INFORMATION ASSURANCE CONSIDERATIONS FOR LIGHTWEIGHT SOFTWARE DEFINED RADIOS AND SYSTEMS

Paul Philip (US Department of Defense,
Fort Meade, Maryland, USA, p.philip@radium.ncsc.mil);
Mark Buckner (Oak Ridge National Laboratory);
Michael Moore (Oak Ridge National Laboratory)

ABSTRACT

The paper will discuss Information Assurance (IA) issues, including security concerns and related countermeasures, for small form-factor Software Defined Radio (SDR) systems. The purpose is to highlight potential privacy and security vulnerabilities and to offer strategies for overcoming these to make the systems and component devices appropriately secure. An example Active RFID (aRFID) system is described that provides high granularity logistics tracking, monitoring, and geo-fencing capabilities in RFID-infrastructure-denied environments to meet the military services requirement for logistics visibility and control to "the last tactical mile." This paper emphasizes the need to design each component with multi-layer IA and quality assurance in mind so that vulnerabilities are addressed at the root level. This is important in light of the fact that nefarious groups start "attacking" the systems before they are even fielded.

1. INTRODUCTION

The purpose of this paper is to discuss primary issues in securing lightweight (small form-factor) SDRs at the device and system level. We will consider information assurance (IA) for an example system that utilizes SDRs as high capability RFID readers and data communications nodes (see Figure 1). The four primary IA concepts will be investigated, including authentication, integrity and confidentiality of data (in transit and at rest), and availability of the SDR-based devices and the system as a whole. In any over-the-air (OTA) system, standard network security issues are exacerbated due to the increased RF signal exposure. Hence, RF signaling and networking system level issues will be investigated as well as device security. SDRs offer a high level of capability and processing power to assure communications systems, however the flexibility in these platforms can create vulnerabilities that must be addressed.

In the aRFID system, tags are attached to items or containers for tagging, tracking, locating (TTL) and monitoring. Tags store identifying information and may manage input data from a number of connected sensors. The lightweight SDR nodes collect tag data, sensor data, control node-to-node communications, and provide a multi-point link to a larger SATCOM network infrastructure. Lightweight SDR systems, though lacking the power (and price tag) of a high-end system such as the Joint Tactical Radio System, are still capable of wireless and cell network interfacing, complex communications processing, and security functionality such as encryption and mutual authentication.

In assessing the level of IA needed for a system, there can be disagreement as to the criticality of the data based upon the frame of reference. In some commercial instances, the desire to keep piece-part and RFID system cost low may have driven some decisions that adversely affect security of systems and customer privacy. Examples include RFID-based security devices [1], RFID medical systems [2], contactless transit tokens [3], etc. For any electronic system, practical security must be defined as the security commensurate with the criticality of the data to be protected and service to be provided. An analysis of the consequences of data compromise, data alteration, system failure due to denial of service (DoS), and other breeches should be performed to apply the security features adequate to reduce the likelihood of the consequences to an acceptable level. The motivation and funding of expected attackers should also be assessed in the risk based development approach. In the US Transportation Worker Identification Credential (TWIC), strong security is applied to counter the threat of cloning and counterfeiting. During the House Homeland Security Committee hearing in October, 2007 (just before the first TWIC pilot program was rolled out for the port of Wilmington, Delaware) a number of committee members highlighted evidence that organized crime had been working to compromise the card for at least a year prior to the hearing [4]. The high levels of funding and motivation (illegal drug profits) of the attackers prompted the FIPS-201 security measures for the card and supporting infrastructure.

The American Bar Association provides thorough guidance of this type for assessing protections and expected diligence for managing security in public key infrastructures for electronic contract systems [5]. The National Security Agency (NSA) also provides algorithm guidance for various security functions (data encryption, hash, key establishment, key wrapping during key update, digital signature, transmission security, etc.) for systems based upon different levels of data classification [6]. The National Institute of

Standards and Technology (NIST) chip level [7] and system level [8] RFID security documents contain comprehensive countermeasures information. This guidance can be used to secure high value applications, such as contactless payment cards, access control badges, and identification credentials (e.g., passports and the aforementioned TWIC.) Here, with the greater payoff for compromise, one would expect attackers to apply greater resources. This threat would warrant the greater cost of applying strong countermeasures.

