A Location based Radio Regulation Enforcement Scheme for Globally Roaming SDR

Chih Fung LAM
Tien Dzung DOAN
Kei SAKAGUCHI
Jun-ichi TAKADA
Kiyomichi ARAKI

Tokyo Institute of Technology

Agenda

- Introduction
- Issues to be solved and current related work
  - SDR system process
  - Local radio regulation compliance
- Solution to the problems
- Security strength of the proposed system
- Components needed in SDR terminal to realize the proposed system process
- Implementability issues
  - Experiment on PDA and PC

Introduction

- Software Defined Radio (SDR)
  - Multi-band RF frontend.
  - Wideband ADC and DAC.
  - IF, baseband and bitstream processing are implemented in general purpose programmable processors.
- Benefits
  - Reconfigurability in radio components by software upgrade. SW = RF control, BB, Comm. Protocol
  - Single terminal architecture for different radio standards.
  - Enable global roaming (CDMA, PCS, GSM, etc.)

Unsolved issues in SDR

- Process flow of SDR system :
  - Making of SW and HW
  - Certification by Telecommunication Certification Body (TCB)
  - SW download (including encryption)
  - Installation flow
- Local radio regulation compliance while roaming.

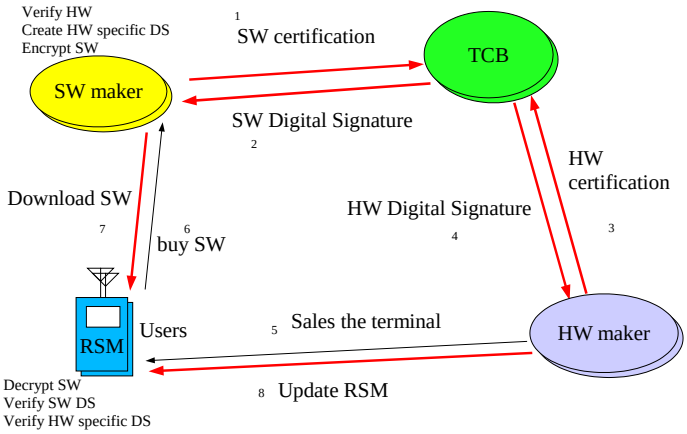
Related research

- FCC Class 3 Permissive Change: TCB tests all combination of SW and HW for certification.
  - large amount of combination
- Secure Download Framework by Yokohama National University: symmetric key encryption during SW download.
  - SW makers (third parties) depends on HW makers
  - HW maker runs out of business ?
- TRUST and Mobile VCE proposed SDR reconfiguration architecture.
  - Non-communication system such as pager, walkytalky?

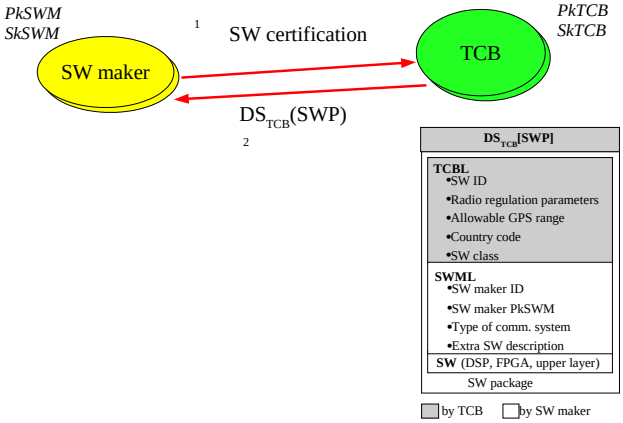
Proposed SDR system process

- Separate SW and HW certification by having run-time radio regulation check (ACU).
- Uses digital signature for
  - verification of HW certification
  - verification of SW certification
  - prevent illegal distribution of SW
- Uses hybrid encryption during SW download.
- Uses GPS information to limit the function of SW within a geographical region.

