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

I2NSF (Interface to Network Security Functions) Framework Project

Champion: Jaehoon (Paul) Jeong (SKKU)

I2NSF Hackathon Project

Professors:

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

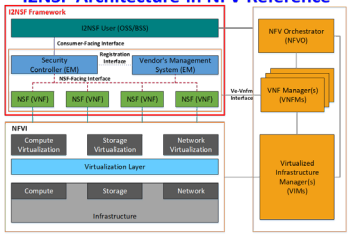
Researchers:

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

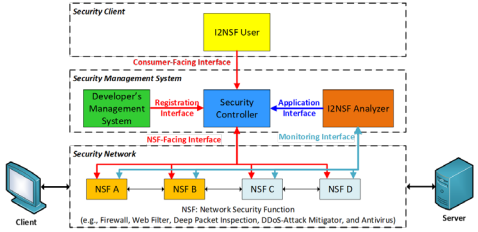
Students:

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

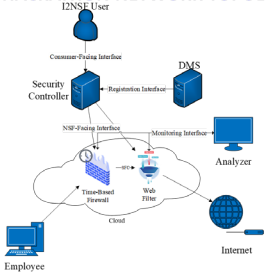
I2NSF Architecture in NFV Reference



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/dAA1WTGhlXE

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

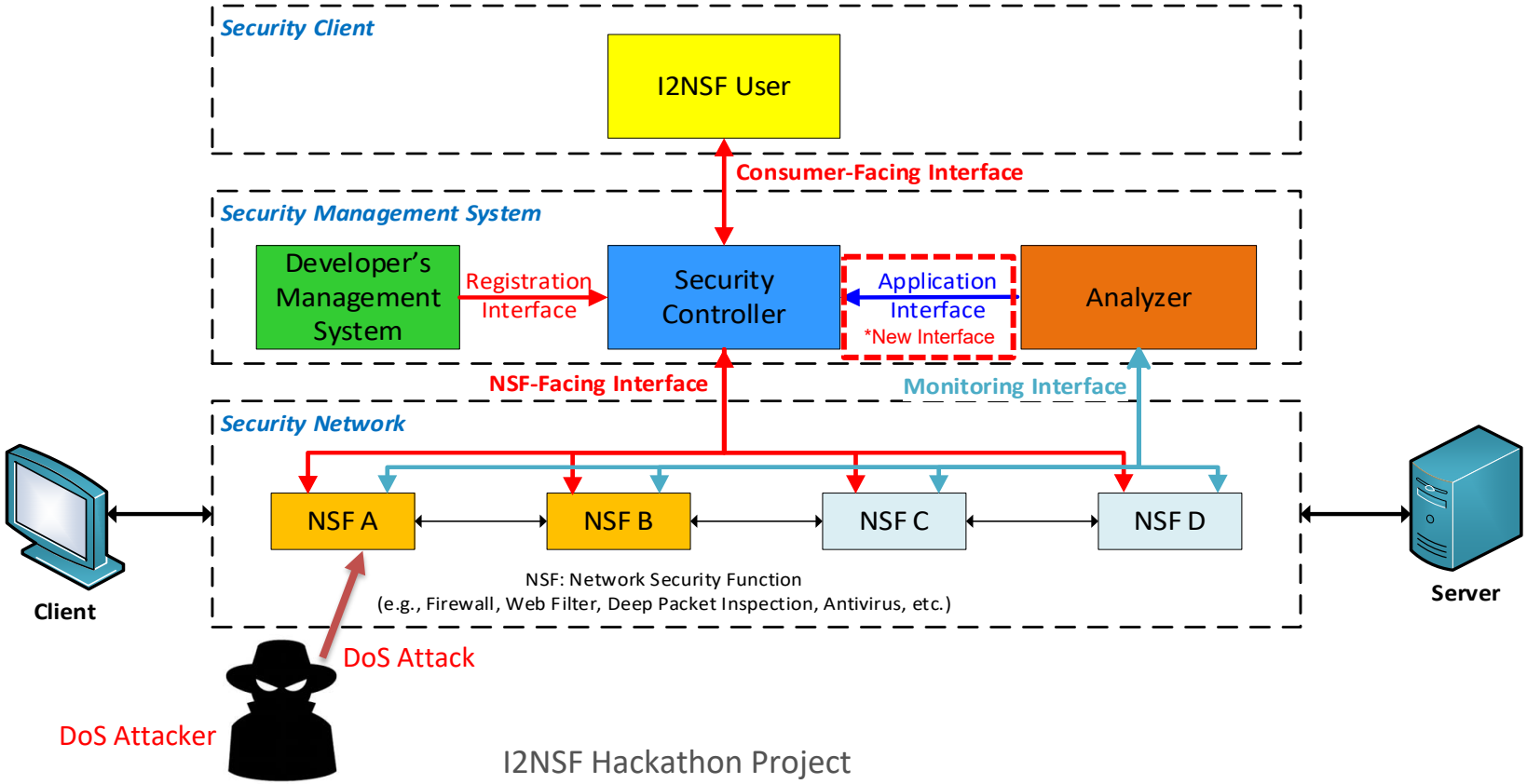
IETF 성균관대학교 SUNG KYUN KWAN UNIVERSITY ETRI openstack. SURICATA ConfD tail-f a Cisco company

