CBRS Threat Model Technical Report

Document WINNF-15-P-0089

Version V1.0.0

11 May 2016

TERMS, CONDITIONS & NOTICES

This document has been prepared by the Spectrum Sharing Committee to assist The Software Defined Radio Forum Inc. (or its successors or assigns, hereafter "the Forum"). It may be amended or withdrawn at a later time and it is not binding on any member of the Forum or of the Spectrum Sharing Committee.

Contributors to this document that have submitted copyrighted materials (the Submission) to the Forum for use in this document retain copyright ownership of their original work, while at the same time granting the Forum a non-exclusive, irrevocable, worldwide, perpetual, royalty-free license under the Submitter's copyrights in the Submission to reproduce, distribute, publish, display, perform, and create derivative works of the Submission based on that original work for the purpose of developing this document under the Forum's own copyright.

Permission is granted to the Forum's participants to copy any portion of this document for legitimate purposes of the Forum. Copying for monetary gain or for other non-Forum related purposes is prohibited.

THIS DOCUMENT IS BEING OFFERED WITHOUT ANY WARRANTY WHATSOEVER, AND IN PARTICULAR, ANY WARRANTY OF NON-INFRINGEMENT IS EXPRESSLY DISCLAIMED. ANY USE OF THIS SPECIFICATION SHALL BE MADE ENTIRELY AT THE IMPLEMENTER'S OWN RISK, AND NEITHER THE FORUM, NOR ANY OF ITS MEMBERS OR SUBMITTERS, SHALL HAVE ANY LIABILITY WHATSOEVER TO ANY IMPLEMENTER OR THIRD PARTY FOR ANY DAMAGES OF ANY NATURE WHATSOEVER, DIRECTLY OR INDIRECTLY, ARISING FROM THE USE OF THIS DOCUMENT.

Recipients of this document are requested to submit, with their comments, notification of any relevant patent claims or other intellectual property rights of which they may be aware that might be infringed by any implementation of the specification set forth in this document, and to provide supporting documentation.

This document was developed following the Forum's policy on restricted or controlled information (Policy 009) to ensure that that the document can be shared openly with other member organizations around the world. Additional Information on this policy can be found here: http://www.wirelessinnovation.org/page/Policies_and_Procedures

Although this document contains no restricted or controlled information, the specific implementation of concepts contain herein may be controlled under the laws of the country of origin for that implementation. Readers are encouraged, therefore, to consult with a cognizant authority prior to any further development.

Wireless Innovation Forum ™ and SDR Forum ™ are trademarks of the Software Defined Radio Forum Inc.

Table of Contents

TERMS, CONDITIONS & NOTICES i
1 Introduction 1
2 CBRS Assets 1
3 CBRS Component Interfaces (Trust Boundaries) 2
4 Threat Profiles 4
4.1 Threat: Malicious anonymous (un-authenticated) communication to SAS 4
4.1.1 Availability related threat profiles: 4
4.1.2 Auditability related threat profile: 4
4.1.3 Privacy/Confidentiality related threat profile: 4
4.2 Threat: A compromised CBSD (including the compromise of CBSD to SAS credentials) 4
4.2.1 Authentication/Authorization related threat profiles: 5
4.2.2 Availability related threat profile: 5
4.2.3 Privacy/Confidentiality related threat profile: 5
4.3 Threat: A compromised intermediate signing key from a CBSD manufacturer 6
4.3.1 Confidentiality related Threat profile: 6
4.4 Threat: A compromised domain proxy 6
4.4.1 Non-repudiation/Confidentiality/Privacy related threat profiles: 7
4.4.2 Availability related threat profile: 7
4.5 Threat: A compromised SAS operator (including credentials validated by CBSD clients and credentials used to authenticate to other SAS) 7
4.5.1 Non-repudiation/Confidentiality/Privacy related threat profiles: 7
4.5.2 Availability related threat profile: 7
4.6 Threat: A compromised ESC operator (including the compromise of an information related to Incumbent operations) 8
4.6.1 Privacy/Confidentiality related threat profile: 8
4.6.2 Data Integrity related threat profile: 8
4.7 Threat: A compromised Certificate Authority or compromised PKI certificate lifecycle 8
4.7.1 Non-repudiation/Confidentiality/Privacy related threat profiles: 9
5 Capabilities of Adversaries 9

List of Tables

Table 1: Trust Boundaries 3

CBRS Threat Model

1 Introduction

The Citizens Broadband Radio Service (CBRS) system is the subject of a rulemaking by the Federal Communications Commission (FCC) in Docket 12-354. The rulemaking governs spectrum sharing of the band around 3.6GHz, by defining a Spectrum Access System (SAS) which organizes interference protections for incumbents and devices (Citizens Broadband Service Devices, or CBSDs) operating in the Priority Access License (PAL) tier and General Authorized Access (GAA) tier.

