SECURITY ISSUES OF DOWNLOADING FOR SOFTWARE RECONFIGURABLE RADIO SYSTEMS VERSUS USUAL INTERNET DOWNLOADING

Miodrag J. Mihaljević[1,2] **and Ryuji Kohno**[3]

[1] ***SONY Computer Science Laboratories, Inc.,***
Takanawa Muse Bldg., 3-14-13 Higashi-Gotanda
Shinagawa-ku, Tokyo, 141-0022 Japan
[2] ***Mathematical Institute, Serbian Academy of Sciences and Arts***
Kneza Mihaila 35, 11000 Belgrade, Yugoslavia
E-mail: miodragm@turing.mi.sanu.ac.yu

[3] ***Yokohama National University***
79-5 Tokiwadai, Hodogaya-ku, Yokohama, 240-8501 Japan
E-mail: kohno@kohnolab.dnj.ynu.ac.jp

ABSTRACT

An origin for developing the appropriate security techniques is identification of differences related to the secure downloading for software defined radio (SDR) versus conventional Internet one. The following issues were analyzed and compared: main security needs; parties involved; required cryptographic techniques; dedicated security requests. In order to ensure that a malicious user can not download illegal software, and cannot illegally redistribute legally downloaded software certain specific requests related to SDR secure download should be fulfilled. These requests include: (i) restrictions on downloading; (ii) certain mandatory parties involved in the secure downloading system; (iii) user inaccessibility to the security system for downloading.

INTRODUCTION

Software Defined Radio (SDR) terminals [1] - [6] aim to be able to dynamically reconfigure the baseband processing part of a wireless device. In order to provide the ability to change or update this portion of the device, a method of software download is necessary. The proces of software download enables the introduction of new functionality (defined in software) into the terminal, with the aim of modifying its configuration and/or content.

To promote the commercial implementation of software download for SDR terminals, a secure method of download is vital. Downloading of all the relevant software is performed via a public channel, and accordingly the security issue of the downloading is one of the key issues.

At this moment, specification of the details related to SDR software download is still work in progress (see [7], for example). On the other hand, in a number of documents and papers the SDR security issue is recognized as one of the substantial ones related to SDR deployment (see [8] - [10], for example).

Finally, the following is a natural question: Is there any difference between the secure downloading issue for SDR and an usual Internet downloading, and if yes, what the difference is.

In this paper, we point out and discuss a number of specific security requests on software download for SDR.

PRELIMINARY DISCUSSION

Software download has been a feature of the Internet for many years. The user connects to the Internet, and after correct choice of the software for the user's operating system (OS), downloads and installs the software. In general there is no restriction on which software may be installed or executed.

For software radio terminals, we have identified several points in which the current model of Internet software download is lacking and cannot be directly applied to SDR download. Particularly, note the following.

- The software to be downloaded must be guaranteed to have been approved by the regulatory authorities, and must be guaranteed to not have been modified since it was approved.

- The user should not be able to implement their own software on a SDR terminal.
- The software must remain secret, to prohibit reverse engineering and loss of important intellectual property in the software.

It can be seen that the first two requirements come from the nature of using a wireless device which emits radiation. Currently, any wireless device or system is required to obtain approval that it conforms to the regulations regarding frequency band, power output, modulation method and so on from appropriate governmental authorities before being manufactured and sold as a commercial device. However for a SDR terminal, since reprogrammed hardware is used, if the software is modified from when it was submitted to the authorities, or indeed has never been approved then the use of that software may cause the wireless device to emit radiation illegally, which may cause interference to other users or even physical harm to the user of the wireless device.

Therefore one of the most important major differences between Internet and SDR software download is the strict requirement of ensuring that the software downloaded has not been modified (verification of integrity) and that it has obtained government approval (authentification). Furthermore, in the event that some illegally modified software is created, there should be some mechanism to prevent the spread of that illegal software.

The third point shows that encryption will be a vital part of the downloading, however this a necessary but not sufficient condition for achieving an acceptable level of security.

Also, it is desirable that software that is able to run on one terminal should not be able to run on another - that is copy protection should be implemented.

Currently available Internet security is rarely used for software download: protection of passwords and credit card numbers are the most common usage.

The current commercial state of the art for downloading of programs to mobile wireless terminals includes usually very small programs such as “applets” with the size of the programs ranging from about 10k-bytes to 50k-bytes. The majority of these programs are entertainment oriented. On the other hand, a program which controls the baseband portion of the SDR will be larger than this, thus the complexity and knowledge which goes into each file will be much larger than current software and therefore worth more to protect this intellectual property. For example the bitfile size for a field programmable gate array (FPGA) of one million gates is approximately 766k-bytes (Virtex 1000).

Finally there are some functions which are desirable in a SDR download system to improve on the Internet downloading model, including the following:

- The users should not have to make any decisions about which hardware, OS type and so on they have when they download software;
- The users should not be able to access or change the security components;
- Government agencies would like to know how many of which types of software are presently being used, and so, accounting measures should be implemented. Note that it is not sufficient to simply count the number of downloads since the same program will be reloaded many times.

