Cybersecurity (Security+) and P4 Programmable Switches Workshop

Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

Instructors / Presenters

Jorge Crichigno
Professor, CEC - USC

Elie Kfoury
PhD student, CEC - USC

Ali AlSabeh
PhD student, CEC - USC

Jose Gomez
PhD student, CEC - USC

Agenda and Materials

- Workshop Agenda and Materials:

http://ce.sc.edu/cyberinfra/workshop_2023_wast.html

- Virtual lab libraries:

http://ce.sc.edu/cyberinfra/cybertraining.html

Cybersecurity (Security+) and P4 Programmable Switches Workshop

Motivation for Cybersecurity Training

Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

Introduction

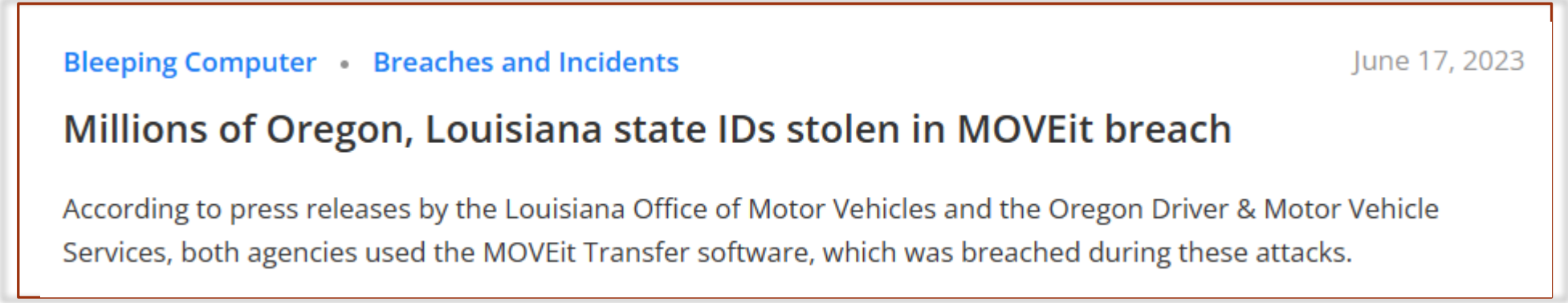
- Widespread attacks on desktops, laptops, smartphone, tablets, servers, etc.
- Information security is focused on protecting electronic information of organizations and users

Introduction

- Widespread attacks on desktops, laptops, smartphone, tablets, servers, etc.
- Information security is focused on protecting electronic information of organizations and users

Introduction

- Widespread attacks on desktops, laptops, smartphone, tablets, servers, etc.
- Information security is focused on protecting electronic information of organizations and users



Bleeping Computer • Breaches and Incidents June 17, 2023

Millions of Oregon, Louisiana state IDs stolen in MOVEit breach

According to press releases by the Louisiana Office of Motor Vehicles and the Oregon Driver & Motor Vehicle Services, both agencies used the MOVEit Transfer software, which was breached during these attacks.

