



# IETF-110 Hackathon

## I2NSF Framework Project

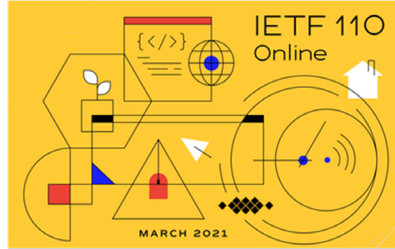
**March 1-5, 2021**  
**Online**  
**(Busan, Korea)**

**Champion:** Jaehoon Paul Jeong  
Computer Science & Engineering  
Sungkyunkwan University (SKKU)  
[pauljeong@skku.edu](mailto:pauljeong@skku.edu)



# I2NSF (Interface to Network Security Functions) Framework Project

Champion: Jaehoon (Paul) Jeong (SKKU)



## I2NSF Hackathon Project Professors:

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

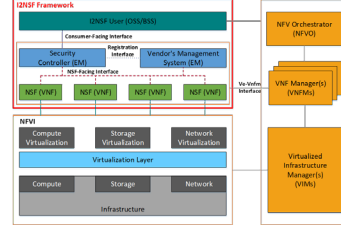
## Researchers:

- Jung-Soo Park (ETRI)
- Yunchul Choi (ETRI)

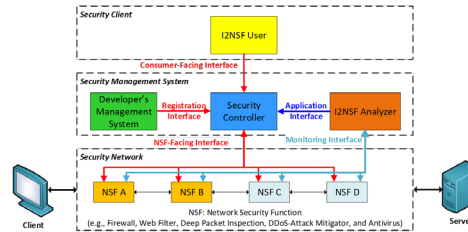
## Students:

- Patrick Lingga (SKKU)
- Jinyong Kim (SKKU)
- Jeonghyeon Kim (SKKU)
- Yoseop Ahn (SKKU)
- Xiaohong Yu (SKKU)
- Mose Gu (Liberty University)
- Kyungsik Kim (KNU)

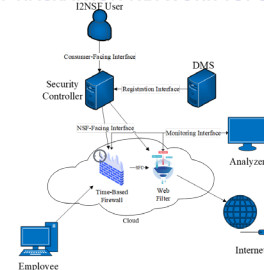
## I2NSF Architecture in NFV Reference



## I2NSF Framework



## I2NSF HACKATHON NETWORK TOPOLOGY



## Where to get Code and Demo Video Clip

- Github – Source Code
  - ✓ <https://github.com/jaehoonpaul/i2nsf-framework>
- Youtube – Demo Video Clip
  - ✓ <https://youtu.be/dAA1WTGhIXE>

## 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

## Manual for Operation Process

- Manual.txt contain detailed description about operation process. (It can be found in Open Source Project folder.)

