Isolating Cross-Domain Links with SDN based E2E Network Slices

Niklas Fuhrberg
Kalsruhe Institute of Technology
niklas.fuhrberg@student.kit.edu

***Index Terms*—slicing, isolation, segmentation, SDN**

I. Introduction

Network slicing has been in the discussion as a tool to provide private connections between networks for some time [1], but now the rise of programmable and virtualized network resources makes a much more widespread use of slicing possible. In this project, we devise an architecture for cross-domain, isolated, and end-to-end network slices to provide private connections between distinct networks. We implement the architecture based on SDN in a testbed and will evaluate its feasibility, isolation, and security.

II. Background

Network slicing is the practice of splitting a physical and shared network into multiple logical networks. Each of these logical networks - the slices - is defined by the requirements of an associated service and a string of network functions providing the respective properties. For each type of service request, a new network slice instance is deployed [2]. This inherently requires the isolation of slice instances from each other and from underlying network resources. This isolation can be used to create private connections, not only for service categories, as is commonly discussed in the 5G context [3], but also for distinct devices or applications. Inside a domain, device or application based slicing can be used to enable micro-segmentation, isolating e.g. vulnerable IoT devices [4]. However, organisations that, for example, span multiple geographical regions, will use more than one internal network. Currently, micro-segments or 5G campus network slices would terminate at network boundaries, so in this project, we devise a network slicing approach to cross the network boundaries of multiple domains, providing continuous slicing from end to end. As such, slices need to be established across multiple domains, while keeping isolation, security, and the required Quality of Service guarantees of the local slices intact. The authors of [5] present a SDN based, hierarchical slice management approach for cross-domain slicing. They include a security management function to provide inter-domain access control, but do not extend intra-domain security aspects. Similarly, other research on multi-domain slicing has focused on deploying standard slice types across domains, instead of extending the properties of intra-domain slices. [6]

III. Concept

A. Exemplary Use-Case

As an example for a service utilizing this type of slicing, we propose a robot being remotely controlled from a different domain. The robots' control and video data have distinct requirements for their network: While video data need high bandwidth, occasional packet loss can be compensated. Control data on the other hand requires lower latency and can make the robot unsafe in case of tampering. A robot (2) in a trusted domain on one end will be remotely controlled with the necessary control components (1) in a second trusted domain on the other end. This includes both a unidirectional video stream and a bidirectional control / feedback stream. Both streams need to be passed through an untrusted domain. Due to its insecure nature, traffic in the untrusted network must be encrypted.

B. Architecture

A core part of network slicing is the orchestration, lifecycle management and deployment of slices [7]. To realize the slicing setup proposed above, we use the architecture described in Figure 1. The control components (1) are connected to a local endpoint (3a) to set up the slices. The endpoint requests a new slice from the E2E Slice Management Function (ESMF) (8) in its local network, which may then negotiate a specific slice configuration with the ESMF at the other end. The primary ESMF then communicates with the Domain Slice Management Functions (DSMF) (9-10) in each of the traversed networks to establish the slice in their respective domains. The DSMFs then decide on the necessary SDN configuration in their domain. The configuration is deployed to the SDN components (4-7), creating the actual slice instance. A secondary ESMF (8) may become necessary, when the control of the DSMFs in the remote domain is not permissible. In this case, both ESMFs negotiate which network capabilities will be provided. The ESMF is now responsible for the remaining lifecycle of the slice, i.e. any requested or necessary changes to the slice, including its termination, while the DSMFs handle their respective subslices in a similar manner.

IV. Approach

As a first step, we systematically analyse the threats to the described system using the STRIDE model to provide a foundation for later assessments of the security of our approach [8], i.e. considering what types of threats each

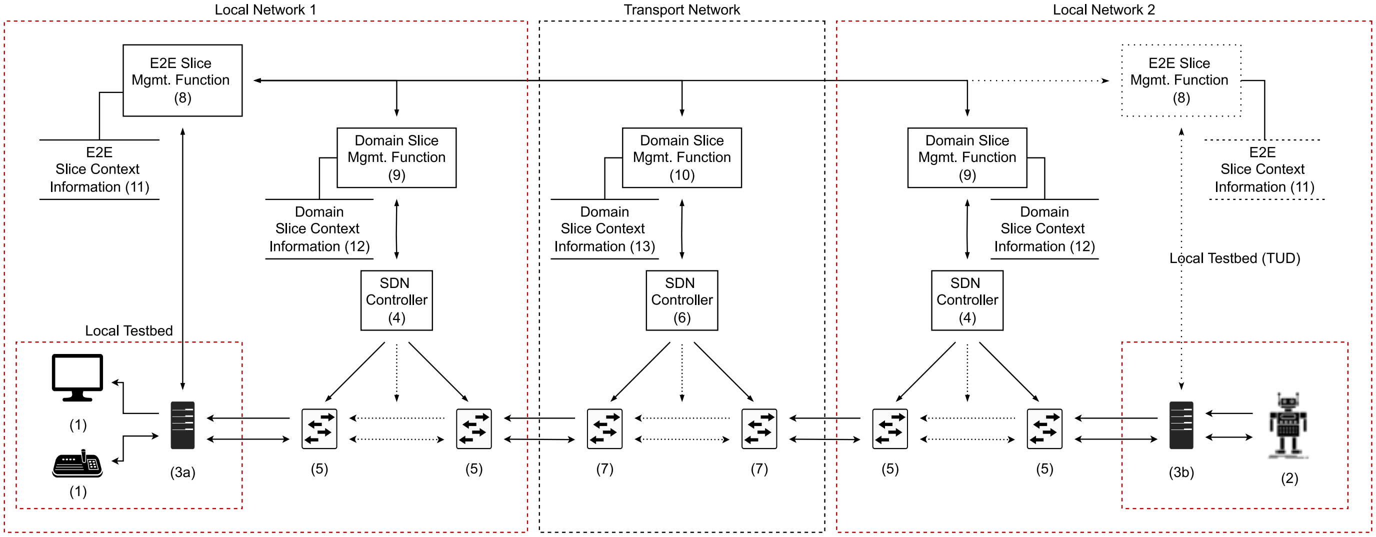
Local Network 1
Transport Network
Local Network 2
E2E Slice Mgmt. Function (8)
E2E Slice Context Information (11)
Domain Slice Mgmt. Function (9)
Domain Slice Context Information (12)
SDN Controller (4)
Domain Slice Mgmt. Function (10)
Domain Slice Context Information (13)
SDN Controller (6)
Domain Slice Mgmt. Function (9)
Domain Slice Context Information (12)
SDN Controller (4)
E2E Slice Mgmt. Function (8)
E2E Slice Context Information (11)
Local Testbed (TUD)
Local Testbed
(1)
(1)
(3a)
(5)
(5)
(7)
(7)
(5)
(5)
(3b)
(2)

