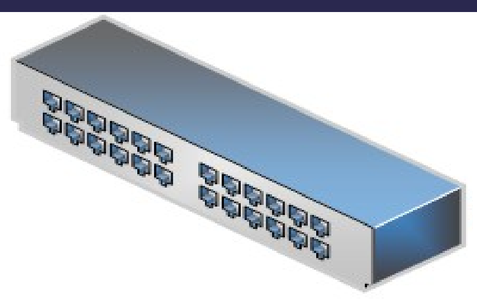
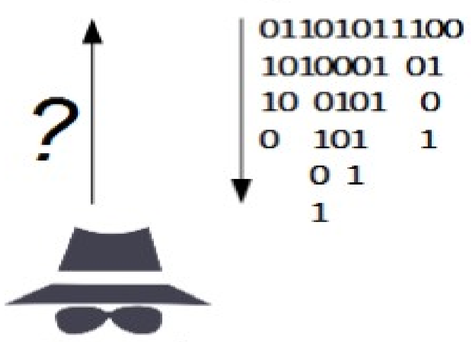
Adversarial Network Forensics in Software Defined Networking

Stefan Achleitner, Thomas La Porta, Trent Jaeger, Patrick McDaniel



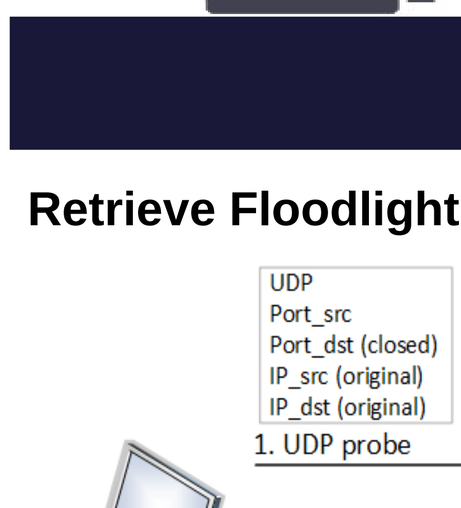
SDN Switch



SDN “Flow Rules”

→ OpenFlow rules are the essential part in SDN
→ Detailed construction of rules is assumed to be invisible for users

Our scanner SDNMap, is able to **precisely reconstruct the exact composition of SDN flow rules** by performing active probing and listening to the network traffic. Adversaries can use such information to plan and execute targeted cyber attacks.

