IETF-113

I2NSF Hackathon Project

March 19-20, 2022

Champion: Jaehoon (Paul) Jeong[1]

Members: Patrick Lingga[1], Jeonghyeon Kim[1], and Cheolmin Kim[2]

[1]Sungkyunkwan University, [2]Kyungpook National University

I2NSF (Interface to Network Security Functions) Framework Project

Champion: Jaehoon (Paul) Jeong

IETF-113 I2NSF Hackathon Project

Professors:

- Jaehoon (Paul) Jeong (SKKU)
- Younghan Kim (SSU)

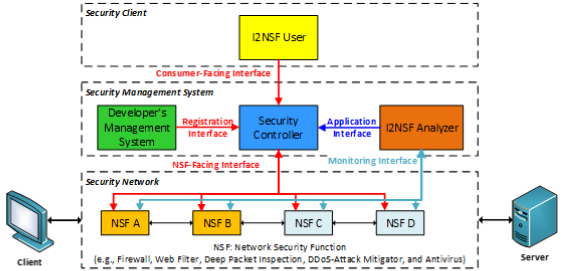
Researchers:

- Jung-Soo Park (ETRI)
- Yunchul Choi (ETRI)
- Jinyong Kim (SKKU)

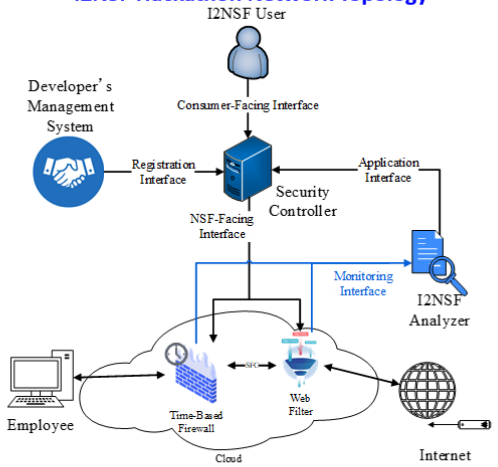
Students:

- Patrick Lingga (SKKU)
- Jeonghyeon Kim (SKKU)
- Cheolmin Kim (KNU)

I2NSF Framework



I2NSF Hackathon Network Topology



Where to get Code and Demo Video Clip

- Github – Source Code
  - ✓ https://github.com/jaehoonpaul/i2nsf-framework

What to pull down to set up an environment

- OS: Ubuntu 16.04 LTS
- ConfD for NETCONF: 6.6 Version
- Jetconf for RESTCONF
- OpenStack: Queens version
- NSF: Suricata
- Hyperledger Fabric: 2.2 version

Manual for Operation Process

- I2NSF-Manual-Hackathon-IETF113.md contains detailed description about operation process. It can be found in the GitHub.