2. SOFTWARE DEFINED RADIO BASICS

The term "software radio" was coined by Mitola [9] in 1991 to designate "multiband multimode software-defined radios." In general, software radios and software designed radios include programmable digital signal processor cores such as microprocessors and Field Programmable Gate Arrays (FPGAs). The digital portions also include memory components, supervisory code, and A/D converters. By and large, the RF stages remain as discrete analog sections with only minimal programmability at this time. (While very high rate sampling at the antenna terminals is possible, this is not feasible for small form factor TTL and communication devices.) Common approaches to SDR involve storing a number of waveform processing components in memory which are loaded as needed into the DSP component in order to demodulate the waveform(s) being utilized at any given moment. For the application discussed in this paper, the waveforms include local links used for ad-hoc routing; longer-range SATCOM or terrestrial links for reachback; one or more aRFID waveforms; GPS processing; and sensor signal processing (e.g., chemical sensors.) Per Figure 1, the Cognitive Radio (CR), or SDR, nodes communicate among themselves using a lightweight ad-hoc routing protocol to determine which node has reachback capability. Various aRFID tags (e.g., WhereNet or Savi) and communication links are available for relaying both asset location and status. The CR nodes utilize GPS signals to determine location and receive command / control via commercial SATCOM links.

3. VULNERABILITIES AND COUNTERMEASURES

There are a number of potential vulnerabilities associated with the non-infrastructure aRFID system components and the wireless links over which these communicate. For each, key vulnerabilities associated with the four primary IA areas and countermeasures will be examined. At both the device and system level, data integrity is a key issue. Compromise of data integrity anywhere in a system can deny access, provide unauthorized access, obscure tag location, provide false or no data for network decision making, etc. Altering logistics inventory data can wreak havoc in any "just-in-time" supply scenario. Adversaries may also seek to alter databases to obtain access for a rogue SDR node using a counterfeit credential. The compromise of authentication,

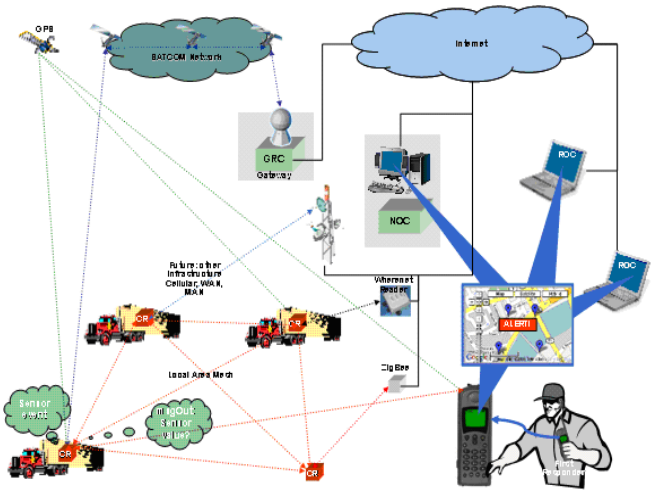

Figure 1 – Cognitive Radio Application for TTL

confidentiality, and availability poses similar risks. These will be discussed and countermeasures will be offered.