SDR DOWNLOAD VERSUS INTERNET DOWNLOAD: SUMMARY OF THE SECURITY ISSUES COMPARISON

First we point out the general security issues which must be considered for a number of data transactions, including secure software download. The issues include the following four aspects (see [5], for example):

- *Privacy*. No one can see the transferred content - this implies employment of encryption techniques.
- *Integrity*. No one can tamper with the content transferred - this implies employment of cryptographic techniques for message integrity/authenticity control.
- *Authentication*. Both parties in a transaction are really who they say there are - this implies employment of techniques for the entities authentication. This can include simple password techniques as well as more sophisticated cryptographic techniques.

- *Non-repudiation*. The user or provider cannot deny their actions - this implies employment of digital signature schemes and appropriate protocols.

Here we outline a summary of comparing the main security issues related to SDR and Internet downloading. For the both cases the following issues were analyzed:
- main security needs,
- parties involved,
- required cryptographic techniques,
- dedicated security requests.

A comparison which illustrates the main similarities and differences between SDR secure downloading and Internet downloading is summarized in Table 1.

Table 1: A comparison of the main security issues related to software defined radio (SDR) downloading and Internet downloading.

Security Issues		SDR Downloading	Internet Downloading
main requests	integrity	yes	yes
	authenticity	yes	yes
	secrecy	yes	yes
	nonrepudiation	yes	yes
parties involved	user	yes	yes
	provider	yes	yes
	approval authority	mandatory	not mandatory
main cryptographic primitives employed	secret key ciphers	yes	yes
	public key ciphers	yes	yes
	hash functions	yes	yes
	digital signature schemes	yes	yes
dedicated SDR requests	user's inaccessibility to the security system	mandatory	usually not required
	approval label	mandatory	usually not required

MAIN SPECIFIC REQUESTS RELATED TO SECURE SDR DOWNLOAD

In order to ensure that a malicious user can not download illegal software, and cannot illegally redistribute (copy) legally downloaded software certain specific requests related to SDR secure download are required. The following main differences between a SDR secure downloading and usual Internet downloading can be identified.

- *Restrictions on Downloading*.

  It should only be possible for approved software to be download into the SDR terminal. Such a request does not exist in conventional Internet downloading.

- *Parties Involved in the Secure Downloading System*.

  A software approval authority is the mandatory party in a secure downloading system for SDR. Usual secure downloading over the Internet does not require the involvement of an approval authority.

- *User Inaccessibility to the Security System for Downloading*.

  One of the most interesting differences between a system for SDR secure downloading and a system for an usual secure downloading via Internet is that in the SDR case an user should not have any control over the security system. Particularly, a SDR user should not have any influence on selection of the involved cryptographic techniques and keys. Note that this request will not have any impact on a legal user. Actually this request means that users do not have to worry about any of the security issues for download - they should be transparent from the users point of view. Accordingly, appropriate measures should be included to prevent any access of the user to the security system. A method for enforcing this rule is employment of tamper resistant hardware.

The issues outlined above should be the origins for developing the secure download system suitable for SDR.

CONCLUSIONS

Software download is a key operation for software defined radio (SDR). The proces of software download enables the introduction of new functionality (defined in software) into the terminal, with the aim of modifying its configuration and/or content.

Downloading of all the relevant software is performed via a public channel, and accordingly the security issue of the downloading is one of the key issues.

An origin for developing the appropriate security techniques is identification of specific differences related to the secure downloading for SDR versus a conventional Internet downloading.

This paper discusses a number of specific security requests on software download for SDR implying that SDR dedicated security frameworks are necessary. Following the analysis given in this paper, a framework for the SDR secure download is proposed in [10].

References

[1] J. Mitola, “The software radio architecture” *IEEE Communications Magazine*, vol. 33, pp. 26 – 38, May 1995.

[2] J. Mitola, “Software Radio Architecture: A Mathematical Perspective”, *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 514 – 538, April 1999.

[3] J.J. Patti, R.M. Husnay and J. Pintar, “A Smart Software Radio: Concept, Development and Demonstration”, *IEEE Journal on Selected Areas in Communications*, vol. 17, pp. 631 – 649 , April 1999.

[4] E. Del Re (ed), *Software Radio: Technologies and Services*. Springer-Verlag: London, 2001.

[5] M. Mehta, N. Drew, G. Vardoulias, N. Greco and C. Niedermeier, “Reconfigurable Terminals: An Overview of Architectural Solutions”, *IEEE Communications Magazine*, vol. 39, pp. 82 – 89, August 2001.

[6] *Software Defined Radio (SDR) Forum*, www.sdrforum.org.

[7] ”Requirements for Radio Software Download for RF Reconfiguration”, *Working Document SDRF-02-W-0003, Software Defined Radio Forum*, Feb. 2002.

[8] *Authorization and Use of Software Defined Radio: First Report and Order*. Federal Communications Commission: Washington, D.C., Sept. 2001.

[9] S.M. Blust, “System Aspects of “Software Based Radio””, *Technical Report of IEICE*, SR01-12, pp. 7-18, Sept. 2001.

[10] L. Michael, M. Mihaljević, S. Haruyama and R. Kohno, “A framework for secure download for software defined radio”, to appear in *IEEE Communications Magazine*, vol. 40, July 2002.