IETF Hackathon

I2NSF Framework Project

IETF 111
July 19-23, 2021
Online

Champions:
Jaehoon (Paul) Jeong and Patrick Lingga
Sungkyunkwan University (SKKU)
{pauljeong,patricklink}@skku.edu

I2NSF (Interface to Network Security Functions) Framework Project

Champions: Jaehoon (Paul) Jeong and Patrick Lingga (SKKU)

I2NSF Hackathon Project

Professors:

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

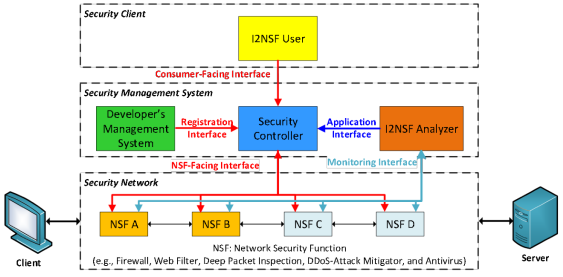
Researchers:

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

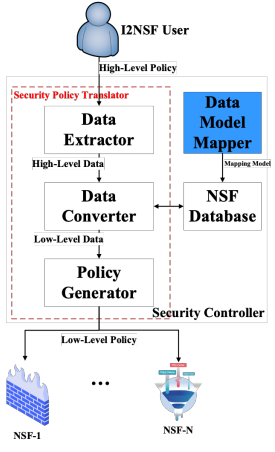
Students:

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

I2NSF Framework



I2NSF Security Policy Translator



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

- I2NSF-Manual-Hackathon-IETF110-v1.md contain 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 Function
  - ✓ Security Policy Translation with Automatic Data Model Mapper
  - ✓ Security Policy Provisioning

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

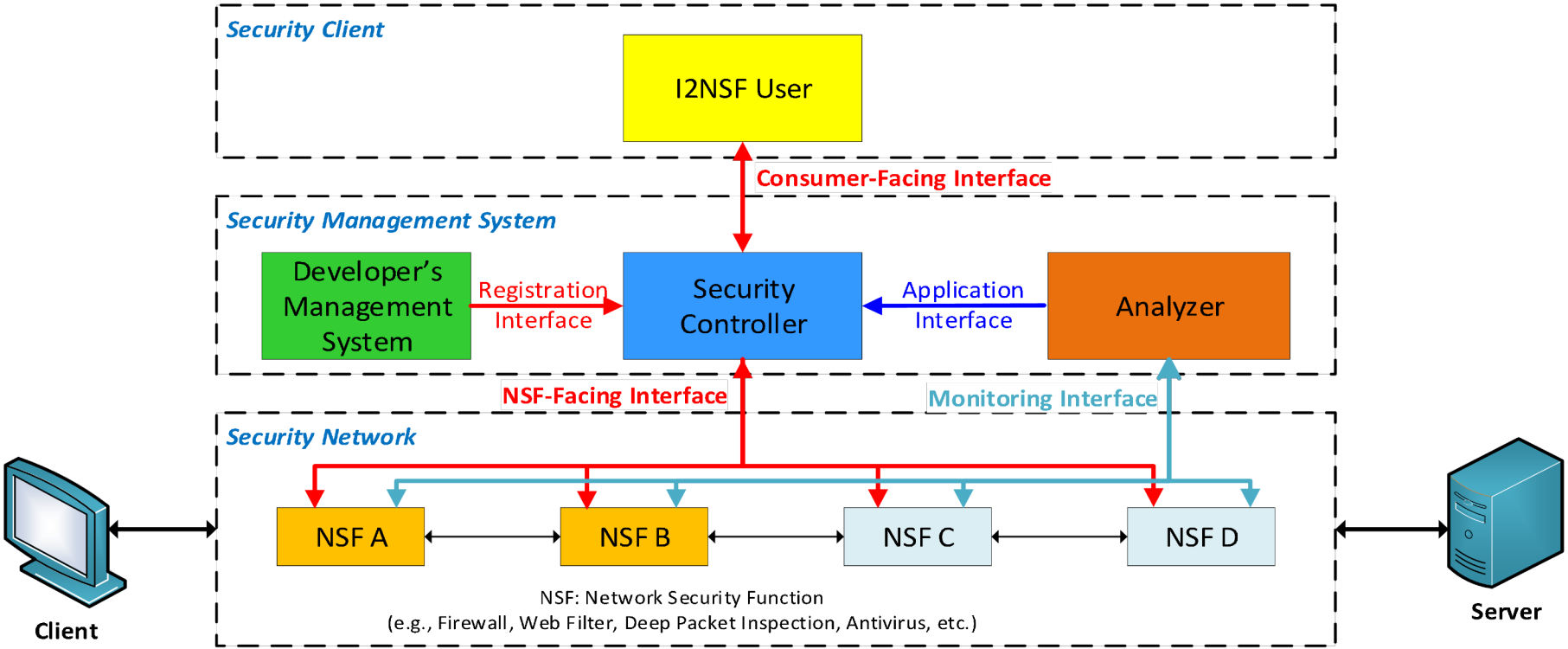
Hackathon Plan (1/2)