3.1. Development Process Security Issues

It should be noted that the process by which system components are developed is a potential source of vulnerability that is often overlooked or minimized. Poor hardware and/or software (including VHDL) development processes permit design and implementation errors to be introduced either maliciously or inadvertently. The bugs can cause unexpected vulnerabilities (per the Mifare card security implementation [3]) and weaken security (such as releasing data in the clear, weakening keys, or rendering challenge-response values non-random). These can also affect device operation, such as increasing the device radiated power (increasing signal exposure range), or causing a DoS. For wireless devices, the impact is exacerbated by the fact that weakened encrypted signals are available for RF reception. For cases in which a system is targeted in advance of fielding (e.g., by organized crime, nation-states, industrial spies, etc.) vulnerabilities can be introduced into the design for later exploitation. A strong development process, per the Carnegie-Mellon University Capabilities Maturity Model Integrated (CMMI), goes a long way in preempting this type of effort. For high-grade military systems, additional controls are typically needed, such as cleared personnel and secured development methods, tools and environments. CMMI-recommended practices, such as rigorous peer reviews and strong configuration management of system products and development tools, help to ensure that neither the products, nor the environment on which they are developed, are manipulated to effect a compromise. To illustrate, much SDR related software and VHDL code is auto-generated from design. It is important that the auto-generation tools are not compromised so that the generated code does not

include undesired "features" that weaken security. For secure military programs, it is recommended that high-assurance design practices are overlaid on CMMI behaviors. These may include the use of software analysis tools and formal methods to verify that the code performs exactly to specification (and nothing more) and conforms to assured coding guidelines. Formal code inspections for hardware and software (including VHDL) also help to ensure that products are implemented to specification and that bugs are detected. For classified systems, the NSA IA Directorate offers the IA Security Requirements Directive (IASRD) as a baseline to define, evaluate and track security requirements throughout the development life cycle.

4. DEVICE LEVEL SECURITY DISCUSSION

The aRFID system devices to be discussed here include the standard military UHF and microwave RFID tags and the SDR communications nodes. For the following discussion, eavesdropping is defined as the unauthorized reception of intelligible communications data. Skimming is the remote enabling of an RF-enabled device. These exposure-based attacks can compromise data and facilitate cloning and counterfeiting. Cloning is typically defined as creating a duplicate of an item in one's possession, or electronically obtaining sufficient information from device transactions to produce a copy. Electronic device counterfeiting can be thought of as the creation of a new, apparently valid device based on what is known about the device. For tags and SDR nodes in the aRFID system, copied devices are of concern as these can provide a vehicle to obtain network access and compromise security in a number of ways.

4.1. Tag and SDR Node Vulnerabilities

Low-end RFID tags have little processing capability to support security and so are inherently vulnerable. The SDR node is a lightweight platform capable of some advanced processing as described earlier. Primary risk areas for these aRFID devices are tamper, data alteration, reverse engineering and malicious software download. Tamper includes physical intrusion into the device as well as tag level masquerading. This can involve attaching a cloned device to a bogus item that is swapped for the valid item, or stealing the item and leaving the tag to be read as normal by the reader. Undetected, non-penalized tamper in the SDR node can result in an adversary obtaining critical security data (such as system and private key material).

Data alteration can be done by tampering, or by maliciously changing the device data in transit. Adulterated SDR data can garble logistics and sensor data, network metrics data on which routing decisions are made, waveforms for internal FPGAs, etc. This can have a severe impact on device and system operation.

Reverse engineering can be done in-system (eavesdropping and skimming) as well on the benchtop via hardware reverse engineering (HRE) and Side Channel Analysis (SCA). Low-end military tags are susceptible to in-system attack due to a lack of authentication and data encryption. The stored license plate data provides no useful information about the asset; however the transmitted data can be used to track a container once it is linked to the unique tag code. Tag characteristic data (such as the tag serial number, protocol number and item identification number for EPC Gen2 tags) also may facilitate cloning the tag. Eavesdropping can also be performed on SDR nodes to obtain any data transmitted in the clear. HRE is typically done to obtain information about cryptography in a device. This attack involves the removal of layers of silicon to reveal gate level circuit components and routing that define the design. For the low-end tags the characteristic data can be reverse engineered for potential tag cloning. HRE is also a threat to the SDR nodes since cryptographic and trade secret design data may be exposed.