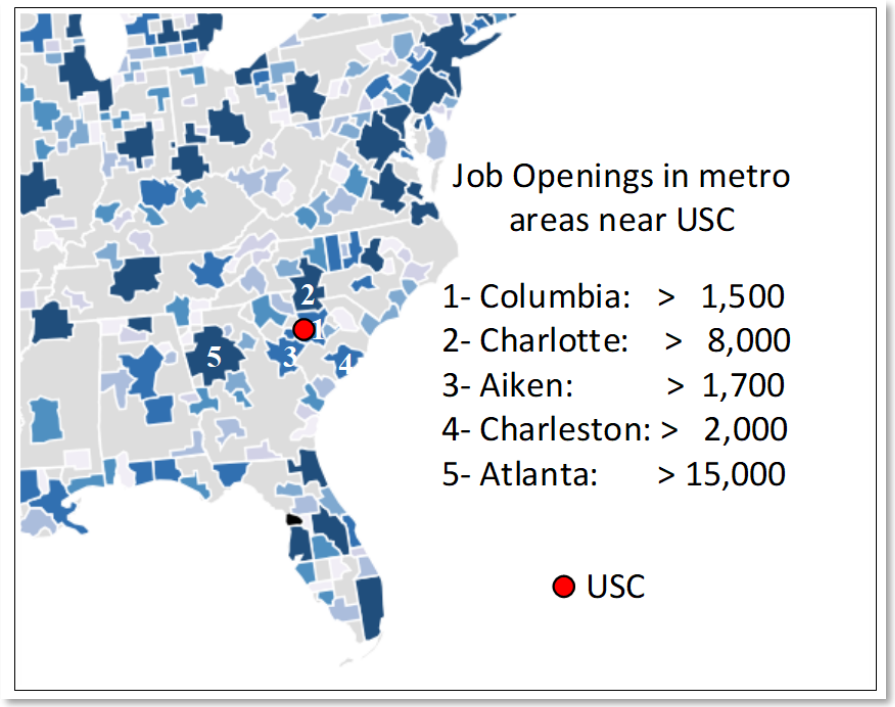
Information Security Employment

- Security is rarely outsourced
- Job outlook is exceptionally strong
- U.S. Bureau of Labor Statistics (BLS)
  - “Occupational Outlook Handbook” indicates job outlook for information security analysts through end of decade expected to grow by more than 32%, much faster than average

Information Security Employment

- Security is rarely outsourced
- Job outlook is exceptionally strong
- U.S. Bureau of Labor Statistics (BLS)
  - "Occupational Outlook Handbook" indicates job outlook for information security analysts through end of decade expected to grow by more than 32%, much faster than average

https://www.cyberseek.org/



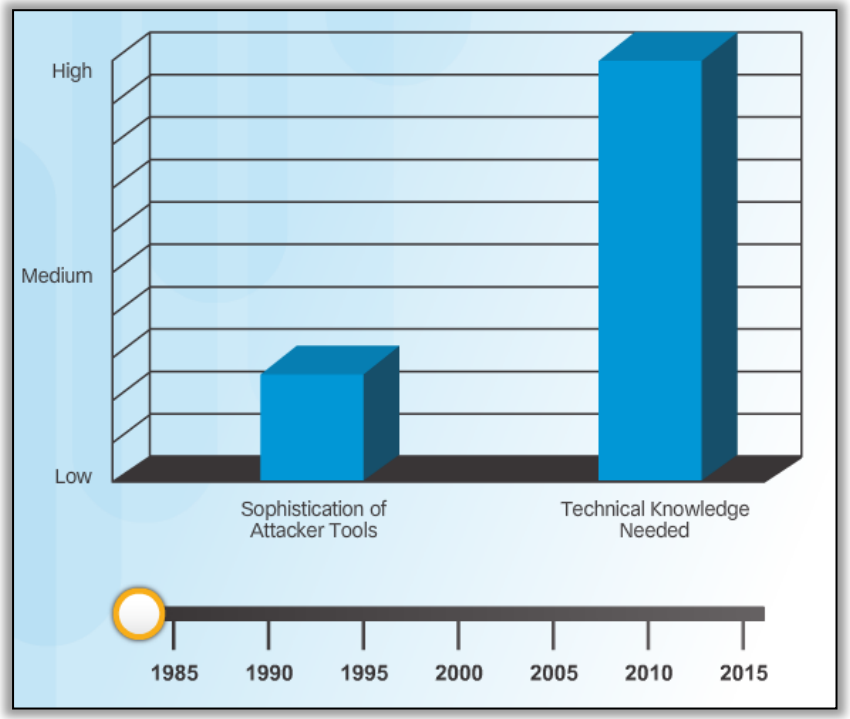
Today's Security Attacks

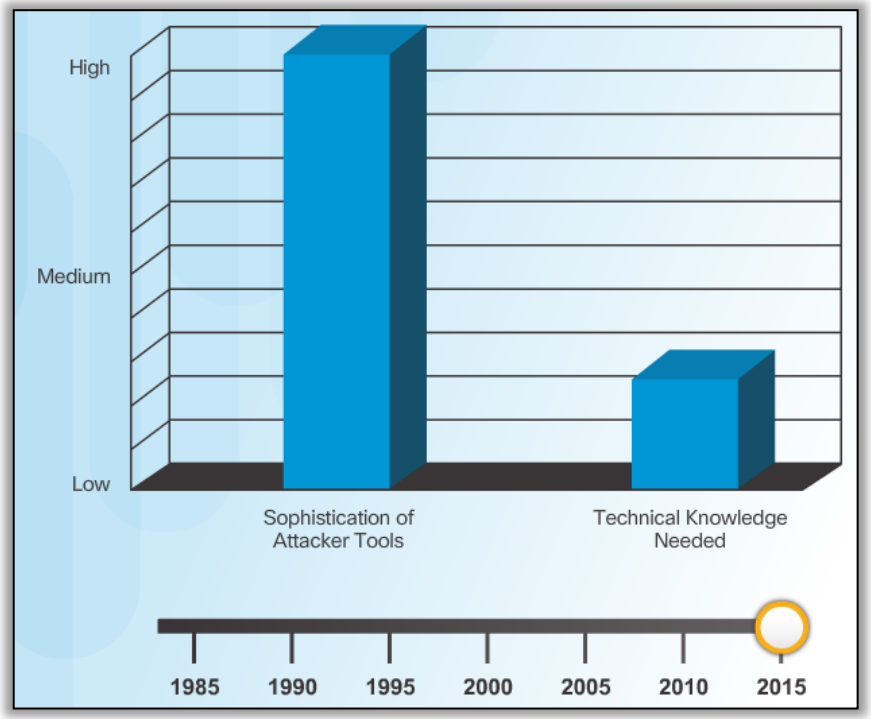
- Balances manipulated on prepaid debit cards (intrusion)
- Twitter accounts exploited
- ATM malware
- Aircraft manipulation
- Computer cluster for cracking passwords
- Electronic data records stolen

