Investigation of a Secure Flow-Based Routing Model Using Information Security Risks

Maryna Yevdokymenko
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
marina.ievdokymenko@nure.ua

Anastasiia Shapovalova
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
anastasiia.shapovalova@nure.ua

Maryna Shapoval
V.V. Popovskyy Department of Infocommunication Engineering
Kharkiv National University of Radio Electronics
Kharkiv, Ukraine
shapoval.maryna@nure.ua

ABSTRACT

A study of an improved flow-based routing model taking into account information security risks using basic vulnerability criticality metrics is proposed. The novelty of the model allows for the introduction of weights into the traditional flow-based model of routing metrics that characterize the risks that are created by vulnerabilities on the network nodes and quantitatively reflect the notional cost of using communication links. The use of these weighting factors within the proposed routing model allows the transmission of packet flows along the most secure routes in the telecommunications network.

CCS CONCEPTS

• Applied Computing • Networks

KEYWORDS

Secure Routing, Security Risks, Vulnerability, Telecommunications Network

1 Introduction

Assessing the vulnerabilities of the telecommunications network (TCN) is a rather difficult task given the heterogeneity of network equipment and its software. Most often, this uses specialized hardware or software that scans the network to identify "vulnerabilities" in the security system and warns of risk areas in TCN [1-3]. In addition, various organizational standards and guidelines for the operation of firewalls and their security policies, as well as artificial intelligence methods can be used to assess security and risks in TCN [4]. One of the effective means of ensuring the protection of TCN is a preliminary information security risk assessment (SRA). SRA can be calculated using the vulnerability criticality metrics specified in the NIST CVSS v3 [5] recommendation: base metric, temporal and environmental metrics. One of the promising areas for assessing the security of TCN is the calculation of information security risks in combination with routing solutions, such as secure routing protocols. The solution of such a complex problem allows to respond adaptively to possible failures and attacks while limiting their negative consequences on the operation of the network, to protect critical elements of the network and its resources (links, nodes, routes). The purpose of this work is to investigate improved the mathematical model of secure routing, taking into account the vulnerabilities of network elements [6]. Within the proposed model for the calculation of weights (compromise weights), which are used to assess the risk posed by the use of vulnerabilities on the node of the TCN, selected basic metrics that, in contrast to temporal and environmental metrics, characterize time-invariant. Existing vulnerabilities on network elements allow to assess the risk of information security of the telecommunications network as a whole.

2 Investigation of the proposed secure flow-based routing model

The research of an improved flow-based routing model taking into account information security risks using basic vulnerability criticality metrics for confirmation of its operability, adequacy and efficiency of the received results of calculation is carried out.

The network consists of seven nodes (routers). The study also generated one packet flow, when the source node was router R_1, and the receiving node – router R_7. The intensity of the packet flow varied from 0 to 750 1/s. To calculate the weights $w_{i,j}$ used the following characteristics of vulnerabilities of network equipment, which are presented in table 1.

The results of solving the routing problem using the proposed model are shown in Fig. 1, in which the communication links with the highest critical weights are indicated in red color. The packet flow with an intensity of 200 1/s was transmitted by the route $R1 \rightarrow R4 \rightarrow R7$, which contained the least vulnerable communication links. When this route was overloaded, the rest of the flow (250 1/s) was transmitted in the following more vulnerable paths:

- $R1 \rightarrow R2 \rightarrow R4 \rightarrow R7$ with an intensity of 100 1/ s;
- $R1 \rightarrow R2 \rightarrow R3 \rightarrow R7$ with an intensity of 150 1/c.

It should be noted that the path $R1 \rightarrow R5 \rightarrow R6 \rightarrow R7$, which included the most vulnerable by weight communication links at an intensity of 450 1/s, was not used at all. The results of the study showed that in the framework of the improved flow-based model of secure routing with increasing packet flow intensity, the paths in

the TCN that included communication links with the lowest weights, i.e. had the least weight of discredit, were loaded first.