SCA involves benchtop analysis of a device to gain insight into internal cryptographic operations. Typical attack methodologies include differential power analysis (DPA), electromagnetic (EM) analysis, timing analysis (hardware and software execution), fault injection, and signal glitching. RF DPA is a variant that can be performed remotely. Here, Oren and Shamir determined that low level perturbations on the tag return RF can betray the internal cryptographic processing [10]. Information obtained by HRE and SCA can be used to copy devices and obtain stored security data such as keys, algorithms and certificates. This type of work is discussed by Nohl, et al, in the HRE of the Mifare chip [3]. The chip level security guide published by NIST has detailed discussion of these attack methodologies [7].

A serious vulnerability unique to SDR-based devices relates to the OTA software update capability. This can be a vehicle for malicious code (malcode) insertion. In addition to changing stored data, this type of attack can alter SDR performance by altering critical operational parameters, changing cognitive decision making algorithms, and compromising FPGA reconfiguration commands.

4.2. Tag and SDR Node Countermeasures

Device level countermeasures include defenses against tamper, data corruption, reverse engineering, and malicious software uploads. Anti-tamper design includes tamper detection functionality as well as tamper indicators. Tamper should be signaled to the system if an attempt is made to detach the device, or to penetrate the device container. If tamper is detected, all sensitive data must be erased and, if possible, the circuitry rendered permanently disabled. This method effectively penalizes the attacker.

Integrity verification is a key assurance measure. SDR critical data (such as sensor, keys, algorithms, operational

data, and FPGA configuration code) should be verified before each use, after each processing step, and periodically while at rest- as much as the SDR processing bandwidth will support. Eavesdropping can be countered by encryption and via the RF methods addressed subsequently. Skimming can be remedied by mutual authentication to ensure that only valid devices can communicate within the aRFID network.

In defense against HRE and SCA, strong anti-tamper will make it difficult for adversary to obtain access to the internal circuitry without destroying some/all of the desired data. Anti-HRE design includes the encryption of SDR critical data and distributing it over physical memory. Obfuscating the circuit layout on silicon is another effective practice. Anti-SCA seeks to balance all operational characteristics so that nothing is revealed about the cryptographic processing. This includes balancing current over time and software execution (DPA), signal routing (EM analysis), execution timing (timing analysis), and decoupling SDR power from crypto processing (RF DPA). Performing all of these countermeasures in unison is difficult.

To secure the SDR software OTA update operation, it is necessary to utilize the inherent processing power afforded by even a lightweight device. OTA transactions must be authenticated. A Kerberos Version 5 Process can be utilized for software download security (per Singh, et al [11]). Software (including configuration code, key material, algorithms) must be digitally signed and encrypted to assure the operation and cover classified code and/or trade secrets. Kerberos can be used for unclassified data, NSA Suite B for both unclassified and classified national security systems, and Suite A for high-security non-releasable data [6]. It is advisable that on-the-fly reconfiguration also be secured. Pursuant to this, critical internal commands should be authenticated to ensure that only valid, expected operations take place (e.g., FPGA reprogramming).

Audit is another important countermeasure to capture forensic data and to log device software changes and decision-making. An audit log can be used to track critical data such as cognitive radio decisions, security test results, security events, Public Key Infrastructure (PKI) certificate pedigree, software version pedigree, and even attack profiles. This file should be protected as critical SDR data with authenticated access at device level, encryption and distribution about memory. The log can be periodically relayed to the Network Operational Controller in the aRFID for background security and operational analysis.

5. RADIO FREQUENCY LINK ISSUES

The aRFID RF links to be discussed include the RFID tag-to-SDR communications node and the SDR node-to-SDR node. The node-to-node wireless networks have issues typically associated with RF communications as well as those associated with networks. Vulnerabilities and countermeasures will be examined in the RF realm and then in relation to wireless networks. There has been much written about network vulnerabilities and countermeasures during the internet years. This paper will address a few of the more important network areas for the aRFID system.

