5G-ENSURE
(Project Number—671562)

Trust Modelling in 5G Networks

SecSoN Workshop, ACM SIGCOMM 2018
Budapest, 24 August 2018

Mike Surridge,
University of Southampton IT Innovation Centre
ms _at_ it-innovation.soton.ac.uk
Overview

- How we defined trust: risks and interdependency
- 5G Trust challenges: virtualisation and new actors
- Machine understandable threat modelling
- Example of 5G specific threats from 5G-ENSURE
- Trust survey results and implications
- Modelling results: threats to trust, root causes and control strategies, quantification of trust
- Stakeholder dependencies and responsibilities
- Status and future work
What is Trust?

- Trust = firm belief in the reliability, truth, or ability of someone or something (OED)
- In practice, trust is (one possible) response to risk
- Risks associated with a socio-technical system can be addressed by
  - refusing to use the risky system features (risk avoidance)
  - assuming the risk will not cause harm (risk acceptance)
  - introducing security measures (risk reduction)
  - making another actor responsible (risk transfer)
- All except the first involve explicit or implicit trust in actors or components of the socio-technical system
5G Trust Challenges

- Trust in 4G networks is based on three main precepts
  - actors are relatively few in number and known to each other
  - mutual trust is largely between actors with similar roles and expectations, e.g. all n/w operators have similar roles
  - market segmentation limits competition and creates a need for cooperation, e.g. across borders

- In 5G networks, especially vertical applications we have
  - more potential n/w operators with more diverse interests
  - less common understanding of security requirements, solutions and dependencies in ‘vertical’ applications
  - new dependencies and risks due to extensive virtualisation
5G-ENSURE Approach to Trust

- Identify risks that are new or require new management strategies in 5G networks
  - 31 scenarios collected by the consortium
  - 43 use cases identified in these scenarios that potentially involve novel risks or novel risk management strategies

- Analyse how these and other common threats would be addressed using the 5G-ENSURE security architecture
  - Analysed using a semantic modelling approach and machine reasoning to ensure nothing is overlooked
  - Handled by the Trust Builder tool developed in the project

- Determine trust dependencies between stakeholders
Example Threats

**Primary Threat**
- Remote Anonymous Exploit Compromises Device Availability

**Secondary Threat**
- Overload on the HW Domain causes a loss of Availability

**Threat to Trust**
- This causes the HW domain operator to lose trust in the network
Threat Coverage

Primary threat models covered
- internal bugs (including dishonest stakeholders)
- unauthorised local and remote access
- remote exploits against devices and services
- remote injection via services on back end databases
- impersonation (spoofing) and interception (snooping) attacks

Secondary threats covered the propagation of overload, unavailability, loss of integrity, loss of control,…

Added specialised threats against 5G Networks from the scenarios developed by 5G-ENSURE partners
Attacker measures responses of the physical network attributable to a SDNC-vH, learns how to provoke an overload in its routing function.
The attack overloads the routing process, leading to loss of availability in the SDNC and the network it provides.
Trust Builder: Analysing Risks
In the 5G-ENSURE project we used two models:
- one capturing diversity of stakeholder roles (see left)
- one capturing virtualisation using a MANO architecture

For the paper we had to present only one model:
- used a simplified version of the first model
- focused on the traditional 4G network roles
- intended for comparison between 4G and 5G cases
Measuring Trust

Guided by a trust survey conducted by VTT (one of our 5G-ENSURE partners)
- covered basic attitudes to technology, specific applications and potential threats
- collected 53 responses, most from ‘tech savvy’ Scandanavians

Main conclusions from the survey
- risk management is a shared responsibility
- almost any type of threat affects trust in the network

We therefore weighted all threats equally
- our measure of trust or dependency is the number of root cause threats prevented from causing a loss of trust
Trust (Dependency) Finding Algorithm

For each stakeholder S (a potential trustor)

Find threats to trust \{T(S)\}: handled by automated analysis in Trust Builder

For each threat to trust

Find root cause threats \{R(T(S))\}: automated analysis in Trust Builder

For each root cause threat

Find control strategies that block the threat (or its secondary effects)

If the control strategy is used in the 5G-ENSURE security architecture

For each control

Find the asset where control is applied

Find they stakeholder(s) (trustees) \{Q\} who must implement it

For each trustee Q add +1 to the dependency of S on Q
Simplified Network Model

- Contains 154 assets with 544 primary threats and 214 secondary threats including 58 threats to trust
- There are 2078 secondary effect chains from primary threats to threats to trust
## Analysis: Causes of Loss of Trust

