SDR Forum Response to FCC MOO

Approved Document SDRF-07-A-0012-v0.0.0

Approved
June 2007

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
Facilitating Opportunities for	)	
Flexible, Efficient, and Reliable	)	ET Docket No. 03-108
Spectrum Use Employing Cognitive	)	
Radio Technologies	)	
	)	

PETITION FOR RECONSIDERATION

I. INTRODUCTION

The SDR Forum respectfully submits this Petition for Reconsideration in the recent Memorandum Opinion and Order in this proceeding.[1] The SDR Forum applauds the Commission for continuing to develop policy that will facilitate the legal operation of software and cognitive radio. In particular, we support the Commission's position that security mechanisms are necessary to ensure that unauthorized radio software does not cause harmful radio interference or have other adverse affects counter to the public interest.

Nonetheless, the SDR Forum is concerned that language in Paragraph 9 of the recent Order may inadvertently pose a barrier to the development and wide implementation of security techniques that would ensure compliance with Commission rules. The following sentences are of particular concern:

> "…manufacturers should not intentionally make the distinctive elements that implement that manufacturer's particular security measures in a software defined radio public, if doing so would increase the risk that these security measures could be defeated or otherwise circumvented to allow operation of the radio in a manner that violates the Commission's rules."
>
> "A system that is wholly dependent on open source elements will have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio." [2]

The SDR Forum recommends that these policy statements be modified. Manufacturers should have the discretion to discuss their security mechanisms in public so long as the intent of the disclosure is not to enable circumvention of the Commission's rules.

[1] *Facilitating Opportunities for Flexible, Efficient and Radio Spectrum Use Employing Cognitive Radio Technologies*, ET Docket No. 03-108, Memorandum Opinion and Order, released April 25, 2007.

[2] Id. at paragraph 9.

Moreover, the Commission should remain neutral on the security of open source elements because, *a priori*, open source approaches are no less secure than proprietary techniques.

II. THE PERILS OF SECURITY THROUGH OBSCURITY

A common misconception about security is that it is always enhanced through secrecy. In practice, some elements of a security framework should remain secret while others should not. An attempt to achieve security by keeping the methods confidential is often termed "security through obscurity." History repeatedly has shown that "security through obscurity" often fails, typically because it precludes a broad and rigorous review that would uncover its flaws and enable experts to fix shortcomings.

Security through obscurity is "brittle" – once the secret is revealed, it may not be possible to return to a secure state. Anyone might be responsible for the breach, including rogue employees of the manufacturer, someone reverse engineering the product's security design, or nefarious individuals able to "hack" into computer files where the confidential material is stored. If the security of a software or cognitive radio depends on the confidentiality of a security method provided to the Commission, then a product recall may be required to restore security whenever information in the certification application to the Commission is revealed. This action would be significantly burdensome to most parties involved. Moreover, it might not eliminate radio interference or other problems during a lengthy interim period.

What is required to remain secret in a security framework are keys, passwords, and biometric data that provide various forms of access control. For example, if a product based its security on publicly available cryptography for which there has been no known failure, then if a key is ever compromised, simply replacing the key may return security to its original state for all transactions going forward. In this case, the Commission never has to maintain secrets because they are held by the private entities that own or operate the radios.

The SDR Forum recommends that in its future opinions and rulemakings, the Commission place less emphasis on the confidentiality of security *methods*, and instead focus on the standards that assure confidentiality of cryptographic secrets in operation.

III. PROVIDING MANUFACTURERS DISCRETION TO DISCUSS THEIR SECURITY MECHANISMS

In the Cognitive Radio Report and Order, the Commission adopted a rule to automatically make confidential information on SDR security features contained in certification applications. The recent Memorandum Opinion and Order reaffirms that position. However, it also prohibits disclosure to third parties "if doing so would increase the risk that … security measures could be defeated or otherwise circumvented to allow operation of the radio in a manner that violates the Commission's rules." As stated, this policy applies to both open source and non-open source elements.

The policy does not clearly delineate who makes the risk determination or who is accountable for the determination once made. Consequently, manufacturers likely will take a conservative approach, keeping their security techniques confidential to provide the greatest assurance of compliance with the policy regardless of the security merits of that approach. If manufacturers follow this strict interpretation of the policy, it could unfortunately become a *de facto* mandate for security through obscurity.

In particular, the SDR Forum is concerned that the policy may discourage standardization of security methods that would be in the public interest. For example, an SDR Forum member might decide to withhold its security approach from the Forum's membership because doing so might reveal aspects of the approach that "could be defeated or otherwise circumvented." However, it is the very revelation of the member's approach that would enable other members to scrutinize it and make improvements to it. The SDR Forum would like to foster this type of industry collaboration to develop the best security practices and increase the likelihood that manufacturers will implement them properly. However, the new policy could make progress of this sort more difficult to achieve.