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

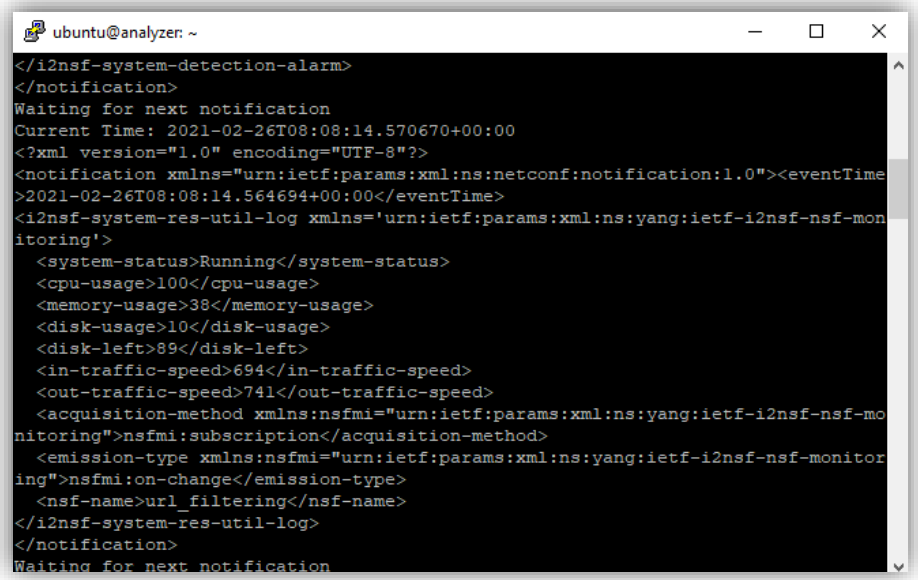
- Implementing Application Interface for delivering Feedback from I2NSF Analyzer to Security Controller.

Hackathon Plan (2/2)

