Chapter 30
Risk Engine Design as a Key Security Enhancement to the Standard Architecture for Cognitive Radio

Andre Abadie
George Mason University, USA

Damindra Bandara
George Mason University, USA

Duminda Wijesekera
George Mason University, USA

ABSTRACT
Even though security research in cognitive radio offers specific countermeasures to address known threats, there are a number of unknown conditions or influences that will shape its eventual realization once it reaches capability maturity. To attempt to secure against such unknowns, this chapter describes a risk engine that can incorporate a risk assessment cognition cycle. In various business sectors, risk management is the preferred mechanism to address unknown conditions and therefore offers promise in this context. The chapter describes how the risk engine can potentially address the vulnerabilities inherent to radio operation: in the sensing/perception of spectrum, in the cognition cycle, or in the device infrastructure. It highlights some well-defined threats, their associated countermeasures, and suggests conceptual approaches for a risk engine to intervene in those scenarios. Finally, a case study is introduced to demonstrate an example risk engine’s ability to accurately assess particular risks in a given operational environment as well as potentially detect adversarial actions.

INTRODUCTION
Though there is a tremendous research effort towards cognitive radio technologies, it is heavily vested in dynamic spectrum access and management. A complementary approach is to create a cognition cycle that executes risk assessment and improves the radio’s security posture. The first half of the chapter examines how the radio can implement a focus on security through a cognition cycle centered on risk

DOI: 10.4018/978-1-4666-6571-2.ch030
management – synthesizing the radio’s knowledge of its location and awareness of its environment to examine potential threats and assess the associated risk they present to existing device vulnerabilities. Offering an example approach, the remainder of the chapter presents a case-study risk engine that provides awareness of heightened risk to system availability based on environmental factors and, more importantly, adversarial attempts to exploit vulnerabilities in SDR technologies. The chapter concludes with recommended research to progress forward with more advanced risk quantification for enhanced security in the emerging cognitive radio operational environment.

BACKGROUND

There is an ongoing project to identify major innovations that would be required to create the foundation of the next generation of wireless devices (Wireless Innovation Forum). These innovations, either technical, business or regulatory, if realized, would address various perceived or real shortcomings in the wireless domain. “Top 10 Innovations” from The Wireless Innovation Forum are widely considered to have the most potential of improving the wireless communications experience. Without listing all ten innovations, two are of specific relevance to the concepts presented in this chapter. Innovation #7 call for a more context aware cognitive radio and Innovation #8 solicits interference mitigation techniques. The premise of a risk engine for the cognition cycle touches both areas and potentially offers an avenue for their further development.

The Software Defined Radio Forum has published a standard architecture for future cognitive radio development, as depicted in Figure 1. Two prominent aspects of this architecture are described as engines. The first, labeled the “cognitive engine,” tries to find a solution or optimize a performance goal based on inputs received from the operating environment and other parts of the radio. The second engine is

*Figure 1. Standard architecture for cognitive radio development (Fette 2006, 222)*