This document summarizes a security threat model for the various actors and systems involved in coordinating CBRS operations within the band. The CBRS threat model is comprised of three element categories:

- CBRS Assets (Targets of Adversaries)
- CBRS Component Interfaces (Trust Boundaries)
- Threat Profiles

We describe each of these categories in detail in the following three sections. The document concludes with few notes around capabilities of adversaries.

2 CBRS Assets

A typical goal of an adversary is to gain access to assets maintained, stored, or managed by system components. While some assets may be the ultimate target of an attacker, other assets (such as credentials) may be intermediary targets and serve to "chain" to either another intermediary target or on to an ultimate target. Each CBRS data and metadata "asset" shall be protected[1].

A second typical goal of an adversary is to diminish or completely block service availability of the service interfaces among CBRS components. Users of CBRS spectrum are fully reliant on the continuous availability of SAS to maintain permission to use CBRS spectrum. "SAS Service availability" is also a vital CBRS asset that shall be protected.

1.1 [1] FCC **§96.61**

3 CBRS Component Interfaces (Trust Boundaries)

Each component interface (including GUI and API services) in the CBRS shall be designed to mitigate both penetration and denial of service attacks via best practice security control requirements[2].

Penetration attacks have the goal to comprise one or more metadata and/or data assets held by CBRS system components. Penetration attacks may leverage any number of known and unknown attack methods (e.g.: brute-force, compromised user/leaked client credentials, vulnerability exploits, etc).

Denial-of-service attacks have the primary goal to compromise the availability of an exposed service. Denial-of-service attacks may include high frequency/volumetric attacks as well as application level vulnerabilities to achieve state/resource exhaustion. Attackers may be in the form of both non-authenticated users/services as well as authenticated users/services (with legitimate credentials).

The following table provides a list of CBRS component Interfaces (trust boundaries between each pair of CBRS communication source and target). For every interaction across a trust boundary, proper Authentication, Authorization, and Accounting (AAA) should occur to protect against penetration attacks. Each target entity of a trust boundary shall[3] have denial of service protection mechanisms in place to ensure its availability is protected against compromised source entities (such as a compromised CBSD or leaked CBSD private key material). The table also lists the assets requiring protection. These assets are shared and/or mutually held by the entities on both sides of the trust boundary.

[2] https://web.nvd.nist.gov/view/800-53/Rev4/impact?impactName=high
[3] FCC Part 96 R&O III.H.2.320

Table 1: Trust Boundaries

Trust Boundary		Assets	Authentication Method
Source Entity	**Target Entity**		
Anonymous Internet Users	SAS	• SAS service availability • SAS client credentials	None
CBSD Operators, Domain Proxy Operators, PAL Holders, Professional Installers	SAS	• Individual or Org to SAS Registration profiles, Authentication credentials • Individual or Org service usage activity metadata	Proprietary – Per SAS Operator
CBSD, Domain Proxy	SAS	• CBSD/Domain Proxy to SAS Credentials, registration and other device metadata • Spectrum grant and revocation data • SAS Service availability	Standardized PKI
SAS	SAS	• SAS to SAS registration profiles, authentication credentials, and communication metadata • SAS to SAS Communication data (including spectrum grants/revocations, obfuscated DoD spectrum usage metadata)	Standardized PKI for all SAS
ESC	SAS	• ESC to SAS Authentication credentials and communication metadata • Obfuscated DoD channel usage metadata (Note: Specific DoD operational activity location data shall not be shared outside of ESC)	Proprietary – Per SAS Operator
CBRS Ecosystem Participant as well as Anonymous Internet Users	CBRS Certificate Authority	• Key pairs trusted to issue other CA certificates or certificates for any CBRS ecosystem participant	Proprietary per CA

This document focuses on threats related to the control plane of CBRS Threat models for communication flows of CBRS End Users are outside the scope of this document. Threat profiles associated with compromised PAL holders, and Professional installers are also outside the scope of this document.

4 Threat Profiles

The following is a list of threat profiles for CBRS assets.

4.1 Threat: Malicious anonymous (un-authenticated) communication to SAS

As with all public Internet facing services, threats exist related to malicious requests of un-authenticated users.

4.1.1 Availability related threat profiles:

4.1.1.1 An anonymous user may attempt to generate a sufficient volume of authentication requests to the SAS with the goal of taking the SAS authentication (or other) service offline.