⋮

Attack Tools Sophistication

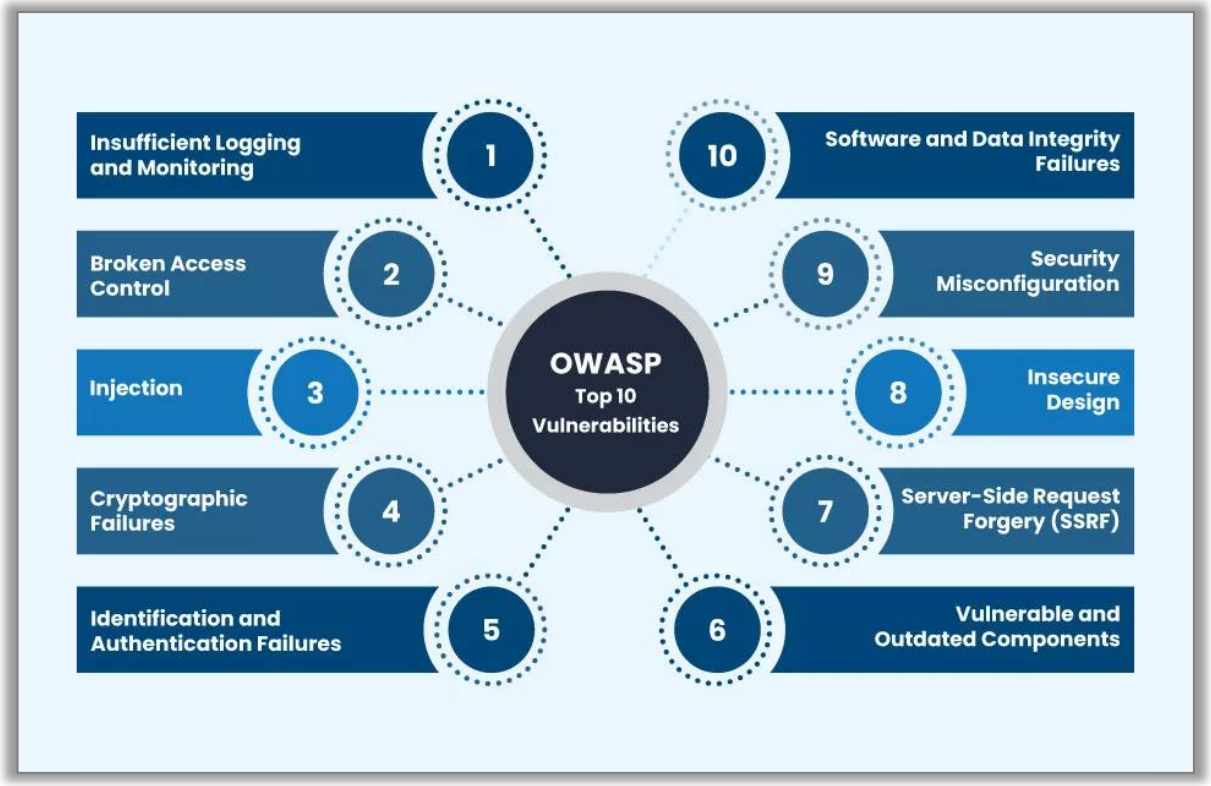
- Script kiddies
  - Unskilled users; goal: breaking into computers (damage)
  - Download automated hacking software (scripts)
  - Attack software today has attack capabilities that are even easier for unskilled users; ~40% of attacks performed by script kiddies