Fig. 1. Proposed architecture for the management functions and underlying SDN setup to enable cross-domain network slicing

component of our architecture is facing. We will then create an adversary model based on the threats we find, defining the goals and capabilities of the adversary.

To allow for quick changes during the initial implementation, we will emulate the network components using Mininet. Mininet is a network emulation tool usable on limited hardware, that allows the quick and flexible deployment of realistic network functions [9]. In this step, we want to achieve a working implementation of the architecture (see Section 1) for management, orchestration, and deployment of slices as well as their isolation mechanisms. We will also consider measures for any further threats deemed critical in the threat analysis.

With the emulated components working as intended, we will start to move components from Mininet to a physical testbed. The testbed will at first consist of local servers and switches, as well as the control device, screen, and robot. We will later link up the local testbed to a similar testbed at another institution over an Internet Exchange Point. This allows us to test the slicing mechanisms in a more realistic environment, both physical and from a networking perspective. Here our goal is to prove the feasibility of our approach on actual heterogeneous hardware, including sufficient Quality of Service and a reasonably fast management of slicing. Lastly, we will empirically test the isolation and other security aspects of our approach based on the adversary and threat model. During this, we will gradually decrease assumptions made on the security and trustworthiness of the components.

V. Conclusion

Network slicing is a key technology for 5G networks, but the isolation property of slices can be utilized further. In this project, we propose an architecture for cross-domain slicing, i.e. connecting intra-domain slices in distinct domains via inter-domain slices with the same properties. We furthermore plan to build a slicing testbed and run experiments to empirically evaluate the feasibility, isolation, and security of the architecture. We would like to invite discussion both on the merit of this slicing applications as well as our approach to implement and test it.

References

[1] S. Gutz, A. Story, C. Schlesinger, and N. Foster, "Splendid isolation: A slice abstraction for software-defined networks," in *Proceedings of the First Workshop on Hot Topics in Software Defined Networks*, ser. HotSDN '12, Helsinki, Finland: Association for Computing Machinery, 2012, pp. 79–84, ISBN: 9781450314770. DOI: 10.1145/2342441.2342458. [Online]. Available: https://doi.org/10.1145/2342441.2342458.

[2] F. Debbabi, R. Jmal, and L. Chaari Fourati, "5g network slicing: Fundamental concepts, architectures, algorithmics, projects practices, and open issues," *Concurrency and Computation: Practice and Experience*, vol. 33, no. 20, 2021, ISSN: 1532-0626. DOI: 10.1002/cpe.6352.

[3] S. Zhang, "An overview of network slicing for 5g," *IEEE Wireless Communications*, vol. 26, no. 3, pp. 111–117, 2019, ISSN: 1536-1284. DOI: 10.1109/MWC.2019.1800234.

[4] A. Osman, A. Wasicek, S. Köpsell, and T. Strufe, "Transparent microsegmentation in smart home IoT networks," in *3rd USENIX Workshop on Hot Topics in Edge Computing (HotEdge 20)*, USENIX Association, Jun. 2020. [Online]. Available: https://www.usenix.org/conference/hotedge20/presentation/osman.

[5] V. Theodorou, K. V. Katsaros, A. Roos, E. Sakic, and V. Kulkarni, "Cross-domain network slicing for industrial applications," in *2018 European Conference on Networks and Communications (EuCNC)*, IEEE, 2018, pp. 209–213, ISBN: 978-1-5386-1478-5. DOI: 10.1109/EuCNC.2018.8443241.

[6] D. Alotaibi, "Survey on network slice isolation in 5g networks: Fundamental challenges," *Procedia Computer Science*, vol. 182, pp. 38–45, 2021, ISSN: 18770509. DOI: 10.1016/j.procs.2021.02.006. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050921004701.

[7] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Network*, vol. 33, no. 5, pp. 242–252, 2019, ISSN: 0890-8044. DOI: 10.1109/MNET.2018.1800267.

[8] D. Sattar, A. H. Vasoukolaei, P. Crysdale, and A. Matrawy, "A stride threat model for 5g core slicing," in *2021 IEEE 4th 5G World Forum (5GWF)*, 2021, pp. 247–252. DOI: 10.1109/5GWF52925.2021.00050.

[9] B. Lantz and B. O'Connor, "A mininet-based virtual testbed for distributed sdn development," in *Proceedings of the 2015 ACM Conference on Special Interest Group on Data Communication*, S. Uhlig, O. Maennel, B. Karp, and J. Padhye, Eds., New York, NY, USA: ACM, 2015, pp. 365–366, ISBN: 9781450335423. DOI: 10.1145/2785956.2790030.