- The Implementation of the Internet Drafts for the I2NSF System for Cloud-based Security Services:
  - draft-ietf-i2nsf-capability-data-model-16
  - draft-ietf-i2nsf-consumer-facing-interface-dm-13
  - draft-ietf-i2nsf-nsf-facing-interface-dm-12
  - draft-ietf-i2nsf-registration-interface-dm-10
  - draft-ietf-i2nsf-nsf-monitoring-data-model-08
  - draft-yang-i2nsf-security-policy-translation-08
  - draft-jeong-i2nsf-security-management-automation-01

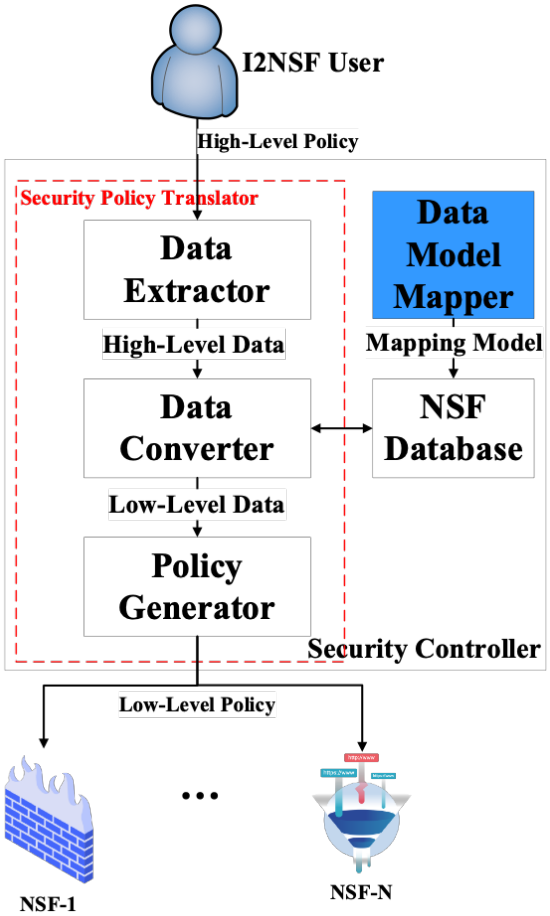
- Automatic Data Model Mapper for the I2NSF Security Policy Translator.

- Real-time Monitoring Data Visualization via Web-Based Monitoring.

Hackathon Plan (2/2)