Information Security Terminology: Vulnerability

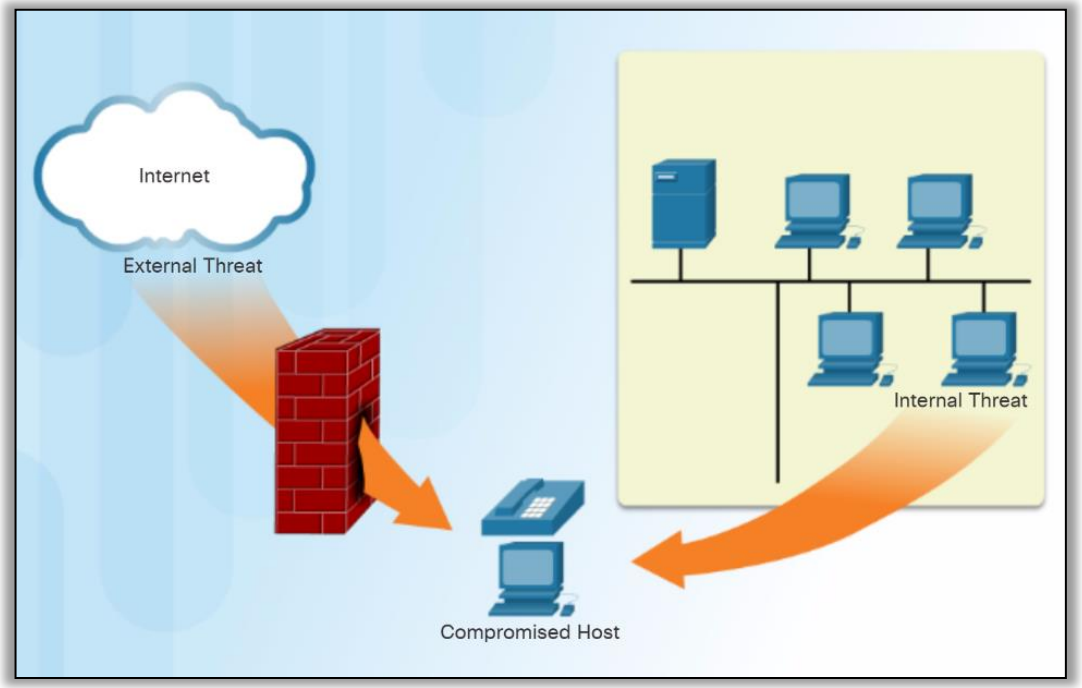
- Vulnerability is a weakness that allows a threat agent to bypass security
- A software defect that allows an unauthorized user to gain control of a computer



Open Worldwide Application Security Project (OWASP)

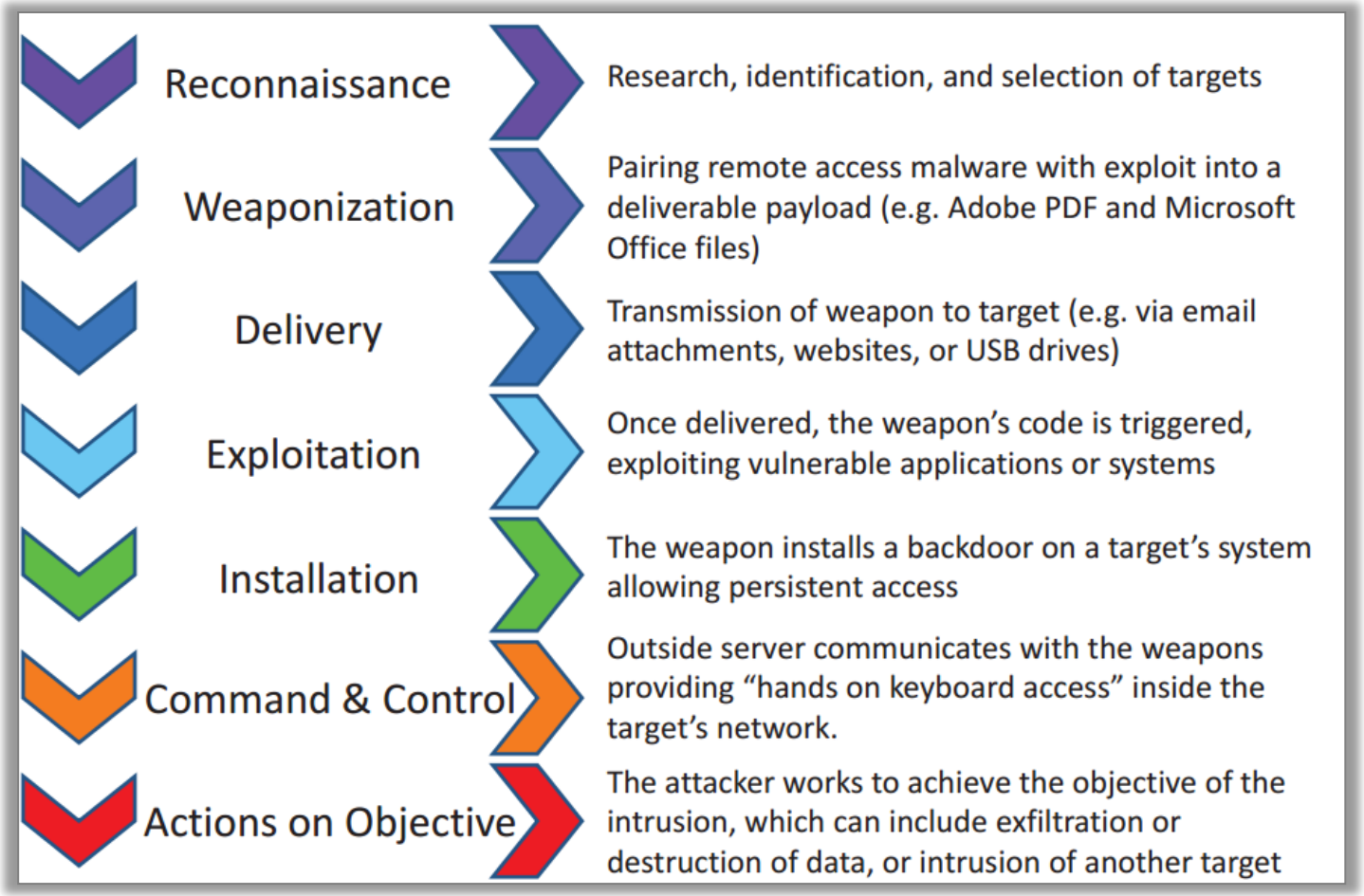
Information Security Terminology: Threat Vector

