Towards a Trustworthy Distributed Architecture for Complex Sensing Networks

Heidi Schubert, Real-Time Innovations
Dr. Nikolai Mansourov and Djenena Campara, KDM Analytics
The Challenge

• Distributed systems face distributed threats

• A human or autonomous decision maker will decide how much to trust a node

• Need to aid decision maker by summarizing knowledge that contributes to trust
Trustworthiness Index

• Objective: Develop a measure of trustworthiness of a node based on static analysis of the software and observation of the runtime behavior.

• Benefits
  – Enable exchange of data between nodes that have no prior relationship
  – Create a trusted complex system by integration of trusted nodes
  – Enable a human or autonomous agent to make decisions on how much they trust a node
Trustworthiness Approach

• Define an a priori trustworthiness index
  – Uses multiple trust factors
  – Based on a software assurance case

• Define a dynamic trustworthiness index
  – Reputation based
  – Looks at multiple methods for observing behavior

• Build infrastructure to support distributed trustworthiness
  – Trusted distribution of trustworthiness
  – Must be secure, scalable, and extensible
Before Operation
Before Establishing Communication

Node A

0.5

Exchange certificates

Node B

0.7

Accept if TI > 0.4

Trust Agent

B cert valid?

OK

A cert valid?

OK

0.3

0.7

A

B
While Operational

Node A

Trust Agent

0.5
A

0.3
B

Node B

0.7

Accept if TI > 0.4

B’s index 0.3

B misbehaves
Communication Framework

- Data Distribution Service (DDS)
  - Publish/subscribe
- Plug and play flexibility
  - Add new nodes at anytime
- Peer-to-peer performance
  - Low latency
- Scalable
- Reliable
Calculating the Trustworthiness Index

• Need a method to calculate the trustworthiness index
• Must be flexible to accommodate different systems
• Must put a quantitative value on qualitative properties
Structured Assurance Case

- **Claim**: what the case is trying to show
- **Argument**: structured argument of how the claim can be satisfied
- **Evidence**: agreed upon facts
Extensions to Calculate Trustworthiness Index

- Use the tree structure to calculate an overall Trustworthiness Index (TI)
- TI normalized to be between 0 and 1
- Weight each sub-claim
- Determine the strength of each evidence
- Calculate a TI up the tree
Example High-Level A Priori TI

GC1.2
Security criteria: a node is sufficiently trusted if all security requirements are fulfilled

G1
Node is sufficiently Trusted

S1
Argument based on development process, verification, and testing security capabilities

G2
Sufficient security capabilities are in place in the environment

G3
Software development process, testing, and verifications are performed on the node’s software

G4
The node’s software is enhanced with security capabilities
Example High-Level Online TI

GC1.2
Security criteria: a node is sufficiently trusted if all security requirements are fulfilled

G1
Node is sufficiently Trusted

S1
Argument based on observed behavior, lack of security violations, and detection of security events

G2
Environmental sensors have not found evidence of vulnerabilities or attacks

G3
The software is performing as expected and meeting its Quality of Service agreements

G4
The security capabilities on the node are in use and security policies have not been violated
Conclusions

• A trustworthiness index provides a measure of trust of a node
  – A priori based on development history and security measures
  – Online based on reputation and behavior

• Trustworthiness architecture distributes and updates the trustworthiness index
Thank You

This material is based on research sponsored by the United States Air Force under contract FA8650-11-M-1112. The content of this work is the responsibility of the authors and should not be taken to represent the views or practices of the U.S. Government or its agencies.