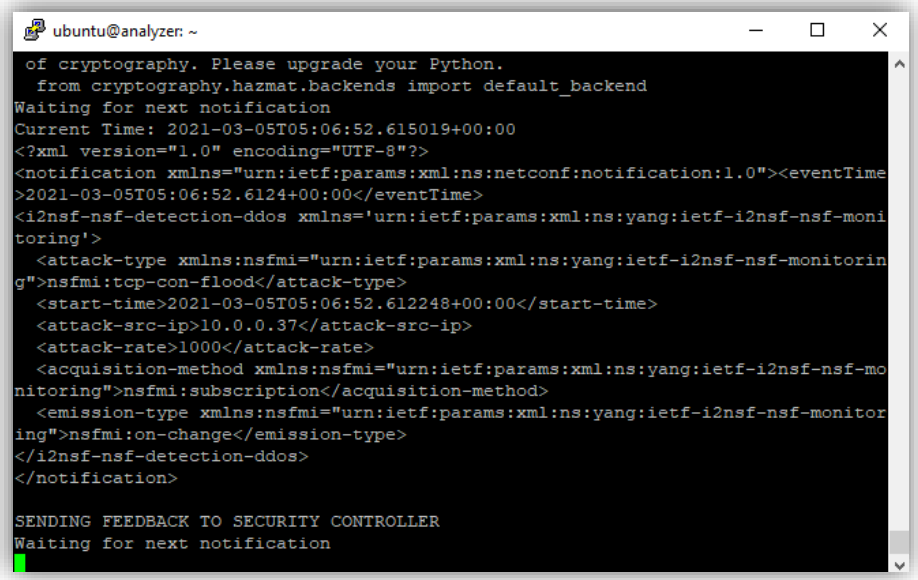


What got done (1/3)

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



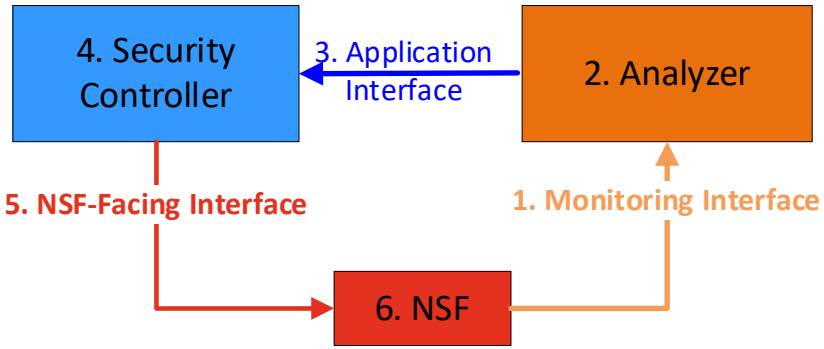
Monitoring NSF's Resources



Monitoring DDoS Detection

What got done (2/3)

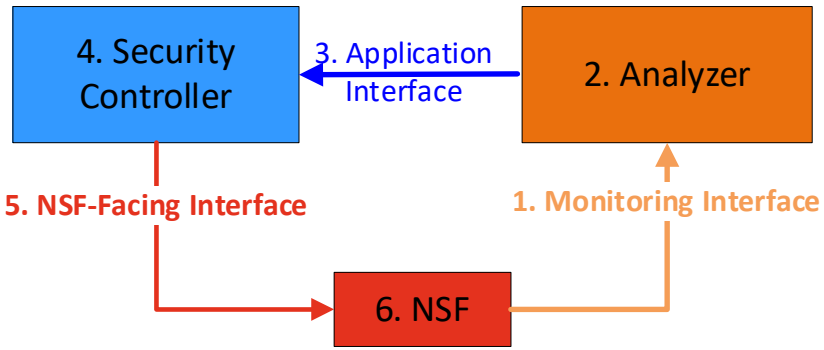
- Implementation of Application Interface for Feedback delivery to create a closed-loop system of I2NSF Framework.



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.

