

Report of I2NSF Framework Project @ IETF-101 Hackathon



IETF 101, London

March 21, 2018

Champions: Jaehoon Paul Jeong and Jinyong Tim Kim

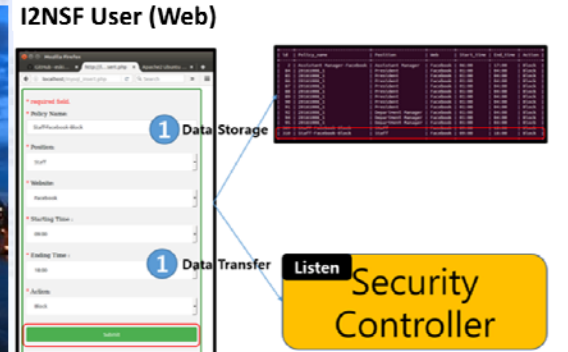
Sungkyunkwan University

Why Did We Do this Project?

- ❖ **I2NSF: Use NETCONF, RESTCONF & YANG Data Models**
 - Is I2NSF reasonable for the management of network security functions?
 - Can we implement I2NSF using open source software?
- ❖ **This work is a student project!!**
 - 7 graduate students at Sungkyunkwan University
 - Source Code on Github
 - <https://github.com/kimjinyong/i2nsf-framework/tree/master/Hackathon-101>

IETF I2NSF (Interface to Network Security Functions) Working Group: I2NSF Framework Project

Champions: Jaehoon Paul Jeong and Jinyong Tim Kim (SKKU)



Professors

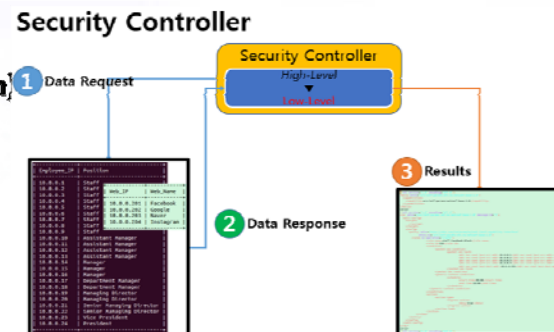
- Jaehoon (Paul) Jeong (Sungkyunkwan)
- Hyoungshick Kim (Sungkyunkwan)
- Sangwon Hyun (Sungkyunkwan)

Collaborators

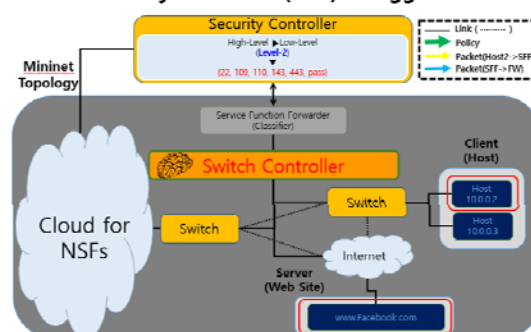
- Jung-Soo Park (ETRI)
- Tae-Jin Ahn (Korea Telecom)

Students

- Jinyong Tim Kim
- Eunsoo Kim
- Dongjin Hong
- Tae-Kyun Roh
- Sarang Wi
- Seungjin Lee
- Jinhyuk Yang



Network Security Functions (NSF) - Triggered Steering



Where to get code

- Github – Source code
✓ <https://github.com/kimjinyong/i2nsf-framework>

What to pull down to set-up environment

- OS: Ubuntu 14.04TL
- Confd for NETCONF: 6.2 Version
- Apache2: 2.4.7 Version
- MySQL: 14.14 Version
- PHP: 5.5.9 Version
- Mininet: 2.2.1 Version
- OpenDaylight: Distribution-karaf-0.4.3-Beryllium-SR3
- XSLT (Extensible StyleSheet Languages Transformations)
- Jetconf: Jetconfs a python Open API for RESTCONF.

