NATIONAL SAFE SKIES ALLIANCE

Program for Applied Research in Airport Security

PARAS 0017 Project Summary

Project Title:	Access Control Card Technology Guidance		
Program Officer:	Jessica Grizzle	865-738-2080	Jessica.Grizzle@sskies.org
Research Agency:	TranSecure, Inc.		
Principal Investigator:	Art Kosatka		
Effective Date:	May 25, 2018		
Contract Time:	12 Months		
Funds:	$147,468		

BACKGROUND

A number of card technologies are available for access control, including magnetic stripe, proximity, memory, smart/Commercial Identity Verification, and multi-technology cards. Many airports use legacy access control cards with varying degrees of inherent security and functionality, which often expand over the years. To address these changes, airports are considering upgrading their access control card technology to achieve enhanced levels of security and functionality.

The Transportation Security Administration (TSA) identified a specific security concern regarding RFID proximity identification media, involving the duplication of cards. TSA recommended that airport operators examine access control card technology in use at their airports to determine if vulnerabilities exist and explore implementing technologies that provide higher levels of security/encryption.

Airports do not have current, authoritative, easy-to-use, and comprehensive guidance to assist in understanding the various access control technologies, associated costs, and mitigation/migration strategies. While some information is available publicly, it is insufficient for effective decision-making. Detailed guidance is needed to aid airports in assessing access control technologies.

OBJECTIVE

The objective of this research is to develop guidance for airports of various sizes to understand access control card technologies, limitations, and vulnerabilities, as well as to plan for upgrades and expansion of their current technologies. At a minimum, the guidance should include:

- Detailed descriptions of underlying technologies
- Security vulnerabilities of each technology and its mitigation strategies, including interim measures
- Installation considerations to maximize security
- Identification of potential pitfalls during implementation
- Encryption options for the card, reader, and access control system
- Data storage possibilities and limitations related to personally identifiable information and certificates
- Physical card considerations and limitations, such as printing capabilities, badge sleeves/holders, potential interference between multiple cards, and read range
- Technology migration planning considerations and lifecycle costs

- Overview of future technology trends

The document produced will address security vulnerabilities of various technologies and may need to be considered Sensitive Security Information.