Threat Model for Software Reconfigurable Communications Systems

Presented to the Object Management Group

6 March 007

Bernard Eydt

Booz Allen Hamilton

Chair, SDR Security Working Group

Overview

- Overview of the SDR Forum
- SDR Forum High Level Security Requirements
- Vision for Object Attribute Authentication
- Threat Model (work in progress)
  - Assets
  - Threats
  - Countermeasures
  - Mechanisms

Overview of the SDR Forum

Overview of the SDR Forum

Mission

- Accelerate the development and proliferation of SDR and cognitive radio technologies to support the needs of all user domains and stakeholders

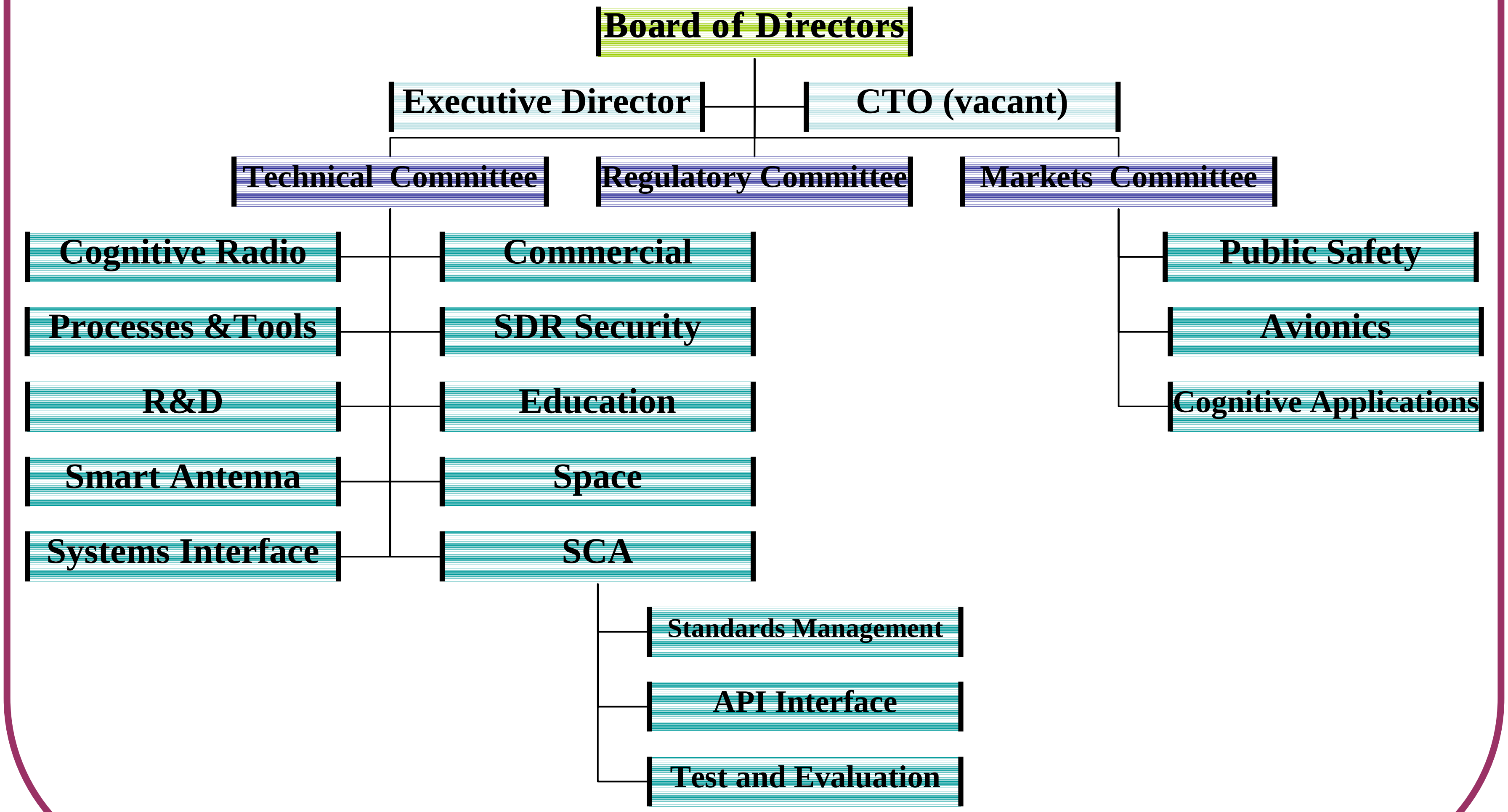
Vision

- Ubiquitous wireless communications

Membership

- The SDR Forum is a non-profit organization comprised of decision makers, planners, policy makers and program/product managers from a broad range of organizations