Manual for Operation Process

- README.txt

Contents of Implementation

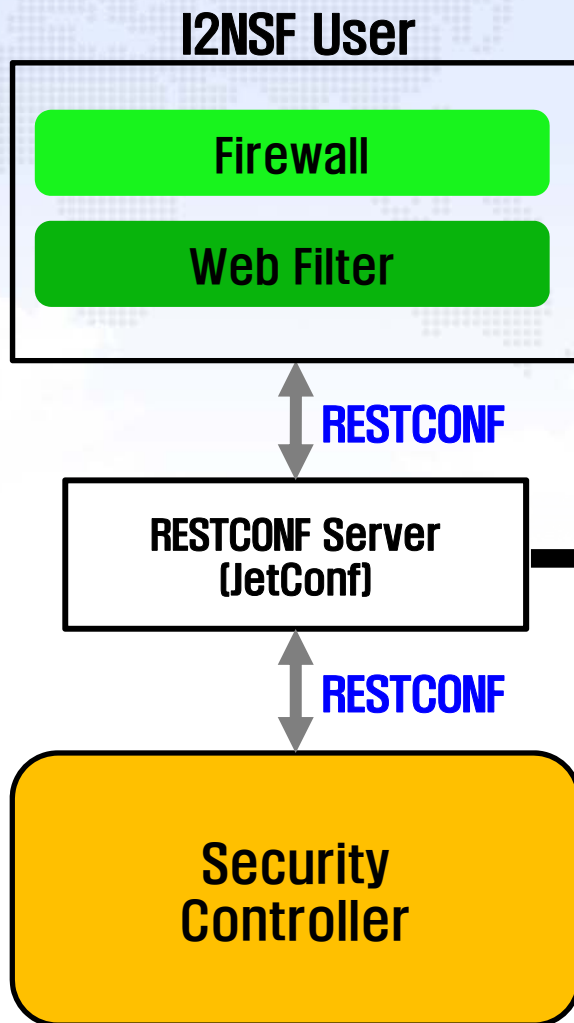
- I2NSF Framework for provisioning Network Security Functions (NSF)
 - ✓ Consumer-Facing Interface via RESTCONF/YANG (New Feature)
 - ✓ NSF-Facing Interface via NETCONF/YANG
 - ✓ Registration Interface via NETCONF/YANG
- Network Security Functions
 - ✓ Firewall using SDN and Suricata
 - ✓ Deep Packet Inspection (DPI) using Suricata
- Advanced Functions
 - ✓ Dynamic Policy Configuration (New Feature)
 - ✓ NSF-triggered Traffic Steering using SFC (New Feature)
 - ✓ YANG Data Modeling for NSF Monitoring

Goal of I2NSF Project

I2NSF Framework is extended with

1. **Dynamic Configuration** to map Security Service to Network Security Function at Security Controller.
2. **Consumer-Facing Interface** based on RESTCONF and the latest YANG Data Model.

