A Quantitative Risk Assessment of AeroMACS Security in SESAR

Mohamed Slim Ben Mahmoud
Nicolas Larrieu
Alain Pirovano
Ecole Nationale de l’Aviation Civile (ENAC), LEOPART Team
Outline

- Problem Statement
- AeroMACS in SESAR
- Simulation Campaign
- Security Guidance
- Conclusion and Future Work
Why network security risk assessment is so important? It helps to:

- Estimate the potential damages caused by cyber attacks
- Decide which security policy is better for the network
  - Critical step in the risk management lifecycle

How many type of network security risks are usually considered?

- Individual risk per node (own vulnerabilities)
- Network risk (considered as the sum of individual risks)
- BUT...in a computer network, nodes are connected

Network security can be compromised by node communications!!
Problem Statement (2)

- What about node interconnections?
- Common mistakes
  - Only vulnerabilities specific to a node can be exploited to attack that node
  - Low (high) individual risks -> Low (high) network risk
  - Network risk = sum of all individual risks + risk due to...
- Service dependency/node correlation
  - Network intrusions/attacks process is transitive!
- Network Security Risk Propagation!
Security Risk Propagation Example
Besides network risk propagation...

Network risk assessment approaches:

- Qualitative
  - Based on security expert’s investigation and past experiences
- Quantitative
  - Based on mathematical/theoretical models

What is wrong with qualitative approaches?
## Problem Statement (4)

<table>
<thead>
<tr>
<th>Point of view</th>
<th>Qualitative Approaches</th>
<th>Quantitative Approaches</th>
</tr>
</thead>
</table>
| **Subjectivity** | ▪ Rely on security experts *intuitivity* and *past experiences*  
▪ *Pedestrian* risk evaluation (e.g. low, medium, high) | ▪ Rely on strong *theoretical* models (e.g. tree-based attack graphs)  
▪ Less subjectivity (...but the model design can always be discussed) |
| **Efficiency** | ▪ Impossible to compare two risks classified in the *same level*  
▪ Impossible to estimate the *distance* between two risk levels  
▪ Exposed to computation errors (*human in the loop*) | ▪ Comparison is always possible  
▪ Less computation errors (*automated procedure*) |
| **Cost** | ▪ *Time-consuming* (e.g. questionnaires collection/analysis)  
▪ Security expertise requires *monetary* founds | ▪ Faster compared to qualitative risk assessment approaches  
▪ No extra-expense for security expertise |

- Quantitative risk assessment methodology for network security based on risk propagation concept!

Published in proceedings of the 6th International Conf. on Network Architectures and Information Systems Security
AeroMACS in SESAR

▶ Aeronautical context
  ◦ EUROCONTROL SESAR WP 15.2.7

▶ ENAC task
  ◦ Apply the developed risk assessment methodology to mitigate the AeroMACS network risk in the airport surface segment
  ◦ According to the results, provide some security guidances

▶ What is AeroMACS?
  ◦ C-band WiMAX-derived technology (IEEE 802.16e)
  ◦ Airport RAMP, GROUND, and TOWER surface zones.
  ◦ Envisaged traffic: ATS, AOC, and NET operational services

▶ Security is a very important concern in AeroMACS communications!
AeroMACS Security

- AeroMACS provides a built-in privacy sub-layer
  - Lessons have been learned from the WiFi experience...
  - PKM framework (key management)
  - Advanced cryptographic algorithms (e.g. AES, RSA, EAP)
  - Security Associations, mutual authentication, etc

- Still...
  - many security weaknesses exist
    - Unauthenticated management messages (MITM attacks)
    - Unencrypted management messages (Eavedrop)
    - Shared keys in multicast/broadcast services (key forgery)

- A risk assessment study could be handy to mitigate the risks related to these weaknesses
AeroMACS Network Topology
Simulation Campaign

Assumptions

- 9 BSs, 10 aircraft, and 12 surface vehicles
- Vulnerability data extracted from the NVD database
- Node correlation data based on statistics from the COCR
- No vulnerability for the on-board embedded network

