Per-user Policy Enforcement on Mobile Apps through Network Functions Virtualization

Workshop on Mobility in the Evolving Internet Architecture
Sep. 11, 2014, Maui, Hawaii, USA

Amedeo Sapio
Fulvio Risso
Politecnico di Torino

Yong Liao, Mario Baldi,
Gyan Ranjan, Alok Tongaonkar,
Ruben Torres, Antonio Nucci

Narus, Inc.
Motivation

Growing BYOD Trends

2013:
- SMBs supporting BYOD will increase by 14%

2014:
- Number of connected devices: 3.3/employee
- Gartner predicts 90% of companies will allow BYOD

Employee tablet use will see a year-to-year increase of 50%

1.2 billion smartphones will enter the market in the next 5 years

Courtesy of SEN Technologies
Motivation

Top Causes of Data Breach in 2013

- Hackers: 34%
- Theft or Loss of Computer or Drive: 27%
- Accidentally Made Public: 29%
- Insider Theft: 6%
- Unknown: 2%
- Fraud: 2%

Mobile Threat Classification

- Send Content: 13% (2012), 8% (2013)
- Adware Annoyance: 8% (2012), 9% (2013)
- Reconfigure Device: 8% (2012), 10% (2013)
- Traditional Threats: 25% (2012), 20% (2013)
- Steal Information: 32% (2012), 28% (2013)
- Track User: 30% (2012), 15% (2013)

Source: Symantec Threat Report 2014
Motivation

• Smartphones can collect a wide range of data
• Different mobile apps have different vulnerabilities
• Mobile apps traffic is largely undistinguishable from web traffic

• Different mobile apps can use the same remote end-point
• Use of encrypted connections by mobile apps is increasing
• Different roles within an organization have different security clearances and necessities
MAPPER
Mobile Apps Personal Policy Enforcement Router

- Network-based approach
- Mobile apps aware policies
- Device independent policies
- Per-user defined policies
- Uniform protection among different APs
- HTTPS support
Mobile Application Identification Module

Flows

XML summary

Features Extraction

Rule set

Features

Lookup

Metadata (Identifiers)

App

Categorization

Application Categories

App profile
FROG – Flexible and pROGrammable network node

Dedicated lightweight VM for each user

- Policy enforcement
- Traffic segregation
- Dynamic allocation
- Flexible policy definition
MAPPER Architecture

- Smart Wireless Access Point
- User dedicated lightweight VMs
- Mobile Apps Identification engine
- TLS proxy (MiMP)
- Application content filtering

![Diagram of MAPPER Architecture]

Network applications Marketplace

- Content Filter
- Malware Detector
- MiMP bridge
- Network Monitor
- Mobile app filter
- Firewall
- Parental Control

Management Server

- User policies
- Users & Groups
- Permissions

Mobile Application Identification Module
- Metadata
- Mobile App Categorization Module
- Classified Flows
- Mobility Classifier

MiMP

FROG

- VM User 1
- VM User 2
- VM User 3

Hypervisor

Parsed HTTP flows

App ID
MAPPER workflow

1. IP redirection
2. TLS proxying
3. Summary extraction
4. App Identification
5. Policy consistency
6. Policy enforcement

PEX: Personal EXecution Environment
GEX: Global EXecution Environment
MAI: Mobile Application Identification module
MiMP: Man-in-the-Middle Proxy
Evaluation – Single user

Average throughput (MByte/s)

```
Average throughput
(MByte/s)
```

<table>
<thead>
<tr>
<th></th>
<th>AP</th>
<th>FROG</th>
<th>MAPPER</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6</td>
<td>5</td>
<td>4</td>
</tr>
</tbody>
</table>

Response time CDF

```
Response time CDF
```

500 requests for 1 KB file
## Evaluation – Multi user

### Memory

<table>
<thead>
<tr>
<th>Number of clients</th>
<th>MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>1000</td>
</tr>
<tr>
<td>20</td>
<td>2000</td>
</tr>
<tr>
<td>30</td>
<td>3000</td>
</tr>
<tr>
<td>40</td>
<td>4000</td>
</tr>
<tr>
<td>50</td>
<td>5000</td>
</tr>
<tr>
<td>60</td>
<td>6000</td>
</tr>
<tr>
<td>70</td>
<td>7000</td>
</tr>
<tr>
<td>80</td>
<td>8000</td>
</tr>
</tbody>
</table>

- **PEXes**
- **FROG**
- **MIMP**
- **MAI**

### CPU, RAM, Throughput, Response time

<table>
<thead>
<tr>
<th>Number of clients</th>
<th>CPU</th>
<th>RAM</th>
<th>Throughput</th>
<th>Response time</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 user</td>
<td>16.13%</td>
<td>3261 MB</td>
<td>104 Kb/s</td>
<td>778.8 ms</td>
</tr>
<tr>
<td>2 users</td>
<td>21.57%</td>
<td>3392 MB</td>
<td>102 Kb/s</td>
<td>751.6 ms</td>
</tr>
</tbody>
</table>

500 online search queries
Conclusions

- MAPPER leverages Network Functions Virtualization for implementing fine-grained policies on mobile devices.
- Policies can be designed according to:
  - Mobile apps
  - Categories
  - Devices
- The system can easily scale to a large number of users exploiting load distribution and cloud computing.
- Future studies will be directed towards performance improvements and additional functionalities.
Questions?
Thank you!

Amedeo Sapio
amedeo.sapio@polito.it

Fulvio Risso
fulvio.risso@polito.it

Yong Liao
yliao@narus.com

Mario Baldi
mbaldi@narus.com

Gyan Ranjan
granjan@narus.com

Alok Tongaonkar
atongaonkar@narus.com

Ruben Torres
rtorres@narus.com

Antonio Nucci
anucci@narus.com