Design and deployment of secure, robust, and resilient SDN Controllers

SDNRG @ IETF 93
Wednesday, 22 July 2015
Sandra Scott-Hayward
s.scott-hayward@qub.ac.uk
Centre for Secure Information Technologies (CSIT)

Est. 2009, Based in The ECIT Institute

Initial funding over £30M (CSIT 2 - £38M)

80 People
- Researchers
- Engineers
- Business Development

Largest UK University lab for cyber security technology research

GCHQ Academic Centre of Excellence

Industry Informed
- Open Innovation Model

Strong international links
- ETRI, CyLab, GTRI, SRI International
- Cyber Security Technology Summit
Increase in components and interfaces for the evolved SDN implementation increases the security challenges of the SDN controller design.

Objective:

• Identify requirements of a secure, robust, and resilient SDN controller;

• Analyse state-of-the-art open-source SDN controllers with respect to the security of their design;

• Provide recommendations for security improvements
Secure, Robust and Resilient (referred to as ‘security’):

- The controller is designed to reduce the risk of intrusion/attack at the network control layer;
- The controller is able to withstand errors in control layer logic;
- The controller is able to recover quickly from disruption and maintain an acceptable level of service in the face of faults.
# Selected SDN Controllers

<table>
<thead>
<tr>
<th>Controller</th>
<th>Source</th>
<th>Version</th>
<th>Release</th>
<th>Architecture</th>
<th>Objective</th>
<th>Security Features</th>
</tr>
</thead>
<tbody>
<tr>
<td>ONOS</td>
<td>ON.Lab</td>
<td>Avocet 1.0.0</td>
<td>2014</td>
<td>Distributed</td>
<td>High-availability, Scale-out, Performance</td>
<td>Security-mode ONOS proposed for v2</td>
</tr>
<tr>
<td>OpenDaylight</td>
<td>OpenDaylight Project</td>
<td>Helium (Karaf 0.2.0)</td>
<td>2014</td>
<td>Distributed</td>
<td>Enterprise-Grade Performance, High Availability</td>
<td>AAA Service, Foundation of Security Group</td>
</tr>
<tr>
<td>ROSEMARY</td>
<td>KAIST, SRI International</td>
<td>-</td>
<td>2014</td>
<td>Centralized</td>
<td>Robust, secure, and high-performance NOS</td>
<td>Process Containment, Resource Usage Monitoring, App PermissionStructure</td>
</tr>
<tr>
<td>Ryu</td>
<td>NTT</td>
<td>3.13</td>
<td>2012</td>
<td>Centralized, Multi-Threaded</td>
<td>High quality controller for production environments</td>
<td>Secure control layer communication</td>
</tr>
<tr>
<td>SE-Floodlight</td>
<td>SRI International</td>
<td>Beta 2</td>
<td>2013</td>
<td>Centralized</td>
<td>Security-enhanced version of Floodlight controller</td>
<td>Security enforcement kernel (AAA)</td>
</tr>
</tbody>
</table>
## Secure Controller Design

<table>
<thead>
<tr>
<th>Controller</th>
<th>ONOS</th>
<th>ODL</th>
<th>ROSEMARY</th>
<th>Ryu</th>
<th>SE-Floodlight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Process (Application) Isolation</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓  (Privilege-Based)</td>
</tr>
<tr>
<td>Implementation of Policy Conflict Resolution</td>
<td>✓ (Data-Store)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✓ (Algorithm)</td>
</tr>
<tr>
<td>Multiple Controller Instances – Resilience</td>
<td>✓ (Clustering)</td>
<td>✓ (Clustering)</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Multiple Application Instances – Resilience</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Secure Storage</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Secure Controller Interfaces

<table>
<thead>
<tr>
<th>Controller</th>
<th>ONOS</th>
<th>ODL</th>
<th>ROSEMARY</th>
<th>Ryu</th>
<th>SE-Floodlight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Control Layer</td>
<td>×</td>
<td>✓</td>
<td>×</td>
<td>✓</td>
<td>✓ (D-CPI, A-CPI)</td>
</tr>
<tr>
<td>Communication</td>
<td>✓</td>
<td>✓ (D-CPI)</td>
<td>×</td>
<td>✓</td>
<td>✓ (D-CPI)</td>
</tr>
<tr>
<td>GUI/REST API Security</td>
<td>×</td>
<td>✓ (weak)</td>
<td>n/a</td>
<td>×</td>
<td>×</td>
</tr>
</tbody>
</table>
Controller Security Services

<table>
<thead>
<tr>
<th>Controller Service</th>
<th>ONOS</th>
<th>ODL</th>
<th>ROSEMARY</th>
<th>Ryu</th>
<th>SE-Floodlight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication and Authorization</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>IDS/IPS Integration</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Resource Monitoring</td>
<td>✗</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>Logging/Security Audit Service</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Recommendations for Future Security Improvements:

1. Design with Software Security Principles
2. Secure Default Controller Settings
3. Application Future-Proofing
ONOS, OpenDaylight
Focus on the provision of a distributed architecture
=>
High availability, Performance

ROSEMARY, SE-Floodlight
Introduce control layer resilience and a security-enforcement kernel
=>
Security, Resilience

Next Evolution in SDN Controller Design …
Security, Robustness, and Resilience
Thank you!

Questions?

s.scott-hayward@qub.ac.uk
ONOS

OpenDaylight

ROSEMARY

Ryu

SE-Floodlight
CSIT: A Global Cyber Innovation Hub

Thought leader in Secure Information Technology Research
Network of Commercial & Research partnerships
Portfolio of successful Technology Transfer