A SDN-operated MEC node for network cybersecurity assurance

Teodor Buchner*,†, ISSA Fellow
*Warsaw University of Technology, Faculty of Physics, Warsaw, Poland, 0000-0003-0030-3194
†EXATEL S.A., Warsaw, Poland

***Abstract*—A concept of distributed system for collecting malicious traffic at its source and the idea of backpropagation of the attack-related data to the originating operator is presented. A basic construction of MEC enabled node SDNbox, capable of collecting cybersecurity evidence emerges as an essential part of the proposed system. The system of distributed nodes may be best orchestrated using SDN approach, and such a proposal is presented and discussed.**

***Index Terms*—SDN, cybersecurity, DDoS, MEC, SDNbox, orchestration,**

I. Introduction

A modern 5G ready optical network is a particularly complex telecommunication structure with several structures, layers, and nodes [1]. Structural complexity is followed by operational complexity, as parts of the network are under the governance of different commercial or state-owned actors. This operational complexity extends to the end users, as typically each UE being an end-point of RAN network belongs to a different individual.

With the advent of 5G [2] which will, as we all hope, introduce new business models, leading to further increase of UE-related (*User Equipment*) downlink and uplink traffic there is a need to address important security issues, which arise from successful scaling of network operations. Massive abuse traffic from a compromised UE is able not only to saturate the existing access network resources, performing a successful Denial of Service attack on the access network, but it is also able to saturate the backhaul optical network. This saturation requires synchronized traffic of thousands of nodes, which operate under central command as a botnet, controlled by a malicious actor [3], [4]. Such attacks have not only been demonstrated; they are frequent: a single botnet used to mount over 15.000 DDoS attacks in 5 months [3]. The potency of such a botnet is well illustrated by the number of infected nodes, which historically has reached at least 600.000 items of UE [3].

This addresses a need to integrate cybersecurity services in a much more responsible way than the one, which has been envisaged so far. Major of the standard network protocols in use have been designed with no inherent cybersecurity mechanisms, which established a popular assumption, that they are "insecure by design". This opens an attack surface, which may compromise, as already mentioned, not only the operation of an attack victim but also the infrastructure of an operator, whose resources are used to mount an attack.

As the connectivity globalizes, we have to cope with many issues of international scope, related to the identification of primary incident responders, picking the right jurisdiction, and separation of their duties. If e.g. a US citizen, who uses a UE produced by an international company and owned by another international company has his/her UE compromised while attending a conference in a non-EU country, due to vulnerability in firmware and this equipment is then used to mount a cyberattack against an EU-based network service, with the malicious traffic passing over the whole network infrastructure, the issue of picking the right primary incident handler and chain of incident responders is definitely a non-trivial task.

Network security assurance in the aforementioned conditions presents itself as particularly challenging. In order to achieve security, the right standards must be identified, the architectures must be designed and the right technologies for performing atomic tasks have to be developed, and finally, the right policies have to be enforced. The aim of this paper is to present an architecture of a distributed solution for securing the network against Distributed Denial of Service (DDoS) attacks [5].

II. Definition of Attack Surface and Scenario

The outline of the attack has been already sketched in Section I. Network traffic related to such an attack has been analyzed by many authors [3], [4]. A botnet operator mounts an attack, which is related to a tiny amount of traffic, composed of DNS queries and passing commands from a C2 center to infected UE.

Outbound traffic, originating from UE passes the whole network from attacking nodes to an attacked server. In the worst case, this may saturate the bandwidth of the datapath. Note, that we should not be misled by the idea, that the attacked server is located at some remote part of the network. One of the purposes of 5G development is to provide a sufficient QoS for the UE to become legitimate servers of microservices and accessibility of a single node may be crucial for global connectivity and business continuity [6]. And current adoption of the zero-trust philosophy in computer security shows, that the idea of an inherently safe network perimeter should be

This work was developed under project no. POIR.01.01.01-00-0787/17 co-financed by the European Union from ERDF funds under the Operational Programme Intelligent Development. Project implemented under the National Centre for Research and Development, Republic of Poland.

978-3-903176-44-7 © 2022 IFIP

abandoned [7]. Any attack, which saturates some bottleneck in network infrastructure affects the business continuity of all entities, which share the same physical resources.

