The Center for Cyber Defenders
Expanding computer security knowledge

A Platform for Developing and Evaluating Security Apps in Software Defined Networks

Isaac Polinsky, North Carolina State University

Project Mentors: David Burton, Org. 5832; Steven Elliott, Org. 5834;
Sherry Gaines, Org. 5838; Tom Tarman, Org. 5824

Problem Statement

Software Defined Networking (SDN) is an emerging paradigm redefining how we manage and monitor networks. P4[1] was introduced as a portable high-level language for processing packets, independent of their protocol, and allows for much more flexibility in how we control the network. Due to the infancy of these technologies, there exists no efficient method for developing and evaluating novel security applications of P4 applications.
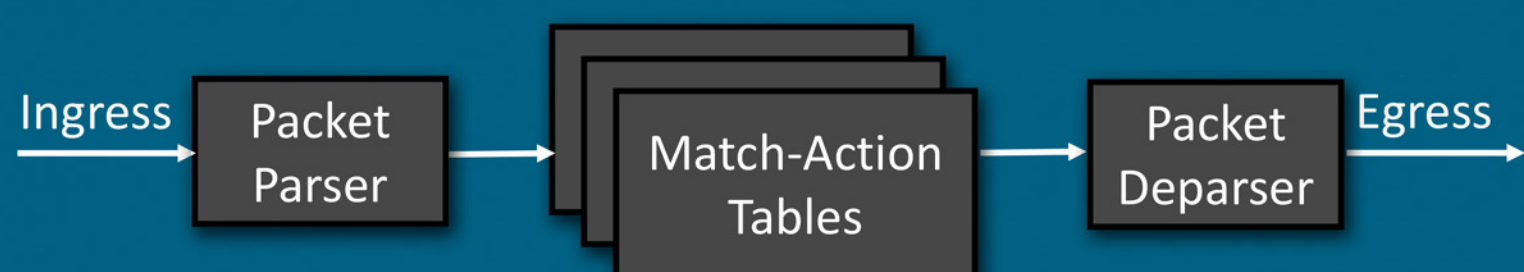

Figure 1: P4 packet processing pipeline
As depicted by Shahbaz et. al[2]

Objective:

In this work we aim to evaluate the network performance overhead and the efficacy of P4 security functions by developing a platform to rapidly prototype and evaluate P4 applications.

```
header_type tcp_t {
  fields {
    srcPort : 16;
    dstPort : 16;
    seqNo : 32;
    ackNo : 32;
    dataOffset : 4;
    res : 4;
    flags : 8;
    window : 16;
    checksum : 16;
    urgentPtr : 16;
  }
}
```

Figure 2: Example P4 protocol parser definition

Approach

Integrate PISCES[2] P4 capable software switch into Sandia National Laboratories' Firewheel network emulation platform[3].
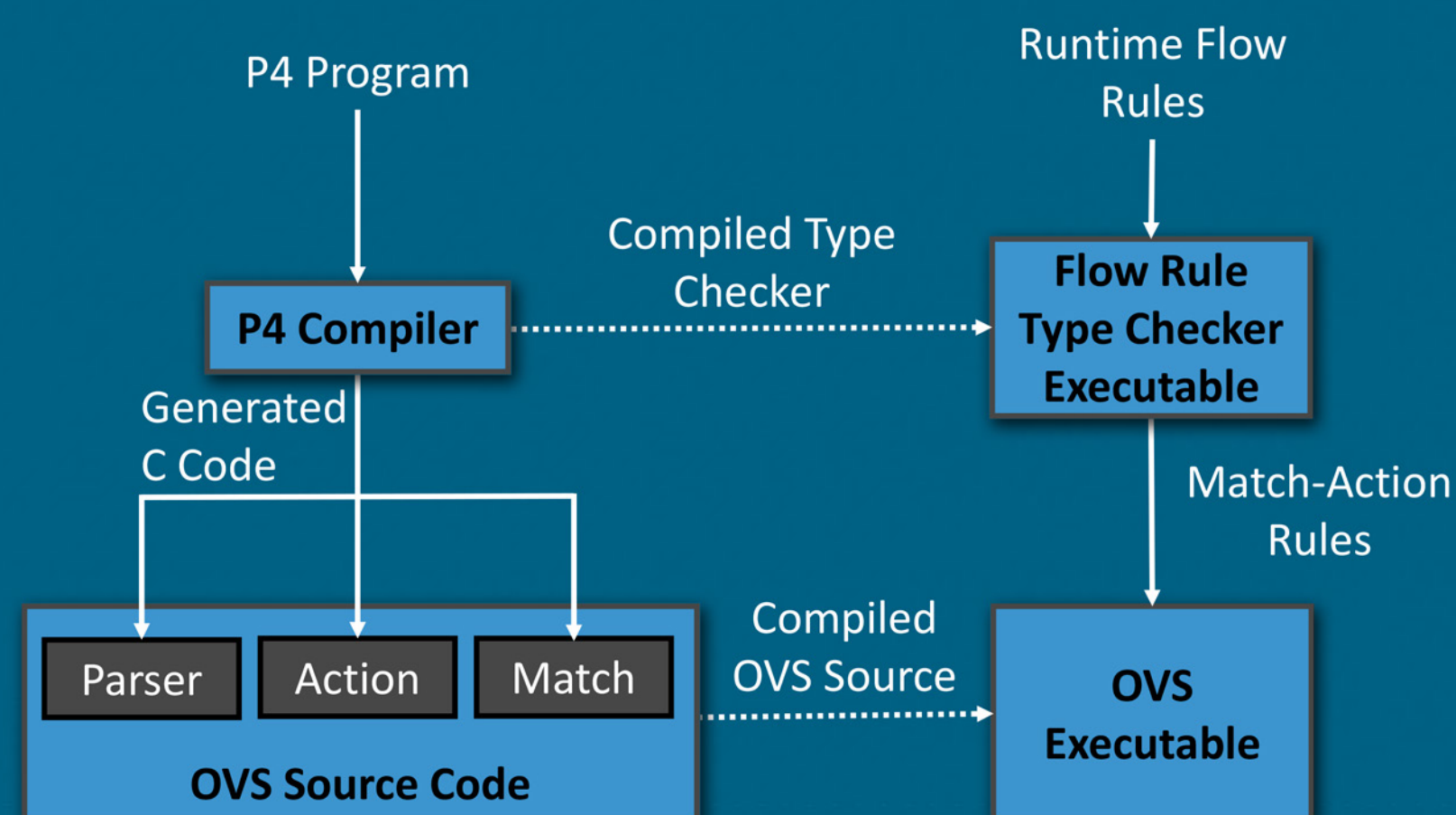