<table>
<thead>
<tr>
<th>Trustor</th>
<th>Remote Exploit on a Service</th>
<th>Remote Exploit on a Device</th>
<th>Network DoS Attack</th>
<th>Impersonation Attack</th>
<th>Snooping Attack</th>
<th>Internal Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access N/W Operator</td>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Home N/W Operator</td>
<td>323</td>
<td>132</td>
<td>96</td>
<td>48</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>Serving N/W Operator</td>
<td>150</td>
<td>70</td>
<td>50</td>
<td>25</td>
<td></td>
<td>8</td>
</tr>
<tr>
<td>Subscriber</td>
<td>523</td>
<td>311</td>
<td>140</td>
<td>122</td>
<td></td>
<td>6</td>
</tr>
</tbody>
</table>
## Analysis: Trust Dependencies

<table>
<thead>
<tr>
<th>Trustor</th>
<th>Access N/W Op</th>
<th>Home N/W Op</th>
<th>Serving N/W Op</th>
<th>Subscriber</th>
<th>ME Manuf</th>
<th>N/W Equip Manuf</th>
<th>UICC Manuf</th>
<th>Depend-encies</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access N/W Operator</td>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>17</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home N/W Operator</td>
<td>30</td>
<td>608</td>
<td>80</td>
<td>18</td>
<td></td>
<td>324</td>
<td>78</td>
<td></td>
</tr>
<tr>
<td>Serving N/W Operator</td>
<td>15</td>
<td>164</td>
<td>152</td>
<td>20</td>
<td></td>
<td>191</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Subscriber</td>
<td>59</td>
<td>804</td>
<td>283</td>
<td>159</td>
<td>56</td>
<td>471</td>
<td>177</td>
<td></td>
</tr>
</tbody>
</table>

- Significantly less trust in the Access N/W
- Significantly more trust in the Home N/W
- Reduced dependency on the Serving N/W
## Analysis: Expectations of Trustors

### Type of Security Measures

<table>
<thead>
<tr>
<th>Trustee</th>
<th>Patch Mgmt</th>
<th>Security Monitoring</th>
<th>Traffic Mgmt</th>
<th>ID/Cert</th>
<th>Client AuthN</th>
<th>Service AuthN</th>
<th>Access Controls</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access N/W Operator</td>
<td>31</td>
<td>30</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home N/W Operator</td>
<td>930</td>
<td>154</td>
<td>106</td>
<td>65</td>
<td>125</td>
<td>5</td>
<td>188</td>
<td>3</td>
</tr>
<tr>
<td>Serving N/W Operator</td>
<td>290</td>
<td>72</td>
<td>60</td>
<td>55</td>
<td>35</td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Subscriber</td>
<td>56</td>
<td>30</td>
<td>75</td>
<td></td>
<td></td>
<td>30</td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>ME Manuf</td>
<td>56</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>N/W Equip Manuf</td>
<td>1003</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UICC Manuf</td>
<td>248</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Monitoring and management is crucial to ensure access to Home N/W services.

Home N/W Operator now controls access.
Major Trust Dependencies in a 5G Network

- **UICC Domain**
- **ME Domain**
- **USIM Domain**
- **HN Domain**
- **SN Domain**
- **TN Domain**
- **AN Domain**
- **Infrastructure Domain(s)**
- **Mobile Home N/W Operator**
- **Serving N/W Operator**
- **Subscriber**
- **Law Enforcement Agency**
- **Regulator**
- **Mobile Home N/W Operator**
- **UICC Manuf**
- **User Equip. Manuf**
- **Access N/W Provider**
- **Interconnect N/W Provider**
- **N/W Equip Manufacturer**
Current Status and Future Work

- 5G-ENSURE is now finished – full report available online
- Presented results to GSMA and promoted use risks (and threats) to describe and measure trust
  - e.g. in vertical application pilots and roll outs
- The trust modelling tool is available to 5G-PPP partners
  - we can’t provide full support for free now the project is over, but we can provide some assistance
  - contact me if you are interested in trying it
- The tool is now being adapted to support ISO 27005 risk analysis for data protection in the cloud
  - see for example H2020 Project 731678 RestASSURED
Acknowledgement

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 671562

See http://www.5gensure.eu/ for more details
5G-ENSURE
(Project Number— 671562)

Trust Modelling in 5G Networks

SecSoN Workshop, ACM SIGCOMM 2018
Budapest, 24 August 2018

Mike Surridge,
University of Southampton IT Innovation Centre
ms _at_ it-innovation.soton.ac.uk