What got done



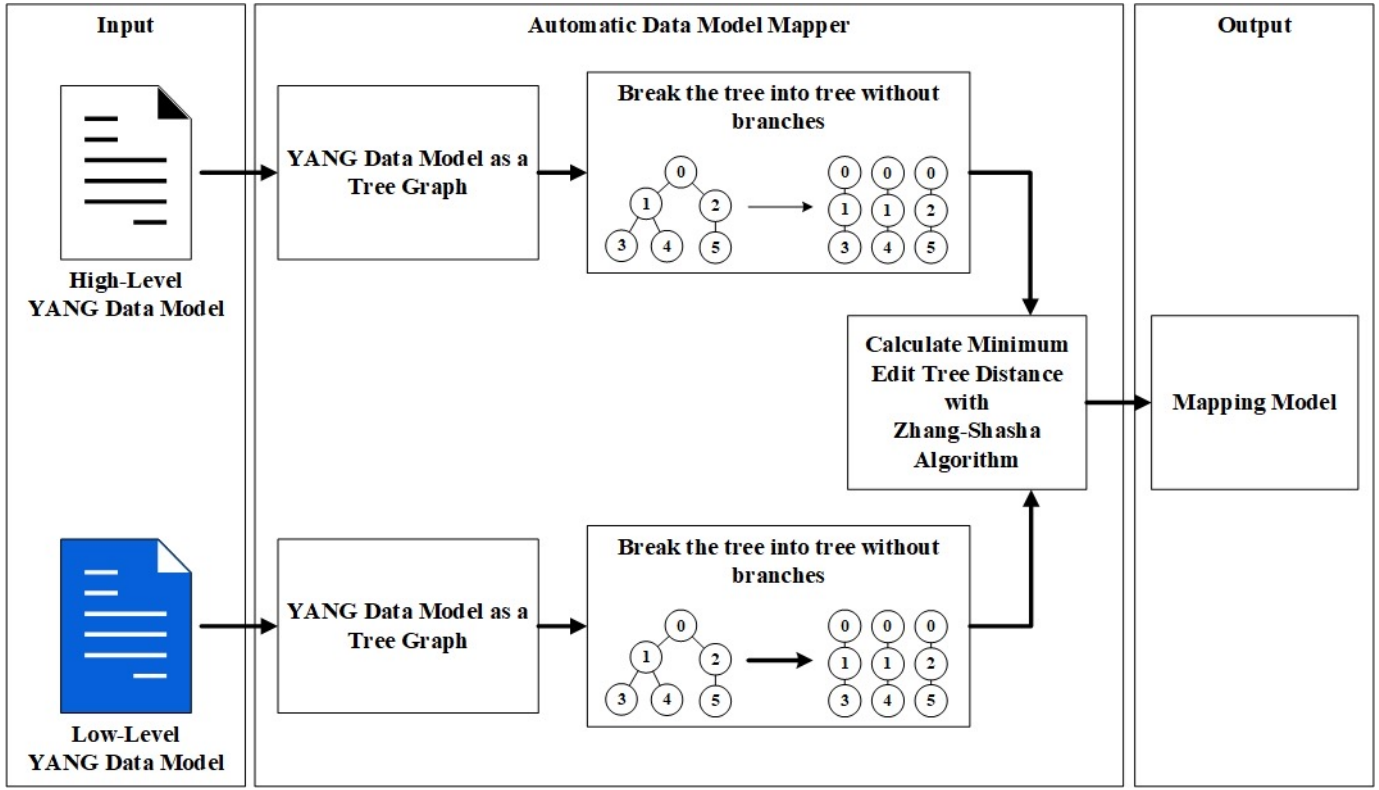
- The overall architecture of our scheme consists of five components:
  - Data Extractor
  - Data Converter
  - NSF Database
  - Policy Generator
  - Data Model Mapper
- Automatic Data Model Mapper
  - Data Model Mapper provides an automatic mapping between the high-level and low-level data models.

Task 1: Automatic Data Model Mapper

- Key Idea: We use Zhang-Shasha algorithm to calculate the Tree Edit Distance between the high-level YANG tree and the low-level YANG tree.