I2NSF Consumer-Facing Interface

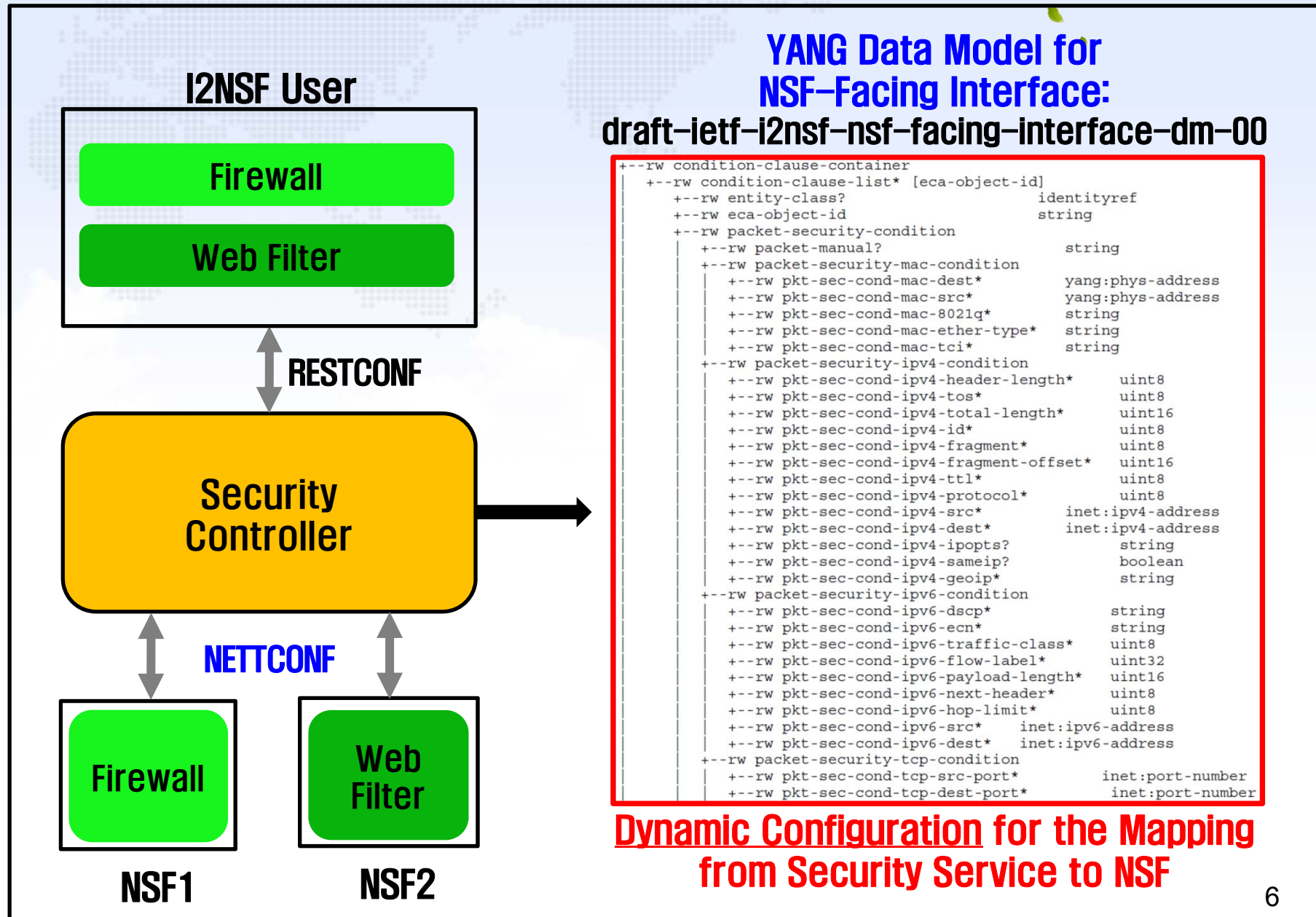


YANG Data Model for Consumer-Facing Interface: draft-ietf-i2nsf-consumer-facing- interface-dm-00

```
module: policy-general
+--rw policy
  +--rw rule* [rule-id]
    +--rw rule-id                uint16
    +--rw name?                  string
    +--rw date?                  yang:date-and-time
    +--rw case?                  string
    +--rw event* [event-id]
      +--rw event-id            string
      +--rw name?               string
      +--rw date?               yang:date-and-time
      +--rw event-type?         string
      +--rw time-information?   string
      +--rw event-map-group?    -> /threat-feed/event-map-group
                               /event-map-group-id
    +--rw enable?               boolean
  +--rw condition* [condition-id]
    +--rw condition-id          string
    +--rw source?               string
    +--rw destination?          string
    +--rw match?                boolean
    +--rw match-direction?      string
    +--rw exception?            string
  +--rw policy-action* [policy-action-id]
    +--rw policy-action-id      string
    +--rw name?                 string
    +--rw date?                 yang:date-and-time
    +--rw primary-action?       string
    +--rw secondary-action?     string
    +--rw owner?                string
```

