Access Control for a Database-Defined Network

Noemi Glaeser, *University of South Carolina*
Anduo Wang, *Computer and Information Sciences, Temple University*
Temple University REU 2016

Introduction

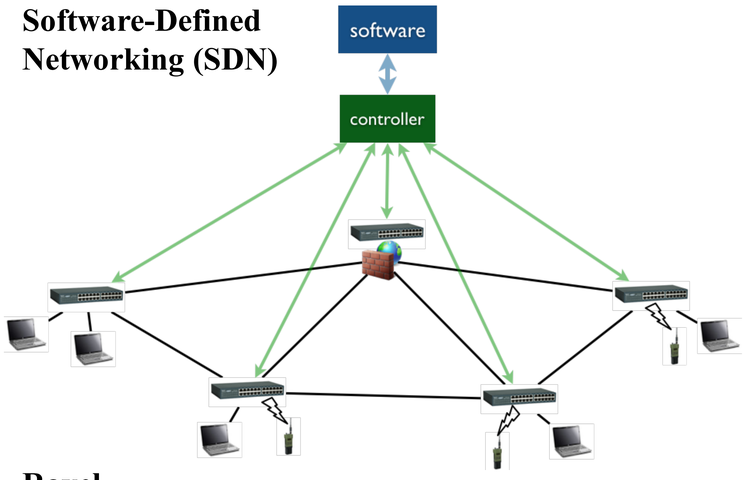
Software-defined networking (SDN) allows the insertion of software that manages the network through a centralized controller. While the controller improves network management through features such as network-wide and higher-level abstraction, the urgent requirement of security is still less well-studied. Ravel, a database-defined controller, like many others currently exposes all network states to its users without implementing any security measures. This project proposes a novel way to implement access control, a specific aspect of security for SDN, in the setting of the Ravel controller.

Objective

Add access control to the database-defined controller Ravel by writing and integrating an application which controls what users can read from and write to the network.

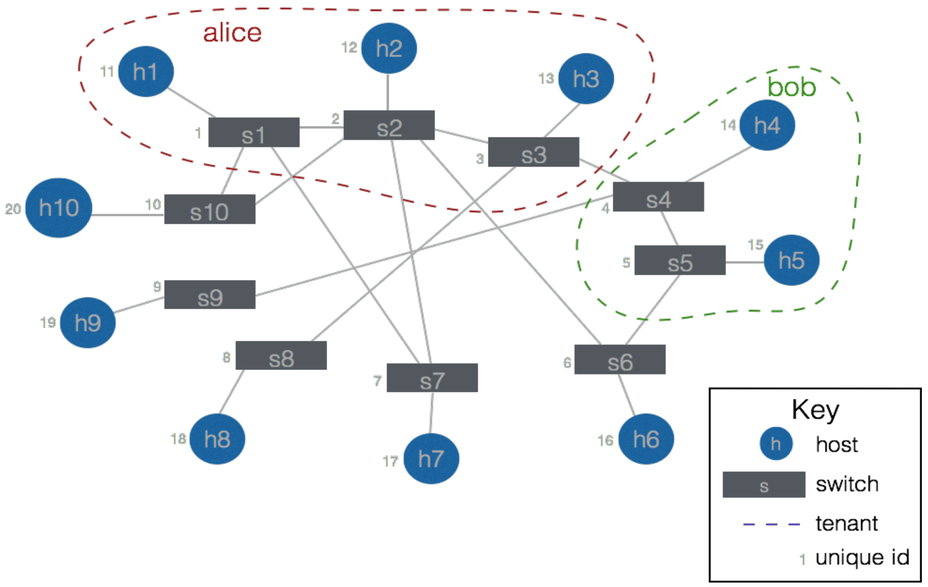
Background

Software-Defined Networking (SDN)



Ravel

- PostgreSQL interface
- Views serve as API between controller and applications
- Orchestration



Read Access

Service-level agreement (SLA)

sla	
name	nodeid
alice	1
alice	2
alice	3
alice	11
alice	12
alice	13
bob	4
bob	5
bob	14
bob	15

topology_acl			
principal	sid	nid	isactive
admin	1	2	1
admin	1	7	1
…			
alice	1	2	1
alice	1	11	1
…			
bob	4	5	1
bob	4	14	1
…			

topology_tenant		
sid	nid	isactive
1	2	1
1	11	1
2	3	1
2	12	1
3	13	1

SQL query → topology table

SQL query → user = alice

```
CREATE OR REPLACE VIEW topology_tenant AS (
    SELECT sid, nid, isactive FROM topology_acl
    WHERE principal = current_user);
```

Install Ravel: *ravel-net.org*
Demo: *github.com/ravel-net/REU-access-control*

Write Access

Add flow → trigger

rm					
fid	src	dst	vol	fw	lb
1	11	13	-	0	-

whitelist	
p1	p2
alice	bob
bob	alice
…	

Path Calculation

Using the whitelist, we create a **routingtp_tenant** view that shows the current user's accessible topology

whitelist, user = alice →

routingtp_tenant		
sid	nid	isactive
1	2	1
1	11	1
2	3	1
…		
3	4	1
4	5	1
…		

Path:

- **Admin:** dijkstra(topology)
- **Tenant:** dijkstra(routingtp_tenant)

Conclusions

- Security is an important area of SDN that has not been sufficiently studied
- This project adds access control (as an application) to Ravel
- **Future research:**
  - Other areas of SDN security