A PROPOSED REGULATORY FRAMEWORK FOR FACILITATING THE INTER-JURISDICTIONAL MOBILITY OF SOFTWARE DEFINED RADIO (SDR) DEVICES

Bernard C. Eydt (Chair, SDR Forum SDR Security Working Group; Associate, Booz Allen Hamilton, McLean, Virginia; eydt_bernie@bah.com)

ABSTRACT

SDR technology must comply with regulations to prevent radio interference. These regulations, which can differ substantially across jurisdictions, have significant implications for device reconfigurability and mobility, which are often touted as SDR's greatest potential benefits. For example, when the user of an SDR device travels from one regulatory jurisdiction to another, what may have been legal radio behavior in the first jurisdiction could be illegal in the second – even if both jurisdictions have regulatory structures that generally permit the use of SDR. This paper presents a regulatory framework that would enable an SDR device to "learn" regulations relevant to its geographic location and restrict its behavior accordingly. The components of the framework include a public key infrastructure (PKI) managed by an international regulatory body such as the International Telecommunications Union (ITU), a meta-language for describing regulatory policy, and a standardized run-time software interface for controlling radio parameters such as frequency, power, and modulation.

1. THE GLOBAL SDR REGULATORY CHALLENGE

The business case for SDR often rests on the notion of reconfigurability – i.e., functionality that enables a radio can change its behavior and operating parameters to meet the needs of its users. Software radios can are inherently more reconfigurable than hardware radios because their radio behavior can be modified by executing new code, something which can be achieved quickly, inexpensively, and, in many cases, remotely. Hardware radios typically require physical modification to acquire significant new functionality, which requires more time and expense than software changes, and requires physical presence to implement the change in all cases,.

While reconfigurability has the potential to bring new services and efficiencies to users, it poses a significant challenge for regulators because if a radio can be easily reconfigured, then regulators cannot determine if it will comply with regulations based on its initial state. In other words, if an SDR device is given type approval based on its intended use with a particular software load, this could be easily circumvented at a later date by downloading different software that performs in an unanticipated fashion. Possible regulatory approaches to address this challenge include requiring approval of each hardware/software combination permitted on the device or prohibiting such changes outside of the scope of the original approval. These approaches, however, have the potential to undermine the business case for SDR, which, as mentioned, requires easy and inexpensive reconfigurability for its value proposition. Thus, the manner in which SDR is regulated in large part determines the market viability of the technology.

The regulatory problem becomes even more challenging when considered in an international context. A key benefit of reconfigurability is that it supports mobility. Users want to maximize the utility of their radios wherever they may be at a given time. To some users, this objective means maximizing data throughput, while to others it may mean improving reliability or reducing costs. How to achieve a particular objective could easily change as the user crosses borders, not only because different areas offer different services at different prices, but also because they can be governed by different rules. Accordingly, for a software radio to be of most use to its mobile users, it should be able to adapt to the regulatory environment in which it finds itself.

One possible solution is global harmonization of SDR regulation. If rules are harmonized, then radio reconfiguration can occur without consideration of regulatory differences. Political reality suggests this is very unlikely to occur, at least not in the time frame most would like to see SDR technology become commercially successful. Furthermore, full harmonization may not even be desirable. Regulators may promulgate better rules if they are competing with and learning from regulators in other jurisdictions. Indeed, SDR and cognitive radio likely will require frequent modifications to regulations on a sustained basis while the technology and its applications evolve. Beneficial regulatory innovations may best occur

when both regulators and the regulated can study how different alternatives work in practice, which could not occur in a fully harmonized environment.

In summary, both SDR technology and regulation should support reconfigurability and cross-border mobility to maximize SDR's commercial potential, but regulations are likely to differ across jurisdictions and for good reason. At first glance, this statement suggests that a conflict might exist between the market and regulatory realities of SDR. This paper proposes a way to resolve that conflict by establishing a universal technical framework for describing and enforcing rules governing radio transmission behavior on an SDR device. The framework provides a level of standardization that would support reconfigurability and mobility, while also allowing for considerable flexibility in the way each jurisdiction chooses to regulate SDR.

