ILLINOIS TECH

College of Computing

An Attestation Capable Programmable Software Switch on FABRIC

Alexander Wolosewicz, Nishanth Shyamkumar , Nik Sultana

Introduction

- Programmable networking elements provides great flexibility on the dataplane.
- But it also creates new risks of misconfiguration and of attacks that dynamically modify security-critical functionality.
- Using **Remote Attestation** techniques we can enable dynamic assessment of network security and configuration characteristics.
- We can create RA policies for programmable networks that specify the generation, collection and evaluation of **evidence of network program and control plane rules integrity**.
- By utilizing such policies network elements in a programmable network can participate in proving their own **trustworthiness**.

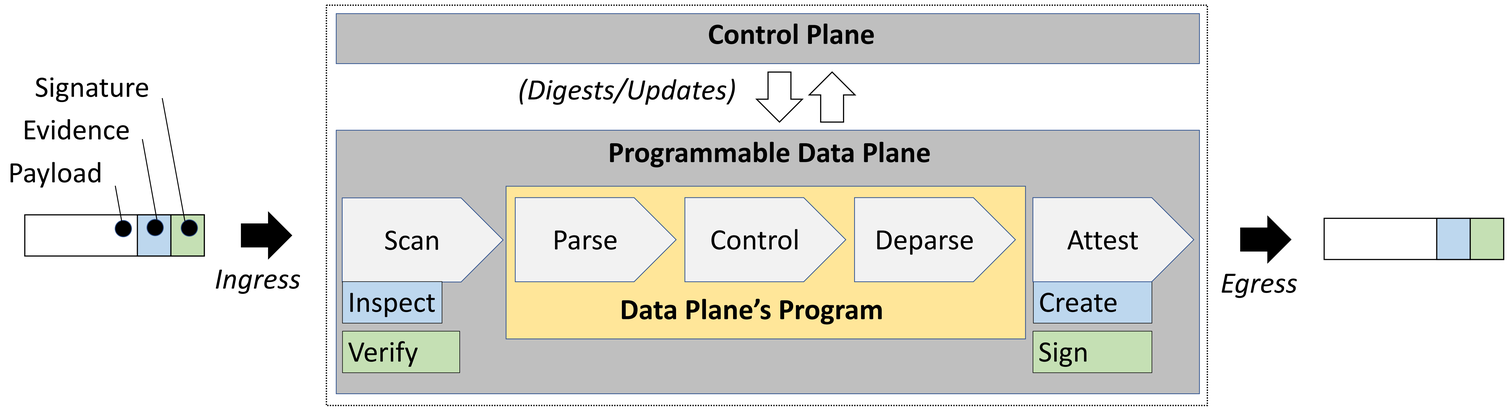
Motivation

1) Configuration transparency of programmable networking elements in a federated testbed.

2) Using configuration transparency for improved diagnostic ability, and reproducibility of research.

Acknowledgement

Our collaborators Ben Ujcich (Georgetown University) and Deborah Shands (SRI Intl), Vinod Yegneswaran (SRI Intl), and Ashish Gehani (SRI Intl).



Approach

- Define security primitives (state elements) that generate evidence of programmable device's dynamic working state.
- Evidence consists of **md5 hash digests** for switch and path state.
- Evidence is transported using **IPv6 Hop by Hop Extension Headers** and ultimately checked by the verifier.
- We extend a programmable network element (**BMv2 switch**) to accommodate our Remote Attestation implementation.
- Conduct verification and performance tests to confirm the working of the programmable element as an attester.

Results

- We display the evidence of the switch STATE and PATH evidence using the command line to query the switch.
- We compare it with the HBH header as seen at the receiver and verify that the state values have been transmitted successfully and correctly.

(Evidence seen from the control plane)

```
RuntimeCmd: get_ra_data
Registers: D41D8CD98F00B204E9800998ECF8427E
Tables: 083908AB3929001D4F94CDC290DC6C53
Program: 99914B932BD37A50B983C5E7C90AE93B
```

(Evidence seen from the data plane)