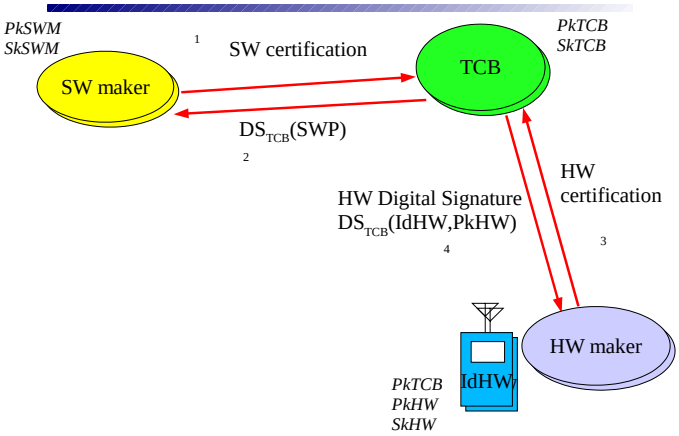
SDR system process



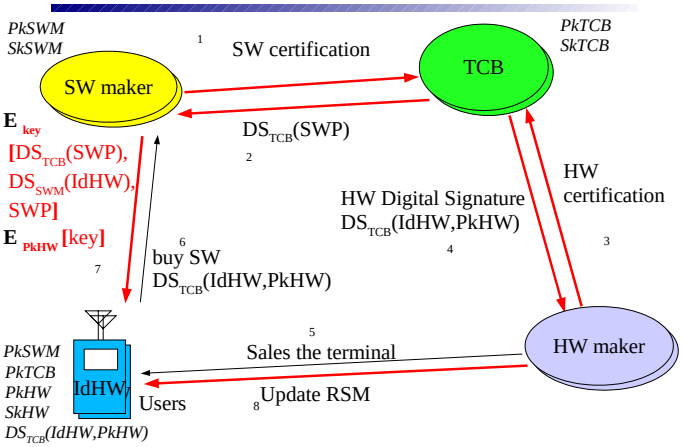
SDR system process



SDR system process



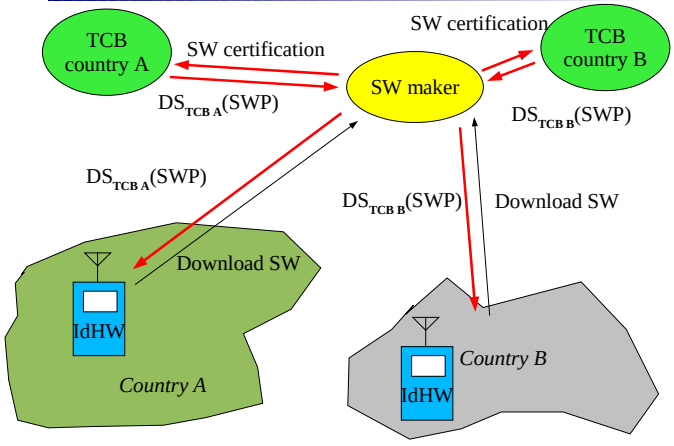
SDR system process



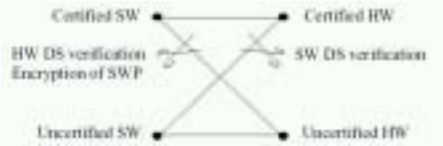
Local radio regulation compliance

- When a terminal roams from Country A to Country B:
  - Due to GPS position check, SW_A is stopped and $[DS, SWP]_B$ is downloaded.
  - DS_B is verified using $PkTCB_B$, which was one of the PkTCBs stored in the terminal by HW maker.
  - If $SW_A = SW_B$, only DS_B verification is necessary.

Local radio regulation compliance



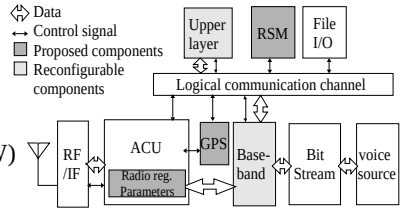
Security case studies



- Illegal SW distribution is blocked by RSM verification of DS_{SWM}(IdHW).
- Uncertified SW and uncertified HW will be eradicated by legal enforcement team.