Contents of Implementation

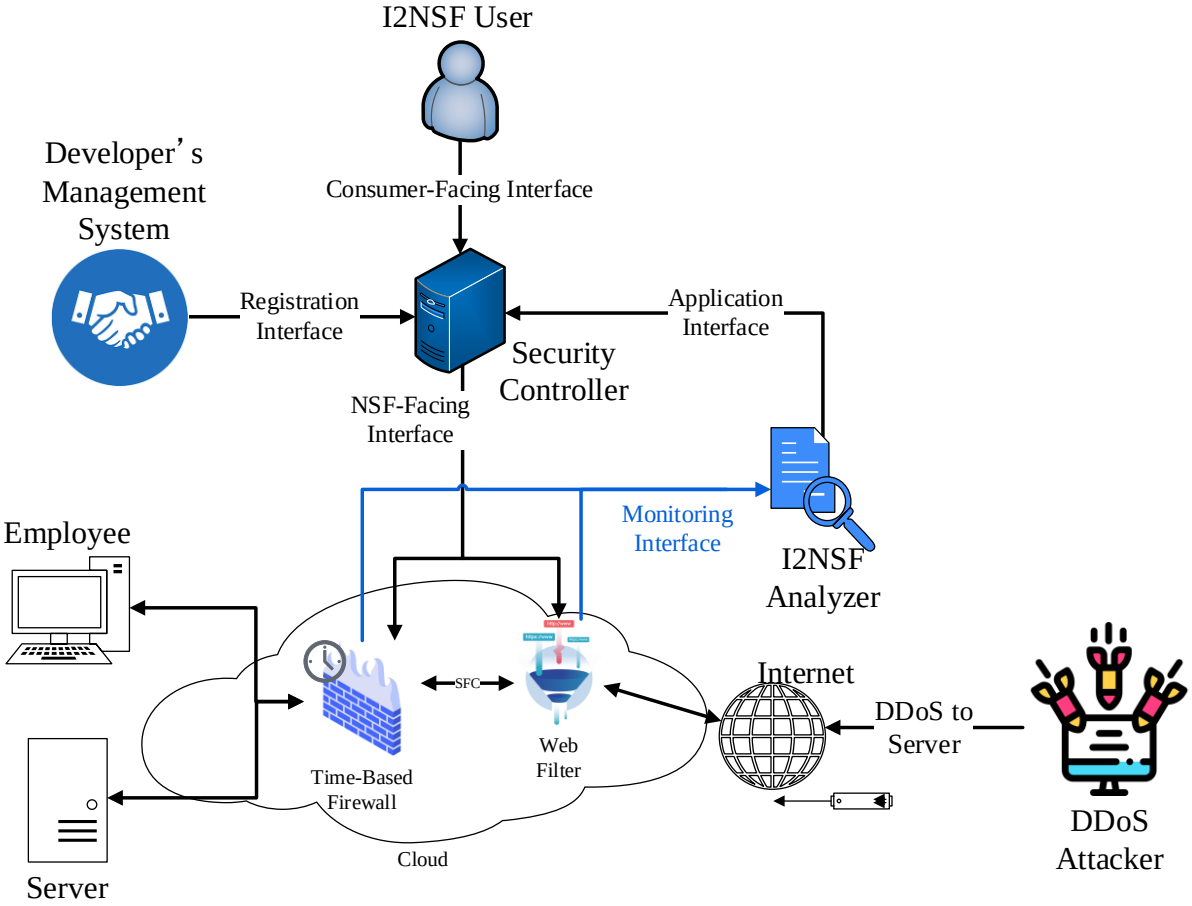
- Cloud-based Security Service System using I2NSF Framework
  - ✓ Web-based I2NSF User
  - ✓ Console-based Security Controller
  - ✓ Console-based Developer's Management System
  - ✓ I2NSF Framework in OpenStack NFV Environment
  - ✓ I2NSF Capability YANG Data Model
  - ✓ Registration Interface via NETCONF/YANG
  - ✓ Consumer-Facing Interface via RESTCONF/YANG
  - ✓ NSF-Facing Interface via NETCONF/YANG
  - ✓ Monitoring Interface via NETCONF/YANG
  - ✓ Web-based NSF Monitoring
  - ✓ Application Interface as Feedback from I2NSF Analyzer
- Network Security Functions
  - ✓ Firewall and Web-filter using Suricata
- Advanced Functions
  - ✓ Security Policy Translation with Automatic Data Model Mapper and Production Rules Generator
  - ✓ Blockchain-based Auditing for I2NSF Policy and Data Transactions

성균관대학교 SUNG KYUN KWAN UNIVERSITY ETRI openstack. HYPERLEDGER FABRIC ConfD tail-f a Cisco company SURICATA

Hackathon Plan (1/2)

- The Implementation of the Internet Drafts for the I2NSF System for Cloud-based Security Services:
  - draft-ietf-i2nsf-capability-data-model-26 (Previous version: 20)
  - draft-ietf-i2nsf-consumer-facing-interface-dm-17 (Previous: 15)
  - draft-ietf-i2nsf-nsf-facing-interface-dm-22 (Previous: 15)
  - draft-ietf-i2nsf-registration-interface-dm-14 (Previous: 13)
  - draft-ietf-i2nsf-nsf-monitoring-data-model-16 (Previous: 11)
  - draft-lingga-i2nsf-application-interface-dm-02

Hackathon Plan (2/2)



What got done (1/2)

- All existing interfaces have been implemented following the latest version of the YANG data model in I2NSF drafts:
  - draft-ietf-i2nsf-capability-data-model-26
  - draft-ietf-i2nsf-consumer-facing-interface-dm-17
  - draft-ietf-i2nsf-nsf-facing-interface-dm-22
  - draft-ietf-i2nsf-registration-interface-dm-14
  - draft-ietf-i2nsf-nsf-monitoring-data-model-16

- Implementation of application interface that follows the YANG data model in the new internet draft for the automated feedback system.

What got done (2/2)

ubuntu@analyzer: ~/application

```
Sending feedback to Security Controller
<i2nsf-security-policy xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf"
                       xmlns:nsffbck="urn:ietf:params:xml:ns:yang:ietf-i2nsf-feedback-policy"
                       xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
  <name>feedback_policy_for_ddos_attack3</name>
  <rules>
    <name>deny_ddos_attack</name>
    <condition>
      <ipv4>
        <source-ipv4-range>
          <start>192.0.2.8</start>
          <end>192.0.2.10</end>
        </source-ipv4-range>
      </ipv4>
    </condition>
    <action>
      <packet-action>
        <ingress-action>drop</ingress-action>
      </packet-action>
    </action>
  </rules>
  <nsffbck:nsf-name>10.0.0.15</nsffbck:nsf-name>
  <nsffbck:problem>
    <nsffbck:ddos-detected>
      <nsffbck:attack-src-ip>192.0.2.8</nsffbck:attack-src-ip>
      <nsffbck:attack-src-ip>192.0.2.9</nsffbck:attack-src-ip>
      <nsffbck:attack-src-ip>192.0.2.10</nsffbck:attack-src-ip>
      <nsffbck:attack-dst-ip>10.0.0.0/24</nsffbck:attack-dst-ip>
    </nsffbck:ddos-detected>
  </nsffbck:problem>
</i2nsf-security-policy>
```

What we learn (1/3)

- The new data models provide the naming of the elements more clearly, which makes the configuration less complicated and less confusing.

