Ex-AS-CRED Method for Inter Domain Routing of BGP

Trishula Hajare, Mrs. D. A. Chaudhari, DYPCOE - Akurdi, Savitribai Phule Pune University

***Abstract*—**Border Gateway Protocol (BGP) acts as a main part of the global infrastructure. Attacks against BGP are increasing and severity. Many of the security mechanisms based on public key cryptography suffer from performance, trust model and other different issues. In this paper we are presenting the new method for solving the security and trust issues in BGP protocol traffic. The recently presented approach is AS-CRED which works on reputation and alert service which not only detect anomalous BGP updates, but also provides a quantitative view of AS tendencies to perpetrate anomalous behavior. The AS-CRED was basically based on the term of credit score. From the practical results, the proposed AS-CRED was efficient for solving the trust issues in complex world of finance which includes the huge amount of entities as well as highly uncertain interactions. However, this limitation of AS-CRED is that prediction approach of future anomalous behavior needs to improve with more accuracy. In this paper we presenting the new method called Ex-AS-CRED [Ex-Extended] with aim of adding the more descriptive AS behaviors and hence the final information of AS reputation is used for prediction of invalid behaviors of BGP.

Index Terms*—Alert Generation Service, Accuracy, Au-tonomous System, AS-CRED, Anomaly Detection, BGP, Repu-tation.*

*****

I. INTRODUCTION

The Internet contains a large number of interconnected autonomous systems (ASes), which exchange their routing table information using Border Gateway Protocol (BGP). BGP was designed to operate in a trusted environment, and there are no internal mechanisms to protect the information it carries [2]. In recent years, it is reported that BGP security vulnerability lead to many negative effects on the Internet at various levels. Since most routing attacks stem from prefix hijacking and path falsification, our aims at the protection and validation of prefix and AS PATH information. A natural approach which provides strong security is to use public key cryptography. S-BGP [7], soBGP [8] and psBGP [9] are among the most representative proposals. However, large-scale network simulation and thorough analysis, [10] concluded that the more they looked at the performance, the more issues they saw and the many potential ways to improve performance.

The RI which is provided by the ASec is valid and hence this main functional considerations of the BGP. The validity of RI is defined as 1) The information in the updates are legal and correct, 2) The ASes in the AS PATH provide a stable route to the prefix, and 3)There is no routing policies are violated in the process of propagating the updates. Present AS-TRUST, a novel scheme for quantifying the level of trust and one can have on ASes in terms of disseminating valid RI. To the best of our knowledge, this is the first attempt to re-examine the operational trust assumption of BGP in a quantitative manner. In AS-TRUST, trust can represented using a metric which is called reputation. [1] Many existing phishing detection techniques are weak against Domain Name System (DNS)-poisoning-based phishing attacks. It is a highly effective method for detecting such attacks Those attacks are usually carried out by ASes which announce anomalous BGP updates containing invalid reach ability information. These attacks fundamentally affect the accessibility of the Internet and can have grave consequences to attacks akin to DNS poisoning [2] one of the solutions that has been widely used by naive users which protect against phishing attacks is security toolbars or phishing filters in web browsers.

The present study proposes a new attack to bypass security toolbars and phishing filters via local DNS poisoning without the need of an infection vector (phishing) [3] reasons for these incidents have usually been found to be malice such as spamming, a study of the network-level characteristics of unsolicited commercial email (spam). The attention has been devoted to studying the content of spam, but comparatively little attention has been paid to spams network-level properties. Conventional wisdom often asserts that most of todays spam comes from botnet, and that a large fraction of spam comes from Asia; a few studies have attempted to quantify some of these characteristics [4] & miss configuration [5] it is well known that simple, accidental BGP configuration errors can disrupt Internet connectivity. The idea here is that although there is no complete and accurate ground trust available which determine the validity of BGP updates in real time, such a task can be effectively performed with the benefit of hindsight, thus addressing the first challenge.

There are many other techniques presented for the detection of malicious flows from the BGP traffic, but each method having its limitations. Therefore for addressing these limitations re-cently we have studied new efficient method in [1]. AS-CRED [1] is an AS reputation and alert service that not only detects anomalous BGP updates but also provides a quantitative view of AS behavior. This method shows effectiveness in order to provide better security for inter domain routing. However this approach further needs to be investigated and extended to use for prediction of invalid BGP behaviors. Thus in this paper we are presenting the new approach called Ex-AS-CRED in which we are adding the more descriptive functionalities of

AS behavior which are more accurately delivers the prediction of invalid BGP behavior.

