3. Dotsenko N., Chumachenko D., Chumachenko I. Project-Oriented Management of Adaptive Commands Formation Resources in Multi-Project Environment // CEUR Workshop Proceedings, vol. 2353, 2019, Pp. 911–923.

4. Dotsenko N. Application of the donor-acceptor approach to resource providing in a multi-project environment //Transformational processes the development of economic systems in conditions of globalization: scientific bases, mechanisms, prospects: collective monograph / edited by M. Bezpartochnyi, in 2 Vol. / ISMA University. Riga: «Landmark» SIA, 2018. Vol. 1. 173. 181 p.

5. Комп'ютерна програма «Програма вирішення задачі забезпечення донорно-акцепторної ресурсної взаємодії в мультипроєктному середовищі» / Чумаченко І.В., Доценко Н.В.: Свід. Держ. реєстр. прав автора на твір № 81629. – Зареєстр. в Держ. департ. інтелектуальної власності Мін. освіти і науки України 21.09.2018 р.

DOI https://doi.org/10.30525/978-9934-588-79-2-1.7

TOPOLOGICAL APPROACH TO THE RISK ASSESSMENT AGAINST THE INTERNET ROUTE HIJACK CYBERATTACS

Zubok V. Yu.
Candidate of Technical Sciences (Ph.D),
Doctoral Student
Pukhov Institute for Modelling in Energy Engineering
of the National Academy of Sciences of Ukraine
Kyiv, Ukraine

Being the global network of networks, the Internet consists of millions of routers and billions of stub nodes. Approaching global connectivity through such large network requires effective and widely adopted solution which the routing protocol BGP-4 is. However it lacks many security requirements and can't provide in most cases data integrity and verification. There are proposed proactive mechanisms such as Resource Public Key Infrastructure (RPKI) [1]. It's part of the Internet Routing Registry system. This service provides a collective method to allow one network to filter another networks routes. Method begins with cryptographic signing the route origin. A Route Origin Authorisation (ROA) is a cryptographically signed object that states which AS is authorised to originate a certain prefix. A ROA contains three informational elements: the AS Number that is authorised, the prefix that may be originated from the AS, and the maximum length of the prefix. However such techniques are fully effective only in global deployment, and operators are reluctant to deploy them because of the associated technical and financial costs. For example, Telia, one of the Tier-I Internet backbone operators, announced that it's using RPKI for security in its internet routing infrastructure since only September, 2019.

In the face of the impossibility of reliable protection against damage associated with an attack, it is necessary to learn how to manage risks arising from cyberattacks on global routing. For this purpose we must use well-studied topological percularities of the Internet to find methods of routing attacks mitigation by aforehead improvement of the connections between Internet nodes.

Anti-hijack protection consists of two steps: detection and mitigation. RPKI mechanism with route origin validation is not sufficient to mitigate AS hijacking. An analysis of the mechanisms of the attack, depending on its objectives and options for its implementation is described in detail in [2]. Detection is mainly provided by third-party services such as BGPMon. They notify the network administrator of suspicious events related to their prefixes based on routing information. They track worldwide routes by tracing and keep track of route announcements in BGP. In the event of an incident, the affected networks begin to mitigate the consequences of the event, for example by announcing more specific prefixes to their networks or by requesting other ASs to filter out false announcements. There are some other studies which offer mechanisms for route attack detection such as ARTEMIS [3] and Peerlock [4]. However, due to the combination of technological and practical deployment issues, existing reactive approaches are largely inadequate. In particular, the most advanced technologies have the following major problems.

