SDN Threat Analysis

Haibin Song haibin.song@huawei.com

SDN Components

- Applications:
  - E.g. QoS management, traffic engineering, VPN coordinator, DDoS protection and etc.
- Controller
  - Forwarding algorithm, topology management, switch management, resource control, forwarding policies and etc.
- Network elements
  - Forwarding tables, and action rules (e.g. packet droping)
- OSS & Management
  - Management configurations and report

If we use a STRIDE model for threat analysis

- STRIDE
  - Spoofing
    - Spoofing of identify between components, if a malicious entity can pretend to be a controller, then disaster happens
    - Malicious entity can also pretend switches, OSS/management, which can cause failure, congestion,
  - Tampering
    - Modify the communication messages among app/controller/switch/OSS, which can be related to anything. For example, attacker's tampering with statistic report can lead to wrong decisions by the controller
    - Tampering with the resource policies/forwarding tables/action rules in the in the controller/switch
    - Tamper with the configuration database in the controller/switch

Threats Analysis with STRIDE model - 2

- Repudiation
  - Malicious entity can deny its resource usage if it can access and modify the logs, in that case you will get no money from the tenants that rent resources from the SDN network
- Information Disclosure
  - Monitor what happens in the communication messages, then can be used for further attacks
  - Use malicious forwarding rules to redirect traffic so as to collect information
  - Resource sharing without isolation may also cause information disclosure in the controller/switch

Threats Analysis with STRIDE model - 3

- DoS
  - Send too many packets that causes flow entry misses, cause the controller to be overloaded
  - Attacker modify forwarding rules, cause too many traffic to one determined port, then the switch is down
- Elevation of privilege
  - Attack to get more resources then allowed, usually by getting access to the controller policies

Particular MITM attack

- This might be only my concern?
- Think about a pure SDN network, SDN controller cannot directly connect to each SDN switch, i.e. each SDN switch is connected to SDN controller through other switches
- It implies that if an attacker compromise an SDN switch, it can do MITM attack to SDN controller and a partial of SDN switches,

Replay attack

- It could be more severe than in other use cases
  - Attacker in the middle store all history command messages from controller to switch
  - Then the attacker has a database with lots of commands that can be replayed according to its needs

Inter-Controller Security

- For two controllers in the same level but in different domains, some security issues are:
  - Inter-controller trust
  - Trust between switches across boarders
  - If you allow a controller to control switches in another domain, it also needs to solve the cross domain trust relationship between switches and controllers
- SDN controllers can be hierarchical, one SDN controller could be seen as a SDN switch from the upper level SDN controller
  - The lower level SDN network is like a virtual switch with ports
- For “connected” SDN controllers with different levels
  - The flow table miss behaviors are exaggerated with the lower level SDN network

Potential actions w.r.t certificates in IRTF/IETF

- ACME WG proposed automated certificate issuance and maintenance
  - SDN environment is different, domain validation certificate is not suitable for SDN, will need different challenge methods
  - Automation is also necessary due to the dynamic creation of SDN elements

Next step

- If the research group is interested in a draft on this topic, then let's do it
- If people would like to focus on one specific security protocol solution to one specific SDN threat, then contact us

Thank You!

谢谢！