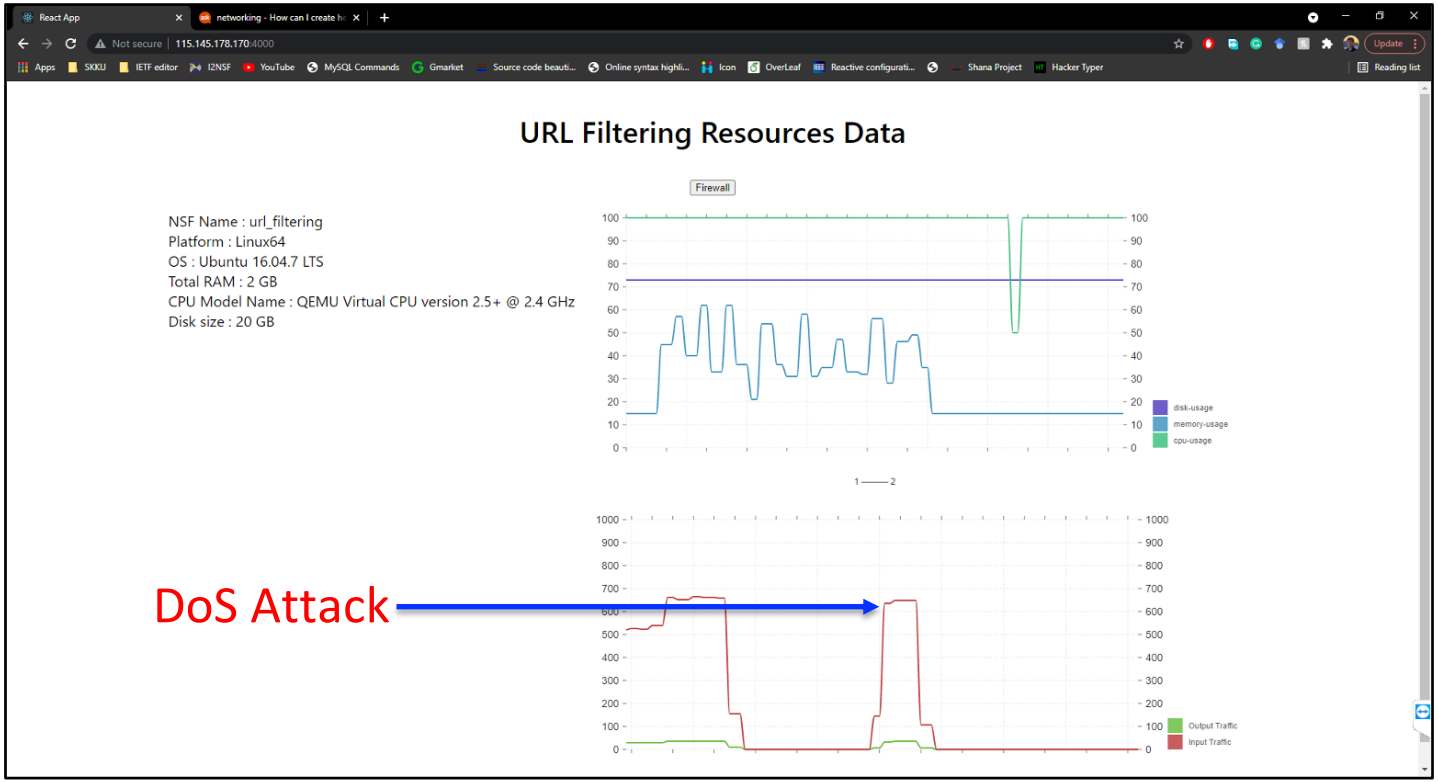
Consumer-Facing Interface Data Model

NSF-Facing Interface Data Model



Task 2: Real-time Monitoring Data Visualization

- We visualize the utilization of resources (i.e., disk, memory, and CPU) and the volume of input and output data traffic to detect a security attack (e.g., DoS attack).



What we learn

- The Security Policy Translator can automatically translate a high-level security policy into the corresponding low-level security policy with the help of an automatic data model mapper.

- The monitoring data visualization can support the monitoring of multiple NSFs in real time in terms of resources and traffic.

- This monitoring data visualization will be useful to perform the analysis of an NSF's behavior (e.g., security attack detection).

