I2NSF
Internet Draft
Intended status: Informational
Expires: April 30, 2017

T. Ahn
S. Lee
K. Kim
U. Kim
KT

October 31, 2016

Use Cases for the Communications Security using Interface to Network Security Functions

draft-ahn-i2nsf-communications-security-use-case-01.txt

Status of this Memo

Copyright Notice

Abstract

This document provides use cases for the IP-based communications security using Interface to Network Security Functions (I2NSF). The use cases in this document cover the detection and prevention of the illegal authentication, call of VoIP/VoLTE and spam message.

Table of Contents

1. Introduction

As VoLTE is a crucial service for telecommunication operators, it becomes more important to provide secure voice and messaging communication services. VoLTE and VoIP are based on IP, attacks such as compromising the telephony application or re-routing the IP signal can be happened.

This document describes IP-based communications security use cases

for Interface to Network Security Functions (I2NSF) such as VoIP, VoLTE and messaging service.

2. Conventions used in this document

VoLTE: Voice over LTE

SND: Software defined Network

NSF: Network Security Function

I2NSF: Interface to Network Security Functions

3. Use Cases

3.1. Framework of the I2NSF communication security

```
+-----------------------------------------------------+
| I2NSF Client                            |
| (Communications Security Service Manager)           |
|                                   |
+----------+-----------------------------------------+
           |
           | Client Facing Interface
           |
+----------+----------+               +-------------+
| Communications      |               | Developer's |
| Security Controller |               | Mgnt System |
+---------------+-----+ <--------->   +-------------+
           |        Registration Interface
           |
           | NSF Facing Interface
           |
     +----------+------------------+------------------+
   |                            |                  |
   |                            |                  |
+---+--------------+    +---------+--------+   +----+------------+
|    VoIP          |    |    VoLTE         |    |    Messaging    |
| Security Function|    | Security Function|    |Security Function|
+------------------+    +------------------+    +-----------------+
        |                         |                      |
        +-------------------------+----------------------+
                                  |
            +---------------------+-------------------+
            |                                         |
    +-------+----------+                     +--------+--------+
    |   SDN-Enabled    |                     |    Non-SDN      |
    |    Network       |                     |    Network      |
    +------------------+                     +-----------------+
```

Figure 1 I2NSF Framework for Communications Security

3.2. Use Case of Voice Call Security

The procedure of VoIP/VoLTE voice call security operations is as follows:

1. Communications Security Manager(I2NSF Client) sends rules to Communication Security Controller to block packets or flows that match conditions that operators configure. In voice call security, those rules can be prevention of the Caller ID spoofing or DDoS attack.

2. Communication Security Controller creates and sends the data model that the Communication Security Function can understand. The data model includes the Events, Conditions and Actions. In this use case Events can be originating call by user action and Conditions can be IP address and port of origination and termination device, User-Agent of device, media information of device such as SDP(Session Description Protocol) and call state such as call setup state, conversation state. Actions can be packet or flow permit, drop, forward to Communication Security Controller or updating and applying Communication Security Profile.

3. Communication Security Function applies the rules which are sent in forms of data model from the Security Controller. After applying the rules, it monitors the flows and packets. If the underlay network is SDN-enabled network, it requests the SDN controller to apply the security rules with APIs. The SDN switches monitor requested events and when the events match the rule, they drop, permit, mirror or forward to the SDN controller.

4. When Communication Security Function detects the flows or packets that meet the Conditions, it performs Actions that Communication Security Controller defines with data model. In case of Caller ID spoofing prevention, Communication Security Function mirrors the packets to Communication Security Controller and Communication Security Controller determine whether they are manipulated or not with the combination of IP address of the call, Caller-ID, and URIs of the call.

5. If Communication Security Controller determines that the forwarded packets must be dropped, it updates the policy rule or Communication Security Profile to drop the packet and send the update rules to Communication Security Function.

6. Communication Security Function updates the rule of data model and performs the Actions that Communication Security Controller defines. In case of Caller ID spoofing, Communication Security Function tears down the call.

3.3. Use Case of prevention of VoIP/VoLTE device scanning

The procedure of detection and prevention of VoIP/VoLTE device scanning to find vulnerable to hacking is as follows:

1. Communications Security Manager(I2NSF Client) sends rules to Communication Security Controller to block packets or flows that try to scan the VoIP/VoLTE devices that are vulnerable to hacking for fraud call. In this case, those rules can be prevention of the scanning of customer's communication devices.

