RADIO SECURITY MODULE THAT ENABLES GLOBAL ROAMING OF SDR TERMINAL WHILE COMPLYING WITH LOCAL RADIO REGULATION

Chih Fung LAM; HengJiang WANG; Kei SAKAGUCHI; Jun-ichi TAKADA; Kiyomichi ARAKI
(Graduate School of Science and Engineering, Tokyo Institute of Technology,
Meguro-ku, 152-8552 Tokyo, Japan. {chihfung,kei,takada,araki}@mobile.ss.titech.ac.jp)

ABSTRACT

Due to the reconfigurability of SDR terminal, there is a urgent need for a new radio equipment certification method. We proposed a SDR security architecture that enables separate SW and HW certification. This reduces the amount of certification needed to be performed by Telecommunication Certification Body (TCB). The security architecture also applies hybrid encryption to protect SW during download process and enable flexible SW distribution by SW maker. System software named Radio Security Module (RSM) is proposed to be installed in every SDR terminal to realise the proposed architecture. RSM takes care of the installation, storage, operation and termination of SW in the terminal. Due to the fact that different radio regulations exist in different countries, when a terminal roams, RSM makes sure that only SW that complies with local radio regulations is allowed to run. This is done by random GPS verification with the allowable GPS range of the running SW by RSM. A model of SDR terminal was implemented in a personal computer to investigate the software complexity of RSM.

1. INTRODUCTION

In a Software Defined Radio (SDR) terminal, radio components can be changed by using software (SW). The term SW here includes binary code for baseband modules, upper-layer communication protocol, and setting for RF controller. Due to this flexibility in SDR, serious radio security problems might occur due to illegal use or modification of SW. Old certification method for current radio equipment is no longer applicable for SDR equipment. Furthermore, this issue becomes more complicated as different countries may have different radio regulations. The current certification method cannot guarantee local radio regulation compliance of SDR equipment while it roams globally. Thus, there is a urgent need for new SDR security architecture.

With respect to this, a new SDR certification method, Class III Permissive Change (C3PC), was proposed by the FCC [1]. In this method, all combination of HW and SW must be tested in the certification process. However, it is almost impossible to perform the test due to large amount of combination of SW and HW in near future. C3PC also does not consider the fact that different radio regulations exist between different countries. This implies that a C3PC certified SDR terminal will not comply with local radio regulations when it roams globally.

On the other hand, there are many research on SDR SW reconfigurable architecture, such as TRUST [2] and Mobile VCE [3]. However, radio regulation certification was not considered in these architectures. It may be assumed that SW is certified before it is distributed by the system. But, this is not applicable for SDR equipment, such as Satellite TV box, bluetooth or Walky-Talky, which does not reconfigure through a communication system. There is a need for a standardized security system for SDR equipment.

In order to construct a new SDR security architecture, we also need to consider a new SW distribution method. The conventional approach (Secure Download Framework [4]) assumes that SW are created and distributed by HW maker. While this is true for current radio device (refering to firmware), it is certainly different for the case of SDR. Third-party SW makers will flourish in future and they should be able to sell their own SW freely without depending on HW makers. This is the flexibility that SDR promises.

Our motivation is to propose a novel security architecture for Software Defined Radios that enables separate HW and SW certification, and allows flexible SW distribution. System software namely Radio Security Module (RSM) [5] [6] is required in every SDR terminal to realize the proposed security architecture. We had implemented a model of a SDR terminal in a personal computer to investigate the software complexity of RSM. Encryption was performed on a PC and a PDA to show the applicability of RSM in small devices.

2. PROPOSED HW ARCHITECTURE

A SDR HW is shown in figure 1. As high sampling rate analog-digital and digital-analog converters are still costly and power consuming, it is likely that analog RF will be used in the near future. In this paper, it is assumed that the SDR HW contains an analog RF module with parameters

Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved

such as RF frequency and output power controlled by a RF manager.