II. RELATED WORK

This section presents the different methods to solve the trust problems in BGP routing. Apart from this we are also discussing the different anomaly detection methods.

J. Chang, K. Venkatasubramanian, A. G. West, S. Kannan, B. T. Loo, O. Sokolsky, and I. Lee, [2] In this paper we presented AS-TRUST, a reputation-based scheme for charac-terizing trustworthiness of an AS with respect to disseminating valid reach ability information. Reputation is computed by evaluating past RI announced by each observable AS in the Internet for the exhibition of specific behaviors. The evaluation utilizes well defined properties for this purpose which includes the presence of stable AS-prefix binding, stable AS-links and valley free AS PATH. It then classifies the resulting observations into multiple types of feedback sets.

H. Kim and J. Huh, [3] in this paper of the existing phishing detection techniques are weak against domain name system (DNS)-poisoning-based phishing attacks. A highly effective method for detecting such attacks is the network performance characteristics of websites are used for classification. Demon-strate how useful approach, explored the performance of four classification algorithms: linear discriminate analysis, naive Bayesian, K-nearest neighbor and support vector machine. 10 000 real world items routing information was observed during a one week period. The experimental results show that the best performing classification method which uses K-nearest neighbor algorithm99.4% positive, a true and a false positive rate of 0.7% is capable of achieving.

S. Abu-Nimeh and S. Nair [4] in this paper A rogue wireless access point (AP) is set up, poisoned DNS cache entries are used to forge the results provided to security toolbars, and thus misleading information is displayed to the victim. Al-though there are many studies that demonstrate DNS poisoning attacks, our best knowledge no investigation whether such attacks security toolbars or phishing filter can circumvent the five well known security tools built into phishing filter strips and three respected browser are scrutinized, and none of them attack detected. Akushlatapurvak so Evidence of false security toolbars, hunting with the indicator that the phishing site is valid.

A. Ramachandran and N. Feamster, [5] This paper has studied the network-level behavior of spammers using a joint analysis of a unique combination of datasets a 17- month-long trace of all spam sent to a single domain with real time trace routes, passive TCP fingerprints, and DNSBL lookup results; BGP routing announcements for the network where the sinkhole are located; command and control traces from the Bobax spamming botnet; and mail logs from a large commercial email provider. This analysis allowed us to study some new and interesting questions that should guide the design of better spam filters in the future, based on the lessons. R. Mahajan, D. Wetherall, and T. Anderson [6] in this paper, they present the first quantitative study of BGP mis configuration. A three-week period, we crossed the backbone of the Internet to explore routing mis configuration incidents table ads analyzed from each event 23 vantage points for ISP operators to verify whether this is a mis configuration, and to learn the cause of the incident they also actively polled Internet connectivity in order to determine the effect of mis configuration and was unable to. Surprisingly, we find that configuration errors are pervasive, with 200-1200 prefixes (0.2-1.0% of the BGP table size) suffering from mis configuration each day. Close to 3 in 4 of all new prefix advertisements were results of mis configuration. Fortunately, the connectivity seen by end users is surprisingly robust to mis configuration.

A. Anomaly Prevention Techniques [1]

In [7] the method S-BGP is presented which is one of the earliest and the most concrete security mechanism to address BGP vulnerabilities. However, the deployment difficulties and computational overhead of S-BGP have made its adoption cumbersome in the inter domain world.
To overcome some of these issues, more incrementally de-ployable schemes such as presented in [9] and [10] called So-BGP and BGPSEC respectively has been proposed. Despite the availability of cryptography based solutions, we believe that the reputation-based solutions still have a place in ensuring proper operation of BGP. Since cryptography-based solutions can only address information security related problems by ensuring the confidentiality, integrity, authenticity of infor-mation exchanged between entities. The vacillation problem however does not violate any information security property, hence cannot be addressed by such secure BGP protocols.

B. Anomaly Detection Methods [1]

Detecting attacks on the BGP routing infrastructure has received its own share of attention. Many of these schemes use data-plane probing where an AS, on suspecting an update to be an attempted hijack, probes the announcer to verify its suspicion [11], [12]. Although they achieve reasonably high detection accuracy, some of these approaches can only be leveraged by the victim originator AS during the attack phase. Therefore, such approach will have limited global impacts without a full network deployment. Another approach is to analyze historical control-plane information for detecting any subsequent problematic updates [13]. The recent proposal of PGBGP [14] uses this approach to delay the selection of suspicious routes. However, as demonstrated in our evaluation with real world traces, it suffers from high error rates.