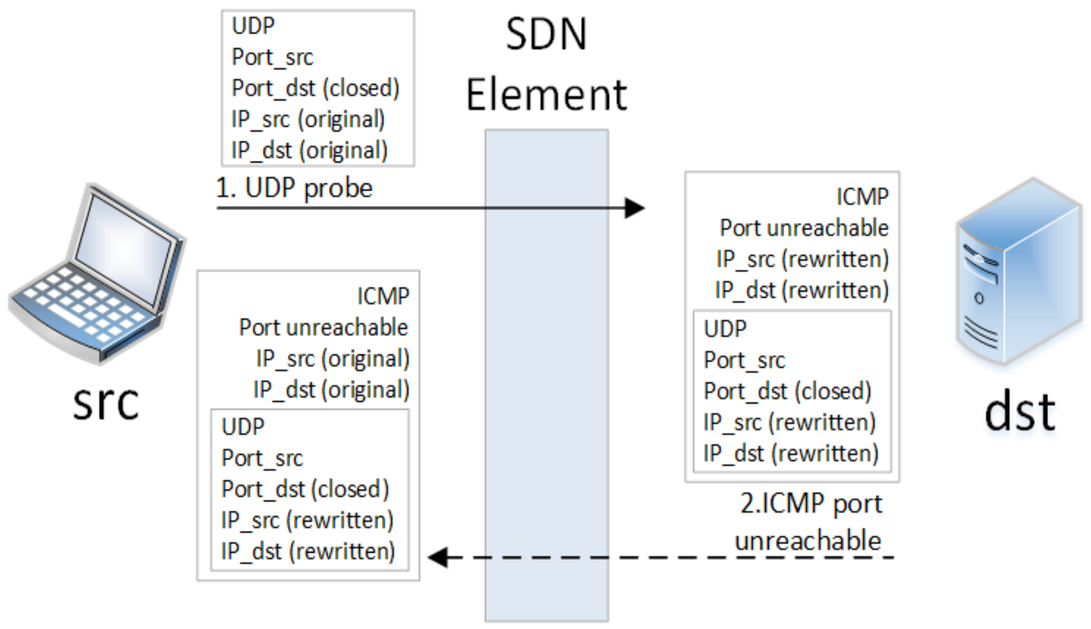


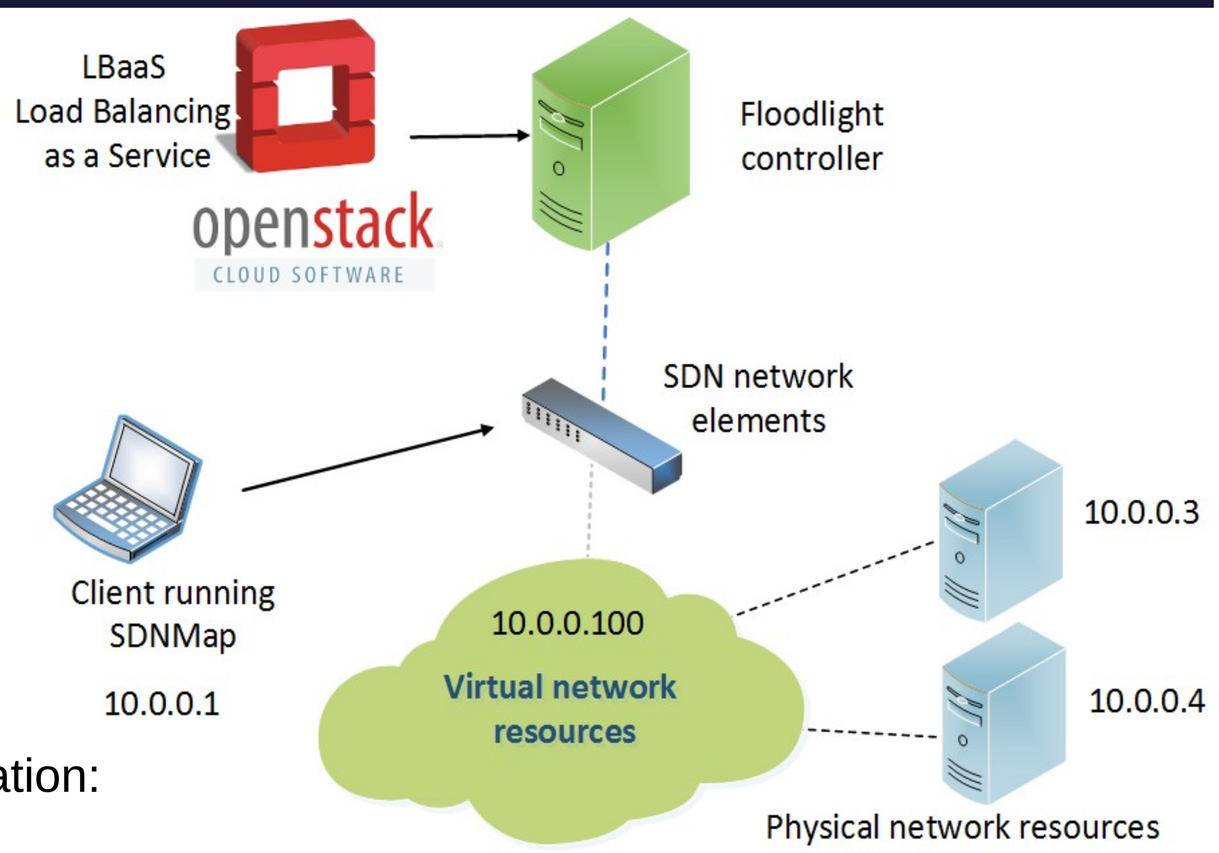
Attacker

IPsrc:10.0.12.234, IPdst:123.111.0.12 → forward
Protocol: UDP → deny
IPdst:157.111.17.89 →mod_IPdst: 10.0.2.15, forward