Distance is the parameter routing attacks are tampering. From a practical point of view, this means that if route is hijacked only if the distance through the fictitious route will be less than through the real route. Then let's find the formula of affecting the node with forged route. The task of finding the best route is complicated and non-linear. Therefore, the TCP/IP stack has adopted the so-called one-step approach to optimizing the packet route (next-hop routing) – each router and destination node only have to choose one step forward of packet transmission. A formal description of the Internet global routing objects and processes is described in [5]. Here are formulated the process of choosing a prefix $p(a)$ by destination IP address:

$$p(a) = \{\min_j(p_j) \; : \; a \in p \subset A, \;\; 0 < j \le |A|\} \text{,}$$

and then choosing a route with shortest path $\pi\,(p)$ among all available routes $m(p)$:

$$\pi_v(p) = \{\min_v(m_v(p)) : \pi \in M_p, v \in V_p\} \text{.}$$

For common case, we assume that our network is connected, that is, at least one route to any prefix is known at each node. If there are two or more of prefixes on a particular node u, BGP chooses one of them based on known criteria, the most important of which is path length. After that, this route is in use at this node, and will it be announced to neighboring nodes. If at some node two or more routes have the same path length, the decision will be made according to secondary criteria. After passing each transit node, the route is extended by 1 node.

Consider at this stage the case of intercepting a route without deaggregation. The hijack of prefix legitimately originated from node v, is that a spoofed route $\pi'(p_v)$ is announced to the network (typically from one particular node), competing with true route $\pi(p_v)$. In Figure 1, we can see that $\pi'(p_v)$ will obviously capture the nodes AS2 and AS3. On the other hand, AS4 and AS7 will receive a false route $\pi'(p_v)$ but it will lose to $\pi(p_v)$. These nodes will not pass it on to their other neighbors. In more complex topology we could see that on some hubs route hijack with initially one forged route can significantly increase number of competing routes on some network hubs.

In more complex topology we could see that on some hubs route hijack with initially one forged route can significantly increase number of competing routes on some network hubs. In our opinion, the most plausible way to model route distribution is method of cellular automation. However forged route leads to information risk only in two cases: (a) if it changes the route of IP packets through malicious node; (b) if it changes final destination of IP packets.

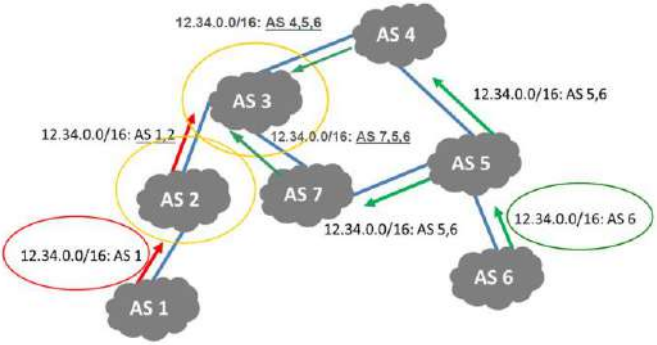

Fig. 1. AS1 performs hijack of the route to 12.34.0.0/16 belonging to AS6.

As described below, likelyhood of inequality $\pi'(p_v) < \pi(p_v)$ seen on particular node *u*, the more likely with increasing of $d(v,u)$. The extreme value of $d(v,u) = 1$ leads to impossibility to provide forged route $\pi'(p_v)$ through the node *u*. So this should also eliminate for node *v* the risk of data loss on node *u*.

It is easier to manipulate the path length if the path is longer. In the long way in the middle there are more nodes through which you can announce a forged route. Therefore, the probability *P* of interception between nodes *u*,*v* increases for distant nodes and decreases for close ones:

$$P(v,u) \sim d(v,u).$$

And also information losses increase with increasing number of affected nodes. $d(v,u)$ affects whether destination node *u* receives false of legitimate route. So does the risk, and we reasonably assume that risk is proportional to distance :

$$R_v \sim \sum_{i=1}^{|V|} d(v,u); \quad u \in V$$

The last expression is relative quantity of route hijack risk for node *v* regarding target group of network nodes *V*. One cannot prophet whether destination node *u* receives false of legitimate route since there no ways to see the BGP processes inside *u* in real time. But one can make subjective probability estimate. Let’s call it “trust”, while the subject of trust is probability that node *u* receives and uses (and further propagates) legitimate route to *v*. The value of trust T is a ratio of average distance between *v* and other nodes, and the distance between *v* and particular *u*:

$$T_u^v = \frac{\sum_i^{|AS|} d(u,i)}{d(u,v)(|AS|-1)} \;\; ; \; \{i,u,v\} \in AS \;\; ; \; u \neq v \; ; \; u \neq i$$

The risk depends on two components – loss and likelihood and the last one is much similar to probability. So we got a new mertrics for Internet nodes related to route protection.