III. IMPLEMENTATION DETAILS

A. Problem Definition

The current design of BGP implicitly assumes complete trust between ASes (Autonomous Systems). This blind trust assumption is problematic for a growing number of attacks on the Internets operation. These attacks are carried out by ASes that announce anomalous BGP updates containing invalid reach ability information. These attacks affects the accessibility of the Internet and can have grave consequences to attacks akin to DNS poisoning and phishing. The reasons of these incidents have usually been found to be either malice such as spamming or mis configuration.

The three major challenges in securing the inter domain routing from these attacks.

Lacks of Ground Trust: There is no one authoritative source of information to determine the validity of BGP updates.

Dynamic as well as Mixed AS behavior: ASes announce valid as well as anomalous updates.

Scale of the Internet: It is often very expensive to deploy a security mechanism covering the entire inters domain routing system.

Hence to solve such security issues of inter domain routing different methods presented in literature. These methods are basically depends on two techniques traditionally been taken for securing inters domain routing prevention and detection. However, these approaches often impose a high deployment and operation cost to be useful for failing to address the third challenge.

To overcome above issues recently we have investigated new efficient method in [1]. AS-CRED [1] is an AS reputation and alert service that not only detects anomalous BGP updates but also provides a quantitative view of AS behavior. This method shows effectiveness in order to provide better security for inter domain routing. However this approach further needs to be investigated and extended to use for prediction of invalid BGP behaviors.

B. EX-AS-CRED

In this project we are first investigating the recently presented efficient method called AS-CRED [1], and then further extend that method by adding the functionality of prediction of invalid BGP behaviors by using past informations and logs in order to prevent then in near future. This new method is called as Ex-AS-CRED. This will increase not only the speed of detection as well as prevention of invalid behaviors but also improve the more security for the inter domain routing. In this proposed method first the construction of AS behaviors done more descriptive form, and use the resulting AS reputation information to predict the likely amount of invalid BGP behaviors that are going to be exhibited at any given time in the future.

Our approach is a five-step process of algorithm

Algorithm EX-AS-CRED:

Step 1: Historical anomaly detection: Evaluate the past updates announced by ASes for establishing hijacked or vacillating bindings.

Step 2: Reputation computation: Compute AS reputation based on the identified anomalous behavior.

Step 3: Alert generation: Use the reputation to trigger alerts for any invalid bindings in subsequent updates.

Step 4: AS Construction: AS behaviors done more descriptive form.

Step 5 Prediction: Using the AS reputation information the prediction of invalid and valid BGP behaviors.

Following figure 1 depicted the overall architecture for proposed system:

C. Mathematical Model

The mathematical model for system which contains input ,output required for system and functionality of system it

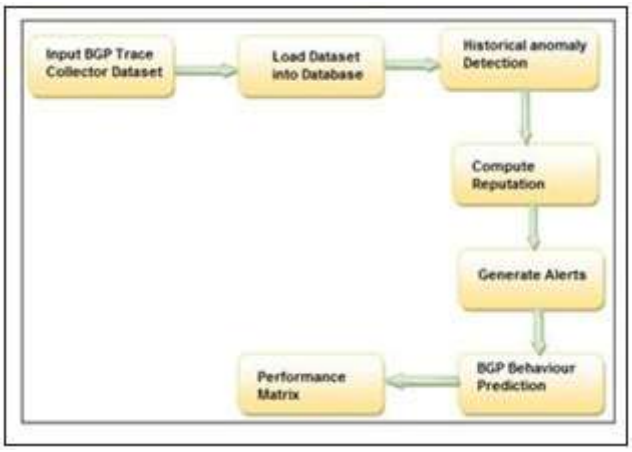

Fig. 1: Proposed system Architecture

also provides details of different constraints used to develop a system.

S=fI, F, Og

Set S contains the inputs, functions and there respective outputs which is described below in form of set theory.