- A threat vector is a path by which an attacker can gain access to a server, host, or network
  - For example, an attacker, knowing that a web server's OS has not been patched, can use the threat vector (exploiting the vulnerability) to steal user passwords
- Web - fake sites; email – links, attachments



Steps of an Attack

- Cyber kill chain model



Cybersecurity (Security+) and P4 Programmable Switches

Motivation for P4 Programmable Switches

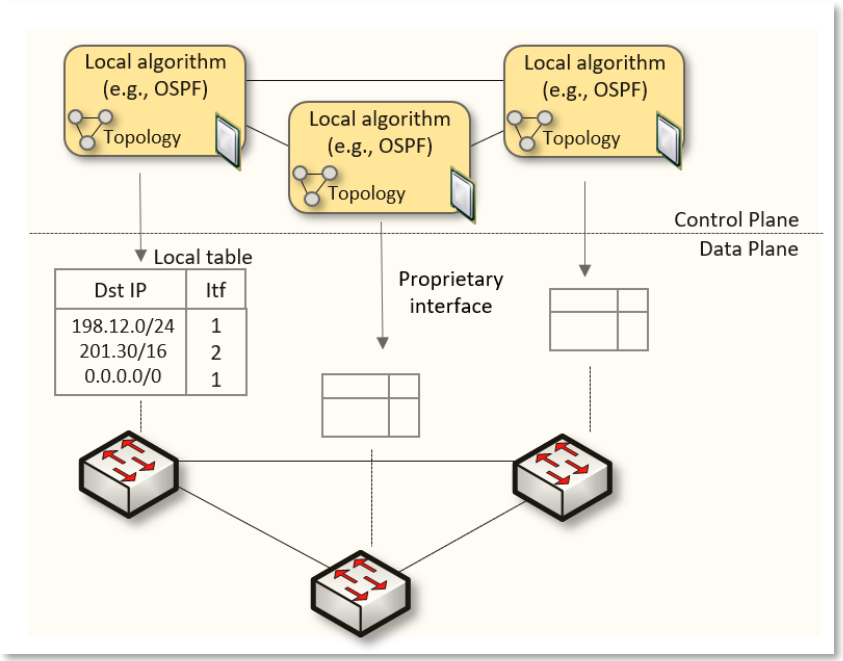
Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 19th, 2023