SDR Forum Organization



SDR Forum
High Level Security Requirements

High-level Security Requirements Overview

- Documented in the SDR Forum publication *High Level SDR Security Requirements* (SDRF-06-A-0002-V0.00, January 2006)
- **High-level**
  - Detailed functional requirements are in development
- **Universal**
  - Intended for all radio market segments, not public safety in particular
  - SDR reconfigurability demands a universal approach
- ***SDR* Security**
  - Address SDR risks, not general communications risks

Requirements List

1. **Policy-driven behavior**
2. **Stakeholder-driven Policy**
3. **Device attestation**
4. **Protected download**
5. **Policy-compliant installation and instantiation**
6. **Run-time control**
7. **Resource integrity**
8. **Access control**
9. **Audit**
10. **Process separation**
11. **Implementation assurance**
12. **Supportive operations**

Requirements Objective: Mitigate Risk

- Bad software can:
  - Adversely impact radio performance, reliability, and availability
  - Cause radio interference
  - Potentially generate unintended harmful electromagnetic radiation

Unauthorized Modification of Hardware versus Software Radio

Hardware Radio	Software Radio
Modify one device at a time	Modify large numbers of devices nearly simultaneously
Requires some radio expertise	No special expertise required (for software download or update)
Requires physical access to the device	Can occur over significant distances using any frequency that the SDR is capable of receiving

Requirement #1: Policy Driven Behavior

An SDR device SHALL enforce a device-specific SDR security policy that governs the behavior of the device *at all times*.

Potential Areas of Standardization:

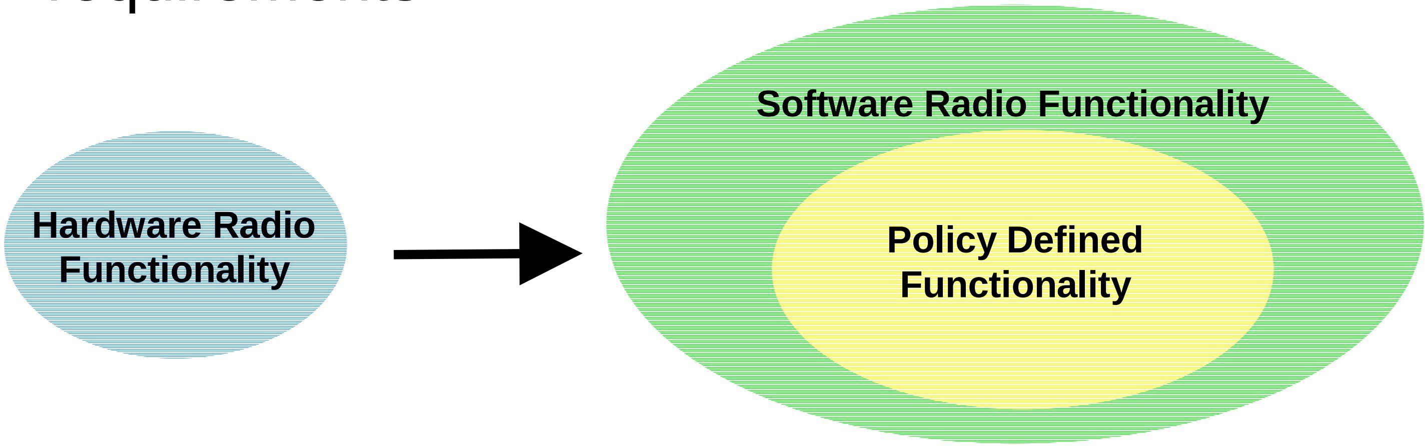
- Policy language
- Trusted boot process

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	●	◑	◑	◑	◑	◑

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Potential Types of Policy and Their Objectives

1. Spectrum Access Policy: Limit functionality to user requirements


Hardware Radio Functionality
Software Radio Functionality
Policy Defined Functionality

To prevent an accidental or malicious use
of additional software functionality, radio is limited by policy

2. Object Attribute Policy: Authenticate list of required attributes (e.g., s/w origin, security certification, platform compatibility)

Requirement #2: Stakeholder Driven Policy

The SDR device SHALL ensure that its device-specific SDR security policy incorporates the SDR security policies of its stakeholders within the scope of their authority.