Simulation goals

- Vulnerability statistics
- Individual/propagated/network risk estimation
- Comparison between two authentication approaches
  - EAP (Enhanced Authentication Protocol) RFC 3748
  - RSA (Rivest, Shamir, Aldman)
- Result analysis and guidance’s provision
Individual risk results are dictated by the vulnerability inputs from the NVD database. 
Strong relationship between the individual risks and the number of specific vulnerabilities.
Individual Risks (2)

- Individual risks as a function of number of vulnerabilities

What about propagated risks?
# Propagated Risks

<table>
<thead>
<tr>
<th>NODE ID</th>
<th>Propagated Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Base stations (1 to 6)</td>
<td>7.474</td>
</tr>
<tr>
<td>Base stations 7 and 8</td>
<td>9.965</td>
</tr>
<tr>
<td>Base station 9</td>
<td>12.456</td>
</tr>
<tr>
<td>Aircraft (1 to 6)</td>
<td>0.812</td>
</tr>
<tr>
<td>Aircraft (7 to 12)</td>
<td>1.082</td>
</tr>
<tr>
<td>Vehicles (1 to 6)</td>
<td>0.812</td>
</tr>
<tr>
<td>Vehicles 7 and 8</td>
<td>1.082</td>
</tr>
<tr>
<td>Vehicles 9 and 10</td>
<td>1.353</td>
</tr>
<tr>
<td><strong>ASN Gateway</strong></td>
<td><strong>538.998</strong></td>
</tr>
<tr>
<td>DHCP Server</td>
<td>1.2</td>
</tr>
<tr>
<td>AAA Server</td>
<td>1.2</td>
</tr>
<tr>
<td>ATS Server</td>
<td>0.398</td>
</tr>
<tr>
<td>AOC Server</td>
<td>0.750</td>
</tr>
<tr>
<td>AP Server</td>
<td>0.135</td>
</tr>
</tbody>
</table>
Propagated Risks (2)

- Node connectivity is an important parameter for the propagated risk

- The ASN Gateway is the point of failure of the risk analysis, why?
Network Risk

Network risk contribution percentage (per node)

ASN Gateway contribution percentage (per node)

AeroMACS security should be discussed to mitigate these risks: RSA vs. EAP protocols
EAP vs. RSA Sub-Scenario
- Individual Risks -

- Surprisingly, RSA is more vulnerable than EAP
- Higher number of vulnerabilities, but...a lower average CVSS score
EAP vs. RSA Sub-Scenario
- Propagated Risks -
EAP vs. RSA Sub-Scenario  
- Network Risks -

No change for the ASN Gateway since we have not modified the node connectivity
Security Guidances

- **Implementation** guidances:
  - Best trade-off between # of vulnerabilities and average CVSS
  - This should guarantee the lowest individual risks on each node

- **Topological** guidances:
  - Two ASN Gateways (point of failure of risk assessment study)
    - Dispatch the base stations and mobile stations
    - Less connectivity and correlation between the Gateway and IP nodes

- **Security** guidances:
  - AeroMACS authentication: EAP instead of RSA
    - Better results (but based on known vulnerabilities...)
  - Higher layer security mechanisms as a backup for AeroMACS security
    - Firewalls, X.509-based certificate authentications
Contributions Summary

▪ Methodology benefits
  ◦ Quantitative risk parameters
  ◦ Network oriented (based on risk propagation)
  ◦ Tool-assistance for security policy establishment
  ◦ Based on existing vulnerability statistics (NVD)

▪ Results for the first simulation scenario
  ◦ Isolated AeroMACS network
    ▪ The ASN Gateway is the point of failure of the risk study
  ◦ Comparative study between EAP and RSA
    ▪ EAP behaves better in a vulnerability-based methodology
  ◦ Guidances provision to enhance the security of the network and mitigate the related risks
Future Work

Currently
- Simulations for an end-to-end connected AeroMACS network
  - Firewalls, on-board segment, additional nodes (mobile agent, etc)

Methodology improvements/enhancements
- Investigation on network risk correlation
  - Bayesian or causal network-based approaches
- Predictive network security state
  - Unknown vulnerabilities (not included in NVD database)

Expand the study to an end-to-end network
- SESAR 15.2.4 WP considering different communication segments
  - LDACS, AeroMACS, and SATCOM
Special thanks to all the SESAR WP 15.2.7 partners for their respective contributions

Questions?