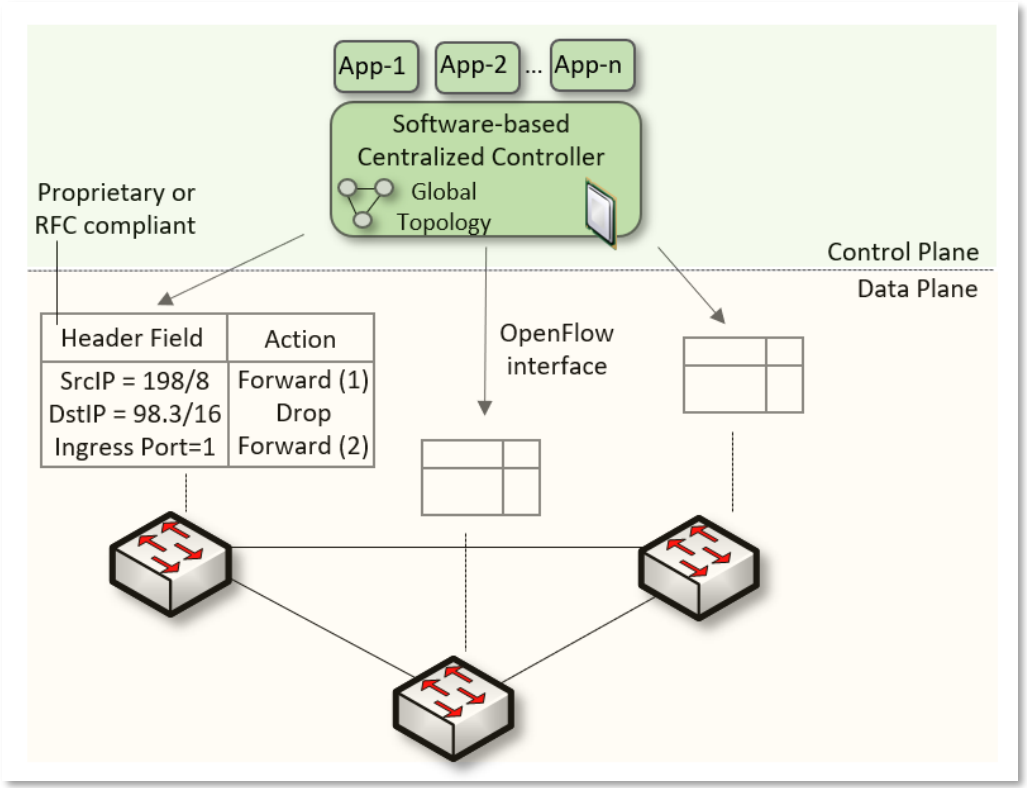
Traditional (Legacy) Networking

- Since the explosive growth of the Internet in the 1990s, the networking industry has been dominated by closed and proprietary hardware and software
- The interface between control and data planes has been historically proprietary
  - Vendor dependence: slow product cycles of vendor equipment, no innovation from network owners
  - A router is a monolithic unit built and internally accessed by the manufacturer only



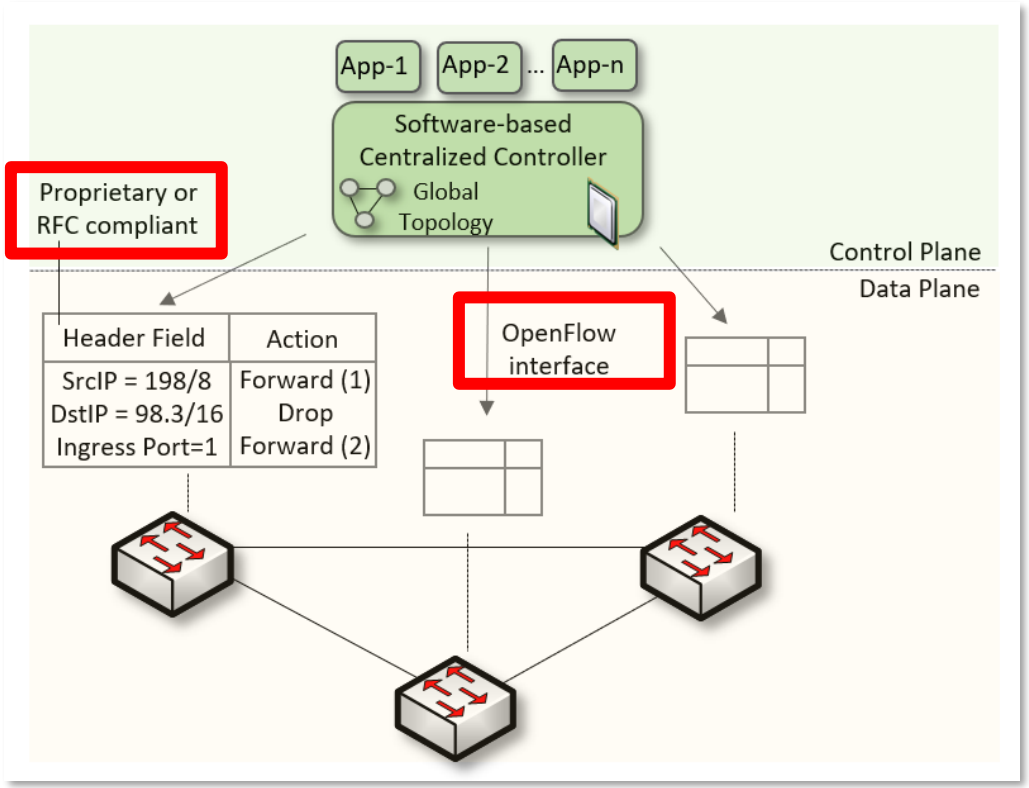
Software-defined Networking

- Protocol ossification has been challenged first by SDN
- SDN (1) explicitly separates the control and data planes, and (2) enables the control plane intelligence to be implemented as a software outside the switches
- The function of populating the forwarding table is now performed by the controller



