Proposal and Evaluation of Security Schemes for Software-Defined Radio

Hiroyuki Shiba
NTT Network Innovation Laboratories
NTT Corporation
Yokosuka-shi, Japan
shiba.hiroyuki@lab.ntt.co.jp

Kazuhiro Uehara
NTT Science and Core Technology
Laboratory Group, NTT Corporation
Atsugi-shi, Japan
uehara@mail.atsu.rdc.ntt.co.jp

Katsuhiko Araki
NTT Network Innovation Laboratories
NTT Corporation
Yokosuka-shi, Japan
araki.katsuhiko@lab.ntt.co.jp

Abstract— **the functions of software-defined radio (SDR) can be changed by changing its software. Therefore, many security problems that have never been seen in the conventional fixed wireless terminals will arise. We assess the security issues of the SDR system by taking the distribution model of SDR terminal software into account. A universal security architecture for the SDR systems is proposed. In the security architecture, security layer 1, involved with radio regulations, is mandatory regardless of the use. In order to keep security, we propose security schemes that use digital signatures in the distribution chain. Three concrete methods are quantitatively compared and discussed. The proposed method can certify the legitimacy of SDR terminals by detecting tampered software and preventing it from being installed on the hardware.**

Keywords- software-defined radio; security architecture; digital signature; public key encryption;

I. INTRODUCTION

The introduction of software-defined radio will trigger new security problems that are unlike those faced by legacy wireless communication systems. A software-defined radio can change its functions by changing its software. On top of the problems posed by hardware modifications, we will see new problems created by illegal software. As the examples of hacking and viruses on the Internet show, illegal software can be significantly easier to implement than hardware modifications. Therefore, new security measures are needed to realize software-defined radio services.

the Federal Communications Commission (FCC) announced the adoption of an approval rule that covered the commercial release of software-defined radio products [1]. A new legal system including technical certification system concerning software-defined radio and the security technology of software-defined radio are being actively discussed in Japan. The Institute of Electronics, Information and Communication Engineers (IEICE), Software Radio Study Group of Japan, the Telecom engineering center (TELEC), and the Software-defined radio Forum (SDR Forum) co-sponsored a workshop on the new approval rule for the practical introduction of software-defined radio in Japan in October of 2001 [2]-[5]. At the request of the Ministry of Public Management, TELEC has been examining the new certification system for the practical use of software-defined radio since 2000 in Japan. In the United States, the SDR Forum issued an Interim Report to the FCC on issues and activities in the area of security for software-defined radio in September of 2002 [6]. The Software Radio Study Group of Japan (established by the Institute of Electronics, Information and Communication Engineers), has been examining security technology for over-the-air download of software-defined radio programs and a security system has been reported in [7]-[9].

This paper describes a security scheme for software-defined radio. Problems anticipated with the introduction of software-defined radio divided into software modifications and problems of existing wireless communication systems in Section II. Section III examines a software distribution model for software-defined radio and proposes a secure architecture. The performance of three concrete methods for implementing security layer 1, which addresses radio regulations and so is the most important of all layers to realize software-defined radio services, is evaluated in Section IV. Section V concludes this paper.

II. PROBLEMS WITH SOFTWARE-DEFINED RADIO

The current laws and "technical regulations conformity certification" consider cellular phone terminals, Japanese Personal Handy-phone System (PHS) terminals, digital cordless phone terminals, etc. in Japan. The software-defined radio terminal, however, raises the complex factor of software. It is assumed that users obtain certified software by various distribution channels independently of the certified hardware. In conventional wireless communication systems, illegal actions such as excessively powerful radio waves and jamming are mainly achieved by altering the hardware. Table I shows the total numbers of licensed radio stations and certified cellular terminals in Japan as of 2000 [10]. Table II shows the number of illegal radio stations detected and those that were prosecuted as of 2000 [10]. The ratio of an illegal radio terminals increases several percents only for a personal radio and amateur radio though the ratio of an illegal radio terminal is about 0.05% in the entire radio terminals. It is assumed that the hardware of software-defined radio terminals will be

0-7803-7822-9/03/$17.00 © 2003 IEEE.