Input

f=fG,B,Ug

f=Feedback

set

fG= gijgi is set of valid AS-prefix bindingg

fB= bijbi is set of not valid but does not subvert the intended BGP operationg

fU=uijui is set of not valid provided each time an AS does not demonstrate good behaviour and subverts the intended BGP operationg

Each feedback triple is exclusively classified into one of the three feedback sets, namely,

G (good), B (bad), and U

(ugly) G=fa, p, tg

B=fa, p,

tg U=fa,

p, tg

 ISSN: 2321-8169
1942 - 1946

a=Autonomous System
p=Prefix
t=Timestamp
F=fRep, Pr, Psg

Reputation can be computed based on a Mathematical function.

$$Rep_X^t(a) = 2^{(tnow\ t)} = h_x \quad (1)$$

Where,
RepX(a)=is the reputation of an AS a for exhibiting poor behaviour type X
tnow=Current Time
t= Time stamp
hX=half-life
Calculate Prevalence

$$Pr(a; p) = \sum_i^N (T\ w^i(a; p)\ \ T\ O^i(a; p)) = T\ obsv \quad (2)$$

Where,
Pr=Prevalence

N=Number
Tobsv=Observation Window
Tw(a, p)=The time prefix p is withdrawn by AS a To(a, p)= The time prefix p is the announced by AS a

Calculate Persistence (Ps) of an AS-prefix binding is defined as the average duration of a binding instance in the observation window.

$$Ps(a; p) = \sum_i^N (T\ w^i(a; p)\ \ T\ o^i(a; p)) = N \quad (3)$$

Where,
Ps(a,p) is a Persistence of an AS-prefix binding of (a,p).
Output
O=fOv, Onvg is a set of outputs.
fOv = vjv a set of valid prefix bindingg
fOnv = nvjnv a set of non valid prefix bindingg

D. Operating Environment

a) Software Requirement
Operating System - Windows XP/7/8
Programming Language - Java
Database - SQL-Yog
Tool - Net beans.
b) Hardware Requirement
Processor - At Least Pentium Processor
RAM - 256 MB (min)
Hard Disk - 2 GB

E. Data Set

The data set is collected by using RouteViews BGP trace collector which is maintained by the University of Oregon, to populate the BGP Activity Manager. In this dataset information of AS announcements, source IP, Destination IP, AS prefix and Path etc are declared traced in time range.

F. Metrics Computed

We find least false Positive (FP) values and True positive (TP) values. We not consider FN values for computation of matrices.

IV. RESULTS AND DISCUSSION

Following figure 2 shows the output screen for historical anomaly detection to conclude white and black list. Figure 3 and 4 shows the white-list and black-list for input dataset divided according to knowledge data values stored in database.

V. CONCLUSION

The AS-CRED method was extended in this paper. The initial aim of this paper is to present the efficient method for anomalous flow identification and prediction of future invalid behaviors of BGP routing. We presented the proposed architecture for EX-AS-CRED which is based on existing method of AS-CRED. The practical study is done using the real time BGP routing packets data which contains both

Fig. 2: Historical Anomaly Detection Screen

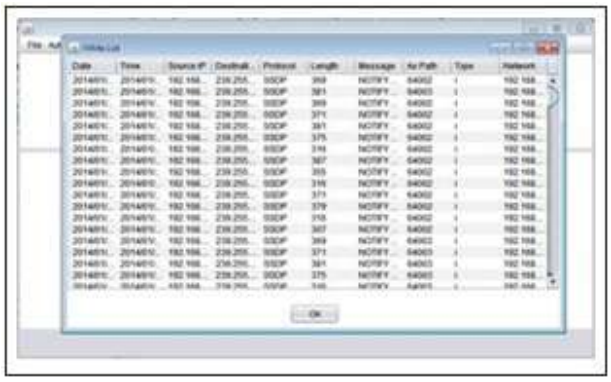
Fig. 3: White List

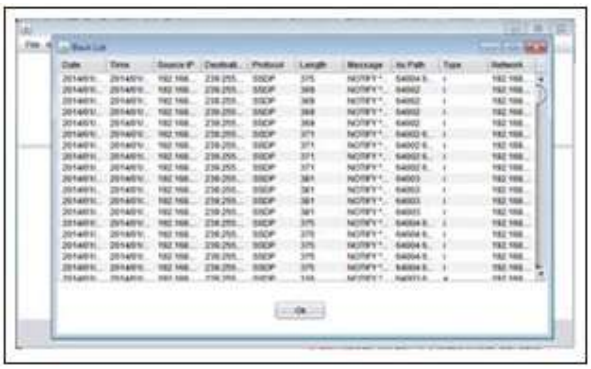

Fig. 4: Black List

normal and abnormal flows. The results presented in this paper are current state of implementation which is later improved more as per our expected results.

