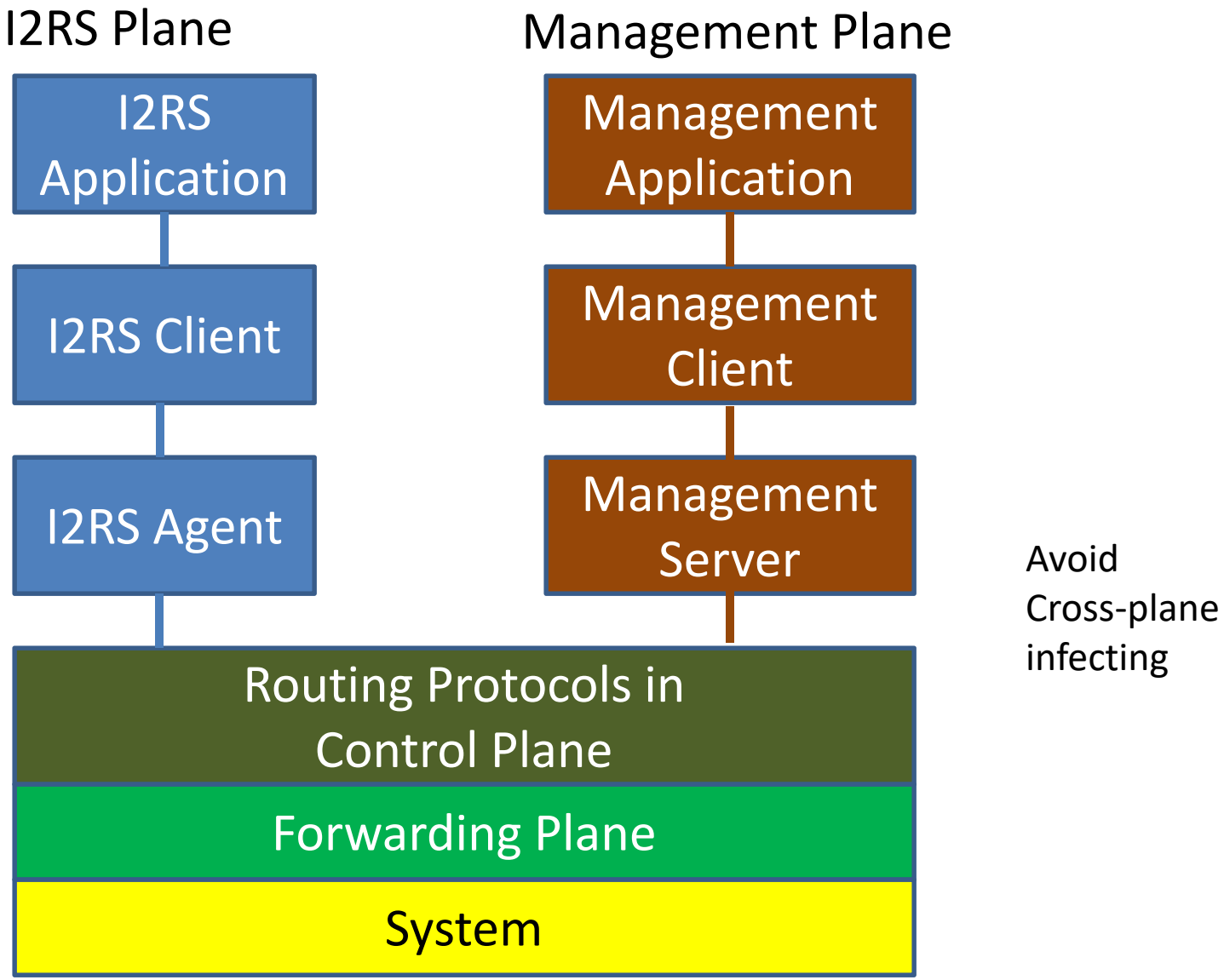
I2RS Security Environment draft-ietf-i2rs-security-environment-reqs

Susan Hares

Huawei

Purpose

- 37 Requirements for those who implement and deploy I2RS regarding:
  - Isolation of Systems management systems
  - I2RS Inter-Plane isolation for Access control
  - I2RS application comments
- Think RESTCONF + Dynamic Control Plane Datastore


