OpenFlow-based authorization mechanism for Wi-Fi roaming systems

Hideaki Goto
NII / Tohoku University, Japan
contents

- Policy-based authorization for WLAN roaming systems
- What’s OpenFlow Network?
- OpenFlow-based authorization and access control mechanism for eduroam
A challenge in Wireless LAN roaming

- Basic access policy in eduroam

<table>
<thead>
<tr>
<th>User-type</th>
<th>SP’s local resources</th>
<th>Internet</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home users</td>
<td>Allowed</td>
<td>Allowed</td>
</tr>
<tr>
<td>Guest users</td>
<td>Forbidden</td>
<td>Allowed</td>
</tr>
</tbody>
</table>

- More flexible access control using users’ attributes
  - Allows the access to local resources
  - Forbids the access to some Internet sites upon request
Access controls using users’ attributes

Background

- Demands for network access control based on the user’s attributes such as affiliation, role, grade.
- Needs to allow the guests to gain access to the local resources such as printers and file servers in lectures, meetings, etc.
- Needs to derive Access Control Rules by combining the Policies of both home and visited institutions.
- We would like to build a simple yet powerful system based on the standard technologies.
Policy-based authorization for WLAN roaming

- Policy example at the home institution
  - No access control except logging at Firewall for local staff/students.
  - Students should not be allowed to use some notorious (troublesome) websites. (as a request to the visited institutions)
  - Allows the professors to use local resources freely at the visited institutions. (as a request to the visited institutions)
Policy-based authorization for WLAN roaming

- Policy example at the visited institution
  - For visitor students, block the accesses to some troublesome websites.
  - Guests basically cannot use the local resources, while guest professors are allowed to use them.
  - At a conference, for example, the secretariat can allow the participants to use the local resources on-site.
What’s OpenFlow Network?

- OpenFlow Network consists of *some* OpenFlow Switches (OFSs) and *one (or more)* OpenFlow Controller (OFC)
- Packet flows are controlled by the flow information (L1-L4 header contents)
Advantages of OpenFlow Network

Conventional system:
- Highly dependent on network hardware topology
- Configuration is required on every network device (high maintenance labor/cost)
- #VLANs is limited up to 4,096 with IEEE802.1q

OpenFlow Network:
- SDN: Software-Defined Network
- Dynamically configurable routing, access controls, etc.
- Simple hardware configuration on a centralized controller
- Quite simple configuration on switches
- Inter-operable across different vendors
- Scalable dynamic VLAN
Access Control mechanism using OpenFlow

- Policy DB is connected to the IdP at the home institution. The policy and the attributes are sent to the SP over RADIUS protocol.
- Switch control rules are derived from the IdP/SP policies, and the access control is performed.
Technical details


What do we need?

- Well-defined, common attribute representations.
- Standardization of popular Access Control rules.
- Inter-operability with backward compatible RADIUS packet definition.
- Middleware (Open Source)