2. Communication Security Controller creates and sends the data model that includes the Events, Conditions and Actions. In this use case Events can be originating call by user action and Conditions can be statistics of accumulated call attempt counts from each source IP address or each originating phone number, signal message type such as INVITE, OPTIONS, REGISTER in SIP. Actions can be packet or flow permit, drop, forward to Communication Security Controller or updating and applying Communication Security Profile.

3. Communication Security Function applies the rules which are sent in forms of data model from the Security Controller. After applying the rules, it monitors the flows and packets. To monitor the statistics of the packet or call attempt count, Communication Security Function needs the Statistics Processor. Statistics Processor counts packets and calls from each source IP address or originating number within specific duration such as per minute, hour or day.

4. When Communication Security Function detects the flows or packets that meet the Conditions, it performs Actions that Communication Security Controller defines with data model. In case of device scanning prevention, Communication Security Function manages the statistics. When a statistics matches the threshold value, Communication Security Function forwards the packets to Communication Security Controller and Communication Security Controller determine whether they are packets for the device scanning or not with the statistics of the accumulated packet or call count within specific time duration.

5. If Communication Security Controller determines that the forwarded packets are for device scanning, it updates the policy rule or Communication Security Profile to drop the packets and send the update rules to Communication Security Function.

6. Communication Security Function updates the rule of data model and performs the Actions that Communication Security Controller defines. In case of device scanning, Communication Security Function drops the packets.

3.4. Use Case of prevention of spam messages

The procedure of detection and prevention of spam messages such as SMS, MMS is as follows:

1. Communications Security Manager(I2NSF Client) sends rules to Communication Security Controller to block packets or flows that sends spam messages. In this case, those rules can be blocking of the messages that exceed the threshold message sending count or contain the banned terms.

2. Communication Security Controller creates and sends the data model that includes the Events, Conditions and Actions. In this use case Events can be sending message by user action and Conditions can be statistics of accumulated message sending counts from each source IP address or each originating phone number and terms in the message within specified range of the message packet. Actions can be packet or flow permit, drop, forward to Communication Security Controller or updating and applying Communication Security Profile and Signature file.

3. Communication Security Function applies the rules which are sent in forms of data model from the Security Controller. After applying the rules, it monitors the flows and packets. To monitor the message sending statistics, Communication Security Function needs the Statistics Processor. Statistics Processor counts message sending counts from each source IP address or originating number within specific duration such as per minute, hour or day. Also Communication Security Function checks the message content whether it contains the banned terms within specified range of the message packet.

4. When Communication Security Function detects the flows or packets that meet the Conditions, it performs Actions that Communication Security Controller defines with data model. In case of device spam message prevention, Communication Security Function manages the statistics. When a statistics matches the threshold value, Communication Security Function forwards the packets to Communication Security Controller. Communication Security Controller determines whether they are packets for the spam or not with the statistics.

5. If Communication Security Controller determines that the forwarded packets are for spam, it updates the policy rule or Communication Security Profile to drop the packets and send the update rules to Communication Security Function.

6. Communication Security Function updates the rule of data model and performs the Actions that Communication Security Controller defines. In case of spam prevention, Communication Security Function drops the packets and updates the Signature file adding the new banned terms.

4. Security Considerations

TBD

5. IANA Considerations

No IANA considerations exist for this document.

6. Conclusions

This document provides use cases for the IP-based communications security using Interface to Network Security Functions (I2NSF). The use cases in this document cover the detection and prevention of the illegal authentication, call of VoIP/VoLTE and spam message.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2234] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

7.2. Informative References

[I-D. hares-i2nsf-problem-and-use-cases]

Hares, S., Zhang, D., Moskowitz, R., and H. Rafiee, " I2NSF Problem Statement and Use cases", draft-ietf-i2nsf-problem-and-use-cases-02 , October 2016.

[I-D.jeong-i2nsf-sdn-security-services]

Jeong, J., Kim, H., and P. Jung-Soo, "Requirements for Security Services based on Software-Defined Networking", draft-jeong-i2nsf-sdn-security-services-01 (work in progress), March 2015.

8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

Authors' Addresses

Taejin Ahn
KT
KT Infra R&D Lab
Korea

Phone: +82 10 6750 6828
Email: taejin.ahn@kt.com

Sehui Lee
KT
KT Infra R&D Lab
Korea

Phone: +82 10 5114 7988
Email: sehuilee@kt.com

Kyoungyoul Kim
KT
KT Infra R&D Lab
Korea

Phone: +82 10 3485 6342
Email: kyoungyoul.kim@kt.com

Utae Kim
KT
KT Infra R&D Lab
Korea

Phone: +82 10 9893 7474
Email: utae.kim@kt.com