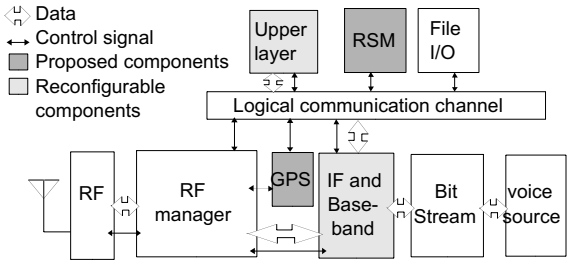


Figure 1: RSM in a SDR terminal

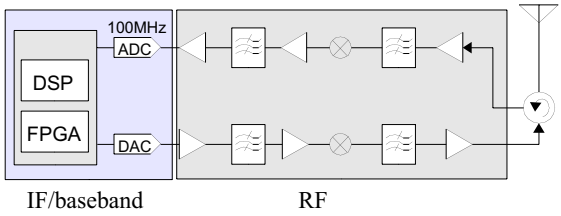


Figure 2: RF and IF/baseband interface in SDR

With standardization of the RF manager interface (or RF and IF/baseband interface), this enables separate development of HW and SW, and eventually leads to separate HW and SW certification. The adjustable RF parameters are:

- overall power amplification factor
- overall frequency up-conversion factor

With RF manager standardization, each HW maker is free to implement their RF design as long as it complies with the standard. An ideal implementation of RF manager is the ACU [7] [8] [9], which has a run-time radio regulation check that help to prevent bugs and hidden operation in SW during operation.

The IF/baseband module contains particular model of DSP or FPGA chips. For a particular SW to operate, the HW must:

- match the RF parameter requirements of the SW, and
- contain the specific IF/baseband chip required by the SW.

It is the function of RSM to perform this compliance check before any SW is allowed to operate in a SDR.

RSM, as shown in figure 1, is a piece of trusted system software which cannot be reconfigured. It manages the whole life-cycle of SW in the terminal. This includes installation, storage, operation and termination of SW. To perform these operations, RSM contains two sets of components, i.e. user-accessible and user-inaccessible components. User-accessible components are:

- a HW digital certificate
- an unique HW identity (IdHW)
- a HW public-key (PkHW)

User-inaccessible components are:

- a corresponding HW secret-key (SkHW)
- public-keys of all TCBs (192 countries)
- GPS range of each country (latitude and logitude values which enclose the area)
- current SW's geographical region
- encryption components (encryption algorithm)

User-accessible components will be used to download new SW. User-inaccessible components can only be accessed by RSM and are updatable by HW makers.

In the installation process, RSM verifies the source of SW which is to be installed. This is done through digital signature (DS) verification of SW. Upon successful DS verification, SW is in storage stage where access right of SW is limited only to RSM. Upon receiving an instruction from the user, RSM operates SW by flashing FPGA, DSP (physical layer) and running system program (implementation of upper-layer protocol). In the operating stage, RSM limits the operation of SW within a geographic region by random GPS position checks. Each SW has a geographical region which the SW is allowed to operate in. It is provided together with the SW as described in section 4. If the current GPS position is outside of its geographical region, RSM will suspend the SW.

In sections below, $DS_A[D]$ means digital signature of message D signed by A. $E_k[D]$ and $E_k^{-1}[D]$ denote encryption and decryption of message D by using key k, while combination of A and B is represented by [A,B]. $V_k[DS]$ is verification of digital signature DS by using key k.

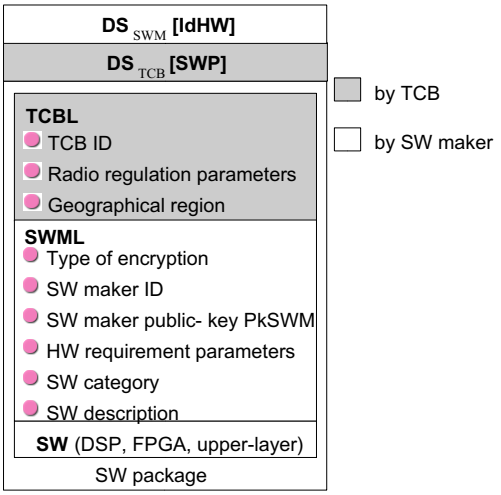


Figure 3: SW package

3. HW CERTIFICATION

A sample of SDR terminal is sent to a TCB by a HW maker for HW certification. The TCB checks functionalities of RSM, RF components, and parameters that are not related to SW such as spurious emission. Upon successful verification, the TCB agrees to certify this model of the terminal. Each terminal of this model will be given a unique hardware identity (IdHW) and a set of hardware

Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved

public and secret keys (PkHW and SkHW) by the HW maker. A hardware digital certificate, i.e. DS_{TCB}[IdHW, PkHW] is signed by the TCB and given to the HW maker to be embedded into each terminal.