III. Incident Response Handling Chain

Any DDoS attack is utilizing some application layer service. There are certain correlations in the outbound traffic of botnet nodes, however until they become aggregated, they do not present an apparent anomaly that could be filtered out using signature-based rules. If the source IP is spoofed, it may and should be filtered upon BCP38 [8]. However, from these considerations, it is clear, that unless the bandwidth of the datapath is saturated first, a primary incident responder is the one related to the perimeter of the attacked service. This incident responder is able to perform the forensics, and elicit the response related to end-point protection. Mitigation methods include Remotely Triggered Blackholing RTBH or offloading traffic: either by outsourcing the task to an external scrubbing center or utilizing on-premise services available to the attacked institution or business enterprise. It has to be noted, that the primary responder may only target the effect and not the cause, due to its distributed nature. However, it is quite clear, that excessive traffic deprived of a clear business function, apart from the business goals of a malicious actor, presents also a threat to the infrastructure of the network, which originates the traffic. This threat may result in saturation of bandwidth and outage, which will compromise the QoS of all customers of the attacked network. As bandwidth oversubscription is quite a common practice, a synchronized request for bandwidth may easily exceed the available resources. Therefore, information on a mounted attack should be propagated back the datapath to all originating networks, so that handling of the incident is holistic and the responsibility is propagated and shared among organizations. There are other good reasons for preventing malicious actors to abuse the UE within any network: the operator infrastructure may become a target of a subsequent attack, especially for the in-band management scheme [9], which is utilized by many commercial networks. The need for information exchange, including specific incident description and prevention has been expressed almost ten years ago [10]. Reports targeting specifically the LTE networks [11], SDN and virtual networks [12] as well as optical networks [13] have been published. However, for the time being, there seem to exist no efficient methods for backpropagation of attack forensics between network operators. Specifically, no protocol for announcing the request to block the offending traffic has yet been defined, and the whole communication is left to standard business methods of communication.

IV. Security Architecture for Intelligence-driven Incident Response Feedback Loop

From the above discussion it is clear, that in order to increase global network security and stability, a certain security architecture has to be introduced. Its goals may be defined as follows:

1) To allow upstream information flow between the operators, which could help the source AS to identify assigned IP addresses,
2) The identified IP should be tracked down to RAN and compromised UE should be identified,
3) The egress and ingress of an identified UE should be monitored and/or blocked, according to a specific policy, defined in a customer service agreement.
4) Forensics for a possible legal action should be collected and the legal owner of compromised equipment should be notified in order to enter the incident response procedure.

As the task of defining procedures, policies and inter-operator protocols for such a response are out of the scope of the current paper, here we will concentrate on the identification of crucial functional requirements, which have to be met in order to successfully enable the introduction of the architecture proposed above. We would only like to note, that if we treat the forensic data as a resource, being shared between operators, some propositions for inter-operator sharing of network resources have actually been proposed [14]. We may also expect that sharing data between operators may also be important for wide adoptions of such ideas as Multi Domain Edge Computing [15], Data-Driven Networks [16] or inter-operator blockchain network announced in 2020 by Deutsche Telekom, T-Mobile US, Telefonica, and Orange.

The most important role in the proposed security architecture is to be played by MEC node for cybersecurity assurance, the features of which we propose below.

V. Integrated Security Requirements for MEC node

Proper incident response must include collection of relevant evidence and a possibility to apply certain policy on a node traffic. For this purpose the offending traffic must be identified, labelled and either filtered or blocked. Each of these actions may be easily achieved with help of OpenFlow protocol on SDN-enabled node. Moreover Deep Packet Inspection process may be introduced in MEC node in order to provide local distributed foresight, which does not require offloading of the PDU outside the operators infrastructure. Therefore a set of requirements for the MEC node, with the corresponding priorization may be defined as follows:

TABLE I
Functional Requirements for MEC node.

Functional requirement	**MOSCOW**
MEC node should identify and label traffic	M
MEC node should report the amount of malicious traffic traffic	M
MEC node should offload PDU for DPI process	S
MEC node should block malicious traffic traffic	S

More functional requirements have to be defined concerning the network elements for forensics backpropagation data exchange; in order to be efficient, this data has to be secured, as it exposes the results of an attack, however here we concentrate only on the MEC node and its orchestration.

VI. SDN as an operating model for a security enhanced MEC node

Process of acquisition of malicious traffic shold not present a burden to the analyzed network. Therefore it is unacceptable to mirror the traffic and route it to a desired central node in order to analyze it, as this will actually increase the total network load. Therefore the system for analysis of malicious traffic has to be distributed. In order to orchestrate the process, which by definition is performed by network nodes of different geographic locations, an orchestration system has to be developed. This is the core of proposal of EXATEL, who develops a prototype of a network device in SDN philosophy. The product of this project, referred to as SDNbox, combines network operations, governed via OpenFlow v 1.4 with computational capabilities, acting as which allow to enable a Deep Packet Inspection system, such as Bro or Suricata. The data analysed by distributed nodes may be naturally collected by a SDN controller, which may aggregate the data and either store them locally or redirect them in a reduced form (by increasing information density) to a central location, where final evidence for the operator or law enforcement units is produced.

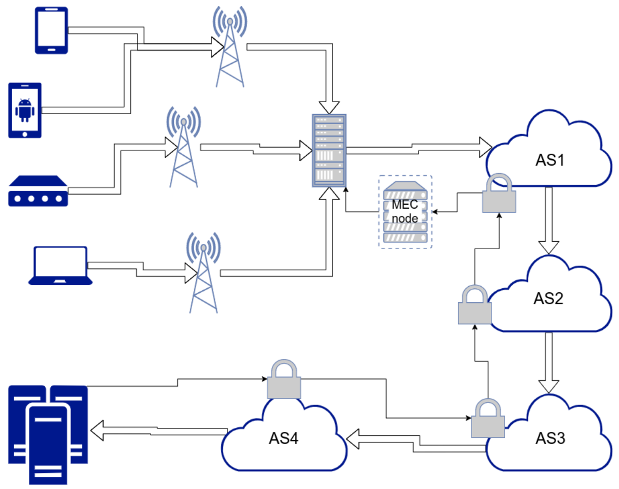

Fig. 1. Network architecture scheme. Datapath is denoted by thick line. Backpropagation of attack forensics denoted by thin line. Security data nodes at each operator denoted by a padlock. Malicious traffic from a compromised EU is a part of an attack on a third party server. Orchestration of MEC nodes is not included.