altered in the same way as with conventional radio terminals. At present, the DEURAS system is used to monitor illegal stations across Japan [11]. Among all radio stations, very few are being illegally altered. However, it is possible that more sets will be illegally modified because the hardware of software-defined radio is high-powered and wide band. Therefore, it will be necessary to create hardware that the user cannot alter. Since this problem is fixable, illegal software is seen as the more serious problem. While expertise and special tools are needed to alter hardware, illegal software can be mass-produced cheaply on a PC and widely distributed across the Internet. Since software-defined radios will common used throughout the world, this problem must be countered. The use of illegal software will damage not only the radio field but also other fields such as medicine. Others problems will arise with copyright infringement. Figure 1 shows the international rate of computer software piracy as released by the Business Software Alliance (BSA) [12]. It is clear that about 40 percent of all software is being used illegally. The dollar losses due to piracy totaled $10.97 billion in 2001. It can be predicted that the problem of copyright infringement will also occur in software-defined radio. Additional problems include illegal service use and the damage caused by viruses. Figure 2 shows the computer virus incidents announced by the Information technical Promotion Agency, Japan (IPA) [13]. While fewer serious damage incidents are being reported (due to more proactive responses), the number of all incidents has exploded. Attacks such as the deletion of data and illegal transmissions triggered by viruses, which are not possible with the conventional wireless radio systems, are predicted to strike software-defined radio. In other words, software-defined radio faces many different, and so various security measures are needed. The different issues raised by the use of illegal software are summarized in Table III. Note that software-defined radio differs from the Internet and computers in that it is must consider compliance with the radio regulations.

TABLE I. TOTAL NUMBER OF LICENSED RADIO STATIONS AND CELLULAR TERMINALS IN JAPAN IN 2000.[10]

Total radio station		66,573
Radio stations for telecommunication business		62,729
Private radio station		3,844
	Personal radio station	736
	Amateur radio station	898
	Others	585
	MCA	729

(K stations)

TABLE II. NUMBER OF ILLEGAL RADIO STATIONS DETECTED AND DEALT WITH IN JAPAN IN 2000.[10]

	Detected number of illegal stations	Prosecuted number of illegal stations
Personal radio station	16,660	1,423
Amateur radio station	9,400	1,270
Civil radio station	6,651	1,689
Others	1,356	604
Total	34,067	4,986

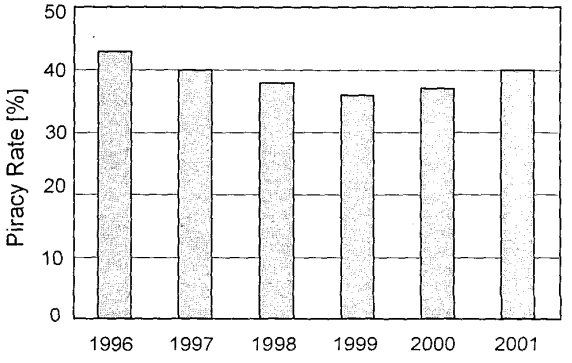

Figure 1. World piracy rate of computer software. [12]

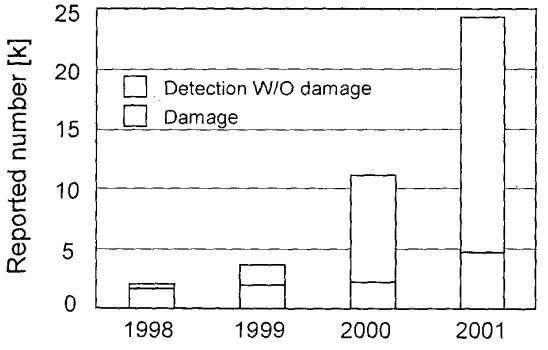

Figure 2. Reported number of damage by the computer virus. [13]

TABLE III. PROBLEMS RAISED BY ILLEGAL SOFTWARE.