4. SW LIFECYCLE

Each SW is attached with labels which are XML styled texts. There are two types of labels for each SW, namely SW Maker Label (SWML) and TCB Label (TCBL) as shown in figure 3. SWML contains a SW maker public-key (PkSWM), type of encryption used during download and other information which describes the SW. TCBL contains radio regulation parameters and a definition of an allowable geographical region.

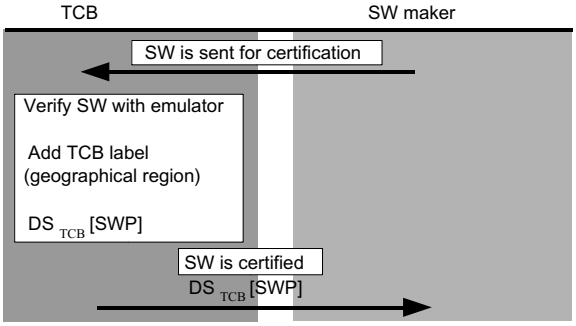


Figure 4: SW certification

Details of SW certification processes are illustrated in figure 4. A SWML is submitted with a piece of SW by a SW maker to a TCB of a country where this SW is to be operated in (in this case Country A). The TCB of Country A (TCB_A) verifies the SW with a HW emulator. If the SW complies with TCB_A's regulations, TCB_A creates a TCBL for the SW. TCBL has a geographical region definition which contains longitude and latitude values that enclose an area where the SW is allowed to operate. This geographical region is smaller or equal to the size of the country where the TCB resides in. Henceforth, the [TCBL,SWML,SW] is denoted by SW package (SWP). DS_{TCB}[SWP] is then created by TCB_A. This completes SW certification process by TCB.

SW downloading processes are shown in figure 5. Hybrid encryption scheme is used during SW download. To download the SW, the [IdHW,PkHW] and the DS_{TCB} [IdHW,PkHW] are transmitted to the SW maker from a SDR HW. After verification of DS_{TCB}[IdHW,PkHW], the SW maker creates a DS_{SWM}[IdHW]. The SW maker then encrypts the [DS_{SWM}[IdHW], DS_{TCB}[SWP], SW] by a random symmetric key using the encryption algorithm written in SWML. This symmetric key is then encrypted by the PkHW and sent together with the TCBL, SWML and $E_{symmetry}$[DS_{SWM}[IdHW], DS_{TCB}[SWP], SW] as shown in figure 6. SW download processes are followed by installation processes by RSM in the following manner:

- Decryption of the symmetric-key by SkHW in RSM.
- Decryption of $E_{symmetry}$[DS_{SWM}[IdHW], DS_{TCB}[SWP], SW] by the symmetric-key using corresponding decryption algorithm.
- DS_{TCB}[SWP] verification by using $PkTCB_A$.
- DS_{SWM}[IdHW] verification by using PkSWM in SWML.
- SW storage where access right is limited to RSM.

Upon an instruction from user, RSM performs operating processes in the following manner :

- Operation of SW (flashing FPGA and DSP, etc.).
- Setting allowable geographical region in RSM (in this case geographic region of TCB_A).

When the SW is running, RSM checks if the current GPS value lies within the GPS range of the SW in a random period. If any of the processes does not proceed successfully, RSM will inform the user to redownload the SW.

