Cybermedia Center

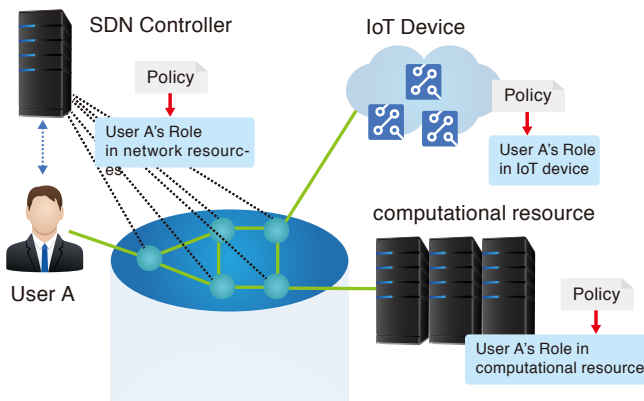# A Proposal of Access Control Mechanism Towards IoT Era

1. Introduction: Network of IoT Era

In the IoT (Internet of Things) era, there is *a large number of IoT devices* distributed widely throughout world.Many groups of users share such devices.In the network that connects such IoT devices, *access control becomes an important problem for assuring security.*
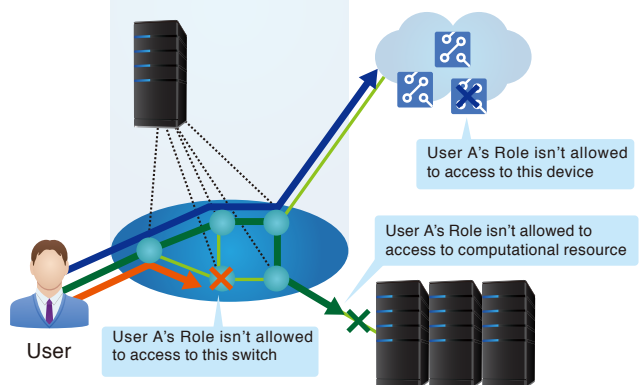
2. Access control mechanism

To date, various security technologies have been proposed and implemented. However, these technologies have targeted only computational resources. We propose an access control mechanism that *targets network resources as access-controlled resources.* We have adopted *RBAC* (Role Based Access Control) and *SDN* to develop the mechanism. The mechanism works as shown below, and *provides user-dedicated infrastructure.*

1. SDN controller authenticates every user connected to the network.

SDN Controller
IoT Device
Policy
User A's Role in network resources
Policy
User A's Role in IoT device
computational resource
User A
Policy
User A's Role in computational resource

2. Each resource has its own security policy, and assigns a role to each user depending on the policy.

User A's Role isn't allowed to access to this device
User A's Role isn't allowed to access to computational resource
User
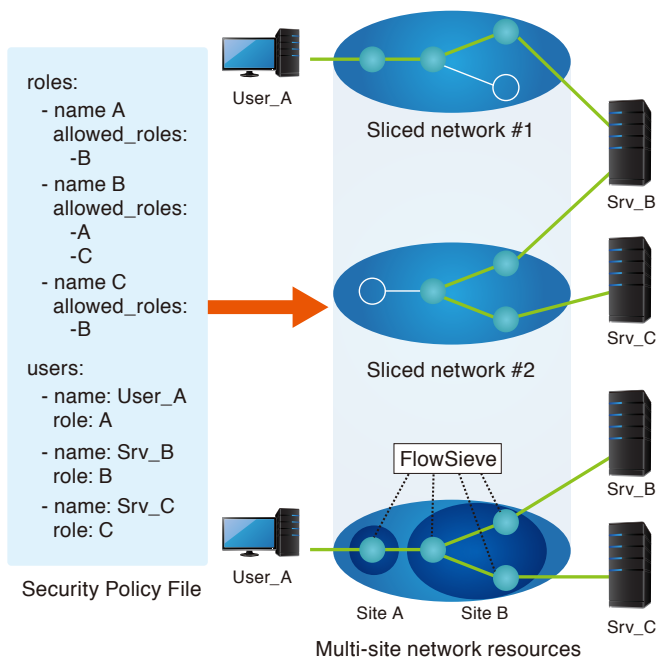User A's Role isn't allowed to access to this switch

3. User's access to any resource is controlled based on user's role.

3. Previous work: FlowSieve

FlowSieve is a preliminary implementation of the access control mechanism.FlowSieve is implemented as an OpenFlow controller, and *controls access to network resources*.

FlowSieve works as follows.
1. FlowSieve works as IEEE 802.1X authentication server, and authenticates every user connected to the network.
2. When a device sends a packet to an OpenFlow switch, the switch handles the packet based on the rules installed in it.
3. If the switch cannot find any rule for handling the packet, the switch sends the packet to FlowSieve.
4. FlowSieve determine how the packet should be treated by the controller, and installs rules for handling the packet to the switch.


```
roles:
  - name A
    allowed_roles:
    -B
  - name B
    allowed_roles:
    -A
    -C
  - name C
    allowed_roles:
    -B
users:
  - name: User_A
    role: A
  - name: Srv_B
    role: B
  - name: Srv_C
    role: C
```

Security Policy File

User_A
Sliced network #1
Srv_B
Sliced network #2
Srv_C
FlowSieve
User_A
Srv_B
Site A   Site B
Srv_C

Multi-site network resources

4. Future works

Under the current version of FlowSieve, all devices and network resources are controlled under one security policy file.
In the next plan, we extend FlowSieve so that *each device and network resource can have its own security policy* towards multi-site network.

Source Code of FlowSieve: https://github.com/shimojo-lab/flowsieve