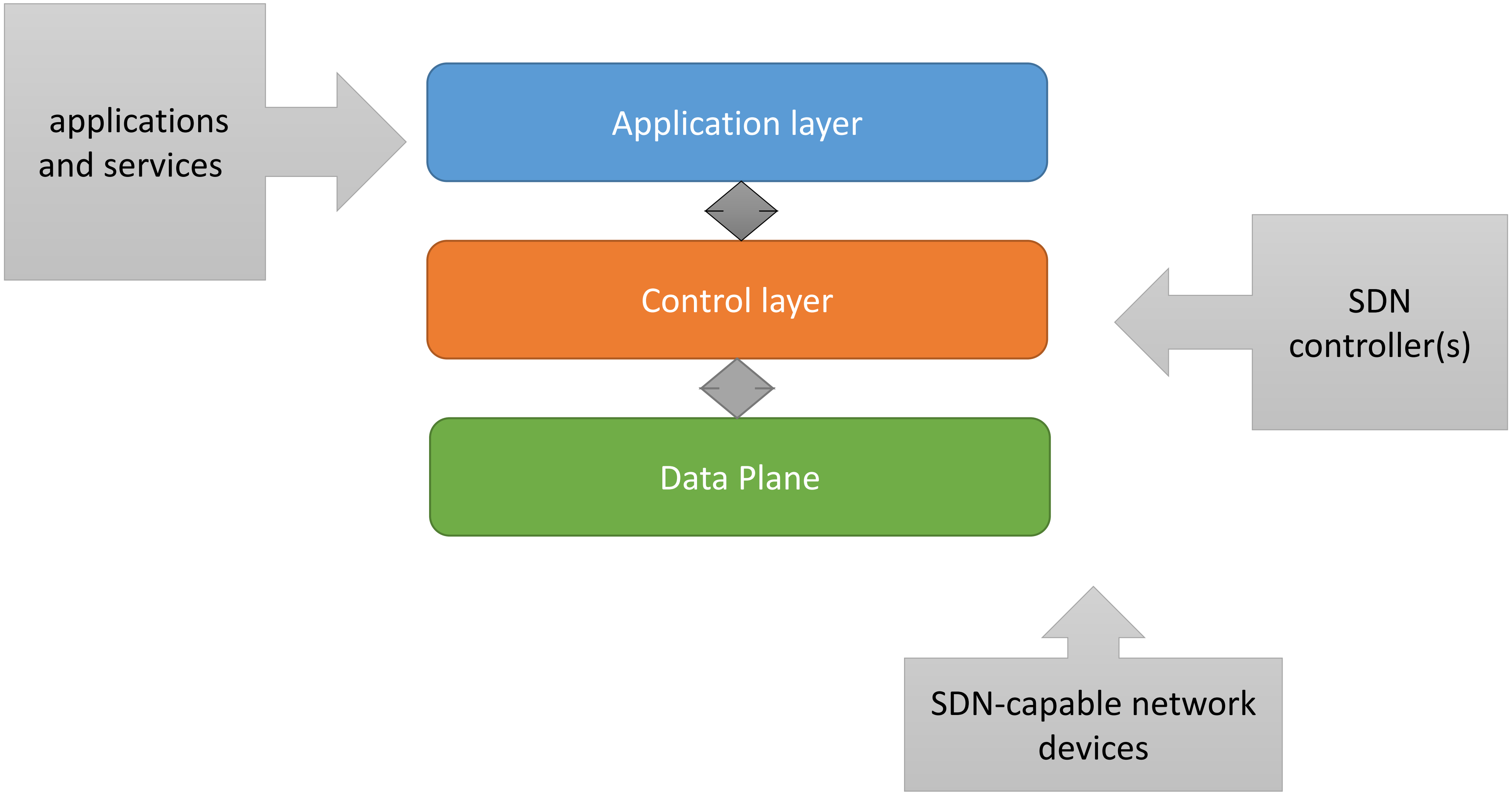
SDN security issues

Suneth Namal Karunarathna

Department of Computer Engineering,

University of Peradeniya.

Overview of SDN architecture



applications and services

Application layer

Control layer

Data Plane

SDN controller(s)

SDN-capable network devices

Attack vectors on SDN systems.

