SDR Security

Contributed by Bernie Eydt, Booz Allen Hamilton

A key value proposition of SDR is that it enables the users, manufacturers, and network operators to modify radios after they have been manufactured. The reconfigurability characteristic makes easy retrofits and upgrades possible. It also is the foundation for next generation wireless communication, in which radios can sense their environment and autonomously change their behavior to optimize user preferences or network efficiency.

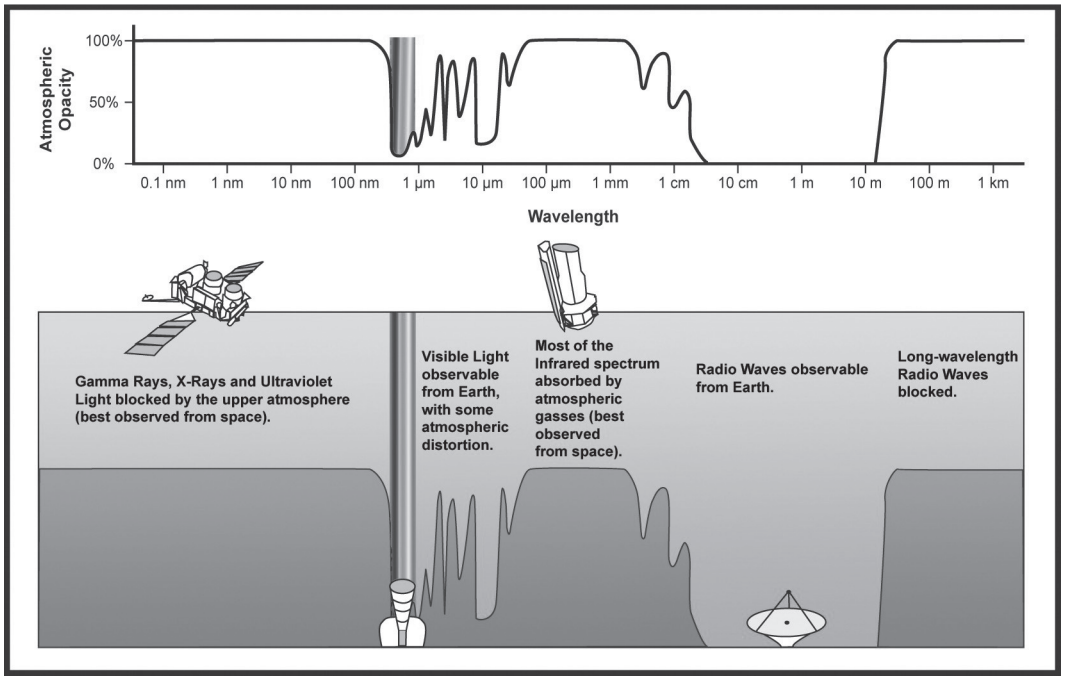
While radio reconfigurability offers many benefits, it also represents a significant new risk to communications and associated computing applications. For instance, radio software is subject to tampering that is often difficult to detect. As a result, radio software may not behave as advertised. Malicious or poorly designed radio software can render a radio inoperable, or degrade its performance. It can cause a radio to transmit in ways that interfere with other radios or that violate spectrum rights. It can also compromise the security of data and applications that the radio software can access.

The SDR Forum has established the SDR Security Working Group in its Technical Committee to identify and develop security requirements, architecture, and mechanisms that mitigate the risk of SDR, in particular the risk introduced by reconfigurability. The SDR Forum published High Level SDR Security Requirements (SDRF-06-A-0002-V0.00) in January 2006. Vendors and academics have referenced the high-level requirements in SDR-related work. The SDR Security Working Group is now developing Security Functional Requirements for a Software Reconfigurable Communications Device that extend the high-level requirements. The security functional requirements are expected to be approved by the SDR Forum in 2007.

The SDR Forum seeks to establish a security framework that pertains to all applications of SDR in all market segments. The framework must be highly flexible to account for differences in the various radio user communities. However, SDR demands a universal approach because once radios are reconfigurable, they can be reconfigured to support applications across existing market boundaries. For example, a SDR-capable mobile phone might be reconfigured to support public safety radio communications or vice versa. In this scenario, it is not appropriate to have different security models support each because either one might be circumvented by reconfiguring to the other. In the near term, most radios do not have the frequency agility to support multi-band reconfiguration, but these transactions are likely in the future. Moreover, the risk is very real for neighboring frequencies today.

The general outline of a universal approach is taking shape. It will involve digital signatures on radio code so that the code can be authenticated and its integrity protected. It will involve process separation to ensure that radio code does not compromise other applications and vice versa. Depending on the level of assurance required, process separation might involve separation kernels or it might be based on operational or network controls. The universal approach also specifies a run-time transmission filter for radios that transmit. The run-time filter helps prevent violations of spectrum access regulations. How such a filter would be technically implemented across differing radio hardware remains a challenge, but the more frequency agile and software reconfigurable a radio platform becomes, the greater the need for this control. Furthermore, the universal approach calls for radios to be "policy defined," meaning machine interpretable instructions will govern permitted radio behavior and how software is downloaded, stored, installed and instantiated.

The universal approach also borrows concepts from the discipline of trusted computing. For example, SDR devices will need integrity measurements and a secure boot process to ensure that the controls listed above are enforced at all times. Additionally, in an environment in which rapid reconfiguration is possible, network operators and individual radio users will want a level of assurance that the radios with which they are communicating have appropriate configurations; therefore, radios will need what is termed attestation to transmit that information. To introduce the SDR community to trusted computing concepts and their benefits to SDR, the SDR Forum convened a panel discussion on the topic at its 2006 Technical Conference.



From Wikipedia (http://en.wikipedia.org/wiki/Electromagnetic_spectrum)