Report of I2NSF Hackathon Project
@ IETF-97 Hackathon
November 14, 2016

Jaehoon (Paul) Jeong
Sungkyunkwan University
pauljeong@skku.edu
Why did we do this project?

- **I2NSF:** Chartered to use NETCONF/RESTCONF + Data Models
  - Is this approach reasonable for management of security devices?
  - Is it better than writing another security protocol?
  - Can we get I2NSF Key Data Model (Capability) refined, and put open source code for VOIP/VoLTE and Firewall?

- **Result:** I2NSF WG approach works, fast time to market
  - NM/OPS should expand their work into Security.
  - I2NSF follows up with MILE, SACM, DOTS, and SECEVENTs.

- **Does this work for a student project – Yes!!**
  - 25 new 1st timers at IETF
  - Put Code on Web
Champions: Jaehoon Paul Jeong, Jinyong Tim Kim (SKKU), Jung-Soo Park (ETRI), and Tae-Jin Ahn (KT)

IETF 97 Hackathon
I2NSF Framework Project

Where to get code
- Github – Source code
  ✓ https://github.com/YunSukYeo/securBrain/invitations
- USB – Source code & environment
  ✓ Provided by USB Driver

What to pull down to set-up environment
- OS : Ubuntu 14.04TL
- Netconfd : 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

Manual for Operation Process
- README.txt

Contents of Implementation
- Firewall
- DPI for VoIP-VoLTE Security Service

Mission
- Firewall
  ✓ Deletion of policy
  ✓ Update of policy
  ✓ Avoidance of the duplication of policy
- VoIP-VoLTE Security Service
  ✓ Deletion of policy
  ✓ Update of policy
  ✓ Avoidance of the duplication of policy

Professors
- Jaehoon (Paul) Jeong (Sungkyunkwan)
- Hyounghshick Kim (Sungkyunkwan)
- Hoon Ko (Sungkyunkwan)
- Sangwon Hyun (Sungkyunkwan)

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

Students
- Jinyong Tim Kim
- Sanguk Woo
- Daeyoung Hyun
- Eunsoo Kim
- Mahdi Daghmehchi Firoozjaei
- Sanghak Oh
- Yunsuk Yeo
- Soyoung Kim
What are Network Security Functions (NSFs)?

*NSF: Network Security Function

Enterprise Network

Switch

NSF1 (Firewall)

How to do?

Forward

Destination Host

NSF2 (DPI)

Valid Packet?

Yes

No

Enough?

packet
Given the code base of I2NSF Framework for provisioning Network Security Functions (NSFs), we implemented two things:

(i) **Firewall** for Web-filtering in I2NSF Framework using SDN and

(ii) **Deep Packet Inspection (DPI)** for VoIP/VoLTE Security Service in I2NSF Framework.
1. Proof of Concept (POC) of I2NSF Framework using Open Sources.


Environment of Hackathon Development

Building 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

> sudo mn

[Diagram of network topology]
I2NSF Drafts of this I2NSF Project

I2NSF Working Group Drafts


Scenario of Security Services in I2NSF Testbed

Enterprise Network with I2NSF

I2NSF User (security policy)

Security Controller

NSF1 (Firewall)  NSFF  NSF2 (DPI)

SDN Network

Host 10.0.0.1 (Employee)

Gateway at Africa

Internet

Facebook 10.1.1.10

Youtube 10.2.1.20

1. Time-dependent Firewall
   e.g.) 09:00 – 18:00 => Block
   18:01 – 08:59 => Unblock

2. VoIP/VoLTE Filtering Rule
   e.g.) Blacklist of SIP URI and User Agent

*NSF: Network Security Function
*NSFF: NSF Forwarder for Traffic Steering
1. **Proof of Concept (POC) of I2NSF Framework using Open Sources:**
   - Confd for NETCONF
   - OpenDaylight for SDN Controller
   - Mininet for SDN Network
   - RestAPI for I2NSF Interface

2. **Validity of I2NSF Interface Design for I2NSF Framework:**
   - Firewall for Web Filtering
   - DPI for VoIP/VoLTE (e.g., Blacklist and Whitelist)

3. **Feasibility of Data-driven Approach (YANG) for Network Security:**
   - YANG Data Models for I2NSF Interfaces among System Entities (I2NSF User, Security Controller, NSFs)
Demonstration of I2NSF Implementation

YouTube Video Clip:
https://www.youtube.com/watch?v=5iflpVt4l6U&feature=youtu.be

1. **GitHub** for I2NSF Open Source Project:
   - Link: [https://github.com/kimjinyong/i2nsf-framework](https://github.com/kimjinyong/i2nsf-framework)

2. **IETF-97 Hackathon** having this Project
   - Link: [https://www.ietf.org/hackathon/97-hackathon.html](https://www.ietf.org/hackathon/97-hackathon.html)
   - Wiki: [https://www.ietf.org/registration/MeetingWiki/wiki/97hackathon](https://www.ietf.org/registration/MeetingWiki/wiki/97hackathon)
   - Slides: [https://datatracker.ietf.org/meeting/97/session/hackathon](https://datatracker.ietf.org/meeting/97/session/hackathon)