2. POTENTIAL TECHNICAL CONTROLS TO ENFORCE REGULATORY POLICY

Although there are huge number of potential security controls that could exists on an SDR device, to generalize we will focus on two broad classes of controls that could be the basis of a universal framework: (1) *code signing* and (2) *run-time filtering*. Code signing involves appending digital signatures to radio software that the SDR device can verify before installing or executing that software. Run-time filtering involves monitoring the radio software's transmission requests and stopping those that violate a pre-defined policy before they are passed to an radio frequency (RF) front end or antenna subsystem.

2.1. Code Signing

Code signing is the primary control under consideration today for SDR. While digital signatures have had a wide variety of applications for many years, the 3rd Generation Partnership Project's (3GPP) Mobile Station Application Execution Environment (MExE) marks their first appearance in the commercial wireless domain [1]. The SDR Forum also discusses a code signing method in its most recent publication on SDR security considerations [2].

The mathematical properties of the cryptographic algorithms used in the code signing process provide a high assurance that (1) the code has not changed since it was signed and (2) the entity that signed the code cannot later deny that it signed the code. The first characteristic is termed *integrity* and the second *non-repudiation*. In short, the digital signature procedure is an excellent mechanism to irrefutably bind an organizational identity to specific radio code.

Unfortunately, the digital signature process does little more than this. In particular, it does not ascribe any meaning to the entity's association with the code. For example, signed code is not necessarily well-behaved code; it could have significant security vulnerabilities or even be a Trojan horse designed to cause radio interference when executed.

Nevertheless, digital signatures provide the characteristics we need for facilitation of inter-jurisdictional mobility of SDR devices. In this case, what would be universal across regulatory jurisdictions is acceptance of the digital signature process as the mechanism to bind radio software to an identity. Digital signatures are already widely used in international e-commerce transactions, so extending the this application of cryptography to SDR does not appear unreasonable.

What could differ across jurisdictions would be the meaning attributed to the signature. For example, in one jurisdiction it might simply mean an entity developed or distributed the code and say nothing about its functionality. In another jurisdiction, it might assert a claim that the code complies with local radio regulations or that it has been certified by an independent lab to do so. In yet another jurisdiction, this claim might be associated with legal liability for problems caused by the code.

Different jurisdictions could also require that different entities sign the code. For example, a regulator might require that hardware manufacturers sign all code permitted to run on their SDR devices (particularly if it holds the manufacturer responsible for interference caused by that device). Another regulatory agency might require that the code be signed by an accredited radio or software assurance laboratory whose signature would provide evidence of successful certification testing. In some cases, the regulator may require that the regulatory authority itself sign the code before it be allowed to operate.

The number of signatures is also flexible. In some jurisdictions, the regulatory may permit radio software accompanied by a single compliance claim, while in others multiple parties may be needed for a compliance claim (e.g., both the hardware manufacturer and the software developer, if these are separate entities).

The potential claims that a signature could represent and varying degrees of the legal liability associated with false claims are countless. The power of the digital signature scheme is that it could provides a universally accepted technical platform that could support a variety of different regulatory regimes.

One remaining issue is how to standardize codification of the digital signature policy for a given jurisdiction so that SDR devices could interpret and enforce the requirements that given jurisdiction during software download and instantiation transactions. A common meta-language is needed for this purpose.

2.1. Run-time Filtering

Run-time filtering has been alluded to in SDR Forum documentation [2] using the terms reconfiguration management and emissions management, but this control has not been explored to the same extent as code signing. Nevertheless, it addresses the main weakness of the code signing control, namely that signed code is not necessarily well-behaved code. If regulators were to rely on code-signing as the sole technical control on SDR devices, it would be very difficult to prevent interference (perhaps even on a mass scale) once bad signed code was distributed.

Malicious radio software could pass through code-signing controls for a number of reasons. First, even well-intended developers and vendors often distribute code that contains bugs of which they were unaware at the time the code was released. Second, nefarious insiders may be able to insert bad code into either the development or signature processes. Finally, someone may be able to compromise the signatory's private key without detection. Certainly these risks can be mitigated, but nonetheless a defense-in-depth strategy dictates that SDR devices should be able to detect and stop rogue radio software during execution.