- The more common SDN security concerns include attacks at the various SDN architecture layers.
  - Application layer attacks
  - Control plane attacks
  - Data plane attacks

Attacks at Data Plane Layer

- Attackers could target the network elements from within the network itself.
  - Gain unauthorized physical or virtual access to the network
  - Compromise a host that is already connected to the SDN
  - Try to perform attacks to destabilize the network elements.

  - This could be a type of Denial of Service (DoS) attack or it could be a type of fuzzing attack to try to attack the network elements.

  Note: **Fuzzing** is a software security and functionality testing method that feeds randomly constructed input to the system and looks for an indication that a failure in response to that input has occurred.

Attacks at Data Plane Layer

- There are numerous southbound APIs and protocols used for the controller to communicate with the network elements.
- These SDN southbound communications could use
  - OpenFlow (OF), Open vSwitch Database Management Protocol (OVSDB),
  - Path Computation Element Communication Protocol (PCEP),
  - Interface to the Routing System (I2RS),
  - BGP-LS,
  - OpenStack Neutron, Open Management Infrastructure (OMI), Puppet, Chef, Diameter, Radius, NETCONF, Extensible Messaging and Presence Protocol (XMPP), Locator/ID Separation Protocol (LISP), Simple Network Management Protocol (SNMP), CLI, Embedded Event Manager (EEM), Cisco onePK, Application Centric Infrastructure (ACI), Opflex, among others.

Attacks at Data Plane Layer

- Each of these protocols has their own methods of securing the communications to network elements. However, many of these protocols are very new and implementers may not have set them up in the most secure way possible.
  - An attacker could also leverage these protocols and attempt to instantiate new flows into the device’s flow-table.
  - The attacker would want to try to spoof new flows to permit specific types of traffic that should be disallowed across the network.
  - If an attacker could create a flow that bypasses the traffic steering that guides traffic through a firewall the attacker would have a decided advantage.
  - hey may try to leverage that capability to sniff traffic and perform a Man in the Middle (MITM) attack.

Attacks at Data Plane Layer

- SDN systems are deployed within data centers.
- Data centers are more frequently using Data Center Interconnect (DCI) protocols such as Network Virtualization using Generic Routing Encapsulation (NVGRE), Stateless Transport Tunneling (STT), Virtual Extensible LAN (VXLAN), Cisco Overlay Transport Virtualization (OTV), Layer 2 Multi-Path (L2MP), TRILL-based protocols (Cisco FabricPath, Juniper QFabric, Brocade VCS Fabric), Shortest Path Bridging (SPB), among others.

Attacks at Data Plane Layer

- These protocols may lack authentication and any form of encryption to secure the packet contents.
- These new protocols could possess vulnerabilities due to an aspect of the protocol design or the way the vendor or customer has implemented the protocol.
- An attacker could be motivated to create spoofed traffic in such a way that it traverses the DCI links or to create a DoS attack of the DCI connections.

Attacks at control Layer

- An attacker would try to target the SDN controller for several purposes.
- The attacker would want to instantiate new flows by either spoofing northbound API messages or spoofing southbound messages toward the network devices.
- If an attacker can successfully spoof flows from the legitimate controller then the attacker would have the ability to allow traffic to flow across the SDN at their will and possibly bypass policies that may be relied on for security.

Attacks at control Layer

- An attacker might try to perform a DoS of the controller or use another method to cause the controller to fail.
- The attacker might try to attempt some form of resource consumption attack on the controller to bog it down and cause it to respond extremely slowly to Packet_In events and make it slow to send Packet_Out messages.

Attacks at control Layer

- If the SDN controller runs on a general purpose operating system, then the vulnerabilities of that OS become vulnerabilities for the controller.
- Often times the controllers are deployed into production using the default passwords and no security settings configured.
- The SDN engineers got it to “just barely” work and then didn’t want to touch it for fear of breaking it so the system ends up in production in a vulnerable configuration.

Attacks at control Layer

- An attacker creating their own controller and got network elements to believe flows from the “rogue” controller????

……

……

……

……

……

Application layer attacks

- Attacking the security of the northbound protocol would also be a likely vector.
- There are many northbound APIs that are used by SDN controllers.
- Northbound APIs could use Python, Java, C, REST, XML, JSON, among others.
- If the attacker could leverage the vulnerable northbound API, then the attacker would have control over the SDN network through the controller.

Application layer attacks

- If the controller lacked any form of security for the northbound API, then the attacker might be able to create their own SDN policies and thus gain control of the SDN environment.