS may broadcast wrongly about the IPs associated with it. In such case, the actual traffic gets routed to some IP other than the intended one. Hence, data is leaked or reaches to some other destination that it should not happen in real time scenario.

In a prefix hijack event, the announced path to the prefix cannot actually be used todeliver data to the prefix.In some parts of the Internet, the false path replaces the authentic route to the prefix and traffic that follows the false path will eventually be dropped or delivered to someone who is pretending to be the legitimate destination. In other words, the traffic flowing over the false path is hijacked. We can say AS that injects false information as an attacker AS, and the AS that actually owns the route as a victim AS.

Autonomous System corresponds to an administrative domain for example University, Company, BackBone network and assign each AS a 16-bit numeric value.

Autonomous System consists of two traffic types:-

- Local: This type of traffic starts and ends within an AS.
- Transit: This type of traffic passes through an AS/

Autonomous System Types are as follows:-

- Stub AS: This AS has a single connection to one another AS which carries local traffic.
- Multihomed AS:- This AS has connections to more than one AS and it does not carry transit traffic.
- Transit AS: This AS has connection to more than one AS and it carries transit as well as local traffic.

There are different properties of AS for using into an organization such as:-

- Each has one or more border routers that handle inter-AS traffic
- One BGP Speaker for an AS which will participate in routing
- BGP speaker establishes BGP sessions with peers and advertises:
  - Local network name
  - Other reachable networks(transit AS only)
  - Gives path information along with path weights
  - Withdrawn routes

In spite of great success in BGP, there are some malicious attacks that can cause serious problems. A simple mistake unintentional or intentional, while configuring a router can leads to an AS to "hijack" traffic intended for the networks. For example an AS might announcement to its neighbors that it is the destination(origin AS) for a block of IP addresses(prefix) that it does not own, and this false information would then propagate to other networks.

IV CONCLUSION

Here we presented various techniques for BGP prefix hijacking. BGP is a gateway protocol. If something happens to BGP, multiple networks can fail. So it is important to prevent failures and attacks on BGP. BGP prefix hijacking is one of the important concepts which can be used for attacking BGP. So we need to develop a full proof method to prevent BGP prefix hijacking.

VII REFERENCES

1. M. G. Jaatun, C. Rong, and S. T. Nguyen, "Beyond lightning: A survey on security challenges in cloud computing," *Computers & Electrical Engineering*, vol. 39, no. 1, pp. 47–54, Jan. 2012.
2. J. Karlin, S. Forrest, and J. Rexford, "Autonomous security for autonomous systems," *Computer Networks*, vol. 52, no. 15, pp. 2908–2923, Oct. 2008.
3. M. Lad, D. Massey, Y. Wu, B. Zhang, and L. Zhang, "PHAS: A Prefix Hijack Alert System," in *15th USENIX Security Symposium*, 2006, pp. 153–166.
4. Balchunas Aaron, "- Border Gateway Protocol -," pp. 1–30, 2007.http://www.routeralley.com/ra/docs/bgp.pdf
5. S. Murphy, "BGP Security Vulnerability," *RFC 4272*, pp. 1–23, 2006. http://tools.ietf.org/pdf/rfc4272.pdf
6. M. Pennington, N. C. Engineer, and D. Cisco Systems, "BGP Deployment and Scalability."2001.http://www.pennington.net/tutorial/bgp_001/BGP_Overview.ppt
7. SugtaSanyal,RohitBhadauria, RituparnChaki, NabenduChaki, "A Survey on Security Issues in Cloud Computing," *arXivPrepr. arXiv1109.5388*, 2011.
8. Behrouz A. Forouzan, *Data Communications and Networking*, Fourth edition.
9. J. Karlin, S. Forrest, and J. Rexford, "Pretty Good BGP : Improving BGP by Cautiously Adopting Routes," *Int. Conf. Network. Protocol*, pp. 290–299, 2006.
10. Y. Z. MakanPourzandi, "Studying Impacts of Prefix Interception Attack by Exploring BGP AS-PATH Prepending," in *Distributed Computing Systems(ICDCS), 2012 IEEE 32nd International Conference*, 2012, pp. 667 – 677.
11. YujingLiux; Wei Peng; Jinshu Su, "Study on IP Prefix Hijacking in Cloud Computing Networks Based on Attack Planning," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference*, 2011, pp. 922–926.
12. AzinOujani, "A Survey of Cloud Computing Simulations and Testings" http://www.cse.wustle.edu/~jain/cse567-13/ftp/cloud/index.html