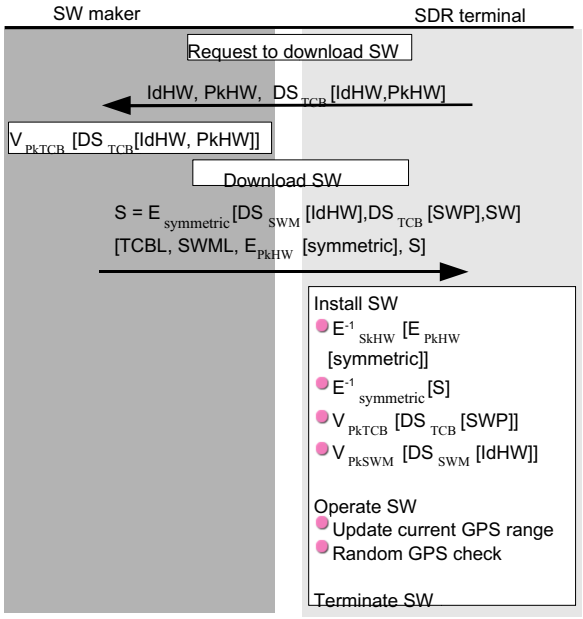


Figure 5: SW download

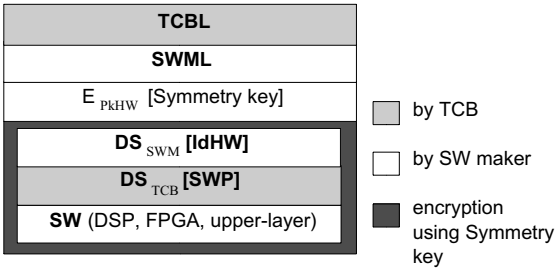


Figure 6: SW hybrid encryption

Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved

5. GLOBAL ROAMING

When the SDR terminal is in Country A, RSM holds the public-key of TCB_A ($PkTCB_A$) and SW_A is running. RSM constantly checks for current GPS value in a random period and compares it with the allowable GPS range of SW_A. When this terminal moves from Country A to Country B (a different geographic region), current GPS value is no longer inside the allowable GPS range. This prompts RSM to suspend SW_A. $TCBL_B$, $SWML_B$ and $[DS_{SWM}[IdHW], DS_{TCB}[SWP], SW]_B$ are downloaded or loaded from local storage in order to use a service in Country B. RSM uses $PkTCB_B$, which is already stored in RSM, to verify the DS of SWP_B. For the case where SW_A is the same as SW_B, it is sufficient to download only $[TCBL, DS_{SWM}[IdHW], DS_{TCB}[SWP]]_B$. After successful verification of $DS_{SWM}[IdHW]_B$ and $DS_{TCB}[SWP]_B$ by RSM, reinstallation is not needed since both SW are the same.

6. RANDOM GPS CHECKING SCHEME

Local radio regulation compliance depends on reliability of GPS signal during random position verification. Unfortunately, GPS signal is not always available. For example, GPS signal is generally weak inside buildings and basements. Jamming of GPS within a locality could also render the SDR inoperational. Thus, a GPS checking scheme as shown in figure 7 is needed to overcome these situations.

It is proposed to group SW into two chategories, namely:

- service provider (SP) independent SW, and
- SP dependent SW.

SP independent SW is SW that does not communicate through a service provider (i.e. which does not perform any handshaking or handover protocol with mobile servers). Example applications of SP independent SW are walkytalky, bluetooth and pager. On the other hand, SP dependent SW is SW that communicates through a service provider. For example, SW for GSM, PHS and CDMA2000.

There are two types of random GPS check, namely normal GPS check and virtual GPS check. Both of them perform random GPS checks once an hour in average. In normal GPS check, the decision to stop SW is based on GPS position. Whereas for virtual GPS check, GPS verification is carried out and recorded as usual except that the decision is based on the connection of SDR with mobile service providers. When SP independent SW operates, normal GPS check is performed. For SP dependent SW, virtual GPS check is performed after current GPS position is obtained.