In future work we will like to suggest deploying this proposed work for testing under real time environment and validate the proposed architecture results against the existing methods.

ACKNOWLEDGMENT

I take this opportunity to express my profound gratitude and deep regards to my guide Ms. D. A. Chaudhari for her exemplary guidance, monitoring and constant encouragement throughout the course of this project. I also take this opportunity to express a deep sense of gratitude to my Head of

the department Mrs. M. A. Potey, PG Coordinator Mrs. S. S. Pawar, for her cordial support, valuable information and guidance. Thanks to all those who helped me in completion of this work knowingly or unknowingly like all those researchers, my lecturers and friends.

REFERENCES

[1] Jian Chang, Krishna K. Venkatasubramanian, Member, IEEE, Andrew G. West, Sampath Kannan, Insup Lee, Fellow, IEEE, Boon Thau Loo, and Oleg Sokolsky, Member, IEEE, "AS-CRED: Reputation and Alert Service for Inter domain Routing", IEEE SYSTEMS JOURNAL, VOL. 7, NO. 3, SEPTEMBER 2013

[2] J. Chang, K. Venkatasubramanian, A. G. West, S. Kannan, B. T. Loo, O. Sokolsky, and I. Lee, "AS-TRUST: A trust characterization scheme for autonomous systems BGP," in Proc. 4th Int. Conf. TRUST, Jun. 2011, pp. 262276.

[3] H. Kim and J. Huh, "Detecting DNS-poisoning-based phishing attacks from their network performance characteristics," Electron. Let. vol. 47, no. 11, pp. 656658, 2011.

[4] S. Abu-Nimeh and S. Nair, "Circumventing security toolbars and phishing filters via rogue wireless access points," Wireless Commun. Mobile Compute. vol. 10, no. 8, pp. 11281139, 2010.

[5] A. Ramachandran and N. Feamster, "Understanding the network-level behavior of spammers," SIGCOMM Compute. Commun. Rev., vol. 36, no. 4, pp. 291302, 2006.

[6] R. Mahajan, D. Wetherall, and T. Anderson, "Understanding BGP mis configuration," in Proc. Conf. Appl., Technol., Arch. Protocols Compute. Commun. 2002, pp. 316.

[7] V. J. Bono. (1997, Apr. 26). 7007 Explanation and Apology [Online]. Available: http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html

[8] S. Kent, C. Lynn, and K. Seo, "Secure border gateway protocol (SBGP)," IEEE J. Selected Areas Commun., vol. 18, no. 4, pp. 582592, Apr. 2000.

[9] J. Ng. (2002, Oct.). Extensions to BGP to Support Secure Origin BGP (soBGP) [Online]. Available: http://tools.ietf.org/html/draft-ng-sobgpbgp-extensions-00.

[10] M. Lepinski and S. Turner. (2012, May 8). An Overview of BGPSEC [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-overview/.

[11] X. Hu and Z. M. Mao, Accurate real-time identification of IP prefix hijacking, in SP: Proc. IEEE Symp. Security Privacy, May 2007, pp. 317.

[12] Z. Zhang, Y. Zhang, Y. C. Hu, Z. M. Mao, and R. Bush, iSPY: Detecting IP prefix hijacking on my own, SIGCOMM Compute. Commun. Rev., vol. 38, no. 4, pp. 327338, 2008.

[13] M. Lad, D. Massey, D. Pei, Y. Wu, B. Zhang, and L. Zhang, PHAS: A prefix hijack alert system, in Proc. 15th Conf. USENIX Security Symp., vol. 15. 2006, article 11.

[14] J. Karlin, S. Forrest, and J. Rexford, Autonomous security for au-tonomous systems, Compute. Newt. vol. 52, no. 15, pp. 29082923, 2008.

Trishula Hajare received the B.E. degree in Information Technology from Annasaheb Dange Col-lege of Engineering and Technology Ashta,Sangali in 2011. During 2012-2013, she did lecturership in D.Y.Patil College of Engineering Akurdi,Pune. Now she is pursuing Master degree in Computer Engineering from D.Y.Patil College of Engineering Akurdi,Pune.

Dipalee A. Chaudhari received the BE degree in Computer Science and Engineering from University of Pune in 2000 and ME in Computer Engineering from University of Pune in 2010 and has 8 years of teaching experience. She is currently working as Assistant professor at D. Y. Patil College of Engineering, Akurdi, Pune.