4.1.1.2 An anonymous user may attempt to generate a sufficient volume of [invalid] authentication requests under the identity of a particular CBSD with the goal of coercing the SAS to blacklist a legitimate CBSD.

4.1.2 Auditability related threat profile:

4.1.2.1 A large volume of audit log entries may be produced by a high rate of Anonymous user actions, possibly exhausting resources on log management system

4.1.3 Privacy/Confidentiality related threat profile:

4.1.3.1 An anonymous user may attempt brute force authentication to a SAS so as to harvest legitimate client-to-SAS credentials or to obtain CBSD registration metadata.

4.1.3.2 An anonymous user may attempt to enumerate and/or footprint the SAS application and infrastructure in an attempt to infiltrate sensitive information, (e.g. version information, valid users/emails, etc) as a means to obtain unauthorized access via social engineering, and/or exploit publicly known and/or 0-day vulnerabilities.

4.1.3.3 An anonymous user may attempt to create their own fake SAS for harvesting credentials of valid consumers of SAS (via DNS pharming, phishing, spear-phishing, vishing, etc).

4.2 Threat: A compromised CBSD (including the compromise of CBSD to SAS credentials)

A CBSD (“device”) needs to be able to provide assurance to the SAS that it is certified for operation, and shall attest to its current operational parameters (such as location and antennae configuration)

4.2.1 Authentication/Authorization related threat profiles:

4.2.1.1 A device registering with false manufacturing information. This profile includes a device claiming to be a certified device when it actually isn't (spoof an fcc ID), a device attempting to spoof its device id, or a device attempting to spoof antennae characteristics.

4.2.1.2 A device claiming to be a different certified device than it actually is (perhaps one with better performance or other advantages).

4.2.1.3 A device registering with false deployment-time information (such as location), thus interfering with the proper operation of legitimate devices in the reported location.

4.2.1.4 A hijack of a device to SAS session (MITM attack) could allow the take over of a device's legitimate authorization by an imposter (e.g. claiming to be the authorized device so as to receive the enabling heartbeat)

4.2.1.5 A hijack of a device to SAS session (MITM attack) could insert an improper device into the request chain (e.g. register in one location and then request spectrum in an alternate (improper) location to get around exclusion restrictions)

4.2.1.6 An authorization replay attack may be used to gain improper authorization for a certified device.

4.2.2 Availability related threat profile:

4.2.2.1 A device under the control of an adversary may flood a SAS with communication and effectively affect SAS availability to that device or other devices.

4.2.2.2 A compromised device may confirm yet ignore a SAS suspension/relocation request of spectrum actively used by an incumbent, thus presenting impairment to spectrum availability or fidelity during incumbent operations. Additionally, a malicious entity may increase TX power on a compromised CBSD to the maximum level supported by the device hardware to further impair incumbent operations.

4.2.2.3 A malicious entity may actively attempt to spoof incumbent spectrum activity via compromised CBSD hardware and firmware potentially resulting in false positives of sensed incumbent operations by nearby ESC nodes.

4.2.3 Privacy/Confidentiality related threat profile:

4.2.3.1 Sensitive end user device communication and spectrum usage metadata may also be collected by an adversary and publically exposed or exploited for economic, political, or other purposes.

4.2.3.2 Compromised CBSDs may be used to store and forward frequency re-assignments, GPS location, and antenna azimuth information. This information may be analyzed and exploited by an adversary to infer time and location of incumbent's operations.

4.3 Threat: A compromised intermediate signing key from a CBSD manufacturer

Each CBSD uses a unique certificate provided by the manufacturer to register for authorized operation with the SAS as well as to receive continued use authorizations (heartbeats). The device will provide various details about itself to the SAS, and then request authorization to operate. The SAS relies on signed CBSD certificates (uniquely signed per CBSD by the CBSD manufacturer) to validate that it is communicating with a legitimate device.

4.3.1 Confidentiality related Threat profile:

4.3.1.1 A compromised intermediate signing key would allow an adversary to generate any number of trusted CBSD certificates and deny band use to legitimate users by introducing “Sybil” (non-existent) nodes. Sybil nodes could also be used to perform analytics on channel availability and quickly determine the geographical and frequency scopes of DoD spectrum utilization.

4.4 Threat: A compromised domain proxy

Domain proxies serve the role of aggregating spectrum requests on behalf of many CBSDs. Domain proxies will be used, for instance, for managed networks with many devices making use of SAS services, and which want to consolidate traffic to the SAS or do central management. It may also be done for remote CBSDs which are being provisioned out-of-band by a domain proxy. A domain proxy communicates with SAS, and acts on behalf of actual devices which are individually certified for operation.