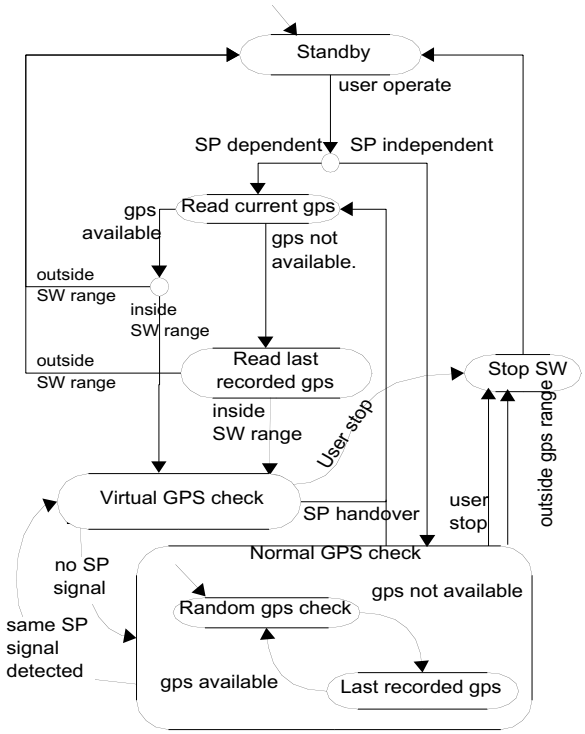
It is assumed that mobile network by a operator does not extend across country borders (eg. no single GSM network across two countries). SP dependent SW uses virtual GPS check because a SDR confirms to stay in the same country if service provider signal is available. Once service provider signal is not present (eg. lost contact to GSM basestation) or service provider handover is performed, it is possible that the SDR is brought to another country. Thus, current GPS position is verified. For the case where service provider signal is not present, current GPS signal is verified by switching to normal GPS check. To realize this, all SP dependent SW must notify RSM when:

- service provider signal cannot be detected, or
- it performs a service provider handover.

This can be enforced by TCB during SW certification where only SWs that comply with this will be certified.

Whenever GPS signal is not available during normal GPS check, last recorded GPS value will be used. Last recorded GPS value can be trusted because users cannot purposely prevent GPS from being recorded since it is taken randomly. As randm GPS check is performed once an hour in average, it is reasonable to assume that current location is same as last recorded location. This applies to situations such as bringing of a SDR into a building/basement where GPS signal cannot be detected.

Ideally, this could be solved by attaching a country ID to broadcast signals of all mobile communication systems. By checking the country ID with TCBL, GPS check is not necessary for SP dependent SW. However, until all systems have been equipped with country ID, which might be slow due to expensive network upgrade, it is sufficient and cost effective to use the above random GPS verification scheme.



Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved

Figure 7: Stateflow of GPS checking scheme

7. SW RECONFIGURATION WITH RSM

The proposed security architecture allows SW reconfiguration through any media. Simplest SW reconfiguration could be from mobile storage such as a memory stick. In this case, the user needs to download SW that has certificates from TCB of countries where the user wish to operate the SDR. In other words, pre-coordination by user is required prior to his/her travel.

For the case of over-the-air reconfiguration, reconfiguration software (RSW) on SDR must also obtain certification from TCBs. For example, if SDR was to be included into 4G mobile communication system, there will be a 4G RSW which has obtained certification from all TCBs (192 digital signatures is small enough to fit in any mobile device). RSM operates RSW after going through the same decryption and DS verification as other SW. RSW monitors other SWs and makes decision to change SW based on signal-noise-ratio, location information and so on. It may then download SW through a standardized over-the-air interface and reconfigure SW through RSM. As certification for RSW is necessary for RSM to operate it, RSW too adheres to local radio regulations which are enforced by random GPS checks. User can manually renew RSW in the future such as an upgrade to 5G.

