

RFID Passport Shield Failure Demonstration: FLX[2006-0605] Video Security Brief

Abstract: The FLX[2006-0605] video security brief demonstrates a real-world vulnerability associated with the failure of the shielding component in the current proposed electronic passport design. When partially open, as could be the case when in a pocket, purse, or briefcase, the currently proposed passport can be detected by a nearby inquiring RFID reader. The security brief also demonstrates an improved shield design that requires a passport to be significantly open before reading is possible.

Demonstration Description: While being tested, both the current proposed passport and the improved passport prototypes are attached to a dummy at waist level where each is fixed open at ½ inch, simulating an accidental opening in a pocket, purse, or briefcase. Each passport prototype is then passed by a trash can containing RFID-reading hardware that will detonate a small charge when it detects a passport's tag in proximity. The current proposed design caused the charge to detonate, indicating that it had been detected by the reader, while the improved shield design did not cause a detonation.

Equipment: The modified trash can used as an RFID detection device contains a loop antenna on its inside-front wall which is driven by RFID reading hardware contained in a protective housing. The RFID-reading hardware interfaces a detonation system that controls a small charge mounted atop the can such that when an RFID tag is detected, the charge will be detonated.

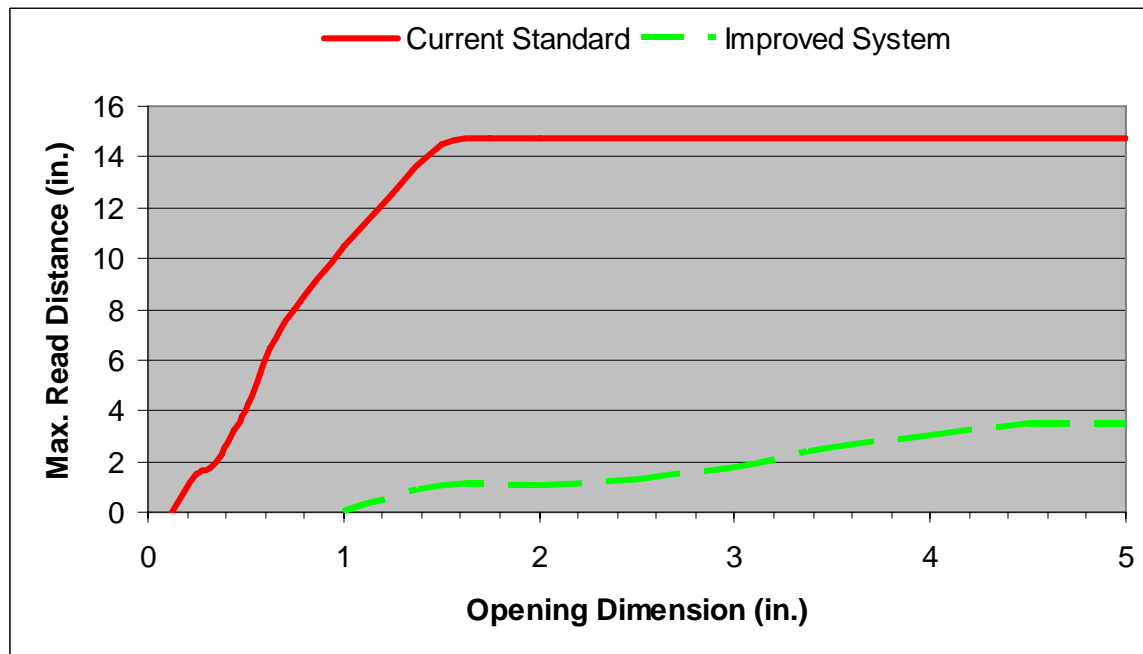
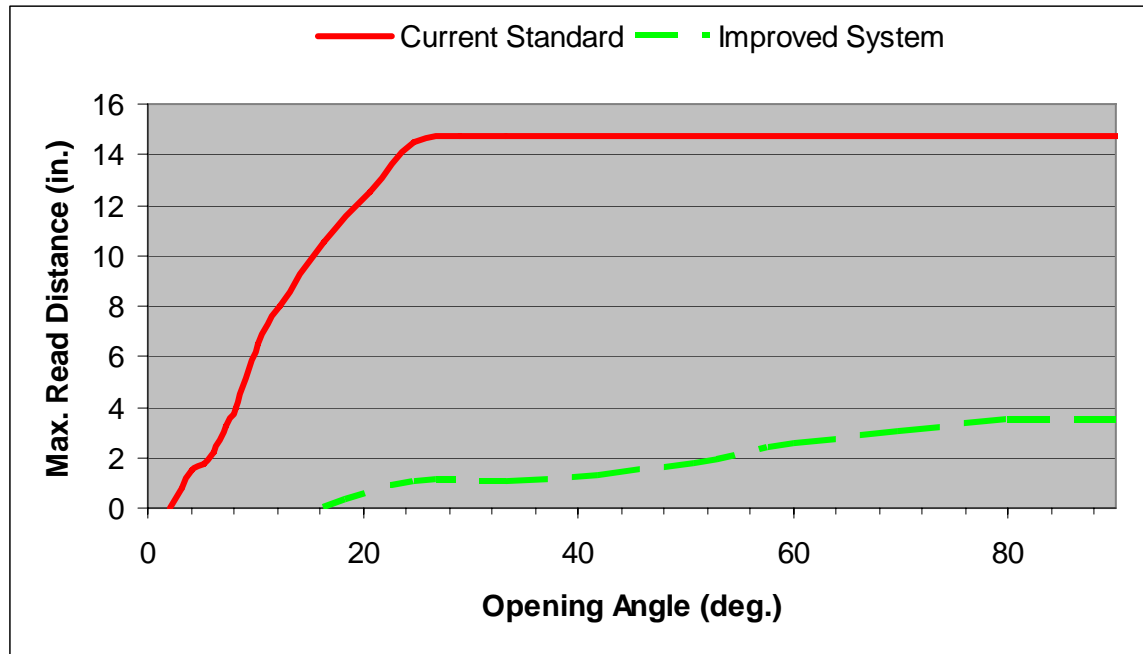
The RFID-reading hardware tests for the presence of any 13.56 MHz tag in its field. The tags being used do not contain Basic Access Control (BAC) functionality: thus, data disclosure is not being tested in this demonstration. When present in a reading field, a passport RFID tag will wirelessly draw power from the reader in order to operate. The change in antenna current is detectable by the RFID-reading hardware; therefore, even if a tag is not directly sending data, it intrinsically discloses its proximity to the reader by its presence in the reading field.