Illegal action	Damage	Method of an illegal action
Radio law • High power • Channel occupation • Out of band use	• Jamming • Interference • Malfunction	• Alteration • Own software
Copyright law • Abuse of software	• Software income decrease	• Copy • Abuse of license
Criminal law • Abuse of a terminal	•Communication charge decrease	• Alteration of ID •Authentication/Account process change

III. PROPOSAL OF A SECURITY SCHEME FOR SOFTWARE-DEFINED RADIO

This section describes concrete security measures against the software-defined radio problems described in Section II using the terminal software distribution model shown in Fig. 3. The first user, the carrier, service provider, distributor, etc. might be the same entity as the software manufacturer. This model differs from the conventional contents distribution model in the following points. The certification agency should always certify software with reference to the radio law, and create evidence of certification in spite of the distribution channel. Because the purchaser cannot be trusted to use software in a legal manner, the distributor must take appropriate security measures according to the distribution channel. Moreover, to prevent the illegal use of services by techniques such as spoofing, the service provider must select the security measures that suit that particular service. It follows that the minimum level of security must guarantee the software certificate issued by the certification agency. Ideally, the security architecture should permit higher levels of security to satisfy the requirements of the carrier, service provider, and user. Figure 4 shows the proposed security architecture for software-defined radio. Security layer 1 implements the security measures concerning compliance with the radio law. National bodies and the certification agency execute layer 1. Security layer 2 execute the security measures needed to guarantee service quality and to protect rights such as copyright. The software maker, the software vender, and the service provider, etc., are involved with security layer 2. Security layer 3, which implements the security measures needed to protect user data and privacy, is executed by the user. In this architecture, security layer 1 is the essential security layer and security layers 2 and 3 are executed according to the use and the system. Figure 5 shows an example of security measures that must be implemented by the carrier. The carrier provides a wireless communication service and implements the security layer 2 shown in Fig. 4. First, the carrier uses software and a hardware that has already passed security layer 1 checks in order to comply with radio law. Next, the carrier prevents the illegal use of the service and spoofing by using the digital signatures and authentication technology. Antivirus software is used to prevent denial of service (DoS) attacks and maintain terminal performance. To prevent the illegal use of software, the user must regularly register his information and software is copy protected.

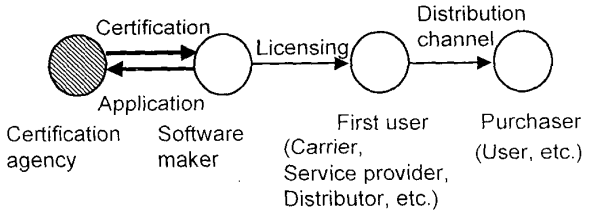

Figure 3. Software distribution model.

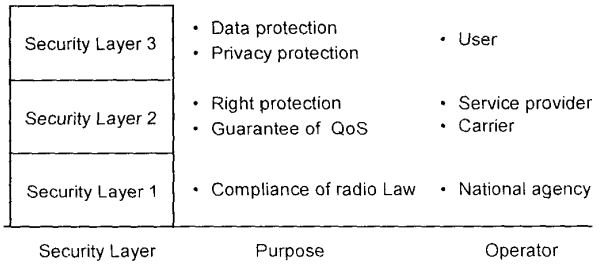

Figure 4. Security architecture for SDR.

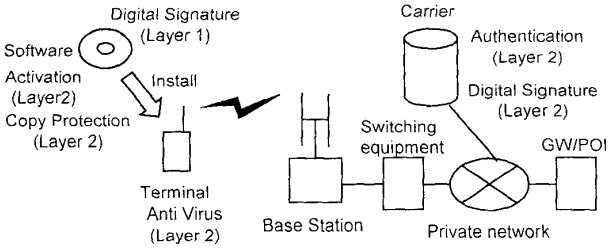

Figure 5. Example of security measures that must be implemented by the carrier.

IV. SECURITY MEASURE FOR SECURITY LAYER 1

We consider a concrete method of implementing layer 1 security in the software wireless terminal software. The software-defined radio terminal works by combining software and hardware. Therefore it is necessary to prevent radio terminal activation unless software and hardware satisfy the following two conditions. 1. Both software and hardware have been certified. 2. Software has not been modified. Digital signatures are one solution. Three methods are shown below as