It is an open question how the forensics backpropagation process should be organized, however it is clear that all network operators will benefit from such a data exchange, which is an example of data driven approach.

VII. Conclusions

Cybersecurity fo information system is an important subject, which should not be left only to the attacked entities, which operate on individual basis. The efforts of operators have to be orchestrated in order to increase their own security level. We present a SDN-based, distributed system for aggregation of data on malicious traffic and discuss the reasons why the proposed action is necessary and what benefits can it bring to the operators. A concept of MEC-enabled telecommunication device SDNbox is preseted andd discussed and some of its most basic capablities are identified and prioritized.

References

[1] A. Tzanakaki, M. P. Anastasopoulos, and D. Simeonidou, “Optical networking: An important enabler for 5g,” in *2017 European Conference on Optical Communication (ECOC)*, 2017, pp. 1–3.

[2] J. Rodriguez, *Fundamentals of 5G Mobile Networks*. Wiley, 2015.

[3] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas, and Y. Zhou, “Understanding the mirai botnet,” in *Proceedings of the 26th USENIX Conference on Security Symposium*, ser. SEC’17. USA: USENIX Association, 2017, p. 1093–1110.

[4] G. Gallopeni, B. Rodrigues, M. Franco, and B. Stiller, “A practical analysis on mirai botnet traffic,” in *2020 IFIP Networking Conference (Networking)*, 2020, pp. 667–668.

[5] R. Doshi, N. Apthorpe, and N. Feamster, “Machine learning ddos detection for consumer internet of things devices,” in *2018 IEEE Security and Privacy Workshops (SPW)*, 2018, pp. 29–35.

[6] J.-Y. Kwak, S.-T. Kim, K. H. Lee, and S. Yang, “Service-oriented networking platform on smart devices,” *IET Communications*, vol. 9, no. 3, pp. 429–439, 2015. [Online]. Available: https://ietresearch.onlinelibrary.wiley.com/doi/abs/10.1049/iet-com.2014.0312

[7] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, “Zero trust architecture,” National Institute of Standards and Technology, Gaithersburg, MD, Tech. Rep. NIST Special Publication (SP) 800-207, 2020.

[8] P. Ferguson and D. Senie, “Network ingress filtering: Defeating denial of service attacks which employ ip source address spoofing,” Internet Requests for Comments, RFC Editor, BCP 38, May 2000, http://www.rfc-editor.org/rfc/rfc2827.txt. [Online]. Available: http://www.rfc-editor.org/rfc/rfc2827.txt

[9] J. Cao, L. Xiao, Z. Pang, K. Wang, and J. Xu, “The efficient in-band management for interconnect network in tianhe-2 system,” in *2016 24th Euromicro International Conference on Parallel, Distributed, and Network-Based Processing (PDP)*, 2016, pp. 18–26.

[10] C. Fachkha, E. Bou-Harb, and M. Debbabi, “Towards a forecasting model for distributed denial of service activities,” in *2013 IEEE 12th International Symposium on Network Computing and Applications*, 2013, pp. 110–117.

[11] J. Henrydoss and T. Boult, “Critical security review and study of ddos attacks on lte mobile network,” in *2014 IEEE Asia Pacific Conference on Wireless and Mobile*, 2014, pp. 194–200.

[12] J. F. Balarezo, S. Wang, K. G. Chavez, A. Al-Hourani, and S. Kandeepan, “A survey on dos/ddos attacks mathematical modelling for traditional, sdn and virtual networks,” *Engineering Science and Technology, an International Journal*, vol. 31, p. 101065, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2215098621001944

[13] S. Kumar and K. M. Carley, “Simulating ddos attacks on the us fiber-optics internet infrastructure,” in *2017 Winter Simulation Conference (WSC)*, 2017, pp. 1228–1239.

[14] X. Ting, P. Zhiwen, L. Nan, and Y. Xiaohu, “Inter-operator resource sharing based on network virtualization,” in *2015 International Conference on Wireless Communications Signal Processing (WCSP)*, 2015, pp. 1–6.

[15] V. K. Rathi, V. Chaudhary, N. K. Rajput, B. Ahuja, A. K. Jaiswal, D. Gupta, M. Elhoseny, and M. Hammoudeh, “A blockchain-enabled multi domain edge computing orchestrator,” *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 30–36, 2020.

[16] X. Li, Z. Wang, V. C. M. Leung, H. Ji, Y. Liu, and H. Zhang, “Blockchain-empowered data-driven networks,” *ACM Comput. Surv.*, vol. 54, no. 3, pp. 1–38, Jun. 2021.