Potential Areas of Standardization:

- Policy language

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	●	◑	◑	◑	◑	◑

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Potential Stakeholders

- Manufacturer
  - Assembler
  - Component manufacturer
- Software Developer
- Network Operator
- Regulator
- Owner
- Others

Requirement #3: Attestation

An SDR device SHALL provide trusted configuration information to the device’s radio communications service providers and other authorized entities on demand.

Potential Areas of Standardization:

- Attestation protocol

Spectrum Availability	System Availability	Oject Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
◑	◑	○	○	○	○	○

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #4: Protected Download

An SDR device SHALL provide confidentiality services for download of SDR-related software and configuration data as determined by the device's SDR security policy.

Potential Areas of Standardization:

- Download protocol

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
○	○	○	○	○	●	○

● Primary control ◐ Secondary control ○ Minimal protection provided / NA

Requirement #5: Policy-compliant installation and instantiation

An SDR device SHALL only install and instantiate SDR-related software and policy that have been appropriately certified to be compliant with the device’s SDR security policy.

Potential Areas of Standardization:

- Most likely left to vendor implementation

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	●	◑	●	○	○	○

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #6: Run-time control

An SDR device SHALL at run-time prevent transmissions that violate its SDR security policy.

Potential Areas of Standardization:

- Policy language
- Radio transmission interface

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	○	○	○	○	○	○

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #7: Resource integrity

An SDR device SHALL detect the unauthorized modification of its SDR-related resources and take actions determined by the SDR security policy.

Potential Areas of Standardization:

- Most likely left to vendor implementation

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
◑	◑	●	○	○	○	○

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #8: Access control

SDR devices SHALL control access to each SDR-related resource on the device.

Potential Areas of Standardization:

- Most likely left to vendor implementation

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
◑	◑	●	○	●	○	○

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #9: Audit

An SDR device SHALL detect security relevant events and notify specified processes as determined by the SDR security policy.

Potential Areas of Standardization:

- Audit record content and format
- SDR SNMP MIB and traps

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
◑	◑	◑	◑	◑	◑	◑

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #10: Process separation

An SDR device SHALL have mechanisms to prevent SDR-related applications from compromising the security of non-SDR-related applications and data.

Potential Areas of Standardization:

- Separation methods

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
○	◑	○	○	○	○	●

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #11: Implementation assurance

Information assurance mechanisms that support enforcement of the SDR security policy SHALL be validated against industry-recognized evaluation standards.

Potential Areas of Standardization:

- Evaluation of cryptographic methods
- Certification of SDR policy enforcement mechanisms

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	◑	◑	◑	◑	◑	◑

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Requirement #12: Supportive operations

Operational practices supporting information assurance mechanisms SHALL be consistent with and supportive of the SDR security policy.

Potential Areas of Standardization:

- Processes (e.g., key insertion for root of trust)
- Software development assurance (e.g., DO 178B)

Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
●	◑	◑	◑	◑	◑	◑

● Primary control ◑ Secondary control ○ Minimal protection provided / NA

Mapping Requirements to Objectives

Requirement	Spectrum Availability	System Availability	Object Integrity at Rest	Object Integrity in Transit	Object Confidentiality at Rest	Object Confidentiality in Transit	Protection of Non-SDR Resources
Policy Driven Behavior	●	●	◑	◑	◑	◑	◑
Stakeholder Driven Policy	●	●	◑	◑	◑	◑	◑
Attestation	◑	◑	○	○	○	○	○
Protected Download	○	○	○	○	○	●	○
Policy Compliant I&I	●	●	◑	●	○	○	○
Run-time Control	●	○	○	○	○	○	○
Resource Integrity	◑	◑	●	○	○	○	○
Access Control	◑	◑	●	○	●	○	○
Audit	◑	◑	◑	◑	◑	◑	◑
Process Separation	○	◑	○	○	○	○	●
Implementation Assurance	●	◑	◑	◑	◑	◑	◑
Supportive Operations	●	◑	◑	◑	◑	◑	◑