Attack Scenario – Retrieve Load Balancing Policy

Retrieve Floodlight's Load Balancer Policy





ICMP destination port unreachable contains nested information:
match=type:nw_src:10.0.0.1,nw_dst:10.0.0.100
actions=mod_nw_dst:10.0.0.4,output:#OUT PORT

Adversaries reconstructing flow rules can **determine the load balancing policy.**

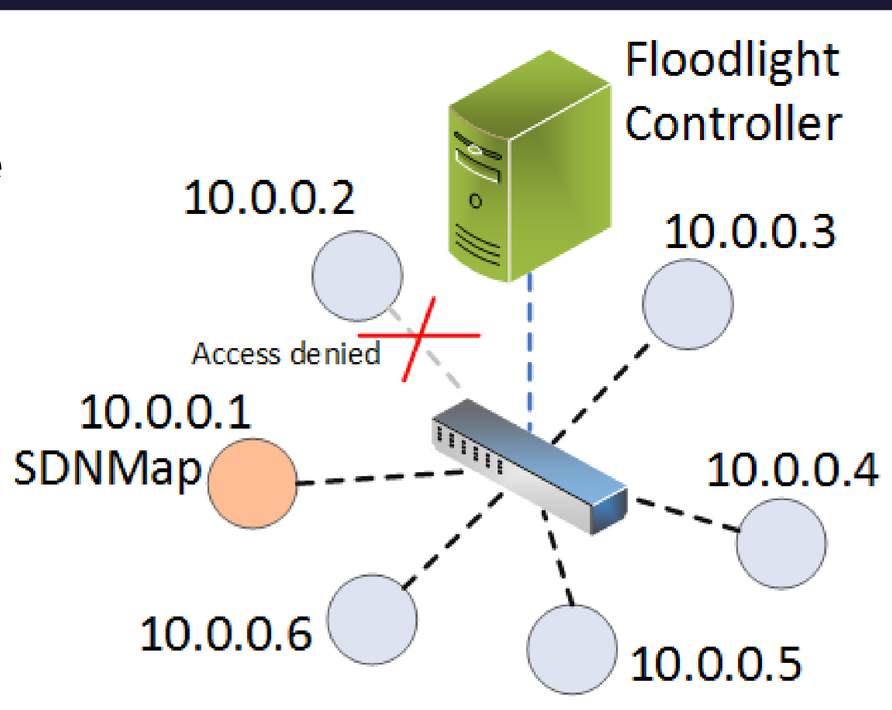
Attack Scenario – Bypassing Access Control List

Bypass Floodlight's Access Control List

Reconstruction of SDN flow rules, shows that packets with specific source and destination IP addresses are dropped:

match=type:ip,nw_src:10.0.0.1,nw_dst:10.0.0.2 actions=drop
match=type:ip,nw_src:10.0.0.2,nw_dst:10.0.0.1 actions=drop

Adversaries spoofing IP addresses can **bypass access control**, since SDN controller falls back to a default learning approach.



Related Publications

“Adversarial Network Forensics in Software Defined Networking”
Stefan Achleitner, Thomas La Porta, Trent Jaeger, Patrick McDaniel
in 2017 ACM Symposium on SDN Research (SOSR 2017) – Best Student Paper Award

Project sponsor: U.S. Army Research Laboratory Cyber Security Collaborative Research Alliance