Figure 3: PISCES Architecture Overview
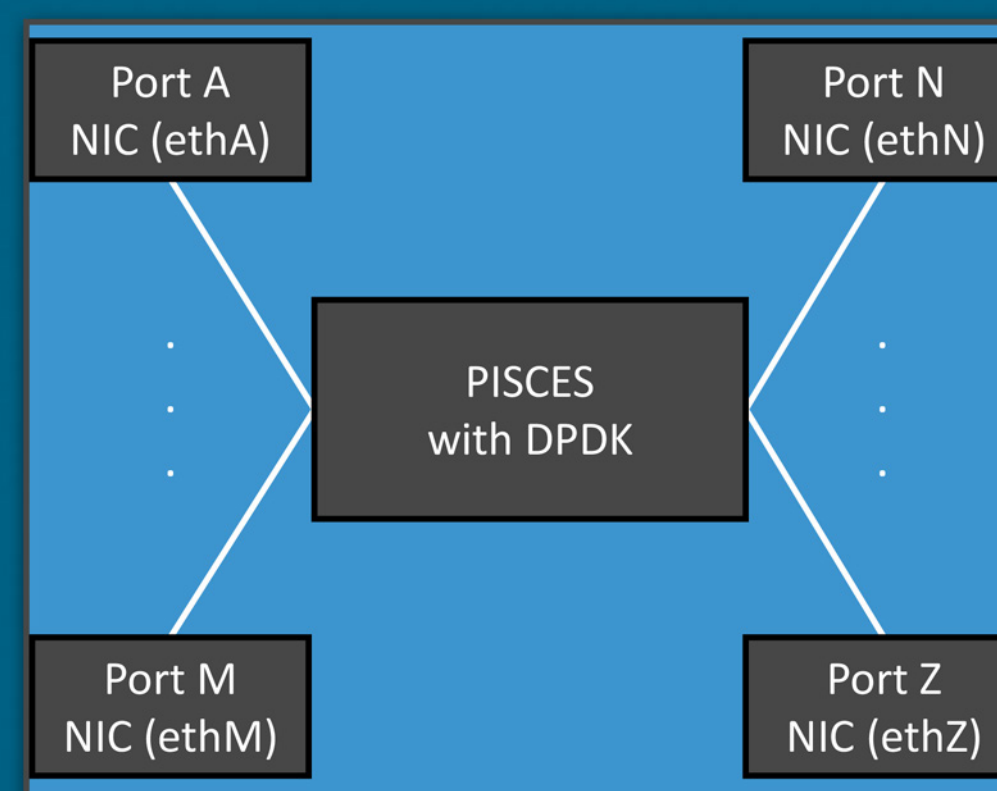Adapted from Shahbaz et. al[2]

Figure 4: PISCES software switch implemented in Firewheel with Z ports.

Impact and Benefits

I.   Rapid production for P4 applications.

II. Programmatically create a reproducible SDN environment without knowledge of system internals.

III. Our future work will use this platform to create and evaluate network security functions written as P4 applications.

[1] P. Bosshart, D. Daly, G. Gibb, M. Izzard, N. McKeown, J. Rexford, C. Schlesinger, D. Talayco, A. Vahdat, G. Varghese, and D. Walker. P4: Programming Protocol-independent Packet Processors. ACM SIG-COMM CCR, July 2014.

[2] M. Shahbaz, S. Choi, B. Pfaff, C. Kim, N. Feamster, N. McKeown, and J. Rexford. Pisces: A Programmable, Protocol-independent Software Switch. AT&T Research Academic Summit, Bedminster, NJ, USA, 2016

[3] http://www.sandia.gov/emulytics/

Sandia National Laboratories

U.S. DEPARTMENT OF ENERGY

NNSA National Nuclear Security Administration