Table 1: Characteristics of network equipment vulnerabilities for research

TCN node	Router	Basic assessment BS_i^q	The probability of using a vulnerability P_i^q	Description of the vulnerability according to a specialized database	The criticality level of the vulnerability
R_1	Cisco RV325 Dual Gigabit WAN VPN Routers	7,5	0,3	CVE-2019-1653	High
R_2	Cisco RV042	5	0,2	CVE-2020-3291	Average
R_3	Cisco Small Business RV160W	9,8	0,5	CVE-2021-1289	Critical
R_4	D-Link DIR-817LW A1-1.04	7,6	0,4	CVE-2020-14098	High
R_5	Cisco RV260W	9,8	0,6	CVE-2021-1292	Critical
R_6	Juniper EX2300	5,8	0,4	CVE-2019-0002	Average
R_7	Xiaomi RM1800	5,5	0,2	CVE-2018-7100	Average

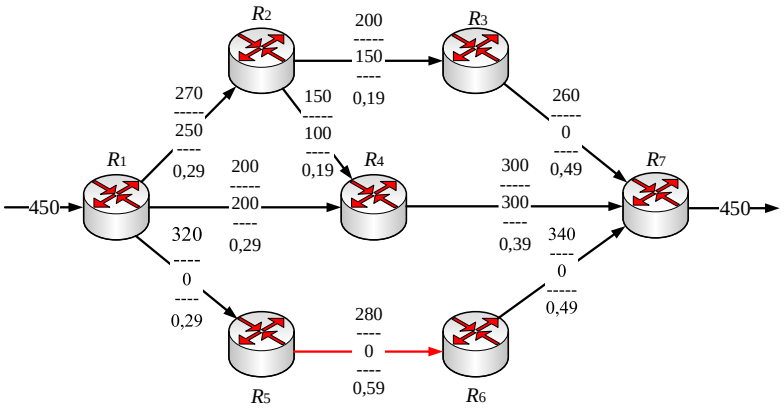

Figure 1: The studied fragment of the TCN.

The results of the study showed that in the framework of the improved flow-based model of secure routing with increasing packet flow intensity, first of all, those paths were loaded in the TCN, which included communication links with the lowest weights, i.e. had the least weight of compromise.

It should be noted that for the worst case scenario when using the vulnerability at the network node, i.e. with 100% compromise of the link with the highest weight, the gain of the improved model compared to traditional models at low network loads was 37%, in medium loads – 25% and gradually decreased. This is due to the fact that in the conditions of congestion all available paths in TCN are used, regardless of the weight of compromise of communication links.

3 Conclusion

An investigation of the improved secure routing flow-based model is proposed, considering information security risks using basic vulnerability criticality metrics. The results of the study showed that within the improved flow-based model of secure routing with increasing packet flow intensity, the paths in the TCN that contained communication links with the lowest weights. The use of the proposed secure routing model allows to calculate and use routes with minimal risk of information security, thereby ensuring the maximum level of network security to packets transmitted in TCN. The proposed approach to the formation of routing metrics can also be used to ensure comprehensive consideration in the process of solving routing problems, both network security indicators and service quality indicators.

REFERENCES

[1] Arnold J. Kelley, Dempsey R. Ross. 2012. *Guide for Security-Focused Configuration Management of Information Systems*, National Institute of Standards and Technology, 2012. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf.

[2] Santi Pattanavichai. 2017. Comparison for network security scanner tools between GFI LanGuard and Microsoft Baseline Security Analyzer (MBSA), *International Conference on ICT and Knowledge Engineering (ICT&KE): Proceedings of the 15th International Conference*, Bangkok. 1–7. DOI: 10.1109/ICTKE.2017.8259628.

[3] Thomas R. Peltier. 2005. *Information security risk analysis*, CRC press, 344 p.

[4] Karen A. Scarfone, Peter M. Mell. 2012. *NIST Special Publication 800-94 Revision 1 (Draft) Guide to intrusion detection and prevention systems (IDPS)*., National Institute of Standards and Technology, URL: http://csrc.nist.gov/publications/drafts/800-94- rev1/draft_sp800-94-rev1.pdf.

[5] Common Vulnerability Scoring System v3.0: Examples, Forum of Incident Response and Security Teams, URL: https://www.first.org/cvss/examples.

[6] Maryna O. Yevdokymenko, Anastaciia S. Shapovalova, Olena B. Voloshchuk, Anders Carlsson. 2018. Proactive Approach for Security of the Infocommunication Network Based on Vulnerability Assessment. Problems of Infocommunications Science and Technology (PIC S&T): Proceedings of the Fifth International Scientific-Practical Conference, Kharkov, Ukraine, 609–612. DOI: 10.1109/INFOCOMMST.2018.8632079.