Policy-Based Approach for Secure Radio Software Download

Antonietta Stango, Neeli R. Prasad
as@es.aau.dk, np@es.aau.dk
Center for TeleInFrastruktur (CTIF)
Aalborg University
Denmark

SDR '09 Technical Conference and Product Exposition
1 - 4 December 2009, Washington DC

Outline

- Introduction
- Software Download
- Radio Software Download
- Regulatory perspectives
  - Europe
  - US
- Proposed Policy-Based Approach for Secure Radio Software Download
- Security Analysis
- Conclusions and Future Works

Introduction

- The feature to be reconfigurable over the air interface is one of the main advantages of the SDR devices
  - benefit for next generation of wireless communication
  - new risks

Software Download

- The motivations to work in the area of software download is mainly due:
  - the need to upgrade wireless devices
  - the need to correct software bugs or deficiencies
  - the need to roam with different air interface standards.
- The most critical is the download of data or software able to modify configuration parameters

Radio Software download

- The radio software download is defined as “the process of delivering reconfiguration data and/or new executable code to a SDR device to modify its operation or performance” [1]
- Security perspectives:
  - new software can change transmitter characteristics
  - protection of contents in the context of download
  - accounting for all billable time
  - assurance that the software load is appropriate for the target terminal and is unaltered

[1] Software Defined Radio Forum, “Overview and Definition of Software Download for RF Reconfiguration”, SDRF-2002-A2, Aug. 2002

Radio Software Download

- The download process can be initiated by: server provider, user, application.

- Radio configuration files (R-CFG) can include new parameters for modulation techniques, new power levels, and new operational frequencies

Regulatory perspective in Europe

- The European Parliament adopted, in March 1999, a Directive, defining new rules for the placing on the market and putting into service of Radio and Telecommunications Terminal Equipment (R&TTE Directive 1999/5/EC)

- Subsequently the Telecommunication Conformity Assessment and Market Surveillance Committee (TCAM), set up a group to discuss about the regulatory aspects of SDR with respect to the R&TTE Directive, which defined:
  - SDR , a radio where essential radio parameters can be altered by changing software
  - Vertical market
  - Horizontal market
  - The **responsibility for the product** is a key issue

Regulatory perspective in US

- FCC (Federal Communications Commission) released, in 2005, a set of rules outlining an alternative method for certification of devices whose radio frequency and power characteristics can be modified by software (SDR devices)

- The FCC allows also the use of Free and Open Source Software (FOSS) on SDR devices

- The FCC's rules allow FOSS developers not affiliated with device manufacturers to continue work on their software without restriction.

Regulatory aspects

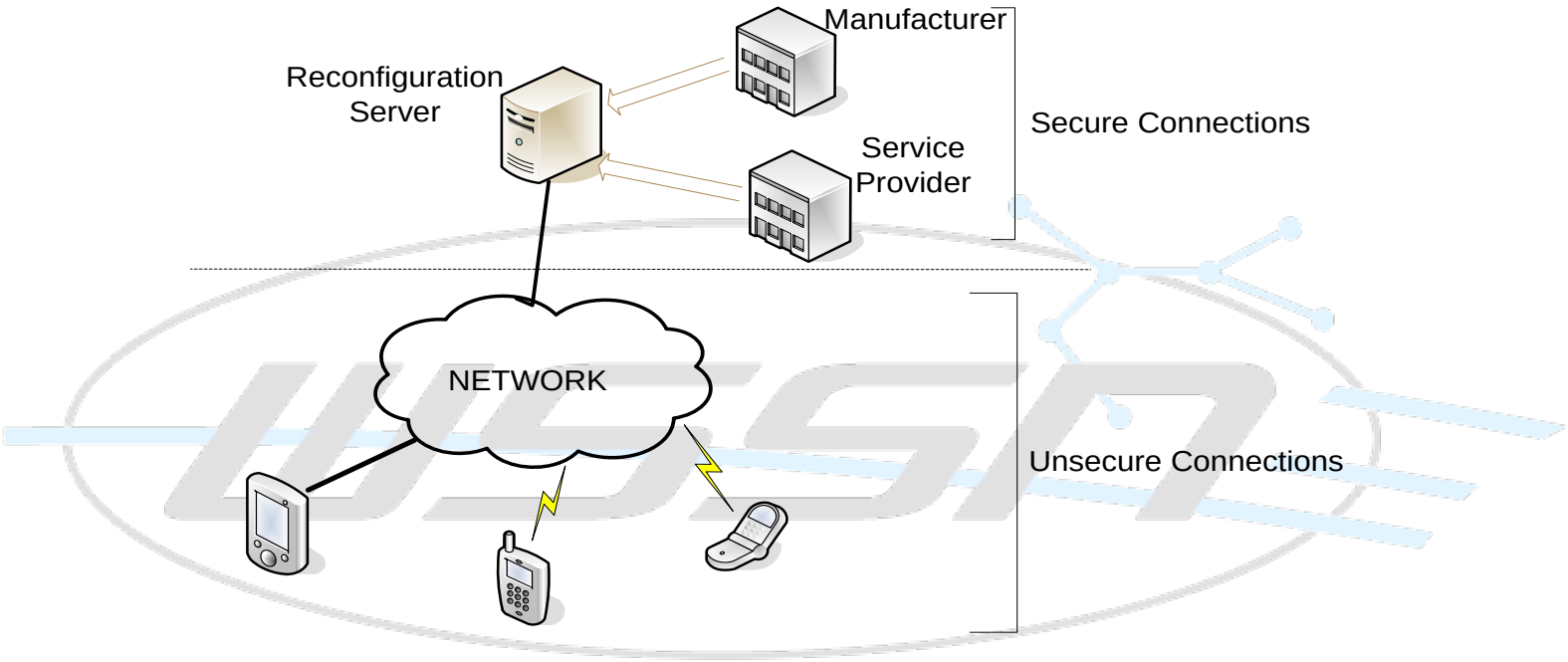
- The regulatory agencies are improving the rules from the point of view of SDR devices, but further reform will be necessary before the maximum benefits from SDR can be realized.
- The radio software download and the following reconfiguration have to respect the legislation in operation in the country where the device is used.