**Enhanced Security Policy Delivery having
Event-Condition-Action Paradigm
to Security Controller via RESTCONF Server**

I2NSF NSF-Facing Interface



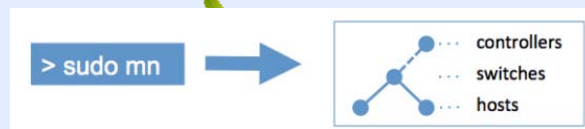
Hackathon Development

Build Environment

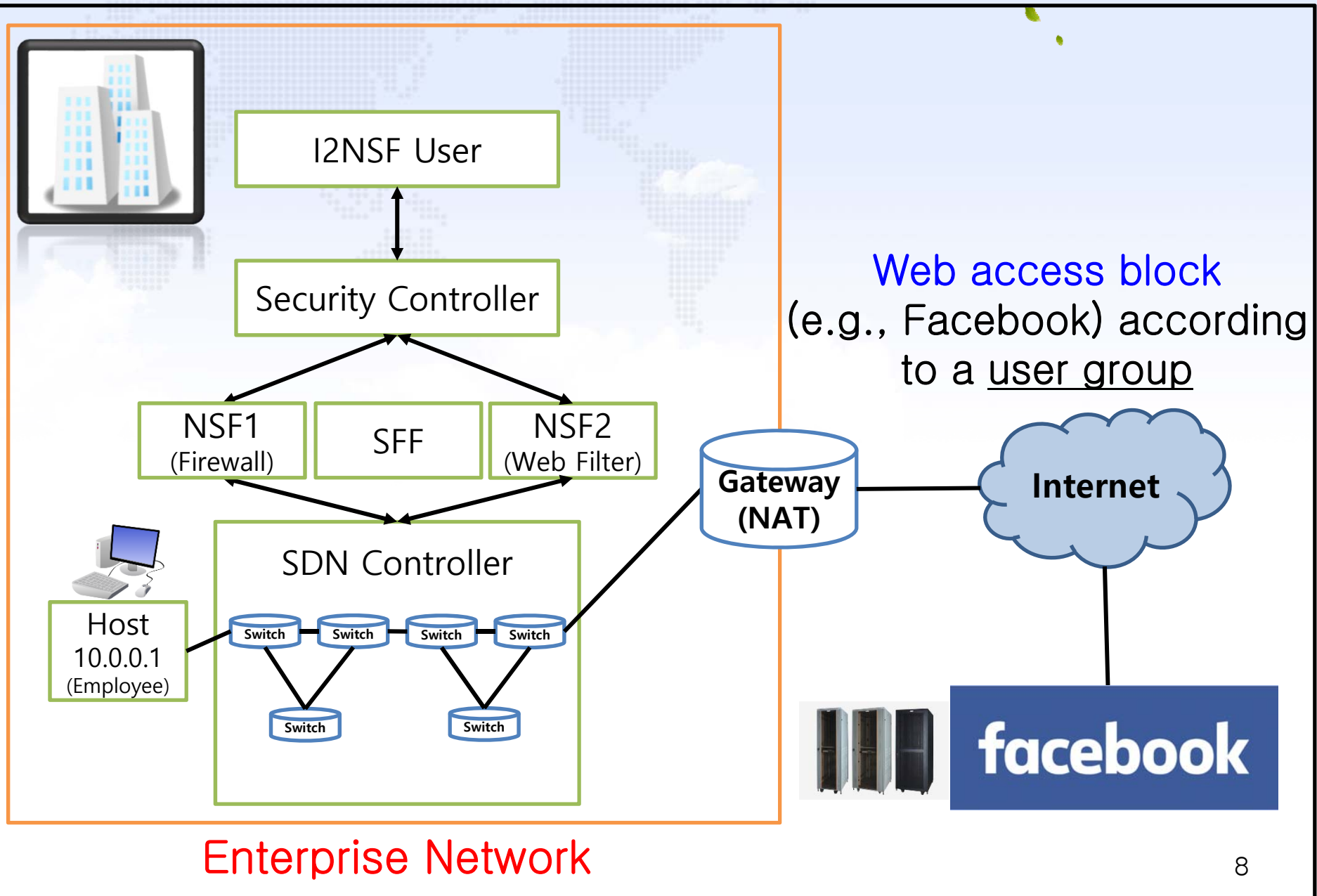
1. OS
 - Ubuntu 14.04TL
2. Netconfd
 - 6.2 Version
3. Apache2
 - 2.4.7 Version
4. MySQL
 - 14.14 Version
5. PHP
 - 5.5.9 Version



