Draft-mglt-i2rs-security-environment-reqs

Daniel Migault

Joel Halpern (presenter)

Susan Hares

Assumption Overview

- The work on I2RS makes assumptions about the way I2RS clients and agents may be deployed
  - I2RS agents are assumed to be collocated with Routing Systems
    - Although that collocation may be more complex in practice
  - I2RS clients may be collocated with single or multiple applications, or may be providing services to individual or multiple separate applications

Security Assumption starting

- Similarly, the I2RS security work makes assumption about the security properties of the environment
- The I2RS architecture does not describe these
  - As it is outside the direct scope of I2RS
- This document provides informational description of those assumptions
  - To enable folks to meet the assumptions by knowing what they are

Categories of environmental aspects

- The document groups the environmental security aspects into three groups
- Plane Isolation
- AAA Policy
- Application isolation

I2RS Plane Isolation

- For discussion purposes, this section treats the I2RS exchanges as a separate plane from the data plane, control plane, and the management plane
- The document discusses a set of requirements that need to be met to ensure the segregation
  - It also talks about the range of techniques, for example whether one uses tunnels for isolation or truly separate physical networks.
  - It also describes aspects where the different planes need to communicate and coordinate

I2RS AAA Policy

- I2RS does not mandate specific AAA protocol or behavior
  - But it does make assumptions about what capabilities AAA provides
- This section of the document walks through the requirements that I2RS assumes on the overall AAA behavior
  - Including interaction with the I2RS client

I2RS Application Isolation

- I2RS implicitly assumes that applications will not harm each other
  - We only talk about this explicitly in terms of direct collision
  - We have explicitly decided not to deal with implicit collision
- In addition to collision on data modification, there are other forms of interaction
  - These need to be dealt with from an environmental perspective
  - So as to prevent deliberate or accidental contamination
    - Or, in the worst case, DoS effects