Secure Radio Software Download

- The issue of secure software downloads into a SDR device has been widely considered in literature and in different ways, like encryption, authentication, non-repudiation.

- The main issues that have been identified are
  - the establishment of a secure connection between the source of the radio software and the SDR device
  - the design of an underlying policy to determine the entity that can certify the parties involved.

Proposed Policy-Based Approach for Secure Radio Software Download



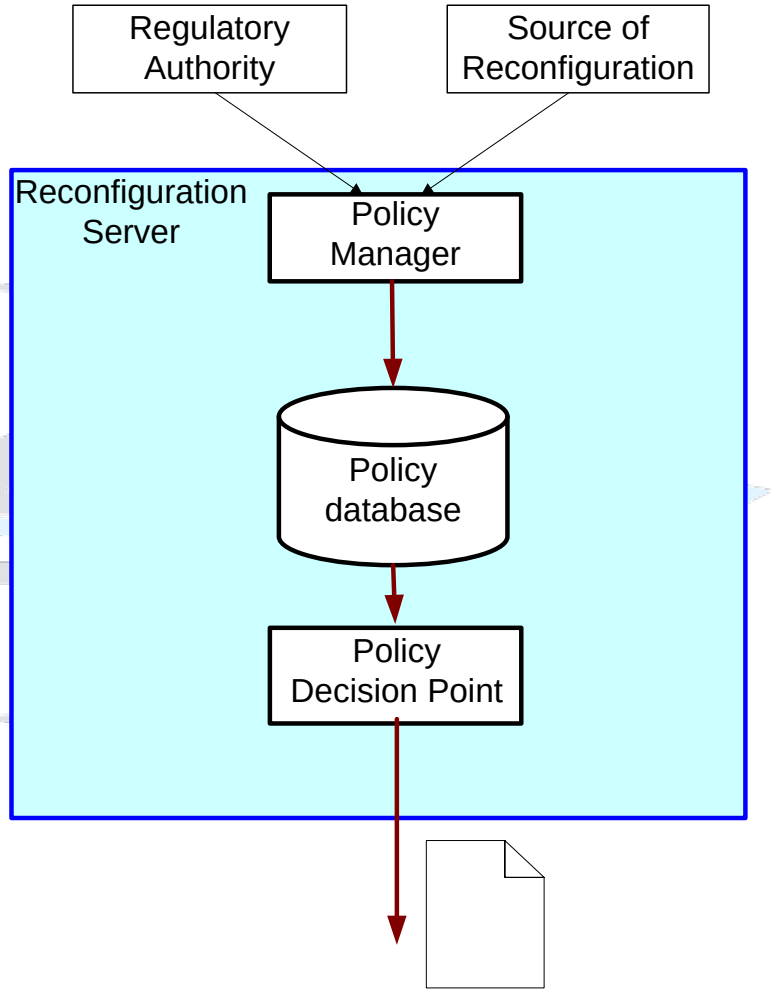
- The proposed mechanism is based on a Reconfiguration Server, which is a TTP able to make decisions about the policy to use for the download and to validate software that is not originating from an official source.