If we express likelihood via trust, let’s express losses using number of nodes impacted by false routes due to route hijack. The more shortest paths $\pi(p_v)$ go through node *u* or prefixes originated by it, the more is impact of this node to routes distribution. This parameter is calculatable by BGP routing tables. Let’s call it “significance”:

$$S_v^u = |\pi_v(p)|$$

Using two metrics “trust” and “significance” we can build a model of route hijack risk based on 2-dimentional nodes distribution by trust and significance:

$$R^u = \frac{\sum_{i \neq u}^{|V|-1} S_i^u T_i^{u-1}}{|V|-1}$$

As a conclusion, using this model the route hijack risk mitigation will be associated with increased trust in the most significant nodes with topology improvement techniques. That is, a direct BGP interaction with the most significant and distant peers should be modeled to achieve acceptable risk level for risk owner.

References:

1. RIPE NCC’s Implementation of Resource Public Key Infrastructure (RPKI) Certificate Tree Validation [Online]. Available: https://tools.ietf.org/html/rfc8488. Accessed on: May 25, 2020.

2. Zubok, V.: Metric Approach to Risk Evaluation of Cyberattacks on Global Routing: Selected Papers of the XVIII International Scientific and Practical Conference “Information Technologies and Security” (ITS 2018). Vol-2318 urn:nbn:de:0074-2318-4.

3. P. Sermpezis. ARTEMIS: Neutralizing BGP Hijacking within a Minute / P. Sermpezis, V. Kotronis, et al. // arXiv:1801.01085v4 [cs.NI] 27 Jun 2018.

4. T. McDaniel. Peerlock: Flexsealing BGP / T. McDaniel, J.M. Smith, M. Schuchard // arXiv:2006.06576v3 [cs.NI] 17 Jul 2020.

5. V.Zubok. Building Formal Model of the Internet Routing for Risk Evaluation of Cyberattacks on Global Routing // CEUR workshop Processing. – Vol. 2577. – pages 292-301 [Online]. Avaliable: http://ceur-ws.org/Vol-2577/. Accessed on Aug 12, 2020.

DOI https://doi.org/10.30525/978-9934-588-79-2-1.8

СИСТЕМА ПІДТРИМКИ ЕЛЕКТРОННОЇ КОМЕРЦІЇ

Киричек Г. Г.
кандидат технічних наук, доцент,
доцент кафедри комп'ютерних систем та мереж
Національного університету «Запорізька політехніка»

Шавло Г. В.
магістр факультету комп'ютерних наук і технологій
Національного університету «Запорізька політехніка»
м. Запоріжжя, Україна

На даний час реалізація систем підтримки електронної комерції є одним з актуальних та перспективних напрямків онлайн-бізнесу. При впровадженні подібних систем можна застосувати системний підхід до проектування, почавши з моделювання окремих модулів системи та реалізації її інтерфейсів. При цьому інтерфейс визначає дані для зв'язку одного модуля системи з іншими [1].

Метою роботи є реалізація системи підтримки електронної комерції. Об'єктом дослідження є процес реалізації та забезпечення взаємодії окремих модулів системи. Предметом – моделі, методи та програмні засоби автоматизації основних процесів. Основними завданнями є визначення структури та окремих модулів системи; отримання загальної моделі; проведення аналізу, вибір методів і програмних засобів для реалізації обов'язкового функціоналу системи; тестування її роботи. В роботі, за основні методи та технології, обрано: метод керування вмістом WordPress з модулем WooCommerce; автоматизований сервіс