Trigger point

Jim Giermanski of Powers International argues that the Department of Homeland Security needs to rethink its support for RFID technology

Dr Jim Giermanski is the Professor of International Business and Director of the Centre for Global Commerce at Belmont Abbey College.
He is also Chairman of the Board of Powers International Inc., an international transportation security company.

Contact:
Jim Giermanski
Powers International Inc.
Email: powersintnlinc@bellsouth.net

There comes a time when one's conscience and sense of right and wrong compel one to speak, especially if speaking may impact the common good in a positive manner. However, often and especially in this case, speaking out can also carry potential negative consequences. On the one hand, the following commentary will expose a serious vulnerability at US seaports and land ports-of-entry in the hope that the **Department of Homeland Security** (**DHS**) will understand the potential consequences of the vulnerability and the cost of not addressing it. On the other hand, speaking out carries the risk of identifying a vulnerability that terrorists have not considered, although that is unlikely considering their skill in improvised explosive device (IED) usage. The dilemma is this: speak out to prompt the DHS to acknowledge its seriousness and defeat the vulnerability; or say nothing, and let a terrorist attack take out a significant US port with relative ease. I have decided to speak out.

Context of concern

Powers International, an international transportation security company, developed a container security system in 2002 (see *Cargo Security International*, February/March 2006, page 40). It obtained a patent on its system in 2006 which has now been issued in 37 countries. Initially, the company believed that radio frequency identification (RFID) technology approved by the **Federal Communications Commission** (**FCC**) for use with shipping containers should be considered for incorporation into Powers International's satellite-based system.

Vulnerability as an IED trigger

Recently, however, concerns about RFID usage in seaports and land ports have developed. Engineers at Powers International now believe that RFID usage, as approved for use in the United States, is a serious vulnerability because of the ease of detecting these RFID emissions. RFID emissions can serve as the trigger-mechanism for detonating an explosive device within the container. Because an explosive device can be easily wired to detonate with the proper RFID frequency signal, all US ports that employ the approved RFID frequency for shipping containers become more vulnerable to terrorist attack.

A review of the literature seemed to confirm what was suspected. There were conflicting claims and the process of selecting a frequency for container security was contentious. Ultimately, a decision was made by the FCC to set aside a frequency of 433.5 to 434.5 MHz spectrum band, and their rule would allow these RFID systems to transmit for 60 seconds, rather than only 1 second. Against objections, especially those of the amateur radio sector, the spectrum and transmission time were approved by the FCC for use with shipping containers and in commercial and industrial areas.

As a result, the US government mandated and published the specific frequency for RFID use with shipping containers. The fact that only approved and published RFID signals are required to be transmitted on a given frequency at US ports by both the private and public sectors, in effect, makes government policy usable as an instrument of terrorists tactics. The need for surreptitious port penetrations, elaborate electronics, intricate timing, or other specialised terrorist tradecraft or operations in the United States becomes diminished, if not eliminated. The US private sector and government agencies, such as the **Customs and Border Protection** (**CBP**), and the **Department of Defense** (**DoD**), can themselves, through routine and normal procedures, detonate those explosive devices carried in containers entering our ports.

Decision to test

To test the validity of its concerns, Powers International constructed controller boards to serve as relays or detonators using off-the-shelf, over-

the-counter products. Using these detonators, Powers International simulated multiple explosions at varying distances using the frequency required by the US government. Further work on this vulnerability revealed that signals emitted to detonate explosive devices could be made at significant distances from locations even outside the port facilities with the use of high-gain antennas. However, since Powers International had not used an actual RFID tag to verify its concerns nor actually detonated explosives in this manner, the company approached experts in the area of IEDs and relevant government agencies to examine these concerns. These included municipal bomb squads, and engineers with blast contracts with the DHS, the DoD and the CBP. All but the DoD, DHS, and CBP initially responded and concurred with Powers International's assessment that RFID usage as approved for containers in US ports appears to be dangerous. Powers International also contacted members of the **US House Homeland Security Committee** to inform them of our concerns and to be on record of doing so.

Blast demonstration

In order to expose this vulnerability in an irrefutable fashion and transparent format, Powers International and **Raytheon Homeland Security Division**, with the cooperation of **Zapata Engineering**, the **University of North Carolina at Charlotte College of Engineering**, the **City of Gastonia Bomb Squad**, and the **321 Equipment Co.**, ran a demonstration on 13 November 2007. The demonstration showed how an actual RFID tag could send a signal to a receiving circuit (detonator) prepared from over-the-counter components. The detonator was made by an undergraduate college student for a cost of approximately $20. The RFID signal detonated a very small amount of live explosives in a container by means of a simple emission of a radio signal traveling on the approved RFID frequency. The demonstration was 'brand agnostic'. At no time during the demonstration was any port, political subdivision, manufacturer, distributor, or user of RFID for container security promoted or criticised for its use.

