Secure Software-Defined Federated Networks

Alvaro A. Cardenas, Assistant Professor
University of Texas at Dallas

As described in the DoE ASCR Intelligent Network Infrastructure Workshop Report [1], while SDNs and virtualization will make the network more agile and flexible, they will also open up new attack vectors for malicious actors. Traditional routers already have a myriad of software vulnerabilities and exploitable bugs; however, attacks to these devices has been limited, because for attackers, they have limited value [2]. Now with the advent of software-controllable network devices, network infrastructure will become more attractive targets for attackers. The key opportunity however, is that SDNs are still in an early stage of development, and security components and technologies can be included as a native part of the transition.

While SDN security has been a growing area of interest (e.g. [3, 4]), most of this research has focused on enterprise networks with a single domain where the SDN controller has total control, and on Ethernet-based networks. On the other hand, Multi-domain networks and federated infrastructures, where SDN controllers can only control sub-domains of a larger distributed controlled infrastructure provide new security and fairness challenges that are unexplored. For example, in a federated multi-domain network untrustworthiness does not only come from internal users and applications; it also comes from peering networks. SDN Exchange Points (SDX) and other peering technologies need to be enhanced with security mechanisms to address multi-domain SDN service provisioning.

SDNs are not necessarily more vulnerable; in fact, they also provide new opportunities for defenses. Previous work on survivability against failures or even catastrophic disasters does not take into account failures due to malicious attacks. For example over-provisioning resources assuming independent failures may work well against random faults, but will not survive attacks by a strategic adversary who knows the architecture of the network. One particularly new functionality SDNs enable is the dynamic reconfiguration and provisioning of network resources. This flexible reconfiguration can be used to dynamically reconfigure the network periodically, thus limiting the information an attacker has at any given moment. This periodic reconfiguration of the network is thus a moving target defense that increases the resiliency of specific network paths against targeted attacks. We will also leverage our experience in network intrusion detection to monitor for suspicious flows and dynamically reconfigure the network accordingly to the specific suspicious activity.

References

[1] "Report of DOE ASCR intelligent optical network infrastructure workshop," August, 2014.

[2] D. Kharitonov and O. Ibatullin, "Extended Security Risks in IP Networks," *ArXiv e-prints*, Sep. 2013.

[3] S. Shin, P. Porras, V. Yegneswaran, M. Fong, G. Gu, and M. Tyson, "Fresco: Modular composable security services for software-defined networks," in *Proceedings of Network and Distributed Security Symposium*, 2013.

[4] S. Shin, V. Yegneswaran, P. Porras, and G. Gu, "Avant-guard: Scalable and vigilant switch flow management in software-defined networks." in *20th ACM Conference on Computer and Communications Security (CCS13)*, 2013.