Terminal system software

- Radio Security Module (RSM) cannot be reconfigured by the user.
- RSM contains
  - SkHW (only RSM can access to it) and PkHW
  - Hardware ID (IdHW)
  - hardware (HW) digital signature
  - public-keys of TCBs
  - GPS range of countries
  - a changeable security component (by HW maker)

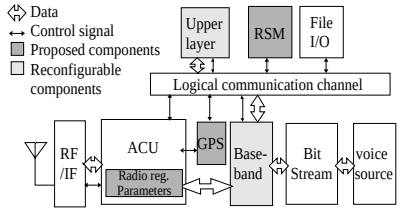


Main functions of RSM

- Manages whole life-cycle of SW in terminal
  - Installation
    - Digital signatures verification
  - Storage
  - Operation
    - FPGA, DSP, Upper-layer protocol, SW auto reconfiguration.
  - Random geographical region verification
  - Termination of SW

Required terminal hardware

- A GPS unit
- Automatic Calibration & Certification Unit (ACU)
  - A hardware unit.
  - A RF manager.
  - Performs runtime radio regulation check.
    - Center frequency
    - Bandwidth
    - Output power
    - ACPR



Issue of speed (1)

- Hybrid decryption and digital signature verification speed

Table 1. Specification of PDA and PC.

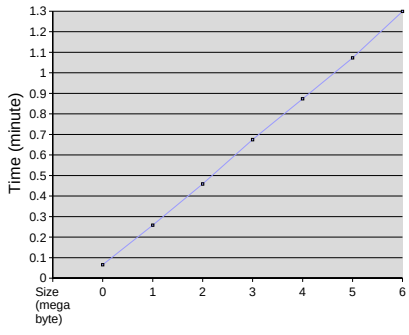
	PC	PDA (iPAQ)
Processor	Intel Celeron 1GHz	Intel XScale 400MHz
Memory	512MBytes	64MBytes
OS	Windows2000	PocketPC 2002
Java version	JRE1.2.2 with bouncycastle and cryptix JCE	Jeode JVM with bouncycastle and cryptix JCE
JVM size	22.8 MBytes	3.5 MBytes

Table 2. Performance of RSM in PC and PDA.

Operation	Time	
	PC	PDA
(1024bit) RSA and DES decryption	2 s	45 s
DS verification	29 ms	139 ms

Issue of speed (2)

(1024bit) RSA-DES decryption on iPaq PDA

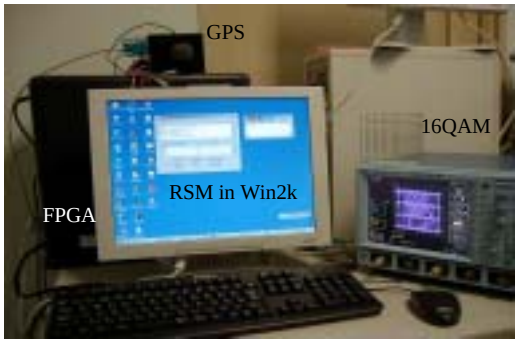


RSM implementation (1)

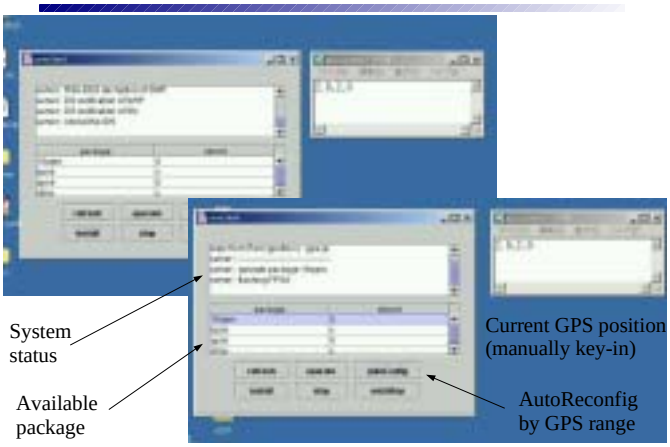
- RSM was implemented by using Java.
  - OS independent and security components are available.
- Windows2000 was used.
  - Privileges for files/processes can be set.
  - Privileges for RSM components (PkTCBs, GPS ranges, security components, SkHW) are set to root/Administrator → user cannot read/modify them.
  - HW makers can upgrade RSM components by root/Administrator access to the terminal.