Proposed Policy-Based Approach for Secure Radio Software Download

- Assumptions:
  - The connections between the server, the SoR (and the storage) can be considered trusted.
  - The access network and the SDR devices are susceptible to attacks.
  - The Reconfiguration Server (RS) is a Trust Third Party (TTP) able to take policy-based decisions
- The entities involved in the management of the policies in this scenario are divided between the RS and the SDR device.

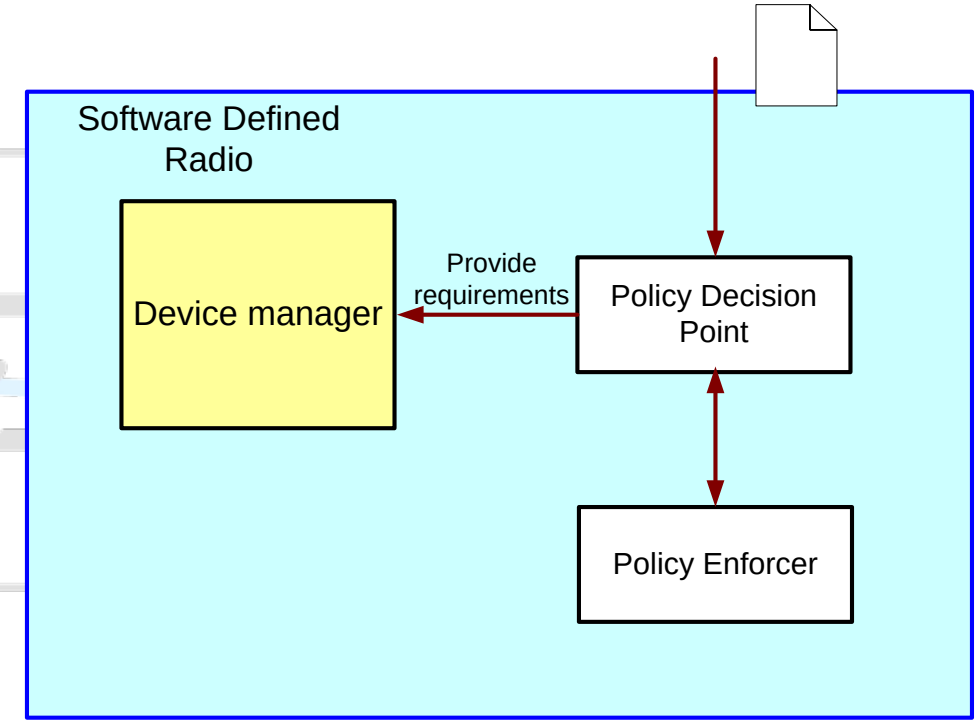
Policy components in the RS

- The Policy manager of RS is in charge of verifying that:
  - the reconfiguration software provided is respecting the regulations of the RA
  - the rights of the SoR are respected
  - the privacy of users is safeguarded
  - validity of the software.



Policy components in the SDR device

- The policy decision point after reading the meta-file can:
  - approve or deny the download based on the information coming from the Policy Enforcer
  - validates the digital signatures.
- When the download has been approved the Policy Decision point provides the communication interface and performs the download/installation of the reconfiguration files.



Download protocol

1. Request of download.
2. Mutual authentication between SDR device and RS.
3. The RS establishes the policy for download.
4. Establishing a connection between SDR device and RS
5. Sign contents, if necessary, and exchange of meta-information for policy and certificates.
6. Download of software.
7. Installation and storage of software by the Device Manager.

Security Analysis

- The solution proposed provides secure transmission from the RS and SDR device, since the confidentiality and integrity of the software are protected by mutual authentication and content signed.
- Radio software can also be stored in the SDR device because the same mechanisms that protect the software in transit from the RS can protect it for future use.

Conclusions and Future Works

- The main advantage to use this approach:
  - use of existing security mechanisms
  - use of software coming from open sources can be used to upgrade the radio characteristics.
- Future works:
  - Development of the policy to manage the download
  - Improvement of the protocol for download

Thank you