concrete examples. Figure 6 shows method 1. The certification agency implements the message digest (MD) algorithm and their public key on the hardware of software-defined radio terminal that has been certified. The certification agency also creates a message digest of the desired certified software; the digest is composed of the software and its approval number. Next, the message digest is encrypted with the secret key of the certified agency. The encrypted message digest is added to the software to create a package is made. When the software is installed on the hardware, the hardware makes another message digest of the software from the package. Next, the hardware decodes the obtained message digest with the public key and compares it to the newly made message digest. The hardware can operate as a radio terminal only when the comparison passes. Figure 7 shows method 2. In method 2, the certification agency encrypts not only the message digest like method 1 but also the whole package composed of certified software and its message digest with a secret key. Next, the hardware of the software-defined radio terminal decodes the obtained package with the public key and compares it to the new message digest. The hardware can operate as a radio terminal only when the comparison passes. Figure 8 shows method 3. In this method, the certification agency embeds their public key into the certified hardware of the software-defined radio terminal. For the software, the certification agency encrypts the entire certified software program with their secret key. Method 3 cannot detect package falsification unlike methods 1 and 2. Table IV compares the methods in terms of required processing power, security technologies offered, and security strength. We implemented the three methods and compared their processing requirements as a function package size. RSA was used as the public key encryption algorithm and MD5 was used as the message digest algorithm [14][15]. The public key of RSA was assumed have the parameters of e= 100bits and n= 1024bits. "e" stands public key length. The platform was a 450MHz Pentium II running Windows 98. Figure 9 plots the results. The processing power is normalized by the processing power required by method 1 for the software size of 100KB. Even if the software size grows, method 1 does not demand significantly more processing power unlike the other two. Moreover, method 1 requires less than 10% of the processing power requirements of the other two. We expect that these trends will also hold true for other CPUs and OSs such as ARM and i-TRON. An important problem is reducing the power consumption of the software-defined radio terminal to realize. Due to its significantly smaller processing requirements, method 1 should be adopted. While this paper used RSA was used as the public key encryption algorithm and MD5 as the message digest algorithm, other digital signature algorithms such as ELGamal signature and DSA signature can be used. The required processing power of cryptography are reported in [16]-[18]. We note that ESIGN signatures are at least ten times faster than the RSA signature. With regard to RSA, [19] is researching the high-speed calculation of the residual operation of RSA. Additionally, the hash function of SHA based on MD5 can be used. When the security measures are to be implemented on the software-defined radio terminal, the most suitable cryptograph algorithm for the system must be determined.

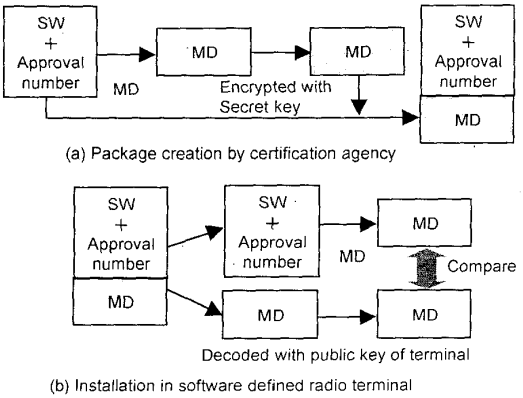

Figure 6. Method 1 of security layer 1.

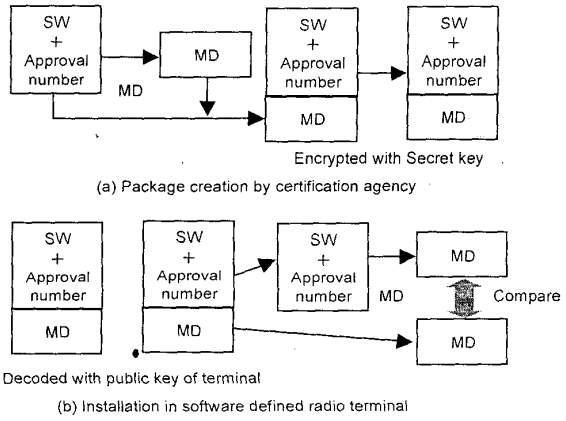

Figure 7. Method 2 of security layer 1.

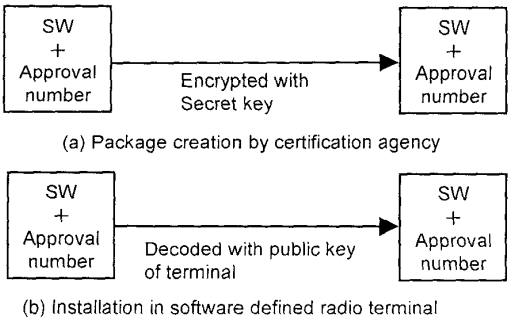

Figure 8. Method 3 of security layer 1.

TABLE IV. COMPARISON OF THREE METHODS.