RSM implementation (2)

- Xilinx vertex-II 1 Million gates FPGA
  Pioneer GPS-2001zz



RSM implementation (3)



Issue of system file size

- JVM size : 22.8 MBytes
- RSM class file size : 300 KBytes
- memory usage : less than 7MBytes

Conclusion

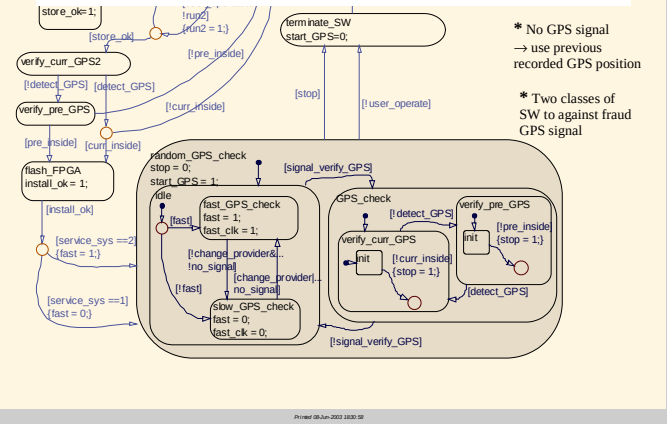
- Process flow of SDR system was proposed.
  - Separate SW and HW certification
  - Independent SW distribution
  - Without expensive extra network and air interface
  - Security strength was discussed
- Local radio regulation compliance was solved with random geographical region verification (GPS).
- The proposed architecture was proved to be implementable by :
  - Speed measurement of decryption and digital signature verification
  - Memory and system file size measurement

Thank you

Any comment please ?

Appendix

GPS verification algorithm (1)



* No GPS signal → use previous recorded GPS position

* Two classes of SW to against fraud GPS signal

GPS verification algorithm (2)

- Two classes of SW
  - Non-service provider :
    eg. walkytalky, pager (only receiving), bluetooth
    - Fast random GPS verification (≈ 3 times a day)
  - With service provider :
    eg. PHS, PDC, GSM, wireless LAN
    - slow random GPS verification (≈ once a week)
    - fast random GPS verification when **not receiving signal** or **change service provider** (particularly global roaming in same system)
    - upper-layer protocol of SW must inform RSM in this case
      ⇒ as criterial to obtain certification from TCB
  - Not all SW is stopped immediately if fraud GPS signal.

Abbreviation

FCC – Federal Communications Commission

Mobile VCE RMA – Mobile Virtual Center of Excellent Reconfiguration Management Architecture

TRUST – Transparently Reconfigurable Ubiquitous Terminal by Information Society Technology (IST)

TCB – Telecommunication Certification Body

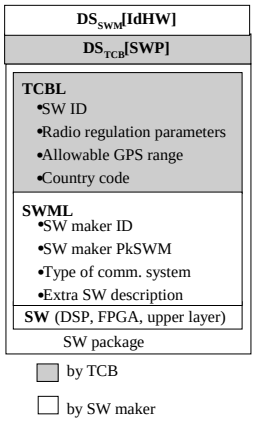
PCS – Personal Communication System

Type of Certification

- HW and SW certification are separated.
- HW certification procedure
  - Telecommunication Certification Body (TCB) checks for:
    - RSM functions, ACU functions of terminal, parameters not related to SW (spurious emission, etc.)
  - TCB signs DS_{TCB} [IdHW,PkHW] to install in each terminal.
- SW certification procedure
  - TCB checks for:
    - Output power, frequency, modulation technique, RF control signals, protocol of SW.
  - Further simplified as ACU performs a runtime checking.