I2RS Plane
Management Plane
I2RS Application
I2RS Client
I2RS Agent
Management Application
Management Client
Management Server
Routing Protocols in Control Plane
Forwarding Plane
System
Avoid Cross-plane infecting

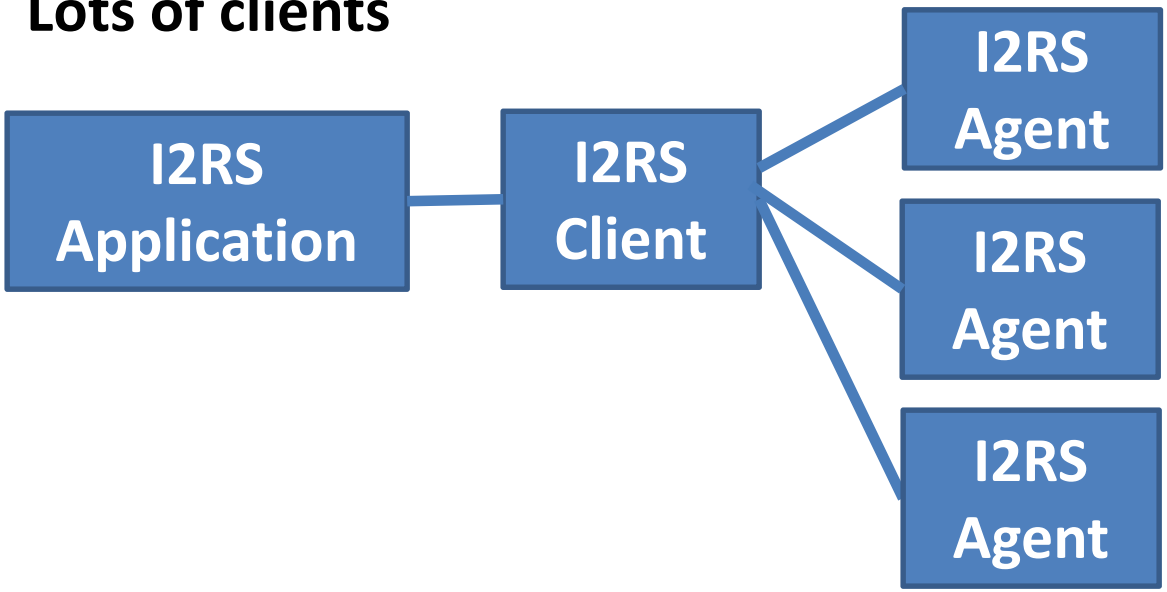
5 Requirements

- Requirements regarding inter-plane isolation:
  - isolated channel,
  - logical interface,
  - set specific permissions for I2RS client,
  - I2RS client notified if routing resource manage
  - Overwrite policy for routing system (I2RS over config, config or I2RS)