## Contents of Implementation

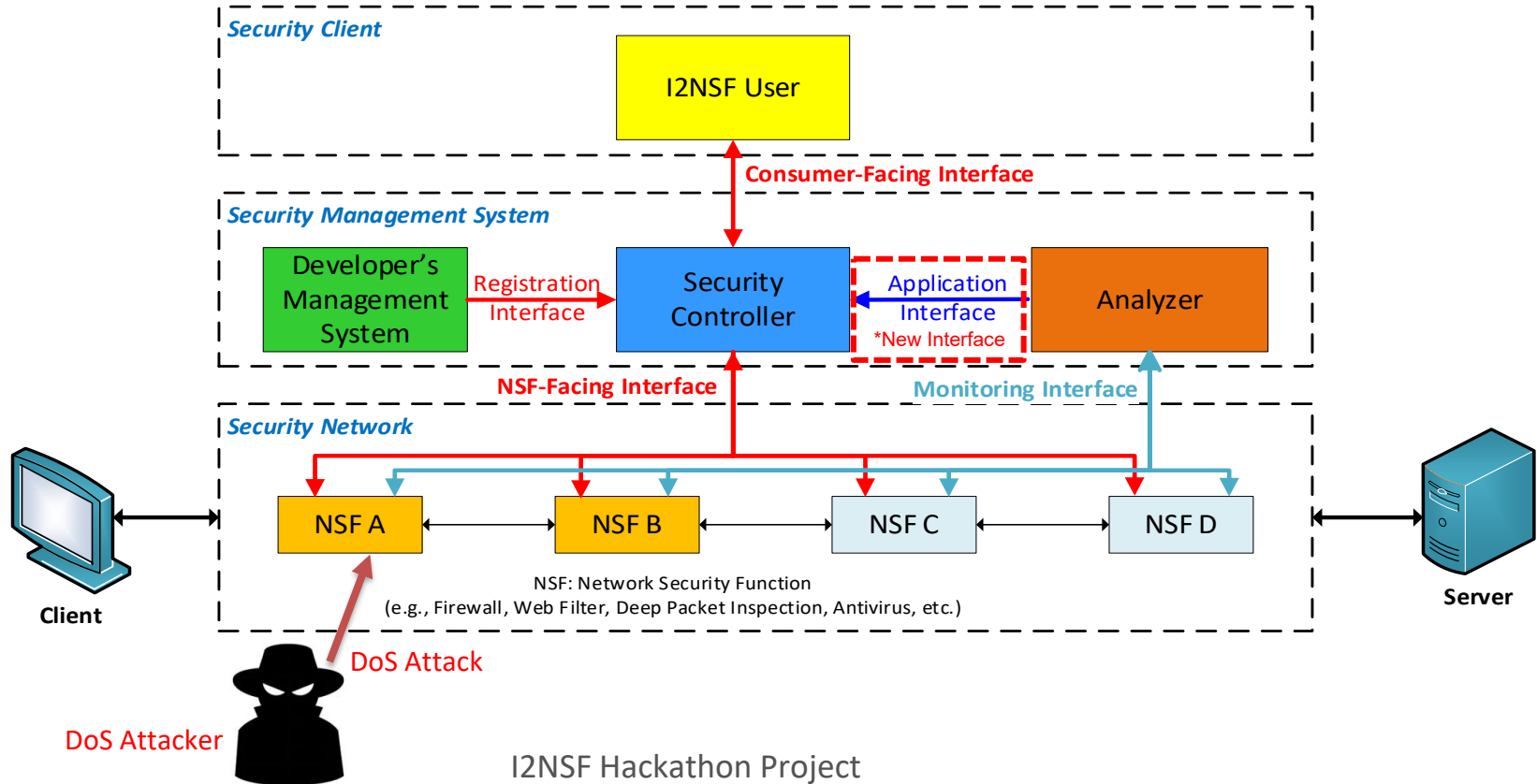
- Cloud-based Security Service System using I2NSF Framework
  - ✓ Web-based I2NSF User
  - ✓ Console-based Security Controller
  - ✓ Console-based Developer's Management System
  - ✓ I2NSF Framework in OpenStack NFV Environment
  - ✓ I2NSF Capability YANG Data Model
  - ✓ Registration Interface via NETCONF/YANG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



# 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-15
  - draft-ietf-i2nsf-consumer-facing-interface-dm-12
  - draft-ietf-i2nsf-nsf-facing-interface-dm-11
  - draft-ietf-i2nsf-registration-interface-dm-10
  - draft-ietf-i2nsf-nsf-monitoring-data-model-06
  - draft-yang-i2nsf-security-policy-translation-08
  - draft-jeong-i2nsf-security-management-automation-01
- ❖ Implementing Application Interface for delivering Feedback from I2NSF Analyzer to Security Controller.