SW Life Cycle (1)

1. SW and SWML (contains PkSWM) are submitted by SW maker.
2. After verification, TCB adds TCBL. Combination of SW, SWML and TCBL is named SWP.
3. TCB generates a digital signature (DS) for SWP.
4. DS_{TCB}[IdHW,PkHW] is used to download SW from SW maker. SW maker verifies if it is a certified terminal by PkTCB.



SW Life Cycle (2)

5.SW maker creates DS_{SWM}[IdHW].

6.Everything is encrypted by symmetric key, SW maker encrypts the symmetric key by using PkHW.

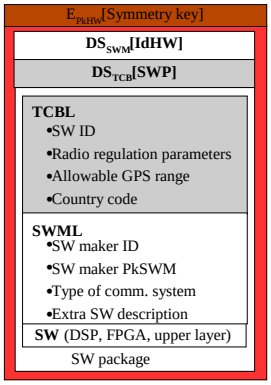
7.RSM downloads them.

8.RSM decrypts using SkHW.

9.RSM verifies DS_{TCB}[SWP] and DS_{SWM}[IdHW].

10.RSM installs the SW.

11.Starts ACU runtime check.



Main Functions of RSM (1)

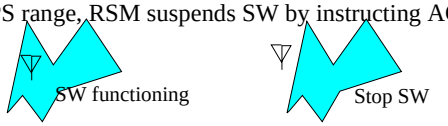
- Verifies source of SW.
  - By DS_{TCB}[SWP] verification of SWP.
- Certification of RSM/terminal can be verified.
  - By DS_{TCB}[IdHW,PkHW] verification by SW maker , since only TCB can sign it.
  - Know who certified this RSM/terminal.
  - If someone copy this DS, it is useless because SkHW cannot be copied. Thus, one cannot decrypt the SWP from SW maker.

Main Functions of RSM (2)

- Installs SW (SW can only be installed through RSM in the terminal).
  - Verifies HW requirement.
  - Flashes FPGA and DSP, installing upper-layer.
  - Updates allowable GPS range in RSM.
  - Updates radio regulation parameters in ACU.
- Synchronizes with ACU for runtime check.
  - Instructs ACU for runtime check.
  - Prevents bugs or Trojan horses in SW.

Main Functions of RSM (3)

- Protect Intellectual Properties of SW
  - By encryption of the SWP during download process.
  - Re-distribution of SW for legal RSM is not possible due to RSM verification of DS_{SWM}[IdHW].
- Limits operation of SW within a geographic region.
  - By GPS position checks in pseudo random period.
  - If current GPS value lies outside of the allowable GPS range, RSM suspends SW by instructing ACU.



Security Threats (1)

- Certified terminal will not run uncertified SW.
  - RSM PkTCB verification of DS_{TCB}[SWP].
- Certified terminal cannot duplicate certified SW.
  - SWP is encrypted by PkHW, only RSM can use SkHW to decrypt it, SkHW is inaccessible by user.
- Uncertified terminal cannot download/run certified SW
  - DS_{TCB}[IdHW, PkTCB] verification by SW maker.
    - Even DS_{TCB}[IdHW, PkTCB] is copied, without SkHW, SWP cannot be decrypted.

Security Threats (2)

- Certified terminal cannot use certified but illegally distributed SW.
  - Certified terminal has a RSM that checks for DS_{SWM}[IdHW]. Only SW maker can sign it.
- Uncertified terminal will runs uncertified SW.
  - There is nothing much we can do about this. Let the law be the judger.

Strength

- Separate HW and SW certification significantly reduces the total number of certification compared to conventional methods.
- Third party SW developers can develop their own SW without going through HW makers.
- Even there are bugs in the radio SW, ACU protects the radio component from emitting error signals.
- Terminal complies to local radio regulation when it roams due to difference DS verification by multiple TCB keys.
- The proposed architecture is suitable for all software radio such as amateur radio set or satellite TV box.

Original works

- Our original works include:
  - The use of hardware unit, ACU in SDR terminal for run-time regulation check.
  - The application of digital signature for HW and SW certification.
  - The use of multiple public-keys and GPS unit for global roaming of terminals.
  - The application of digital signature, symmetric and asymmetric key to protect the downloaded SW.