High-Level SDR Security Requirements

Approved Document
SDRF-06-S-0002-V1.0.0

(formerly SDRF-06-A-0002-V0.00)

12 January 2006

Table of Contents

High-Level SDR Security Requirements

1 Introduction

The SDR Security Working Group is focusing on a broad set of security issues that arise from the introduction of SDR technology. In particular, it seeks to manage the following SDR-related risks:

- Propagation of malicious radio software
- Radio interference
- Adverse health and safety impacts to SDR users (i.e., those caused by inappropriate electromagnetic radiation)
- The unauthorized release of trade secrets incorporated in radio software
- The circumvention of billing systems related to SDR (i.e., fraud)

The high-level security requirements listed in this document address these risks, not all possible risks that might be associated with SDR communications. In particular, they do not attempt to restate general information, communications, transmissions, or network security requirements, all of which have been well-studied in other forums.

The high-level SDR security requirements apply to any use of SDR; they are not targeted at a particular market segment (e.g., commercial wireless telephony). They apply to both infrastructure and terminal devices. They also apply to broadcast, peer-to-peer and ad hoc networking applications of SDR.

The statement of high-level security requirements are the beginning of a process that will culminate in the specification of SDR security mechanisms. First, the high-level requirements will be used to develop detailed security requirements, each of which will be traceable to one or more of the high-level requirements. The detailed requirements, in turn, will be used as the basis for an SDR security architecture. Finally, the architecture will lead to a integrated set of SDR security solutions.

The SDR Security Working Group seeks to maximize the potential future growth and social value from SDR technology. It does not seek to create a maximum security solution or one tailored for the highest assurance environments. It is cognizant that there are tradeoffs between cost of security controls and the risks they mitigate. It also understands that there can often be a tension between security and functionality. At the same time, robust and flexible security solutions must be built-in to SDR technology from the early stages on if SDR technology is to achieve wide regulatory and consumer acceptance.

2 Definitions

Download Transfer of data from outside the device into the device. Download may occur through a variety of means, including over-the-air, using wired media, or using device peripherals such as jump drives or memory cards.

Installation The process of storing and configuring software so that it can be subsequently instantiated.

Instantiation The process of setting up for execution. [Source: SDR Forum DL-SIN]

Operating state The current configuration of the SDR device’s resources including access control rules and radio parameters such as frequency, power and modulation.

Radio communications service provider Network operators (e.g., commercial cellular wireless, public safety agencies), radio broadcasters (including FM/AM, television and satellite), peers in peer-to-peer or mobile ad-hoc networks, and other entities that provide radio communication to a device. An SDR device that is serving in an infrastructure capacity (e.g., a base station or access point) may not have a radio communication service provider if its distribution system is a wired network.

Resource Hardware, software (to include firmware), configuration data and policy

Run-time The period of time during which a program is being executed, as opposed to compile-time or load time. [Source: *The Free On-line Dictionary of Computing*, © 1993-2005 Denis Howe]

SDR device A computing platform or integrated collection of computing platforms that provide radio functionality using SDR technology.

SDR-related Something on which the operation or security of radio communications is dependent. SDR-related items include radio and computing resources such as boot read-only memory, the operating system, hardware drivers, SDR middleware, cryptographic modules, software enforcing the SDR security policy, as well as the radio software itself (i.e., software implementing the “waveform”).

SDR security policy A set of permitted operating states. The SDR security policy may also contain rules regarding authentication mechanisms, events to be audited, and actions to be taken in response to an event.

Stakeholders Hardware component manufacturers, regulators, radio communications service providers, device owners and entities authorized by a device owner.

Trusted Established using cryptographic mechanisms such that invalidation is computationally infeasible if cryptographic secrets are maintained.

3 Requirements

3.1 Policy-driven behavior

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

3.2 Policy freshness

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.

3.3 Device attestation

An SDR device SHALL provide trusted configuration information to its communications service providers on request.

3.4 Protected download

An SDR device SHALL provide confidentiality and integrity services for download of SDR-related software and configuration data.

3.5 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.

3.6 Run-time control

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

3.7 Resource integrity

An SDR device SHALL detect the unauthorized modification of its SDR-related resources and use that information to prevent additional unauthorized behavior.

3.8 Access control

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

3.9 Audit

An SDR device SHALL detect, log and notify specified processes of security related events.

3.10 Process separation

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

3.11 Implementation assurance

Information assurance mechanisms SHALL be based on industry standards and validated technology.

3.12 Supportive operations

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