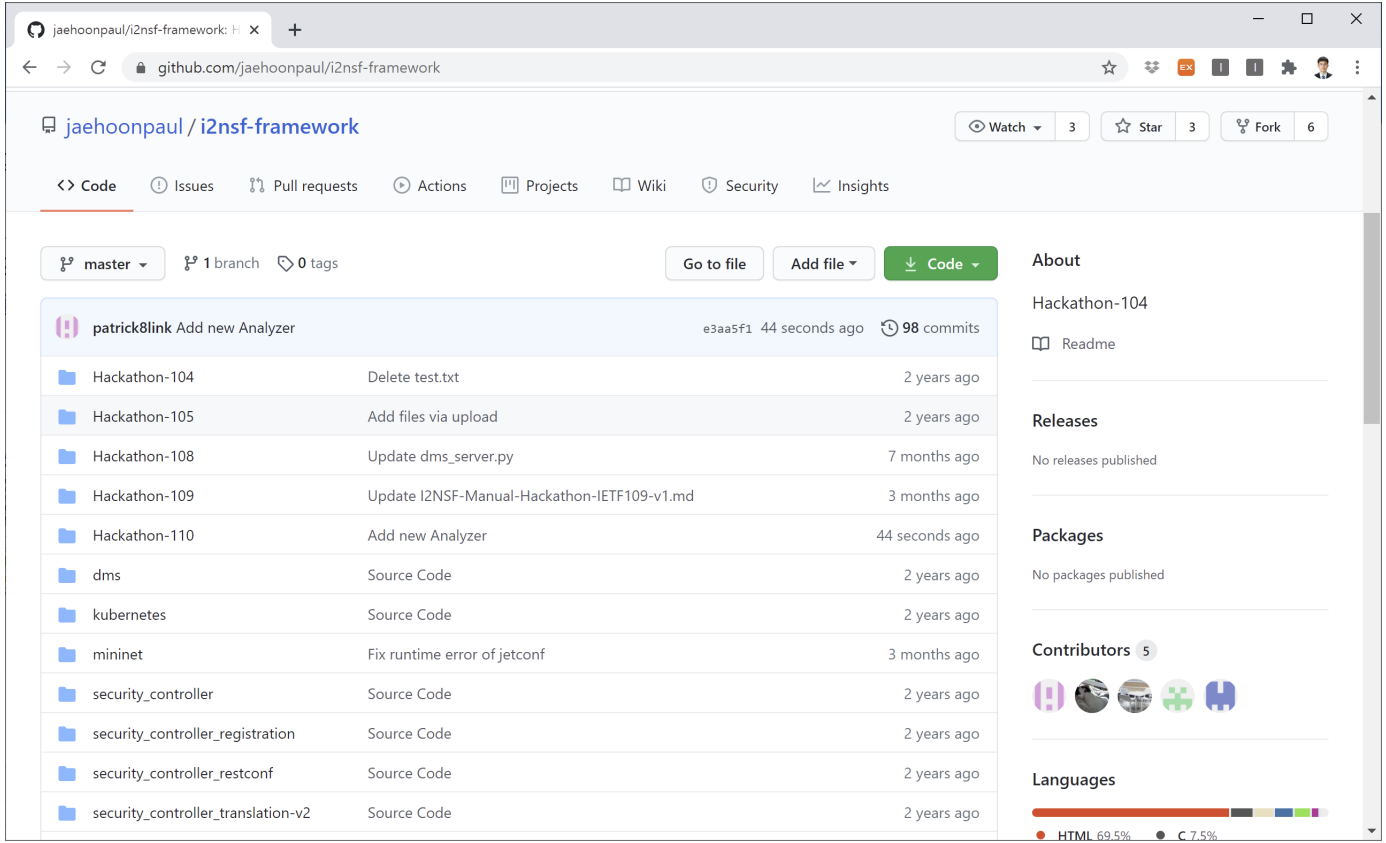
- The Feasibility of Application Interface in I2NSF Framework is demonstrated for Security Management Automation.

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



Wrap Up

I2NSF Hackathon Team

Champion:
- Jaehoon Paul Jeong (SKKU)

Professor:
- Younghan Kim (SSU)

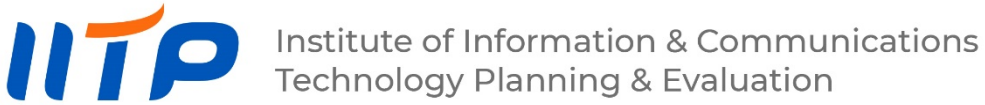
Researchers:
- Jung-Soo Park (ETRI)
- Yunchul Choi (ETRI)

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


NRF
National Research
Foundation of Korea


IITP
Institute of Information & Communications
Technology Planning & Evaluation


TTA
한국정보통신기술협회
Telecommunications Technology Association


SUNG KYUN KWAN UNIVERSITY
성균관대학교
1398


숭실대학교
Soongsil University


ETRI
한국전자통신연구원
Electronics and Telecommunications Research Institute


K-IETF
KOREA IETF FORUM