Like the code-signing control, the objective for regulators is to identify universal technical mechanisms that could support a wide range of different policies. In the case of run-time filtering, the universal technical mechanism might be a simple lookup table of radio frequencies and permitted transmission power levels in each frequency range (with a power level of 0 for prohibited frequencies). All radio software transmission requests would be filtered through the run-time filter, which would check the request against the table. Valid requests would pass through the filter while invalid ones would be dropped (and perhaps an alert sent to a audit subsystem).

As is the case with the digital signature policy, the various regulators would need to agree on a standard way of representing the filtering policy (e.g., using a meta language expressed in XML). With a standard policy language, each regulator could codify the policy corresponding to its jurisdiction in a standard manner. SDR devices could then move from jurisdiction to jurisdiction, loading the policy appropriate for its current location without requiring different devices for different locales.

Unlike digital signatures, the technology supporting the filtering mechanism is not yet widely available, in large part because SDR itself is relatively immature. Once well established, the policy language might be expected to evolve as regulators permit new means of sharing spectrum that rely on cognitive techniques. In the interim, even simple filters would provide an adequate control against the realization of the worst risks, such as widespread and uncontrolled interference resulting from malicious radio code that was mass distributed by a large operator or that had worm-like propagation behavior.

3. POLICY OBJECTS, THEIR VERIFICATION, AND SUPPORTING PKI

To support inter-jurisdictional mobility, both code signing and run-time filtering must be accompanied by jurisdiction-specific policy objects. As mentioned, regulators should establish a meta-language for describing both the digital signature and filtering policy. The common meta-language is what allows devices to move from jurisdiction to jurisdiction and remain in compliance even when the polices of each jurisdiction differ substantially from one another.

A technical problem that must be resolved with respect to the policy objects is to determine how to load the policies on each SDR device. One approach is to install the policies during manufacture and assembly of the device, but these policies could be outdated with regulatory changes. Another approach is to have operators supply the policy objects during service connections, but this assumes a service model that might not exist for every SDR device. Moreover, it implies a trust relationship between the regulator and operator that might not exist or which the regulator may not desire.

Perhaps the best solution is to handle policy objects in same manner as radio code objects – i.e., digitally sign them. The digital signature on a policy object would verify the source of the policy and that the policy received is the one that was signed. In most cases, regulatory agencies would sign their own policies, but they could enlist third parties to provide signatures on their behalf if they chose to do so.

The next challenge is how to verify the regulator's digital signature. The SDR device must either store the public key certificate of each regulator or the regulatory authorities must establish a trust relationship with a common certification authority. In the latter case, each SDR device would only have to be seeded with a single public key certificate, that of an umbrella organization issuing certificate to each legitimate regulatory authority. The SDR device manufacturer would be best positioned to install this initial certificate. The umbrella organization could be the International Telecommunications Union (ITU), or another body that manages international regulatory relationships.

While the certificate hierarchy may at first seem complex, it would be relatively simply to implement. The root authority (e.g., ITU) would only need to issue at most several dozen certificates each year and could outsource this function to PKI specialists.

Each regulator would decide the digital signature and filtering policies for its own jurisdiction. Those with few SDR requirements or minimal technical capabilities or interest could forgo digital signatures altogether, thereby accepting the risk of proceeding without legally required technical controls. Some regulators may opt to sign the certificates of organizations that have the authority to certify compliance with SDR rules. This approach would provide assurance that a rogue organization could not falsely certify malicious code, preventing inadvertent installation of such code. Some regulators might sign its own policies but not sign the certificates of other organizations, instead opting for legal enforcement and liability mechanisms that do not involve technical controls on each device. The general idea is that local regulatory flexibility can exists within a standard international technical framework.

4. HYPOTHETICAL EXAMPLE OF FRAMEWORK IMPLEMENTATION

How the proposed regulatory framework might work in practice is described in the hypothetical example that follows.

During the manufacturing process of a handheld SDR device, the manufacturer installs its own public key certificate and the root ITU public key certificate along with hardware and software mechanisms that ensure that valid cryptographic modules are loaded during the boot process and that the ITU certificate cannot be replaced or modified. The device also contains an ITU digitally signed world map with the coordinates of each recognized regulatory jurisdiction and an ITU digitally signed radio software implementation of the global positioning system (GPS).