Use in different deployments

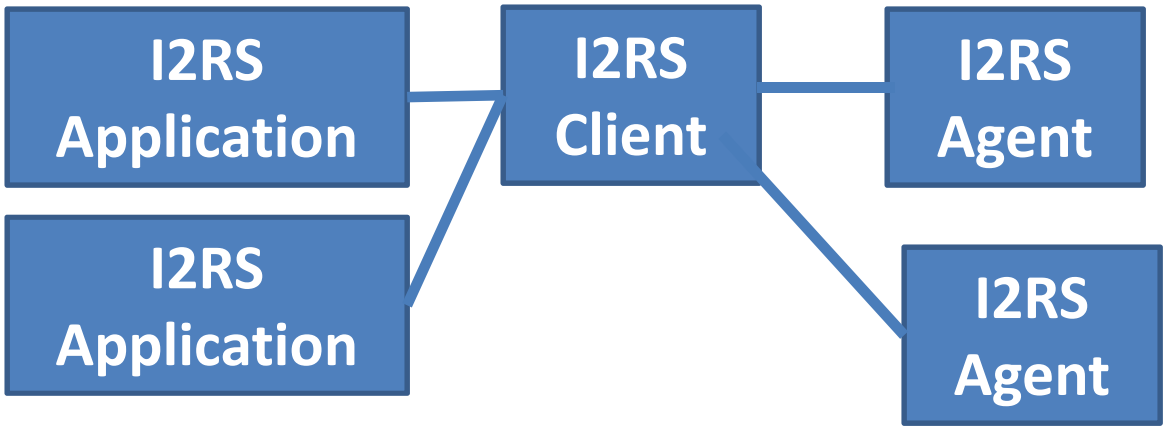
Simple

Lots of clients

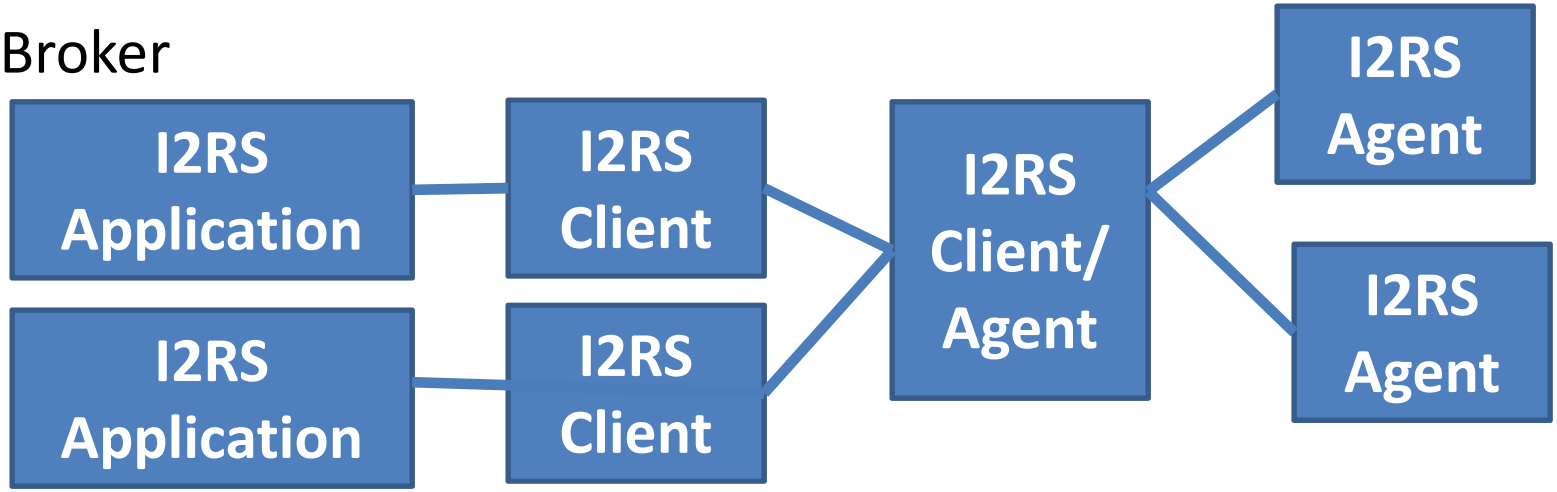


Use in different deployments

Two applications



Broker



Trust + Tell

- Access control active through-out plane
  - If something is changed, tell reason through chain back to application
  - Used trusted communication to reduce chance for attacks/ Can refuse channel not secure enough
  - I2RS Agent/Client inform if policies change
  - Applications can request security policies from I2RS Client - so does not send info tossed
  - Applications may subscribe to notification

Prevent Permissions Escalation Attack

- High-priority/Low priority application share client – can allow attacks
  - 2 Application (configure/monitor) share 1 I2RS Client
  - Monitor client get permissions escalated to configuration status

- How to fix: Application and client have same level of permissions + tracing
  - Configuration applications talk to configuration client to I2RS agents (aka restconf servers)
  - Trace what happens,
  - Authentication Application←→ Client

I2RS Agent – Final link

- Agent have uniquely policies
- Application/Clients that bind may depend on agent to enforce access policies, but this weakness protection
- Track who changed Agent last
- Enforce overwrite policy (I2RS

Automate Security

- Grant or revoke across whole domain similarly
- Update frequently
- Identify parts of system uniquely – to prevent permissions escalation
- Look for who changes what in whole system