Object Attribute Authentication

Object Attribute Authentication Principles

- Stakeholders state required attributes of objects
- Attributes are open-ended; defined by stakeholders
- A platform’s object attribute policy (OAP) is the conjunction of stakeholder contributions
- Developers/distributors of objects or their agents make attribute *claims*
- Claimants generate digital signatures on objects for each claim to provide:
  - Binding of claim to object (assurance of integrity)
  - Non-repudiation of the claimant’s identity
- Radio platforms verify digital signatures (claims)
- Assurance of truth of claim is provided through out-of-band process

Examples of Object Attribute Policy (OAP)

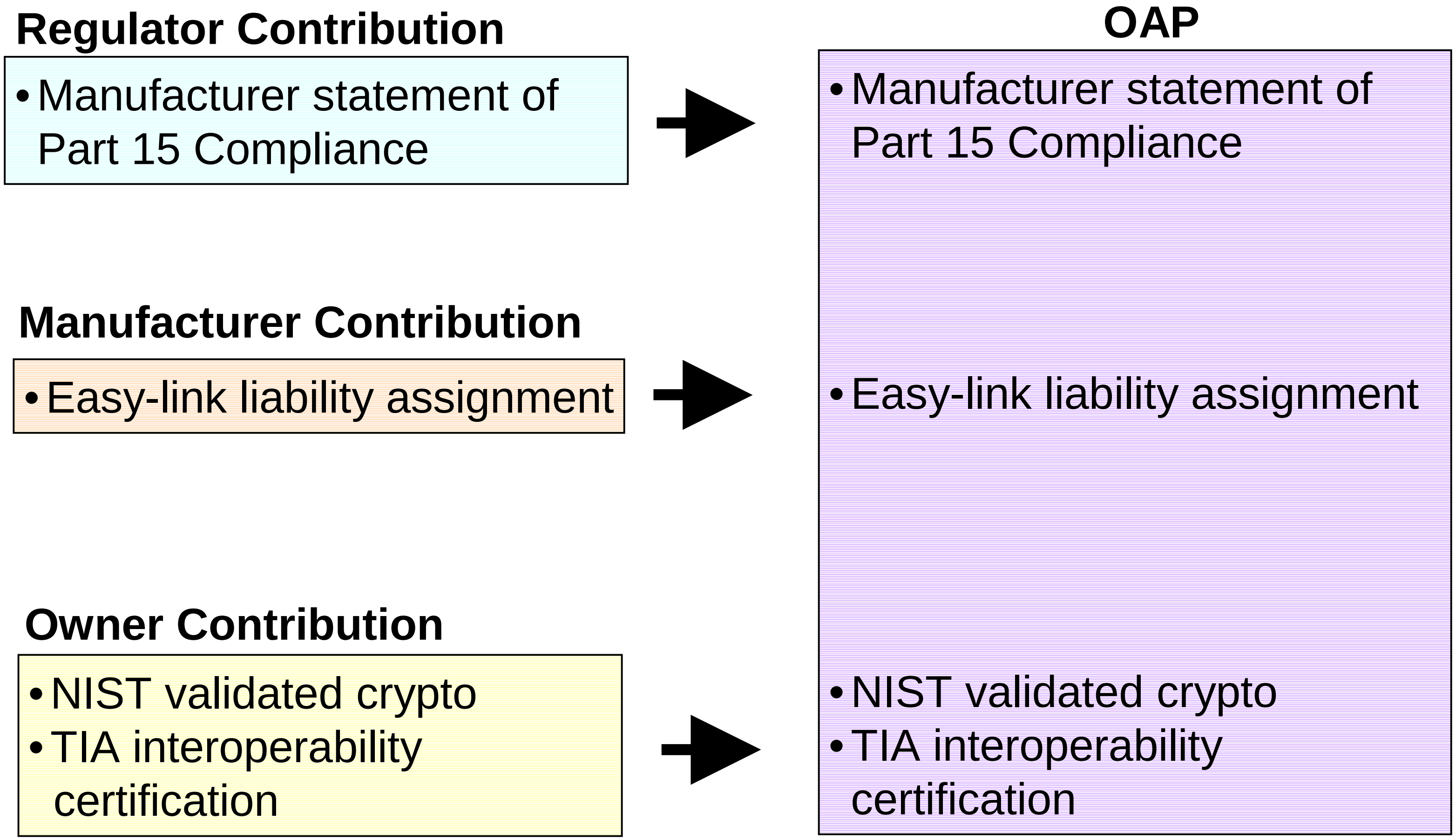
Simple OAP example

Stakeholder	Claimant	Attribute Claim	Authentication Method
Acme Radio (manufacturer)	Acme Radio	This radio software functions properly on radio model 123	RSA 1024

Extended OAP policy example

Stakeholder	Claimant	Attribute Claim	Authentication Method
FCC (regulator)	Acme Radio	This radio software operates in compliance with FCC Part 15 rules	ECC 163