Next Step

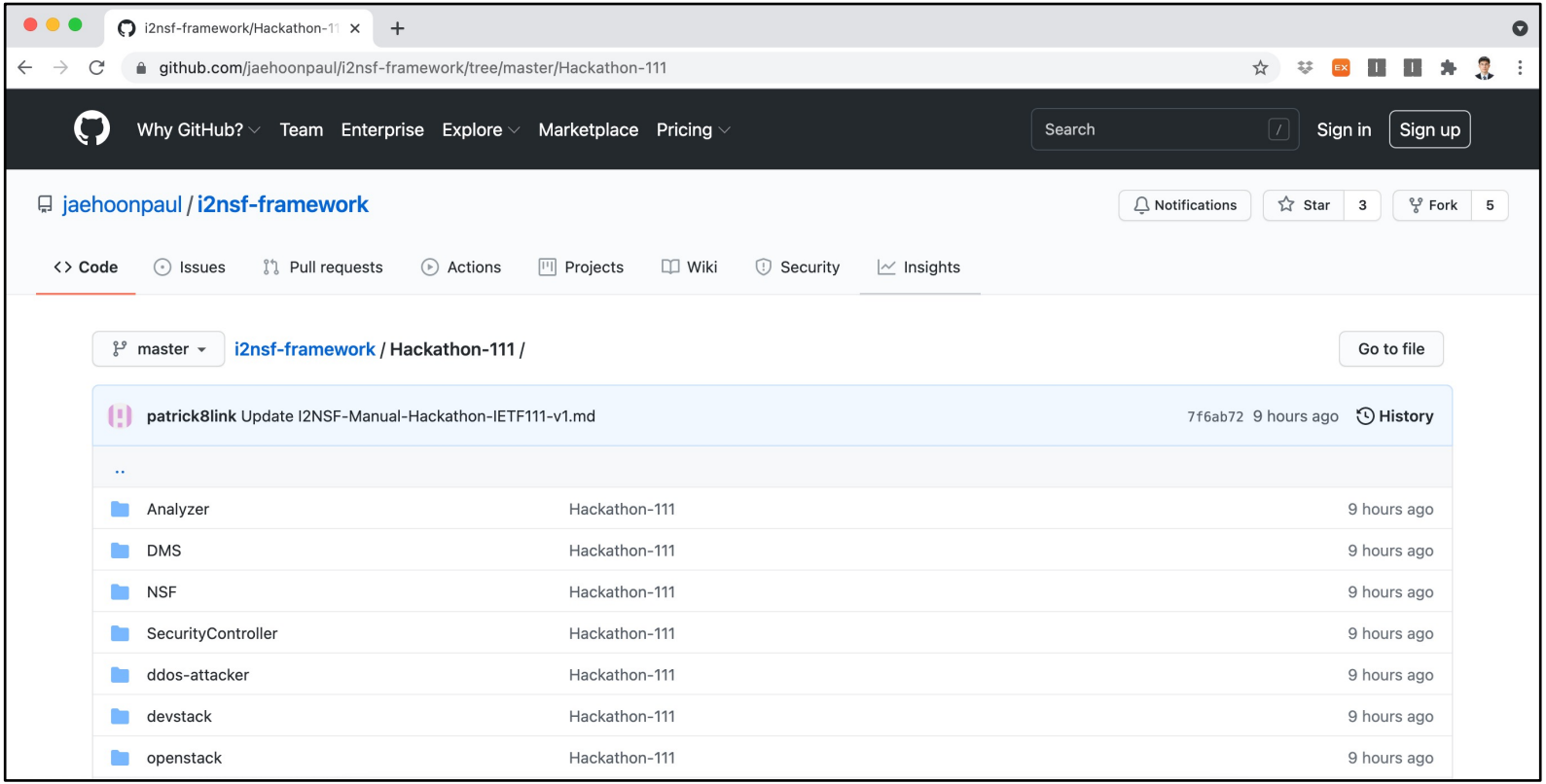
- Security Policy Translator needs to be improved with Context-Free Grammar Auto-Construction for Policy Generator.

- Improvement of I2NSF Analyzer with Machine Learning to update and create a security policy.

