

# Integer overflow and underflow in Floodlight

Seungwon Woo

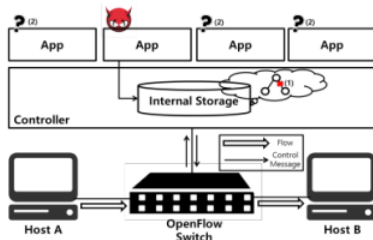
ETRI

## OpenFlow

- **OpenFlow** is a **standard protocol** that allows SDN controller to control network switches.
- Using OpenFlow, each switch can receive flow rules from the controller and **determine how it handles network traffic** by storing the **flow rules** in its own **flow table**.
- By default, **the type and range** of each parameter in the flow rule are defined in **OpenFlow specification**.
- **The flow rule is the most important factor in controlling the entire network in SDN.**

## Attacker and malicious application

- In SDN, the remote **attacker** can deploy a **malicious application** or install **malformed rules**.



## checkFlow() function in StaticFlowEntryPusherResource.java (RESTful service)

- A network administrator (or attacker) can install unintended flow rules in the switch by mistake.
- This function checks some fields and returns the result in a state field (valid or invalid).
- However, there is no input-validation related to numeric fields such as priority, port number, and so on.

```
/**
 * Validates if all the mandatory fields are set properly while adding an IPv6 flow
 * @param Map containing the fields of the flow
 * @return state indicating whether a flow is valid or not
 */
private int checkFlow(Map<String, Object> rows) {
    //Declaring & Initializing flags
    int state = 0;
```