8. RSM IMPLEMENTATION

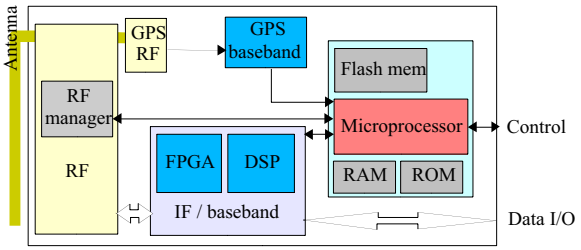


Figure 8: RSM implementation

The hardware structure shown on figure 8 is proposed for the implementation of RSM. The IF/baseband component consists of FPGA and DSP chips. A microprocessor, RAM, ROM and flash-memory are built into a single chip (similar to the structure of a smartcard). The ROM stores a real-time OS with RSM. User-inaccessible components are stored in the flash-memory. Only logical access to the flash-memory through RSM is allowed, therefore user-inaccessible components are tamper resistant. Logical access to the flash-memory is protected by a password which is set by hardware maker during manufacturing process.

Two main implementation issues related to RSM were investigated. They are:

- speed of hybrid decryption and DS verification, and
- RSM memory and disk usage.

Table 1: Specification of PDA and PC

Processor	Intel Celeron 1GHz	Intel XScale 400MHz
Memory	512MBytes	64MBytes
OS	Windows 2000	PocketPC 2002
Java version	JRE1.2.2 with bouncycastle JCE	Jeode JVM with bouncycastle JCE
JVM size	22.8 Mbytes	3.5 MBytes

To examine the speed issue, hybrid decryption (1024bit RSA and 256bit-key AES) and DS verification were performed on a PDA by Java. The specifications of the PDA can be found in table 1. It took 16s for hybrid decryption and 139ms for DS verification of a 3.8MBytes FPGA binary file.

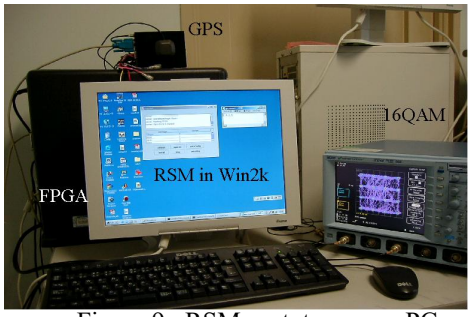


Figure 9: RSM prototype on a PC

A RSM prototype was implemented in a PC with a Xilinx Virtex-II FPGA and a Pioneer GPS kit as shown in figure 9 and table 1. The RSM was implemented by using Java 2 SE edition 1.2.2 in Windows 2000. It is a system service listening for instructions (installation, operation, termination, etc.) at a specific port number. User-inaccessible components of the RSM were protected by administrator password (Unix's root equivalent). The RSM system file size (java class) was 300 KBytes and executing memory size was less than 7 MBytes.

9. DISCUSSION

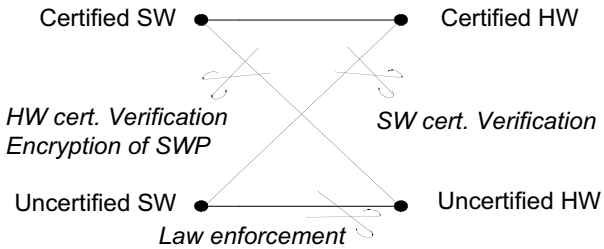


Figure 10: Case studies

Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved

In the proposed security architecture, SW certification and HW certification are separated. This reduces total amount of certification that is needed to be performed by TCB. It is also clear that with hybrid encryption, SW makers particularly third parties can sell or distribute its SW without depending on HW makers. Local radio regulation compliance is assured with random GPS verification performed by RSM.

Several situations are illustrated in figure 10 to show the security strength of our proposed architecture. A certified terminal does not run uncertified SW because of DS_{TCB}[SWP] verification by RSM. A certified terminal cannot duplicate SW because only RSM can access to the corresponding SkHW and decrypt it. Uncertified terminal cannot download SWP because it does not have DS_{TCB} [IdHW,PkHW]. Even if DS_{TCB}[IdHW,PkHW] is copied, the uncertified terminal will not be able to decrypt SWP because it does not have the corresponding SkHW. However, uncertified SW will run on uncertified HW. In this case, it is left for the law enforcement team to eradicate these illegal terminals.

Illegal distribution (by parties other than SW maker) of certified SW to other certified HW is prevented by DS_{SWM} [IdHW] verification, where IdHW is a particular terminal's identity number. Note that no one can sign DS_{SWM}[IdHW] other than SW makers.