5. Mininet
 - 2.2.1 Version
6. OpenDaylight
 - Distribution-karaf-0.4.3-Beryllium-SR3
7. Suricata
 - 3.2.1 RELEASE



Network Configuration for Hackathon

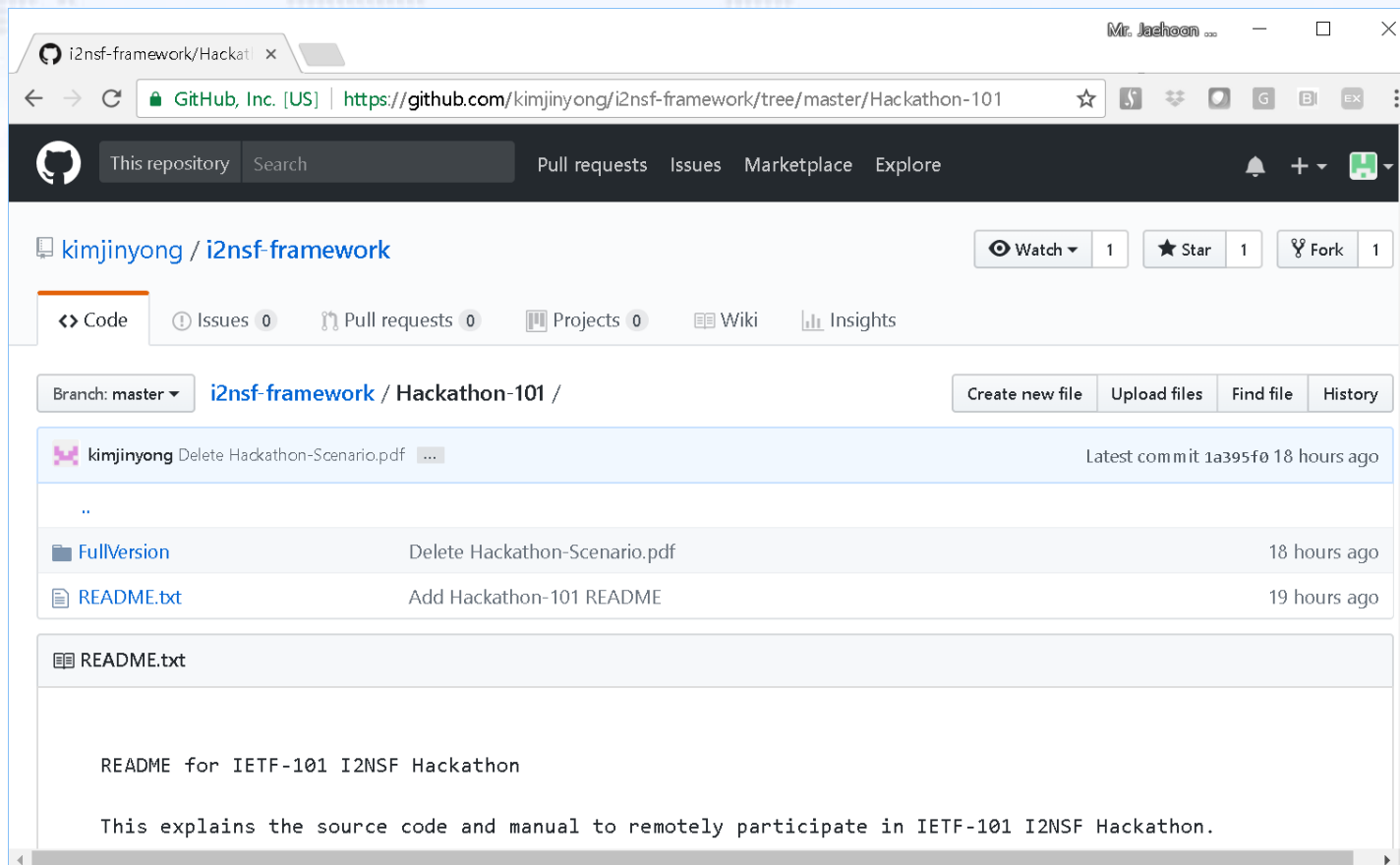


Information of I2NSF Hackathon Project (1/2)