The policy may also discourage new business models that would improve the quality of SDR security and lower its costs. Seemingly implicit in the Commission's order is that the radio manufacturer and security mechanism developer are vertically integrated – i.e., one company provides both functions. However, for the most effective techniques to be implemented across SDR and cognitive radio markets, they need to be shared across multiple manufacturers. In some cases, radio manufacturers may want to license their security technology to other companies. In other cases, independent security software companies could develop specialized competencies to meet the needs of multiple radio manufacturers. While discussion of some aspects of the security mechanisms could be limited by non-disclosure agreements, firms must have the ability to make many aspects of their security techniques public to perform effective marketing and outreach campaigns. Indeed they probably will need to "intentionally make the distinctive elements that implement…security measures in an [SDR] public." Without this ability, the businesses may not be viable, which would prevent the radio industry and the Commission from capturing the benefits of a free and competitive marketplace.

<u>SDR Forum Recommendation</u>: To address these concerns, the SDR Forum recommends that the Commission revise its policy to read "a manufacturer may make public its SDR security mechanisms so long as the intent is not to circumvent compliance with Commission rules." For example, a manufacturer may explain publicly why distinguishing security features of its product reduce the likelihood of malicious code, but it shall not provide instructions on how to disable the security features on which it based its certification.

IV. REMAINING NEUTRAL ON THE MERITS OF OPEN SOURCE APPROACHES

The recent Memorandum Opinion and Order states that “A system that is wholly dependent on open source elements will have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio.” The presumed rationale behind this opinion is that “making information on security measures publicly available could assist parties in determining ways to defeat them.” In short, the position appears to advocate security through obscurity.

While there is active debate on the security posture of open source software, considerable evidence exists that open source code typically is more secure than proprietary code. The reason is that open source code is exposed to a wide range of experts with an interest in the success of the software and the willingness to update it to correct known flaws.

Some of the most successful security techniques in information and communications technology today are based on open source approaches. For example, most web-based e-commerce transactions today use a technique called Secure Socket Layer (SSL), which is also referred to as Transport Layer Security (TLS). The specification for SSL was vetted through the open processes of the Internet Engineering Task Force. The code underlying many implementations of SSL/TLS is public, including routines to support the popular Mozilla Firebox web browser. Credit card fraud, identity theft, and Phishing[3] are common, but despite the public nature of SSL/TLS, millions of e-commerce transactions are completed daily without incident.

The Federal Government pursues a policy of openness for security controls to protect sensitive but unclassified information. By law, the US Department of Commerce’s National Institute of Standards and Technology (NIST) is responsible for developing Federal Information Processing Standards and security guidelines for all civilian agencies. All of NIST approved standards, algorithms, and security guidelines are public. For instance, NIST led the effort to create the Advanced Encryption Standard (AES) and Secure Hash Algorithm (SHA). These security mechanisms are highly regarded and used by organizations around the world to protect information even though they are in the public domain. Indeed, many experts argue that these standards are successful *because* of their openness and not in spite of it.

If the Commission continues to pursue a policy of holding a “high burden” for “open source elements,” it will inevitably be drawn into discussions of what these terms mean. However, it is not clear how testing and certification procedures or thresholds might differ for open source elements in practice. Moreover, there are many interpretations of what constitutes open source. The Commission may find that resolving these debates is

[3] Phishing is “the practice of luring unsuspecting Internet users to a fake Web site by using authentic-looking email with the real organization's logo, in an attempt to steal passwords, financial or personal information, or introduce a virus attack; the creation of a Web site replica for fooling unsuspecting Internet users into submitting personal or financial information or passwords.” *Webster's New Millennium™ Dictionary of English, Preview Edition* (v 0.9.6). Lexico Publishing Group, LLC.

not a particularly productive use of its staff resources, particularly given that the underlying policy may not provide a meaningful security benefit.

SDR Forum Recommendation: The Commission should remain neutral with respect to open source security methods. Academic inquiry and industry discussion coupled with a market test is more likely to lead to the correct outcome with respect to the open source debate than regulatory intervention. According, the SDR Forum recommends that the Commission withdraw the statements in Paragraph 9 that express a bias against open source software.

IV. SUMMARY

The Commission should create an environment in which SDR security mechanisms can achieve the same level of performance as SSL/TLS, AES, SHA and many other publicly available and highly successful security standards, algorithms, and protocols. This requires that industry organizations such as the SDR Forum freely discuss best security practice among their membership and make their findings available to the general public. Standards development in particular requires that organizations provide contributions without any reluctance that they may be violating FCC policy by doing so.

To best serve the public interest and facilitate the growth of new radio technologies, the SDR Forum recommends the Commission change its policy statements in Paragraph 9 of the recent Memorandum Opinion and Order to instead read:

> A. “Manufacturers may make public its SDR security mechanisms so long as the intent is not to circumvent compliance with Commission rules.”; and
>
> B. Strike the statement stating: “A system that is wholly dependent on open source elements will have a high burden to demonstrate that it is sufficiently secure to warrant authorization as a software defined radio.”

Respectfully submitted,

Bruce Oberlies
Chair, Regulatory Committee
SDR Forum