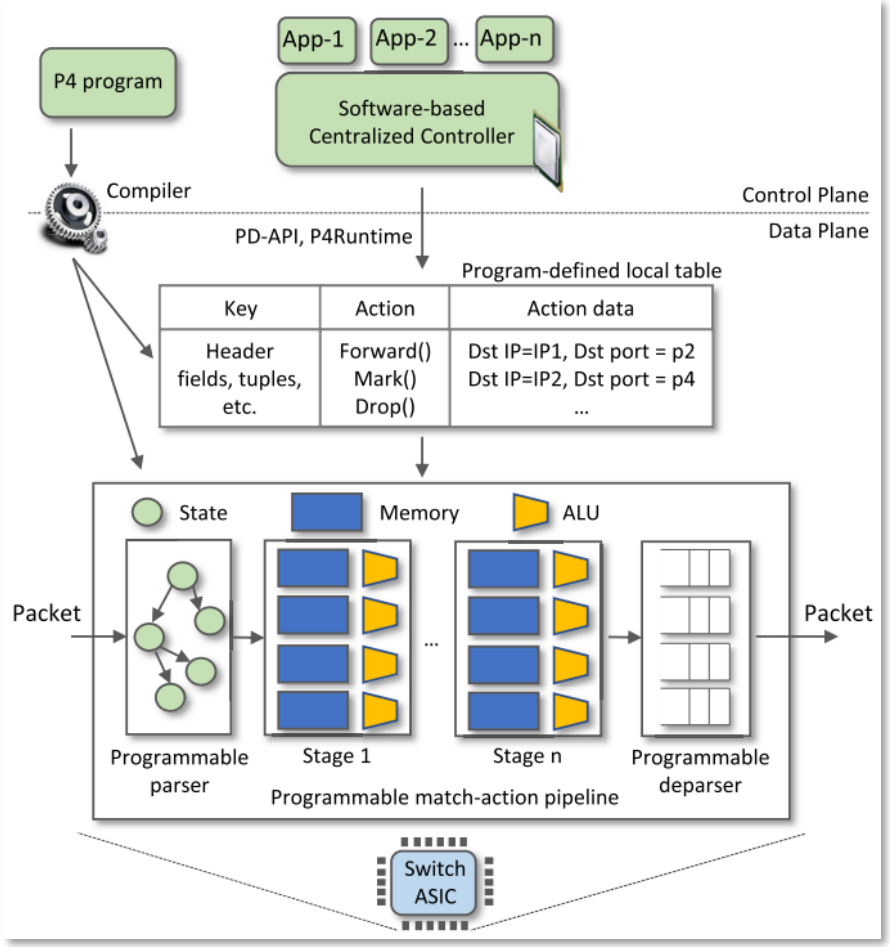
Software-defined Networking

- SDN is limited to the OpenFlow specifications
  - Forwarding rules are based on a fixed number of protocols / header fields (e.g., IP, Ethernet)
- The data plane is designed with fixed functions (hard-coded)
  - Functions are implemented by the chip designer