Acme Radio (manufacturer)	Easy-link Software	Easy-link wrote this software and is liable for performance failures	RSA 2048
DHS (owner)	NIST	Crypto modules are validated against FIPS 140-2	RSA 1024
DHS (owner)	Conformance Testing Laboratory	This software running on Acme Radio model 123 has passed interoperability tests specified in TIA TSB-102.CABA	ECC 224

OAP = Conjunction of Policy Contributions



Regulator Contribution

- Manufacturer statement of Part 15 Compliance

Manufacturer Contribution

- Easy-link liability assignment

Owner Contribution

- NIST validated crypto
- TIA interoperability certification

OAP

- Manufacturer statement of Part 15 Compliance
- Easy-link liability assignment
- NIST validated crypto
- TIA interoperability certification

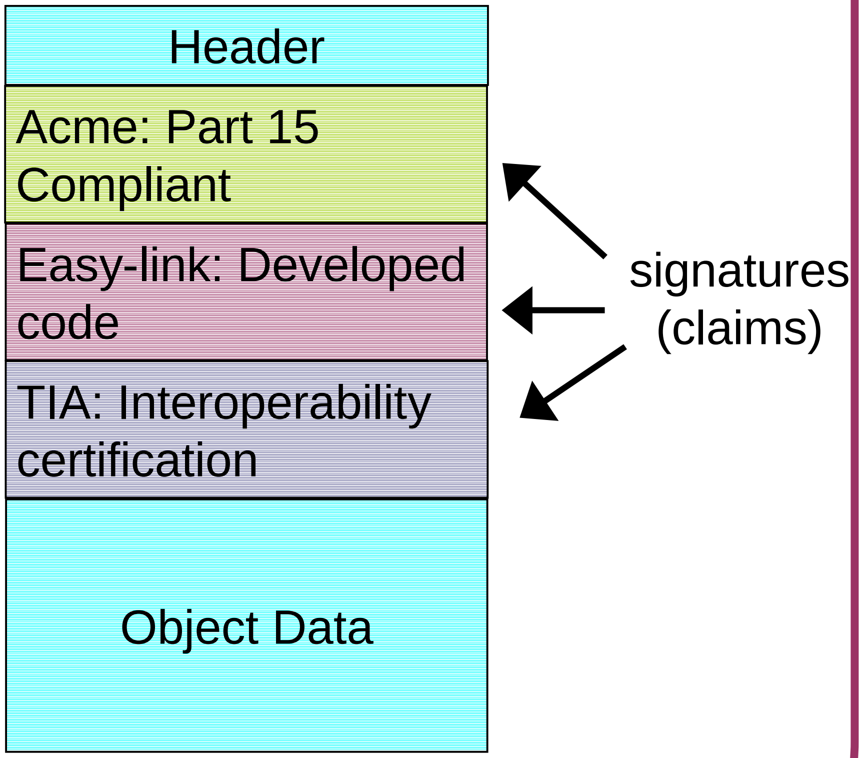
Note: Each Contribution and OAP can be implemented as an array of public key certificates

Object Attribute Authentication Transaction

OAP

- Manufacturer statement of Part 15 Compliance
- Easy-link liability assignment
- NIST validated crypto
- TIA interoperability certification