	Method 1	Method 2	Method 3
Required processing Power (Cf. Fig.9)	Small	Large	Large
Approval function	○	○	○
Falsification detection	○	○	×

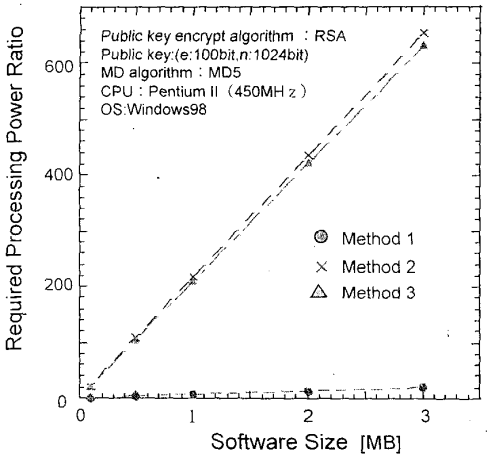

Figure 9. Required processing power ratio vs. software size.

V. CONCLUSION

The new security threats that will arise with the use of software-defined radio were summarized from the viewpoints of radio law, service quality guarantees, and rights protection. A security architecture for software-defined radio was proposed. The proposed architecture requires that the national agency, carrier, service provider, and user should take the appropriate security measures according to their responsibility. Digital signatures were described as the key security technique in implementing security layer 1, the fundamental security level in software-defined radio. Three methods of implementing digital signature security in security layer 1 were shown and estimated. The results confirm that method 1 was the most suitable due to its superior processing power requirements.

REFERENCES

[1] Federal Communications Commission, "Authorization and Use of Software-defined radio: FIRST REPORT AND ORDER," Washington, D.C., Sept.2001.

[2] M. J. Marcus, "New FCC Software-defined radio Policy," IEICE Technical Report SR01-08, pp. 1-6, Oct. 2001.

[3] S. M. Blust , " System Aspect of "Software Based Radio" Regulation," IEICE Technical Report SR01-09, pp. 7-18, Oct. 2001.

[4] K..Sekiguchi, "Activity of SDR Development in JAPAN," IEICE Technical Report SR01-10, pp. 19-21, Oct. 2001.

[5] K.Sasanami , " Study on Software Technology for Radio Equipment," IEICE Technical Report SR01-11, pp. 23-32, Oct. 2001.

[6] http://www.sdrforum.org/

[7] M. J. Mihaljevic, L. B. Michael, S. Haruyama, and R. Kohno, "On Specific Security Requests for SDR Downloading," IEICE Technical Report SR02-05, Apr. 2002.

[8] M. Togooch, K. Sakaguchi, J. Takada, and K. Araki, "Automatic Callibration Unit in SDR," IEICE Technical Report SR01-25 , Dec. 2001.

[9] K. Okuike, H. Uchikawa, K. Ikemoto, K. Umebayashi, and R. Kohno, "A study on On-Board Automatic Certification System (ACS) for Software-defined radio," IEICE Technical Report SR02-010, July 2002.

[10] http://www.soumu.go.jp

[11] http://www.tele.soumu.go.jp

[12] http://www.bsa.or.jp

[13] http://www.ipa.go.jp/security/

[14] http://www.rsasecurity.com

[15] RFC 1321

[16] M. Sugita, K. Uehara and S. Kubota, "Flexible Security Systems and a New Structure for Electronic Commerce on Software Radio, " Proc. 52nd IEEE Vehicular Technology Conference, vol. 6, pp. 3033-3040, Sept. 2000.

[17] K. Itoh, M. Takenaka, N. Torii, S. Temma, and Y. Kurihara, "Fast implementation of publick key cryptography on a DSP TSM320C6201," First International Workshop, CHES'99, LNCS1717, pp. 61-72, Springer-Verlag, Berlin, 1999.

[18] S. Itoh, J. Anzai, N. Matsuzaki, and T. Kato, "A Design for Cryptograpic Copprocessor and Mobile Telecommunication System," The 2000 Symposium on Cryptography and Information Security, SCIS2000-D38, Okinawa, Japan, Jan. 2000.

[19] S.Ishii, K. Tanaka, K. Ooyama, "2048-bit High-Speed Modulus Processor for Public Key Encryption," IEICE, vol.J82-D-I, no.4, pp.571-580 Apr 1999.