P4 Programmable Switches

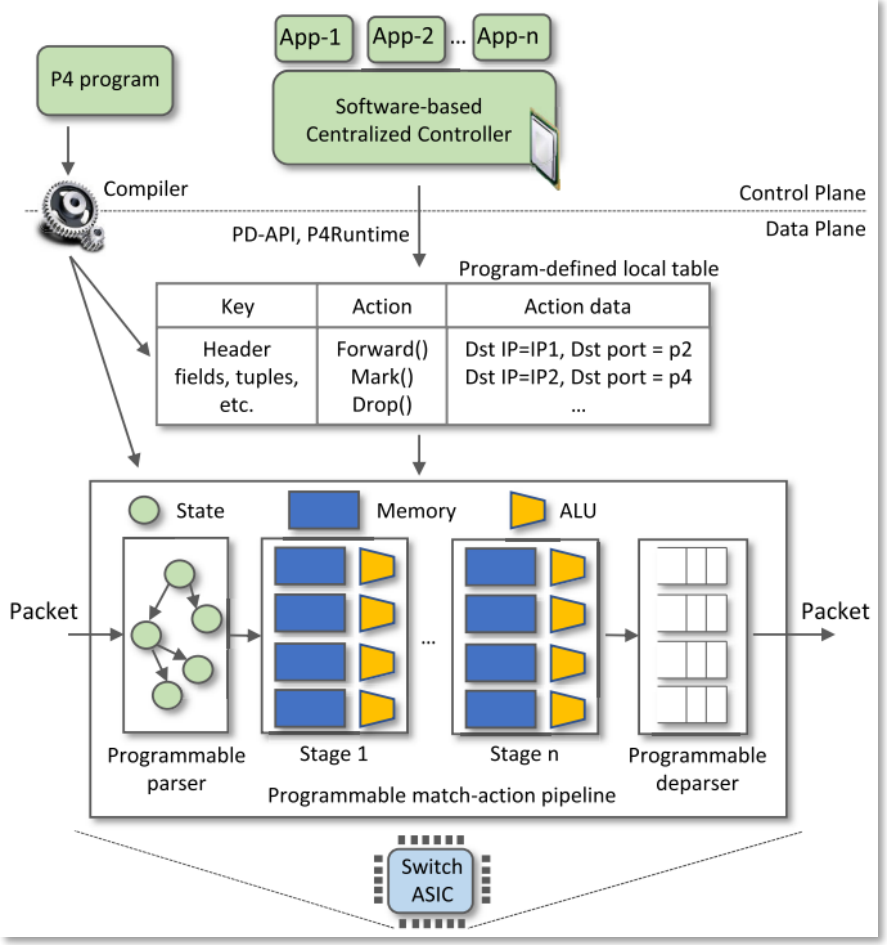
- The programmable forwarding can be viewed as a natural evolution of SDN
- P4 programmable switches permit a programmer to program the data plane



P4 stands for stands for Programming Protocol-independent Packet Processors

P4 Programmable Switches

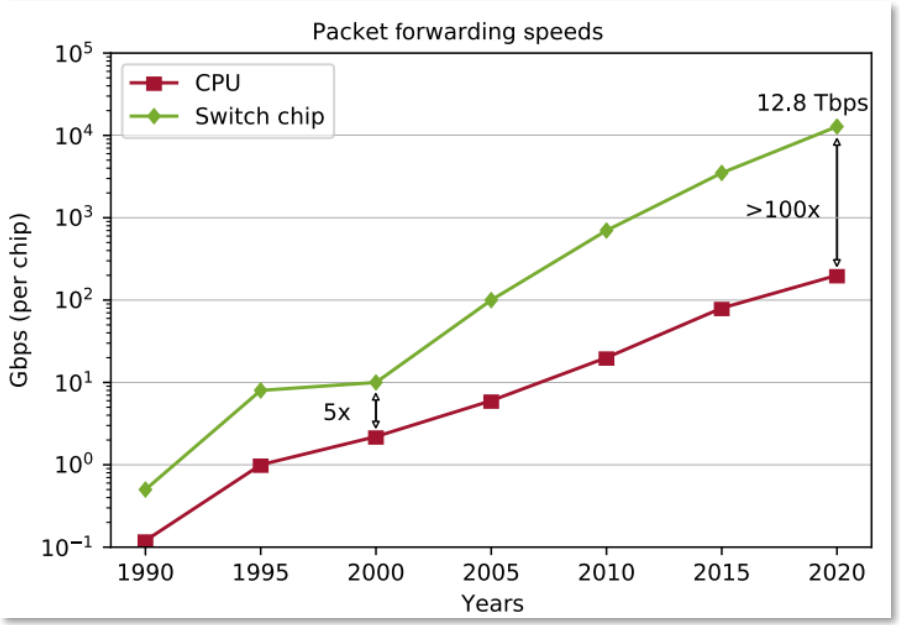
- The programmable forwarding can be viewed as a natural evolution of SDN
- P4 programmable switches permit a programmer to program the data plane
  - Defining and parsing new protocols
  - Customizing packet processing functions
  - Measuring events occurring in the data plane with nanosecond resolution
  - Inspecting and analyzing each packet (per-packet analysis)



P4 stands for stands for Programming Protocol-independent Packet Processors

P4 Programmable Switches

- The programmer can implement
  - New encapsulations and secure tunnels
  - Mitigation techniques for DDoS attacks at terabit rates
  - Traffic anonymization systems at line rate
  - Customized firewalls
  - DNS deep packet inspection at line rate



Reproduced from N. McKeown, "Creating an End-to-End Programming Model for Packet Forwarding." **https://www.youtube.com/watch?v=fiBuao6YZl0&t=4216s**