# Hackathon Plan (2/2)



# What got done (1/3)

- NSF Monitoring using I2NSF Monitoring Interface via NETCONF.
  - Subscription-based NSF Monitoring.

```
ubuntu@analyzer: ~  
</i2nsf-system-detection-alarm>  
</notification>  
Waiting for next notification  
Current Time: 2021-02-26T08:08:14.570670+00:00  
<?xml version="1.0" encoding="UTF-8"?>  
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0"><eventTime  
>2021-02-26T08:08:14.564694+00:00</eventTime>  
<i2nsf-system-res-util-log xmlns='urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-mon  
itoring'>  
  <system-status>Running</system-status>  
  <cpu-usage>100</cpu-usage>  
  <memory-usage>38</memory-usage>  
  <disk-usage>10</disk-usage>  
  <disk-left>89</disk-left>  
  <in-traffic-speed>694</in-traffic-speed>  
  <out-traffic-speed>741</out-traffic-speed>  
  <acquisition-method xmlns:nsfmi="urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-mo  
nitoring">nsfmi:subscription</acquisition-method>  
  <emission-type xmlns:nsfmi="urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-monit  
oring">nsfmi:on-change</emission-type>  
  <nsf-name>url_filtering</nsf-name>  
</i2nsf-system-res-util-log>  
</notification>  
Waiting for next notification
```

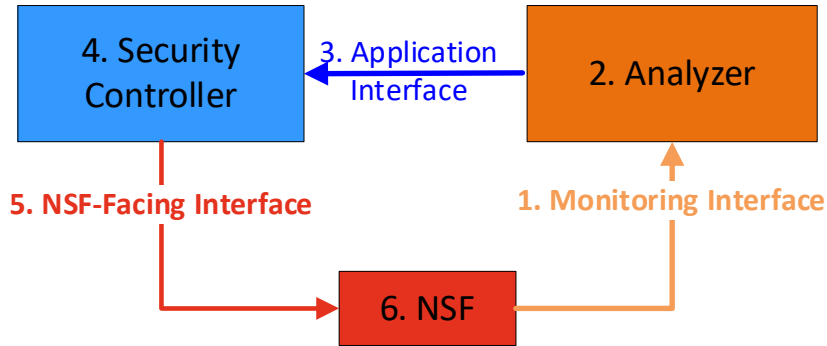
Monitoring NSF's Resources

```
ubuntu@analyzer: ~  
of cryptography. Please upgrade your Python.  
from cryptography.hazmat.backends import default_backend  
Waiting for next notification  
Current Time: 2021-03-05T05:06:52.615019+00:00  
<?xml version="1.0" encoding="UTF-8"?>  
<notification xmlns="urn:ietf:params:xml:ns:netconf:notification:1.0"><eventTime  
>2021-03-05T05:06:52.6124+00:00</eventTime>  
<i2nsf-nsf-detection-ddos xmlns='urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-mon  
itoring'>  
  <attack-type xmlns:nsfmi="urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-monit  
oring">nsfmi:tcp-con-flood</attack-type>  
  <start-time>2021-03-05T05:06:52.612248+00:00</start-time>  
  <attack-src-ip>10.0.0.37</attack-src-ip>  
  <attack-rate>1000</attack-rate>  
  <acquisition-method xmlns:nsfmi="urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-mo  
nitoring">nsfmi:subscription</acquisition-method>  
  <emission-type xmlns:nsfmi="urn:ietf:params:xml:ns:yang:ietf-i2nsf-nsf-monit  
oring">nsfmi:on-change</emission-type>  
</i2nsf-nsf-detection-ddos>  
</notification>  
  
SENDING FEEDBACK TO SECURITY CONTROLLER  
Waiting for next notification
```

Monitoring DDoS Detection

# What got done (2/3)

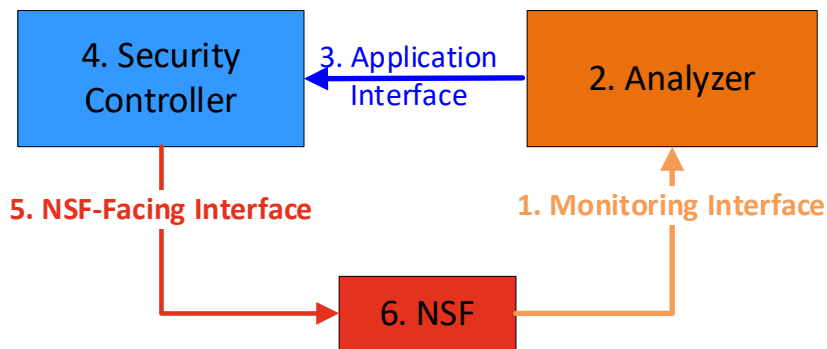
- Implementation of Application Interface for Feedback delivery to create a closed-loop system of I2NSF Framework.