4.4.1 Non-repudiation/Confidentiality/Privacy related threat profiles:

4.4.1.1 A domain proxy under the control of an adversary could manipulate and/or falsify any data that the domain proxy is trusted to aggregate and attest to.

4.4.1.2 A domain proxy under the control of an adversary may log, replay or disrupt device-to-SAS communication and effectively disrupt operation of all CBSDs under that domain proxy. Sensitive spectrum usage metadata for a large number of CBSDs, be they real or artificial, may also be collected by an adversary and publically exposed or exploited for commercial or other purposes. The compromise of such spectrum usage metadata in aggregate poses an Incumbent Opsec threat by allowing frequency usage of Incumbents to be more easily estimated.

4.4.2 Availability related threat profile:

4.4.2.1 A domain proxy under the control of an adversary may be used to generate a massive number of artificial ("Sybil") CBSDs with the intention of maliciously consuming SAS resources and/or wireless spectrum grants.

4.5 Threat: A compromised SAS operator (including credentials validated by CBSD clients and credentials used to authenticate to other SAS)

The compromise of a SAS itself would be considered as a catastrophic event in the CBRS ecosystem. The ecosystem participants should deploy mechanisms to avoid such a compromise.

4.5.1 Non-repudiation/Confidentiality/Privacy related threat profiles:

4.5.1.1 The forwarding of CBSD registration data or metadata means that the entire SAS system is potentially limited to the security properties of the weakest SAS

4.5.1.2 A SAS under the control of an adversary could manipulate and/or falsify any data that the SAS is trusted to aggregate and attest to.

4.5.1.3 Any information available to a compromised SAS may be exploited by malicious entities to infer incumbent activity information. Specifically: ESC-to-SAS information, frequency re-assignments, as well as GPS location and antenna azimuth information of all CBSDs visible to a SAS may be analyzed and exploited by an adversary to infer time and location of incumbent's operations.

4.5.2 Availability related threat profile:

4.5.2.1 A SAS under the control of an adversary may replay or disrupt device to SAS communication, SAS to SAS communication, and effectively disrupt operation of all CBSDs under that SAS and potentially peer SAS. Sensitive spectrum usage metadata

may also be collected by an adversary and publically exposed or exploited for commercial purposes.

4.6 Threat: A compromised ESC operator (including the compromise of an information related to Incumbent operations)

Given that one of the incumbent systems in the band is radar operated by the Department of Defense (DoD), there is a class of security concerns around signaling and information retention which would provide an attacker with a novel source of high-grade information about incumbent activity.

4.6.1 Privacy/Confidentiality related threat profile:

4.6.1.1 The compromise of one or more ESC components would provide an attacker with a novel source of data about incumbent activity

4.6.2 Data Integrity related threat profile:

4.6.2.1 A compromised ESC could inject false DoD activity into the SAS ecosystem and effectively bring the entire CBRS ecosystem to a halt in the geographical area covered by the compromised ESC(s).

4.7 Threat: A compromised Certificate Authority or compromised PKI certificate lifecycle

Given that mitigation techniques of the above threats will heavily rely on PKI, protection of the certificate chain and certificate lifecycle is critical. Threats related to PKI certificate lifecycles including documentation validation requirements for issuance and private key security of certificate issuers shall be mitigated.

4.7.1 Non-repudiation/Confidentiality/Privacy related threat profiles:

4.7.1.1 A compromised Certificate Authority would provide an attacker with the ability to generate and spoof identities of any participant in the PKI structure. Such a compromise can lead to a service disruption (DoS) for possibly all participants in the CBRS ecosystem.

4.7.1.2 Weak certification requirements or weak validation requirements of documentation to provide assurance of hardware, software, or service certification can lead to certificates being issued to un-authorized entities. The result could have the same DoS potential as a fully compromised Certificate Authority.

4.7.1.3 Weak certificate revocation requirements or weak mechanisms for communication and validation of revocation information can allow malicious entities to deny service to legitimate users.

5 Capabilities of Adversaries

We make the following minimum assumptions about the capabilities of adversaries:

- adversary can gain access to client credentials for the General Authorized Access (GAA) tier of SAS service and as a result has the necessary credentials to make spectrum authorization requests to one or more SAS providers;
- adversary has the ability to make requests from any quantity of source IP addresses using multiple GAA credentials, for example leveraging a BotNet;
- adversary has sufficient computational resources to make probabilistic inferences about incumbent activity based on exchanges with SAS; and
- adversary can perform a denial of service (DoS) or distributed DoS (DDoS) against Internet-connected SAS interfaces.