5.1. Radio Frequency Vulnerabilities

Air gap issues are important to the overall risk scenario for the aRFID system. In some cases, modifications applied to the RF characteristics of the system can help to minimize network related vulnerabilities. The OTA communication in RFID and SDR systems provides an adversary with inherent access that wired systems do not afford. Access to the signaling enables the eavesdropping activity necessary to perform network based attacks such as traffic analysis, Man-in-the-Middle, and spamming. Increasing the effective transmission range of the devices in the system, as an adversary might do with high-gain antennas and high-sensitivity receivers, makes eavesdropping and skimming easier. Eavesdropping and skimming can reveal information such as the location and quantity of RFID tagged containers and possibly the type of equipment or supplies tagged. This can lead to operational security issues. Jamming is another RF vulnerability that can pose a major DoS threat. Geo-location is yet another RF security issue. If the SDR nodes employ non-short burst signaling, radio direction finding equipment can potentially locate emitters. This can be combined with metadata from transmissions (such as quantity and characteristics of transmissions from individual devices) to help adversary can locate specific devices, such as controllers, within a network.

5.2. Radio Frequency Countermeasures

A basic premise in RF countermeasures is to minimize the exposure of system signaling. This impedes eavesdropping, skimming, and all associated vulnerabilities. Limiting the playing field can be done by encrypting the traffic, covering the signals via transmission security (TRANSEC) techniques, and by bounding signal propagation. To limit transmission range one can take advantage of the laws of physics, at least within the atmosphere, and utilize the Oxygen absorption frequency band. The University of California at Berkeley has developed systems to operate in this spectrum [12]. This band (56-64 GHz, 7 GHz of which is open in the US) is inherently short-range due to the absorption of the RF energy by oxygen molecules in the atmosphere. This is a natural anti-eavesdropping and anti-jam method since an adversary must be very close to receive the signal. For the aRFID, directional repeaters can be used to overcome the limited range to effect the mesh network topology. The SDRs can also limit range through the use of antenna beamforming. Here highly directional antennas can focus energy in a narrow beam to the receivers. Another method of limiting the emanations is to enclose the system in

a Faraday enclosure. This is most realizable for the node-to-tag communications, particularly if the SDR node and tag group are located within a trailer or large shipping container. Here the tag signals will not radiate beyond, and jamming signals cannot penetrate through, the anechoic boundary.

The cognitive radio capability in SDRs is ideal for adapting to a jamming scenario through the use of on-the-fly varying waveforms. Cognitive capability permits SDRs to sense the environment and respond with adaptive anti-jam, Low Probability of Interception (LPI), and Low Probability of Detection (LPD) communications. LPI/LPD serves to hide the communications from an eavesdropper using a variety of methods, including band-spreading the energy or blending into the ambient emission spectrum. This hides the fact that a transmission is taking place. For classified systems, there is a number of NSA recommended TRANSEC algorithms [6]. TRANSEC is an effective countermeasure for all RF vulnerabilities as it greatly reduces or removes the exposure problem. Anti-jam methodology includes but is not limited to LPI/LPD. Anti-jam can include brute force methods such as "burn-through" using very high power, or detecting and disabling the jammer. Adaptive antenna beam control can also counter jamming. The aRFID ad hoc self-healing mesh is also useful to evade jamming by routing signals through an area of the mesh that is not affected. Self-healing networks can work around other problems such as communications node failure.

5.3. Wireless Network Vulnerabilities

Radio frequency network issues are similar to wired systems; however wireless medium provides adversaries with easy access unless the previously discussed steps are taken. This section will examine a few more compelling issues specific to the security of the aRFID network.

