Exploring Security and Mobile Operator Use Case for SDX

Z. Morley Mao, (zmao@umich.edu), University of Michigan

There are three topics I would like to discuss at the workshop: (1) SDI/SDX for security management, (2) SDX design for mobile service operators, (3) Applying formal techniques to ensure isolation of SDN apps running at SDX. Each topic has some unique requirements and challenges on the testbed infrastructure but can be addressed with both design and engineering effort.

SDI/SDX for security management: SDX/SDI located at the Internet Exchange Points present as an interesting opportunity for enabling information sharing, especially for the purpose of supporting cooperative security management, e.g., to push back DDoS attack traffic sources to realize the goal of aggregate pushback. The peering agreements essentially constitute a contract between networks. We propose to include SLAs related to security properties of the traffic as part of these agreements, specifying assurance such that no malicious traffic (based on some definitions) should be exchanged for the purpose of harming the end-hosts. Resource-based DoS attacks are just one such example, where throttling the upstream sources with the help of neighboring ISPs is essential. We will also explore other types of security properties that can be achieved collaboratively by tracking data flows within and across networks with the help of SDN support at the switches to mark and measure traffic. One such property would be guarantees of data privacy following pre-defined security policies of data access in the form of information flow control. Going a step beyond the current functionality of SDX of applying traffic forwarding policies satisfying peering agreements, the SDX controller can also interface with the other SDN controllers in the corresponding network to influence their traffic management policies in response to identified security attacks through data exchange among the SDXes. Finally, cooperating SDXes may help defend against global network threats such as fast-spreading worms. The relevant experimental infrastructure support for this work includes realistic IXP traffic patterns and the SDX controller and switch support to evaluate the diverse security policies for various network attack models.

SDX design for mobile service operators: The structure of IXPs has been undergoing significant changes recently with more networks peering at public IXPs. Some IXPs (e.g., AMS IXP) are offering mobile peering services that support global data roaming and may also facilitate the operations of MVNOs. It remains to be seen how SDX should offer specialized services for mobile networks, as they have different requirements because of more scarce radio network resources and user mobility/roaming support. Mobile networks also tend to have more specialized network topologies, which are typically organized in a more hierarchical fashion compared to their wired Internet ISP counterpart. Such unique topologies have lead to more limited peering locations between the mobile ISP backbone and their peering ISPs. We propose to investigate how SDX can offer peering services specific for mobile ISPs or more generally perform application-specific customization of network policies to help efficiently manage network resources. MVNOs also impose new challenges on how to globally balance traffic across networks. Cellular networks themselves are also increasingly adopting SDN technology; thus, the interaction between the SDX controller and SDN controller of the cellular backbone network can offer opportunities for new functionality. To effectively evaluate this, we need to emulate various cellular network components, including MME, SGSN, GGSN and associated signaling protocols and network management functionality (e.g., PCRF) for comparison. Realistic mobile user traffic would be helpful to illustrate the benefit of the architecture.

Applying formal techniques to ensure isolation of SDN apps running at SDX: Multiple SDN applications running on the same controller, e.g., the SDX controller can lead to conflicts in terms of how they want to modify the underlying network, e.g., rules in the flow table or the forwarding behavior of switches. We plan to investigate the use of formal techniques (e.g., model checking, compiler techniques with provable properties) to build a framework to ensure the isolation properties between SDN apps.