- The new monitoring data model has a better data structure that can provide more information in a single notification.

- The YANG data model for the application interface enables automatic policy feedback. The data model also provide the "problem" information that helps to identify why a certain feedback is needed.

What we learn (2/3)

OLD:

```
<i2nsf-security-policy
 xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf"
 xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
 <system-policy>
  <system-policy-name>sns_access</system-policy-name>
  <rules>
   <rule-name>block_access_to_sns_during_office_hours</rule-name>
   <condition-clause-container>
    <packet-security-ipv4-condition>
     <pkt-sec-ipv4-src>
      <range-ipv4-address>
       <start-ipv4-address>10.0.0.5</start-ipv4-address>
       <end-ipv4-address>10.0.0.30</end-ipv4-address>
      </range-ipv4-address>
     </pkt-sec-ipv4-src>
    </packet-security-ipv4-condition>
   </condition-clause-container>
   <time-intervals>
    <absolute-time-interval>
     <start-time>09:00:00Z</start-time>
     <end-time>18:00:00Z</end-time>
    </absolute-time-interval>
   </time-intervals>
   <action-clause-container>
    <advanced-action>
     <content-security-control>
      url-filtering
     </content-security-control>
    </advanced-action>
   </action-clause-container>
  </rules>
 </system-policy>
</i2nsf-security-policy>
```

NEW:

```
<i2nsf-security-policy
  xmlns="urn:ietf:params:xml:ns:yang:ietf-i2nsf-policy-rule-for-nsf"
  xmlns:nc="urn:ietf:params:xml:ns:netconf:base:1.0">
 <name>sns_access</name>
 <rules>
  <name>block_sns_access_during_operation_time_for_ipv4</name>
  <condition>
   <ipv4>
    <source-ipv4-range>
      <start>10.0.0.5</start>
      <end>10.0.0.30</end>
    </source-ipv4-range>
   </ipv4>
   <context>
    <time>
      <start-date-time>2021-03-11T09:00:00.00Z</start-date-time>
      <end-date-time>2021-12-31T18:00:00.00Z</end-date-time>
    </time>
   </context>
  </condition>
  <action>
   <advanced-action>
    <content-security-control>
      url-filtering
    </content-security-control>
   </advanced-action>
  </action>
 </rules>
</i2nsf-security-policy>
```

What we learn (3/3)

OLD:

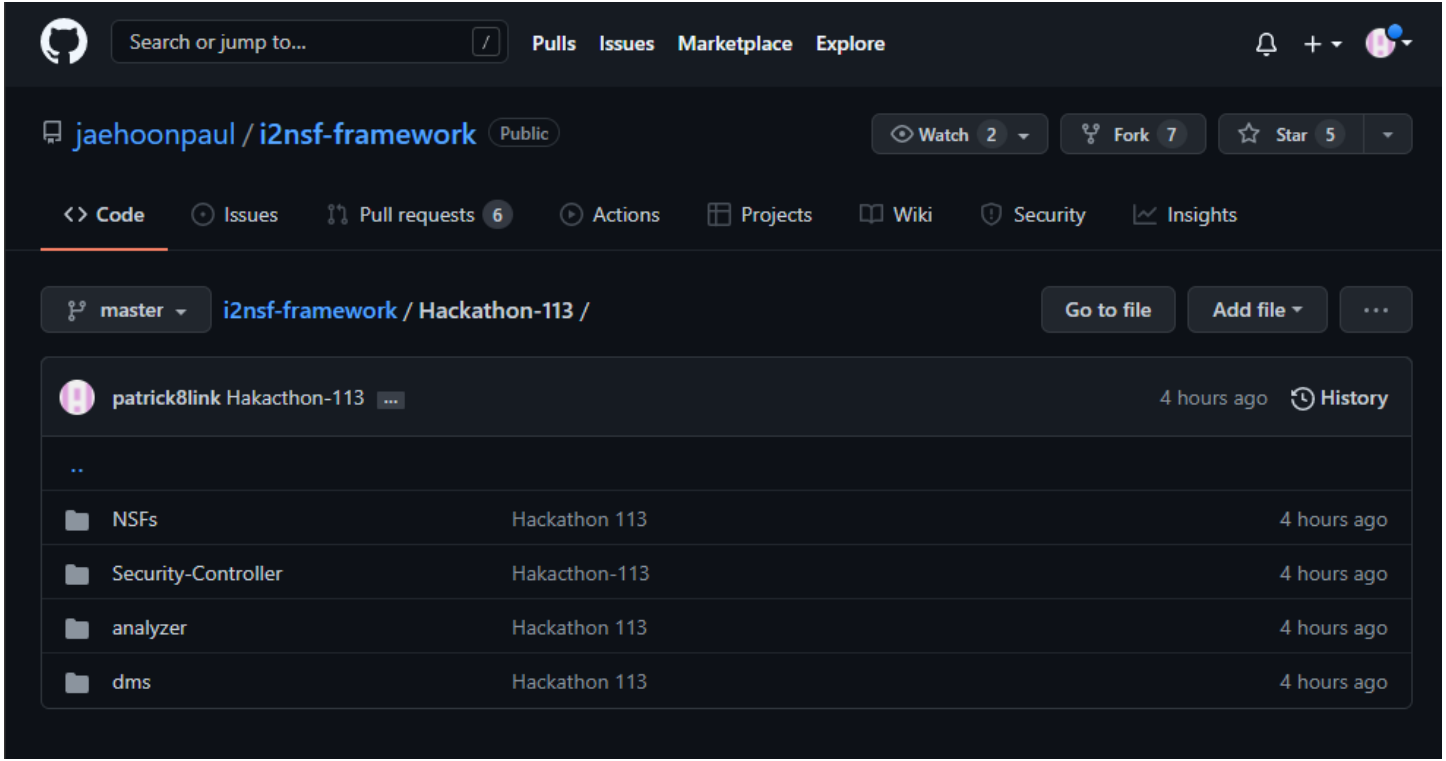
```
<i2nsf-nsf-event>
   <i2nsf-nsf-detection-ddos>
     <start-time>2022-03-17T11:53:21.00Z</start-time>
     <attack-src-ip>192.0.2.8</attack-src-ip>
     <attack-rate>10625831</attack-rate>
   </i2nsf-nsf-detection-ddos>
 </i2nsf-nsf-event>

<i2nsf-nsf-event>
   <i2nsf-nsf-detection-ddos>
     <start-time>2022-03-17T11:53:21.00Z</start-time>
     <attack-src-ip>192.0.2.9</attack-src-ip>
     <attack-rate>69163832</attack-rate>
   </i2nsf-nsf-detection-ddos>
 </i2nsf-nsf-event>

<i2nsf-nsf-event>
   <i2nsf-nsf-detection-ddos>
     <start-time>2022-03-17T11:53:21.00Z</start-time>
     <attack-src-ip>192.0.2.10</attack-src-ip>
     <attack-rate>42010605</attack-rate>
   </i2nsf-nsf-detection-ddos>
 </i2nsf-nsf-event>

<i2nsf-nsf-event>
   <i2nsf-nsf-detection-ddos>
     <start-time>2022-03-17T11:53:21.00Z</start-time>
     <attack-src-ip>203.0.113.1</attack-src-ip>
     <attack-rate>19602967</attack-rate>
   </i2nsf-nsf-detection-ddos>
 </i2nsf-nsf-event>

...
```

NEW:

```
<i2nsf-nsf-event>
   <i2nsf-nsf-detection-ddos>
     <start-time>2022-03-17T11:53:21.00Z</start-time>
     <attack-src-ip>192.0.2.8</attack-src-ip>
     <attack-src-ip>192.0.2.9</attack-src-ip>
     <attack-src-ip>192.0.2.10</attack-src-ip>
     <attack-src-ip>203.0.113.1</attack-src-ip>
     <attack-src-ip>203.0.113.5</attack-src-ip>
     <attack-src-ip>203.0.113.29</attack-src-ip>
     <attack-rate>1020763837</attack-rate>
   </i2nsf-nsf-detection-ddos>
 </i2nsf-nsf-event>
```

Open-Source Project at GitHub

URL: https://github.com/jaehoonpaul/i2nsf-framework



Wrap Up

Hackathon Team

Champion:

- **Jaehoon Paul Jeong (SKKU)**

Professor:

- **Younghan Kim (SSU)**

Researchers:

- **Jung-Soo Park (ETRI)**
- **Yunchul Choi (ETRI)**
- **Jinyong Kim (SKKU)**

Students:

- **Patrick Lingga (SKKU)**
- **Jeonghyeon Kim (SKKU)**
- **Cheolmin Kim (KNU)**

Hackathon Team Photo

I2NSF Hackathon team worked together with IPWAVE and BMWG hackathon teams.