In the case where the same SW is used while the SDR terminal roams, only [TCBL, DS_{SWM}[IdHW], ___DS_{TCB} [SWP]] is downloaded. This reduces the need to redownload and reinstall the same SW while local radio regulation compliance is still ensured.

The radio security of SDR can be further enhanced by having a run-time radio regulation check of RF feedbacked signal. A RF manager that checks for center frequency, bandwidth, output power and Adjacent Channel Power Ratio (ACPR) will help to prevent bugs or hidden operation in SW during operation. The Automatic Calibration Unit, ACU [7] [8], which has a run-time radio regulation check, can obtain radio regulation parameters (frequency, bandwith, etc.) securely from TCBL. RSM and ACU can be both implemented in amateur radio equipments and satelite TV boxes to prevent illegal modification by users.

Memory usage and file size show that RSM can be implemented even in small devices such as PDAs. The AES decryption time can be further speedup with better-optimized algorithm. The proposed architecture allows HW maker to change the encryption component in RSM. This allows upgrade of new encryption algorithms as old algorithms are not secure enough as time goes. Type of encryption during download is chosen by SW maker and is monitored by TCB due to certification of SWML that contains the encryption information. This gives TCB the power to oversee the security level of distributed SW in the market.

10. CONCLUSION

A new security architecture which utilizes RSM was proposed for Software Defined Radios. It enables separate certification for SW and HW while allows flexible SW distribution. Local radio regulation compliance is assured with a random GPS verification by RSM. To examine the implementation issues such as speed and memory usage, a model of RSM was implemented on a PDA and a PC. We have shown that RSM can be implemented even with today's commercial off-the-shelf products such as Java and general purpose operating system.

10. REFERENCES

[1] "Authorization and Use of Software Defined Radio", Federal Communications Commission Report, FCC01-264, Sep. 2001.

[2] D. Bourse, M. Dillinger, T.Farnham, N.Olaziregi, "TRUST System Research - Architectures and UML Modelling", SDR Forum Document Number SDRF-02-I-0017-V0.00, Jan. 2002.

[3] K. Moessner, R. Tafazolli, "Software Radio Integration and Reconfiguration Management", SDR Forum Document Number SDRF-01-I-0064w-V0.00, Oct. 2001.

[4] L.B.Michael, M.J.Mihaljevic, S.Haruyama, R.Kohno, "A Framework for Secure Download for Software-Defined Radio", IEEE Communications Magazine Volume 40 Issue 7, Jul. 2002.

[5] J.J.Fitton, "Security Consideration for Software Defined Radios", Proceeding of the 2002 Software Defined Radio Technical Conference, Vol.1, Pg.137, Nov. 2002.

[6] C.F.Lam, T.D.Doan, K.Sakaguchi, J.Takada, K. Araki, "Novel Security Architecture that Enables Global Roaming of SDR Terminal", Proceedings of the 2003 IEICE General Conference, SB-10, Mar. 2003.

[7] M. Togooch , K. Sakaguchi, J. Takada, K. Araki, "Automatic Calibration Unit (ACU) and ACU eMployed Authorization Procedure (AMAP) for SDR", Software Defined Radio Forum, SDRF-02-I-0020-V0.00, Mar. 2002.

[8] T. D. Doan, C. F. Lam, K. Sakaguchi, J. Takada, K. Araki, "Digital Pre-distortion Linearizer for a Realization of Automatic Calibration Unit", Proceedings of the SDR '02 Technical Conference, HW-3-02, Nov. 2002.

[9] Kei SAKAGUCHI, Chih FUNG LAM, Tien DZUNG DOAN, Munkhtur TOGOOCH, Jun-ichi TAKADA, Kiyomichi ARAKI, "ACU and RSM based Radio Spectrum Management for Realization of Flexible Software Defined Radio World", IEICE TRANS. COMMUN., VOL.E86–B NO.12, Dec. 2003.

Proceeding of the SDR 03 Technical Conference and Product Exposition. Copyright © 2003 SDR Forum. All Rights Reserved