When the consumer who purchases the SDR handset first powers it on, it the boot process securely loads supporting operating system software, which includes a cryptographic module that can verify digital signatures. The boot process also specifies that GPS radio software loads on initiation of the device. Before instantiating the executable GPS code, the device validates its ITU digital signature using the tamper-proof ITU public key certificate on the device.

The GPS software determines the location of the device and, after verifying the digital signature on the regulatory map, uses the map to identify the jurisdiction corresponding to its coordinates. In this case, assume the location is in country with a regulatory agency named National Spectrum Management Authority (NSMA). The device then downloads the NSMA public key certificate and the relevant NSMA digitally signed code-signing and run-time filtering policy objects using methods specified in the regulatory map. The device can verify that the objects are indeed from NSMA because the NSMA's certificate has been digitally signed by the ITU. The device effectively uses its initial trust relationship with the ITU to establish a new trust relationship with NSMA.

The NSMA code-signing policy specifies that the device can only instantiate radio code that has been digitally signed by the hardware manufacturer. When the user issues a command for the SDR device to connect to a subscriber network available in that area, the SDR device initiates a software download process. Through a negotiation procedure, the operator provides code that has been signed by the manufacturer of the SDR device. The device can verify the signature using the public key certificate installed on the device during the manufacturing process.

The user now travels with the SDR device to another jurisdiction with a regulatory agency named Ministry of Communication Technology (MCT). The SDR device identifies the new jurisdiction using its GPS module and regulatory map. It queries MCT for its code-signing and run-time filtering policy objects using a method specified in the regulatory map. MCT's code signing policy requires that the device only instantiate radio code that has been digitally signed by one of four authorized radio certification testing companies, whose public key certificates are include in the policy object.

The user wishes to connect the same subscriber network she had used in the previous jurisdiction. When attempting to instantiate the previously downloaded code, the SDR device blocks the transaction because that code is not accompanied by a digital signature from one of the MCT authorized radio certification testing companies. The SDR device then queries the operator for code with the required signature, which is obtained using another download transaction.

The new code is instantiated because it has the requisite signature, but it is actually malicious code designed to create noise on local law enforcement radio bands. The MCT run-time filtering policy object specifies that the radio cannot transmit at power levels greater than zero in these bands, which effectively is a prohibition. When the malicious code attempts to transmit on an frequency reserved for the law enforcement use, the SDR device recognizes the violation, drops the transmission request, and notifies the user that radio software is behaving improperly.

The scenario presented above is just one example of how the framework might work in practice, but should give the reader a sense of the basic elements of the framework. In this scenario, the fictional regulatory agencies NSMA and MCT have distinct policies, but the SDR device is able operate in both jurisdictions because the digital signature mechanism and policy object descriptions are common between them. The SDR device

does not have to have a prior understanding of either jurisdiction. Instead, it "learns" the local policy through network queries. Moreover, it trusts that these policies are legitimate because cryptography provides high assurance that they have been issued by the ITU-recognized authority for that geographic area. Activities in the MCT jurisdiction demonstrated how the controls would work in practice, In this case, the code-signing control blocked code that was not signed by an authorized certification testing company and the run-time filtering control stopped the code from transmitting on law enforcement frequencies.

5. SUMMARY

For SDR to be a commercial success, it must support reconfigurability and mobility. Differences in regulatory structures could significantly restrict the functionality needed to make SDR commercially viable. Regulatory harmonization is neither likely nor, in many cases, desirable. However, if regulatory bodies were able to agree on common techniques to implement general code-signing and run-time filtering controls, they could develop a regulatory framework that would permit considerable diversity in regulatory requirements while also allowing the technology to work seamlessly across jurisdictions.

6. REFERENCES

[1] 3rd Generation Partnership Project, Partnership Project, "Mobile Station Application Execution Environment (MExE); Service description, Stage 1", 1999

[2] Software Defined Radio Forum, "Security Considerations for Operational Software for Software Defined Radio Devices in a Commercial Wireless Domain" (Document SDRF-04-A-0010-V0.0.), 27 October 2004.