Both passports under test are prototypes constructed using copper mesh (100 wire/inch) as the shielding component to allow flexibility and simulate proper functionality of a production shielding inlay. The current proposed design prototype contains mesh on the front cover with the RFID tag positioned in the center of the rear cover. The improved passport design prototype contains mesh on both the front and rear cover with the uni-directional tag read inlay¹ positioned in the center of the inside rear cover.

Lab Data: This demonstration relies on results from research conducted in the Flexilis lab regarding the readability of an electronic passport's RFID tag with respect to its opening

¹ See Technical Analysis document for specifications of the uni-directional tag read inlay

dimension and distance from the reading antenna.² Using a medium-power RFID interrogator, the distance from the reading antenna's plane to the center of the tag's antenna was measured where the passport prototype was positioned at its optimal orientation with respect to the reader's antenna. Both calculated angle of opening and measured dimension of opening are shown for the dataset. Opening angle (dimension) measurements are accurate to +/- 2 degrees (1/8 inch).



² It is important to note that any read distances pertaining to RFID tags are affected by many factors including the power of the reader, the noise level of the environment, and tag antenna detuning.

Results: When the current proposed passport prototype passed the trash can the charge detonated, indicating that the shielding system had failed and, therefore, the partially open passport was detected. When the improved passport prototype passed the trash can, its shielding system remained operational and no detonation occurred even though the booklet was partially open.

It is possible that criminal or terrorist organizations could develop a device similar to the one used in this demonstration that is both self-contained and significantly reduced in size.

From lab tests using medium-power RFID hardware, a passport using the current proposed shielding design is readable from at least an inch away while only open ¼ inch. As a passport is repeatedly used, the natural opening of the booklet increases, thereby allowing RFID reading from a significant distance. The results of this demonstration suggest that the current proposed passport design contains critical security vulnerabilities and should be re-evaluated before deployment.

Pre-Production Improvements: The lesser maximum read range for a passport using the improved system is caused by parasitic capacitance affecting the tuning of the RFID transponder's inductor. In a production environment, the maximum read range will approach that of the current proposed design with the added benefit of a much greater minimum angle of opening required for tag readability. Additionally, multiple material formulations for the uni-directional tag read inlay need to be tested to find the optimum combination of cost, bulk, magnetic permeability, and resistivity.

Once such parameters are optimized, the improved shielding system will provide much better security in a cost-effective, user transparent manner.