Object



Header

Acme: Part 15 Compliant

Easy-link: Developed code

TIA: Interoperability certification

Object Data

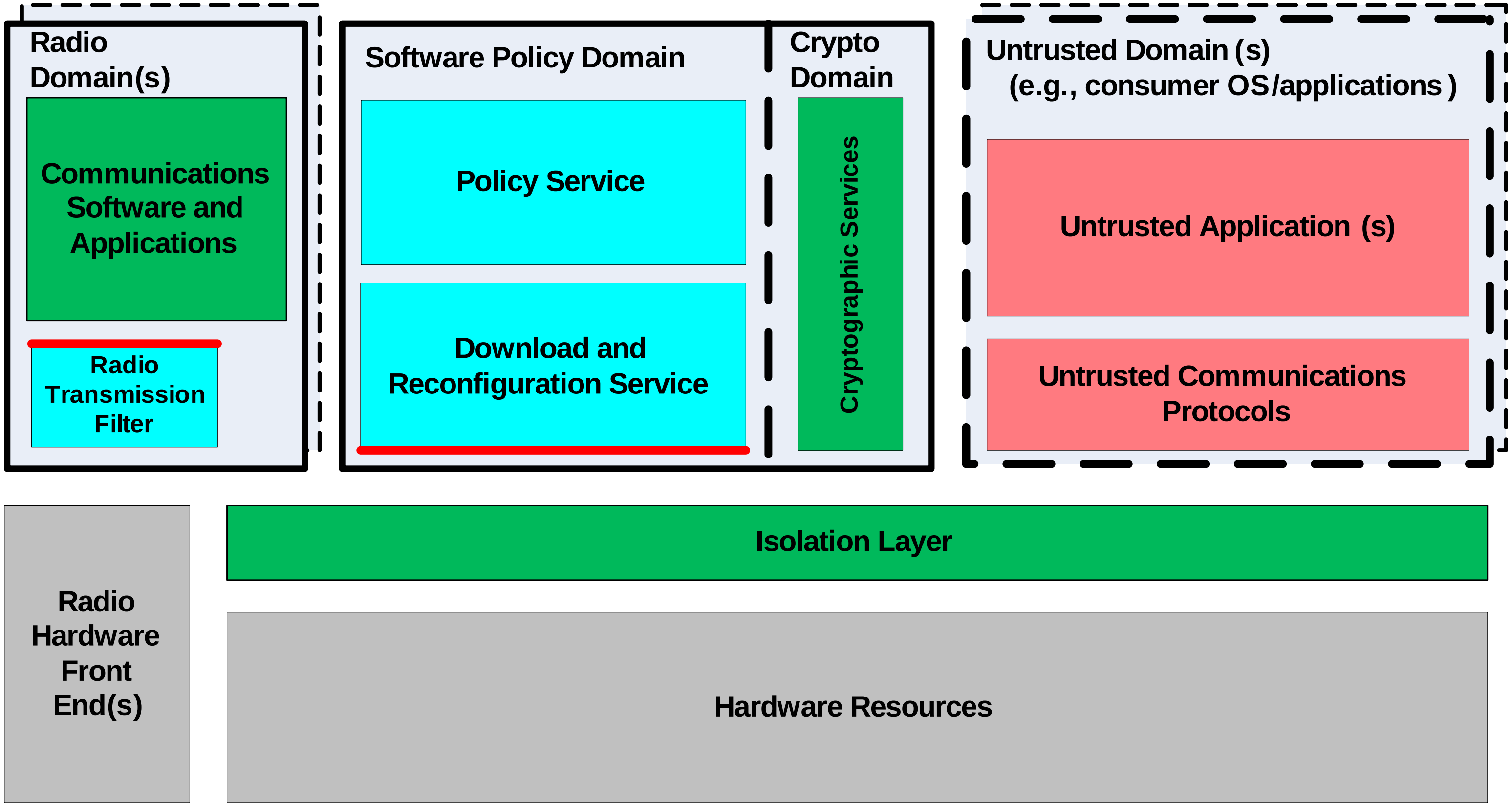
signatures (claims)

Should this object be instantiated?

No.