Network vulnerabilities are related to masquerading, DoS, and traffic analysis. In an aRFID system, an adversary may seek to gain access to network devices as a rogue tag or SDR communications node. Low end tags possess only a very small amount of storage with which to generate a malicious command set, and rudimentary data checking can stop this exploitation. The complexity of SDR signaling can afford an attacker a greater ability to spoof the system, and potentially to inject malcode, acquire system data or become a man-in-the-middle. Another potential masquerade is session highjacking, where a rogue SDR can listen in to the network traffic and, at an opportune time, assert itself to replace a valid node. This denies service to the valid node and can allow the rogue to access or disrupt system assets. Network device spamming is another spoofing method which can deny service. An intruder can busy a node with meaningless exchanges so that it cannot operate as required. Many tools are available to engineer this type of attack (e.g., sending de-authentication or disassociation packets to force the client to attempt to reconnect. For a battery powered device (see Defend, et al [2]) such as the aRFID SDR node, this process can also exhaust the battery to bring about a more permanent DoS.

Traffic analysis involves the analysis of characteristics of network digital transmissions (e.g., transmit timing, header data, traffic volume, packet/frame length, timing, and duration) to obtain information about the network and/or data transmitted. The metadata can supply an attacker with information sufficient to deduce encrypted data. For an aRFID system, data throughput of a SDR node can reveal the quantity of tags associated with a particular node, perhaps types of tagged units. For example, if data packet size equals 96-bits (the payload of an EPC Gen2 tag) for each RFID tag read in a polling session, and tag data values are concatenated to form a network payload, the packet length will reveal the number of tags in the SDR read zone. Nodes may also be identifiable based on the fingerprint of their routine transmissions. Within the packet transmissions, the header data, protocol indicators, and command/control messages are often discernable even if the payload is encrypted. With node-unique identifying data in header and the signal origin detectable by direction finding, individual nodes may be located. Defend, et al, describe a similar scenario for an RFID-based medical telemetry system [2].

5.4. Wireless Network Countermeasures

Network security recommendations include countermeasures for masquerading, DoS and traffic analysis. Strong mutual authentication will force devices to provide valid credentials prior to receiving access. This will protect the network from spoofing, man-in-the-middle, active traffic analysis, session highjacking and device spamming DoS attacks. Encryption can be used to supplement authentication. This serves to hide data that can be used to gain unauthorized entry to the system. Additionally, integrity checks on network data can detect suspicious behavior. Verifying received data can detect data alteration in transit. Checking at each protocol layer can ensure that no header and control data is unexpectedly altered. Defense against spoofing attacks is particularly important for network configuration commands and SDR software uploads. As previously discussed, methods involving Kerberos and NSA recommended authentication algorithms can protect these operations. The SDR nodes can also support RF firewall operations to perform access control and authentication.

On a larger scale, the use of wireless intrusion detection systems (WIDS) and wireless intrusion prevention systems (WIPS) is advisable if this can be supported by the network devices. These control access to the wireless network and are designed to detect the types of behavior typical of masquerading attacks. A WIDS will detect signatures of tools used for fake messaging. There is also potential for network defense devices to check SDR audit logs to learn attack profiles and guide network defense measures. Firewalls, WIDS and WIPS also make traffic

analysis significantly more difficult. Traffic analysis can be countermeasured by removing any unique details of the metadata. This involves balancing packet (timing, length, header data) as well as RF characteristics (transmission duration, frequency, spacing of packets and frames, etc.) to deny an adversary information about the transmitted data. Fixed packet characteristics will likely necessitate padding at the frame and packet level. Padding patterns should be chosen to be non-indicative so that an attacker is unaware of the pad. Network timing must also be controlled such that packet transmit frequency, timing and spacing are equal for all operations, i.e., fixed transmission lengths, fixed frequency spectrum of transmission (unless LPI/LPD is used); and fixed header/packet sizes for all types of transmissions (data, command, control, etc.). Finally, the communications protocol should not betray the type of signaling so as not to highlight specific packet types.