- Migration from VNF-based Virtualization to Container-based Virtualization for the I2NSF Framework

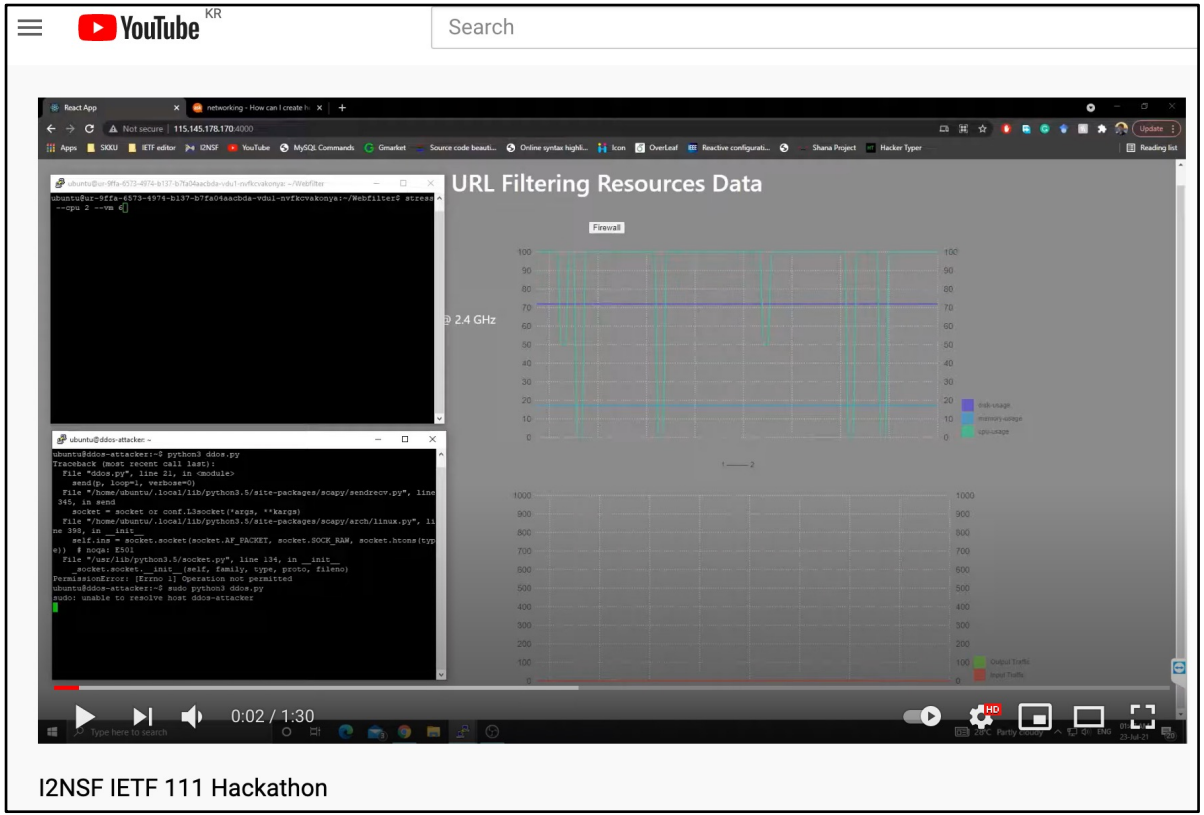
Open Source Project at Github

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



Demo Video Clip at YouTube

- URL: https://youtu.be/gHzZKpJ9zak



Wrap Up

Hackathon Team

Champions:

- Jaehoon (Paul) Jeong (SKKU)
- Patrick Lingga (SKKU)

Professor:

- Younghan Kim (SSU)

Researchers:

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

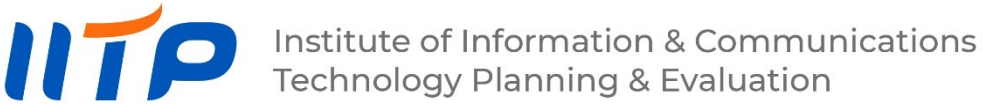
Students:

- Jeonghyeon Kim (SKKU)
- Mose Gu (SKKU)
- Yoseop Ahn (SKKU)
- Xiaohong Yu (SKKU)
- Kyungsik Kim (KNU)

Our I2NSF Hackathon Team worked with IPWAVE and BMWG Hackathon Teams in the Westin Josun Busan Hotel in Korea this hackathon week.

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

IETF Korea Hackathon Teams