- Easy-link made claim for wrong attribute
- Missing claim for NIST validated crypto

High-Level Security Architecture for Reconfigurable Radio Communications v0.09



Radio Domain(s)

Communications Software and Applications

Radio Transmission Filter

Software Policy Domain

Policy Service

Download and Reconfiguration Service

Crypto Domain

Cryptographic Services

Untrusted Domain (s) (e.g., consumer OS/applications)

Untrusted Application (s)

Untrusted Communications Protocols

Isolation Layer

Radio Hardware Front End(s)

Hardware Resources

Legend

━━ Security Domain Boundary

━ ━ Optional Domain Boundary

━━ Universally-defined interface

🟦 = Reconfigurable Radio Resource

🟩 = Other Resources Within Scope of Reconfigurable Communications Policy

🟥 = Out of Scope of Reconfigurable Communications Policy

⬜ = Hardware

Digital Signature-based Verification Today

- 3GPP Mobile Execution Environment (MExE)
- Symbian Signed program
- Microsoft Windows Mobile OS and .net framework
- Java JSR118 Mobile Information Device Profile (MIDP) 2.0

What’s New About SDR Forum Approach

- Multiple signatures
  - To date, most authenticated code systems rely on one signature
- Stakeholder contributions
  - To date, most systems involve single stakeholder
- Claimant/Claim framework
  - Today, signatures primarily only used for object origin and in some cases certification

SDR Threat Model

(work in progress)

Threat Model Overview

Model Layer	Example
Primary Assets	Electromagnetic Spectrum
Supporting Assets	Radio Software
Threats	Unauthorized Modification
Countermeasures	Integrity Services
Mechanisms	Hash value in digital signature

Primary Assets

- Electromagnetic Spectrum
- Health and Safety
- Communications Service
- Intellectual Property
- User Applications and Data
- Reputation

Supporting Assets

- Radio Software
- Operating Environment
  - Operating System Software
  - Device Drivers
  - Memory

Threats

- Unauthorized Modification
- Unauthorized Reading

  }
  - In transit
  - In storage
  - While Executing

- Masquarade/Impersonation
  - Of user/organizational entity
  - Of device/infrastructure

- Software Misuse

- Rogue Software

Countermeasures

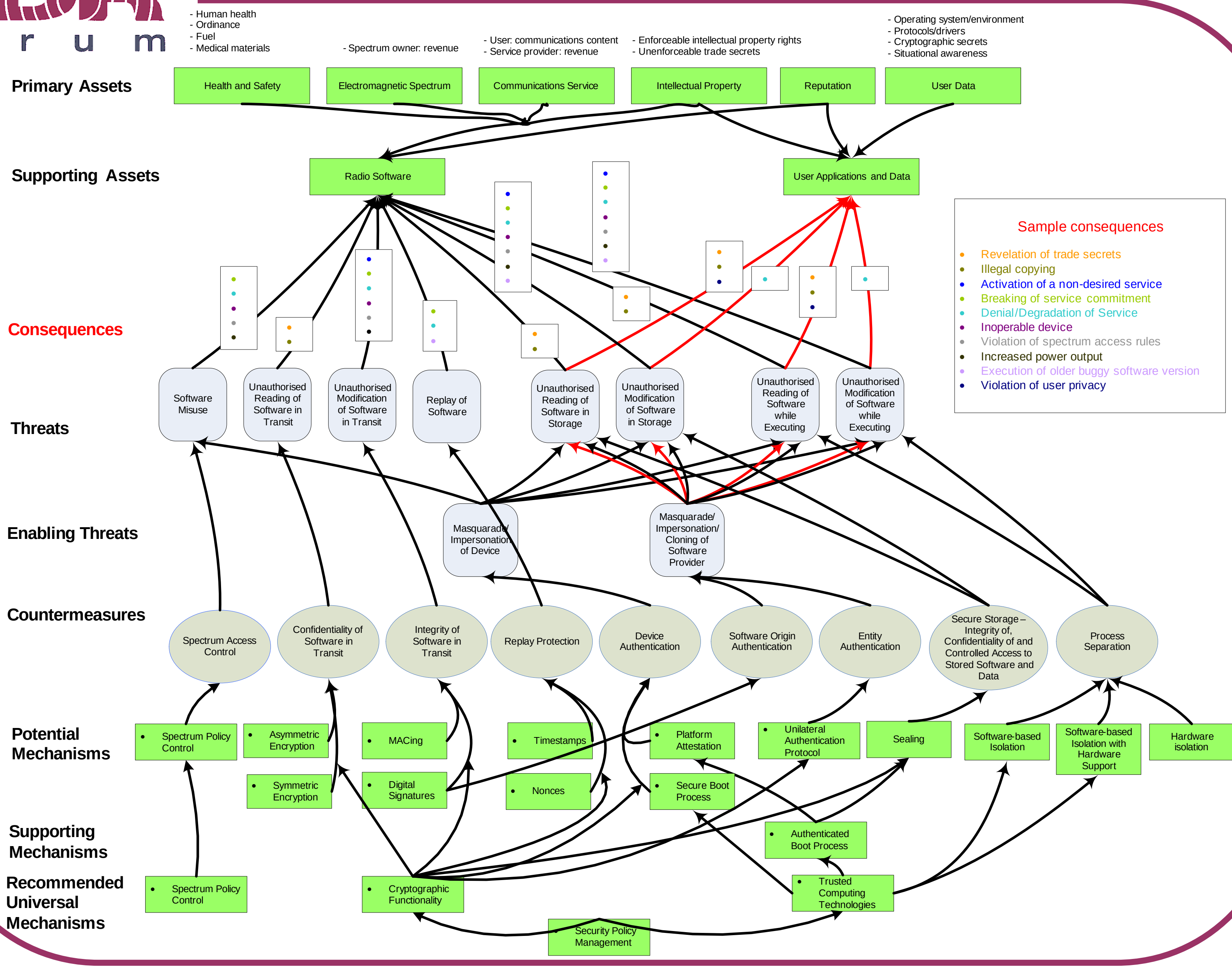
- Integrity Services
- Confidentiality Services