6. INFORMATION ASSURANCE SUMMARY

For the aRFID and similar systems, it is important to note that the radio frequency links increase the system exposure and therefore the risk of attack. Unlike wired systems, there is no innate control over the transmission medium. Attacks can be carried out remotely, passively, and are difficult, if not impossible, to detect. To determine the assurance level needed for the system, the level of security must be related to the data sensitivity, the risk to the system and the cost of compromise to the system owner/user. This should be done through an informed risk-benefit-cost analysis enlisting information system security engineering expertise. The countermeasures detailed herein should be implemented as determined by the analysis. Multiple layers of countermeasures should be considered as these raise the level of difficulty (and cost) to an adversary of penetrating the network and/or the associated devices. For high-security military developments, the NSA Information Assurance Directorate should be consulted for security engineering guidance and the IASRD should be utilized.

Some key areas of focus for information assurance for the aRFID system include:

- A secure, controlled development process is critical to minimizing the threat of unintentional and intentional defects in the product that can compromise system and device security.
- Data integrity should be verified within devices and at each network access point – especially application software in devices and system data on which network routing decisions are made.
- Mutual authentication should be utilized to assure access to the network, communications between devices, and importantly, to protect the SDR software uploading process- a key area of vulnerability. Authentication can also be used to control access to internal device critical operations (such as reprogramming SDR FPGAs).
- Assure device-level security with anti-reverse engineering, anti-side channel, and anti-tamper design.
- A secured audit log should be used for each SDR to retain critical device configuration, operational and software pedigree information.
- RF signaling should be covered using TRANSEC and adaptive techniques (such as beamforming, band spreading and self-healing mesh architecture). Limiting the signal range reduces the system exposure profile.
- Protect network communications from analysis using secure wireless solutions that include metadata and network timing obfuscation techniques and encryption.

The processing power inherent in SDRs can be a significant advantage in applying system and device level countermeasures.

7. REFERENCES

[1] S. Bono, M. Green, A. Stubblefield, A. Juels, A. Rubin, and M. Szydlo. “Security Analysis of a Cryptographically-Enabled RFID Device”. Proceedings of the 14th USENIX Security Symposium, USENIX, Baltimore, MD, USA, 2005.

[2] B. Defend, M. Salajegheh, K. Fu, and S. Inoue. Protecting Global Medical Telemetry Infrastructure, 2008.

[3] K. Nohl, D. Evans, Starbug, and H. Plotz. “Reverse-Engineering a Cryptographic RFID Tag”. Proceedings of the 17th USENIX Security Symposium, USENIX, San Jose, CA, USA, 2008

[4] Website: http://homeland.house.gov/hearings/index.asp?ID=98, US House of Representatives, Committee on Homeland Security, “Homeland Security Failures: TWIC Examined”, October 31, 2007.

[5] American Bar Association, Information Security Committee, Electronic Commerce Division, Section of Science and Technology Law. PKI Assessment Guidelines, PAG v0.30, Public Draft for Comment, 2001.

[6] Website: http://www.nsa.gov/ia/programs/suiteb cryptography/index.shtml, National Security Agency, NSA Suite B Cryptography, January 15, 2009.

[7] National Institute of Standards and Technology, Chip-Level Security for RFID Smart Cards and Tags. Boulder, 2008

[8] National Institute of Standards and Technology, Computer Security Division, Guidelines for Securing Radio Frequency Identification (RFID) Systems. Gaithersburg, 2007

[9] Mitola, Joseph, “Software Radio—Cognitive Radio: Wireless Architectures for the 21st Century,” found at http://ourworld.compuserve.com/homepages/jmitola/ (copyright Mitola’s Statisfaction. All rights reserved. Used by permission for educational purposes).

[10] Y. Oren and A. Shamir. Power Analysis of RFID Tags, 2006.

[11] Ankita Taneja, Ved. P. Mishra, Ajay Kr. Singh, G. Singh and S. P. Ghrera. “Security Architecture For SDR System Using OTA Download Sequence”. Proceedings of the SDR ’08 Technical Conference and Product Exposition, SDR Forum, Washington, DC, USA 2008.

[12] Website: http://bwrc.eecs.berkeley.edu/Research/RF/ogre project, University of California at Berkeley, 60-GHz CMOS Radio Systems Project