Government interest and support

Because of the serious and potentially controversial nature of this demonstration, many government officials and personnel of the US Administration were invited, including the DoD. Due to its interest in and extensive use of RFID, the DoD sent two people, the chief engineer of an RFID DoD programme and his supervisor. So, representatives from the US Army were among the attendees at the 13 November event. They observed the preparation and demonstration of an RF-detection and triggering device utilised to detonate explosives in a shipping container at the City of Gastonia Ordinance Range. Subsequently, the US Army confirmed in writing that its representatives examined the device and wiring and validated that a commercial RFID interrogator was used to 'wake up' a commercial RFID tag. When the RFID tag responded on the 433 MHz frequency, the relay closed and the blasting cap set off the explosive charge. Thus, the DoD representatives recognised and confirmed the validity of Powers International's concern over the routine RFID use, its vulnerable nature, and the accuracy and relevance of the demonstration to homeland security. In the DoD's own words, the 'US Army representatives examined the device and wiring and confirm that a commercial RFID interrogator was use to "wake up" a commercial RFID tag. When the RFID tag responded on the 433 MHz frequency, the relay closed and the blasting cap set off the explosive charge.' Other witnesses were invited to attend and verify the process used at, and the results obtained from, the demonstration. The demonstration was filmed and is available for review. The demonstration was 100% successful, and it showed empirically the vulnerability of RFID transmissions as approved for use with containers passing through international ports-of-entry.

Governmental responses

Unfortunately, Powers International met resistance from both the DHS and the CBP, who refused to attend or to indicate any recognition of the demonstration's value, even though both had local offices and personnel within 20 minutes of the demonstration site. The CBP actually attempted to put obstacles in the path of the demonstration by not allowing its transceiver or activators to be used at the demonstration, even by their own personnel. Ten major US ports and the **American Association of Port Authorities** (**AAPA**) were also invited. None of these entities responded or attended. The **US Coast Guard** (**USCG**) refused to attend. The **Government Accountability Office** (**GAO**) was invited but did not respond to the invitation nor attend. A total of approximately 50 invitations were sent with marginal results. Finally, invitations were made to some members of **US Congress** in those states which have seaports. Only one staff member of one US Congressional representative attended. There were, however, follow-up calls made by a southern border Congressman, personally indicating an interest in and an acknowledgement of the importance of the demonstration.

Conclusion and recommendation

First, this demonstration proved beyond doubt that RFID usage can become a trigger of container IEDs in our ports. Second, this demonstration produced agreement among those present that because this vulnerability is real, it must be recognised by those government entities whose mission it is to protect the United States. Pointing out the vulnerability was relatively easy. Fixing it may be more difficult.

Nevertheless, this vulnerability is proven, and must be addressed without delay. In light of the potential impact on the US economy of closing one or more US seaports or land ports-of-entry and the cost of human life at and around

those ports, it seems imperative that cooperative steps be taken by both the public and private sector to remove or minimise this recognised, demonstrable vulnerability and potential threat to the United States.

In January 2008, two months after the demonstration, the DHS made an official statement regarding it. It is self-explanatory and represents the thinking and management posture of the DHS:

'DHS recognises and benefits from the use of RFID technology to ensure the smooth and secure movement of both people and cargo into the United States. It is accurate that RFID systems are in use at US ports of entry (air, sea and land) and have been adopted by a number of private-sector companies for supply chain management, asset and shipment tracking and inventory purposes. While RFID systems used in maritime ports rely upon a variety of transmission frequencies for port and terminals operations, there is currently no one common RFID frequency in use throughout the global supply chain.

'While it is technically feasible that the detection of RFID emissions could be used to trigger an explosive device within a container, DHS does not agree with the report's assessment that ports that employ RFID technology become more vulnerable to terrorist attack.'

The DHS admits in writing that using this frequency to trigger an explosive device is technically feasible (capable of being carried out) but we shouldn't worry about it. The logic is indicative of the DHS. It seems that DHS is saying: 'We know this can happen, but let's wait until it happens.'

'The demonstration was 100% successful, and it showed empirically the vulnerability of RFID transmissions as approved for use with containers passing through international ports-of-entry'