1. NSF sends monitoring data to Analyzer via Monitoring Interface, such as DoS Detection Report.
2. Analyzer creates a new policy based on the received data through machine learning.
3. Analyzer sends the new policy to Security Controller via Application Interface.

# What got done (3/3)

- Implementation of Application Interface for Feedback delivery to create a closed-loop system of I2NSF Framework.



4. Security Controller translates a high-level security policy of Application Interface to a low-level security policy of NSF-Facing Interface.
5. Security Controller sends the new low-level security policy to NSF via NSF-Facing Interface.
6. NSF enforces the requested security policy.

# What we learned

- The draft-ietf-i2nsf-nsf-monitoring-data-model-06 may be extended for monitoring packet flows in NSFs to detect DoS/DDoS attacks.
  - The monitored packet flow data can be useful to protect the I2NSF Framework.
- The Feasibility of Application Interface in I2NSF Framework is demonstrated for Security Management Automation.



# Next Step

- Extension of the monitoring YANG data model to monitor packet flows.
- Usage of sFlow for network traffic monitoring the NSFs.
- Improvement of I2NSF Analyzer with Machine Learning to update/create a security policy.
- Automatic Update of the SFC Path of NSFs for a new security policy
- Enhancement of Security Policy Translator for security management automation.

# I2NSF Open-Source Project at Github

<https://github.com/jaehoonpaul/i2nsf-framework>

jaehoonpaul / i2nsf-framework

Watch 3 Star 3 Fork 6

Code Issues Pull requests Actions Projects Wiki Security Insights

master 1 branch 0 tags

Go to file Add file Code

patrick0link Add new Analyzer e3aa5f1 44 seconds ago 98 commits

|                                    |   |                |
|------------------------------------|---|----------------|
| Hackathon-104                      | Delete test.txt                             | 2 years ago    |
| Hackathon-105                      | Add files via upload                        | 2 years ago    |
| Hackathon-108                      | Update dms_server.py                        | 7 months ago   |
| Hackathon-109                      | Update I2NSF-Manual-Hackathon-IETF109-v1.md | 3 months ago   |
| Hackathon-110                      | Add new Analyzer                            | 44 seconds ago |
| dms                                | Source Code                                 | 2 years ago    |
| kubernetes                         | Source Code                                 | 2 years ago    |
| mininet                            | Fix runtime error of jetconf                | 3 months ago   |
| security_controller                | Source Code                                 | 2 years ago    |
| security_controller_registration   | Source Code                                 | 2 years ago    |
| security_controller_restconf       | Source Code                                 | 2 years ago    |
| security_controller_translation-v2 | Source Code                                 | 2 years ago    |

About

Hackathon-104

Readme

Releases

No releases published

Packages

No packages published

Contributors 5

Languages

HTML 69.5% C 7.5%

# Wrap Up

## I2NSF Hackathon Team

### Champion:

- Jaehoon Paul Jeong (SKKU)

### Professor:

- Younghan Kim (SSU)

### Researchers:

- Jung-Soo Park (ETRI)
- Yunchul Choi (ETRI)

### Students:

- Patrick Lingga (SKKU)
- Jinyong Kim (SKKU)
- Jeonghyeon Kim (SKKU)
- Yoseop Ahn (SKKU)
- Mose Gu (Liberty University)
- Kyungsik Kim (KNU)



I2NSF hackathon team worked in collaboration with IPWAVE and BMWG teams.

# Sponsors