}
  - In transit
  - In storage
  - While executing

- Authentication Services
  - Entity
  - Device
  - Object Attribute
- Access Control
  - Physical (to the device)
  - Computing Environment
  - Spectrum

Countermeasures

- Integrity Services
- Confidentiality Services
- Authentication
- Computing Resource Access Control
- Spectrum Access Control



Primary Assets

- Human health
- Ordnance
- Fuel
- Medical materials

Health and Safety

- Spectrum owner: revenue

Electromagnetic Spectrum

- User: communications content
- Service provider: revenue

Communications Service

- Enforceable intellectual property rights
- Unenforceable trade secrets

Intellectual Property

Reputation

- Operating system/environment
- Protocols/drivers
- Cryptographic secrets
- Situational awareness

User Data

Supporting Assets

Radio Software

User Applications and Data

Consequences

Sample consequences

- ● Revelation of trade secrets
- ● Illegal copying
- ● Activation of a non-desired service
- ● Breaking of service commitment
- ● Denial/Degradation of Service
- ● Inoperable device
- ● Violation of spectrum access rules
- ● Increased power output
- ● Execution of older buggy software version
- ● Violation of user privacy

Threats

Software Misuse

Unauthorised Reading of Software in Transit

Unauthorised Modification of Software in Transit

Replay of Software

Unauthorised Reading of Software in Storage

Unauthorised Modification of Software in Storage

Unauthorised Reading of Software while Executing

Unauthorised Modification of Software while Executing

Enabling Threats

Masquarade/ Impersonation of Device

Masquarade/ Impersonation/ Cloning of Software Provider

Countermeasures

Spectrum Access Control

Confidentiality of Software in Transit

Integrity of Software in Transit

Replay Protection

Device Authentication

Software Origin Authentication

Entity Authentication

Secure Storage – Integrity of, Confidentiality of and Controlled Access to Stored Software and Data

Process Separation

Potential Mechanisms

- Spectrum Policy Control
- Asymmetric Encryption
- Symmetric Encryption
- MACing
- Digital Signatures
- Timestamps
- Nonces
- Platform Attestation
- Secure Boot Process
- Unilateral Authentication Protocol
- Authenticated Boot Process

Sealing

Software-based Isolation

Software-based Isolation with Hardware Support

Hardware isolation

Supporting Mechanisms

Recommended Universal Mechanisms

- Spectrum Policy Control
- Cryptographic Functionality
- Trusted Computing Technologies
- Security Policy Management

Summary

- The SDR Forum has published high-level SDR security requirements
- A major component of the security framework is code signing using public key cryptography
- Current work:
  - Understanding threat profile under which controls are desirable
  - Developing compete set of mechanisms