Github for I2NSF Framework Project

➤ Documents and Source Code

<https://github.com/kimjinyong/i2nsf-framework/tree/master/Hackathon-101>

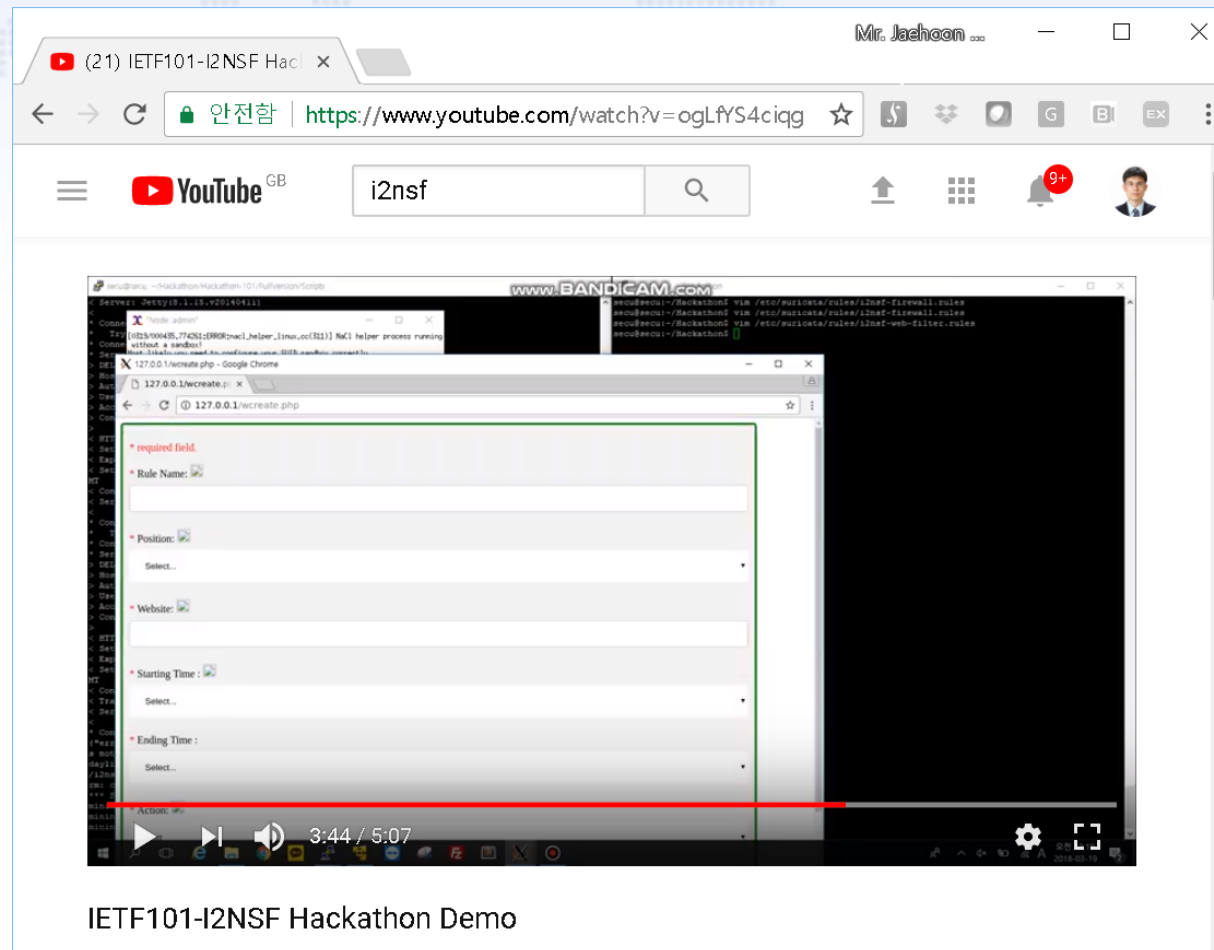


Information of I2NSF Hackathon Project (2/2)

YouTube for I2NSF Framework Project

➤ Videoclip for Demonstration

<https://www.youtube.com/watch?v=ogLfYS4ciqg>



Lessons from the Implementation @ Hackathon

- **Proof of Concept (POC) of I2NSF Framework and YANG Data Models using Open Sources:**
- **Confd** for NSF-Facing Interface and Registration Interface
 - **JetConf** for Consumer-Facing Interface
 - **Suricata** for NSFs (i.e., Firewall and Web Filter)
 - **OpenDaylight** for SDN Controller
 - **NSH and tunneling** for packet steering over NSFs
 - **Mininet** for SDN Network