A Systematic Process for Vulnerability Assessment of Biometric Systems at Borders

B. Cukic, E. Marasco, A. Bagavathi, S. Krishnan, M. Shehab

Problem Statement

Biometric identification is a critically important technology in traveler, immigration and refugee management. This role makes biometrics the prime target for identity theft, spoofing and vulnerability exploitation.

Project beneficiaries and end users

Biometric Technology Rallies - system evaluators; CBP risk analysts;

GAINS desired

- Connect human factors motivating travelers, immigrants and refugees to identity concealment efforts;
- Understand and quantify misidentification and concealment risks.

PAINS at present

- Attack vectors or comprehensive processes to mitigate ID risks lacking.

Project products & services

- Created the methodology for classifying identity attack vectors for biometric systems in Homeland Security Enterprise.
- Developed software tool for risk inference from specific ID attack vectors.

GAINS created

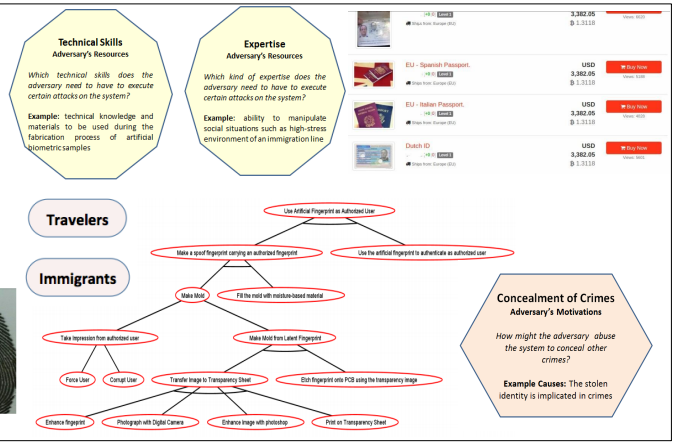
- Developed eight biometric identity fraud scenarios (attack vectors)
  - Include motivation factors and perpetrator's capabilities.
  - All vectors come from publicly available stories and interviews.
- Security risks related to transnational flows of people cannot be studied in stovepipes (biometric spoofs, motivation, expertise, passport fraud).
  - Need coordination and integration of concerns.

PAINS alleviated

- Identification of common biometric attack vectors.

STORY:

A South Korean woman who had been blocked from entering Japan apparently slipped past the screening system by placing special tape over her fingerprints. The silicon covering foiled the scanning device and didn't alert officials that she had been deported in 2007 for overstaying and was barred from re-entry for five years. Immigration officials later found her inside the country. She had succeeded passing the biometric identity check at the airport.



Key Accomplishments:

- Surveyed biometric system vulnerabilities and past exploitation attempts.
- Created a methodology to enable the analysis of misidentification threats
  - Motivation, resources and methods.
- Developed attack trees to quantify risks of specific attack vectors.
  - Traveler, immigrant and refugee management scenarios.
- Found preliminary evidence of ID attack support from Dark Web

Next Steps:

- Improving risk analysis by examining the support for identity attack vectors on Dark Web markets.
- Reorganization of attack vectors – separating motivation, resources and methods to improve flexibility.

UNC CHARLOTTE

This material is based upon work supported by the U.S. Department of Homeland Security under Grant Award Number 2015-ST-061-BSH001. This grant is awarded to the Borders, Trade, and Immigration (BTI) Institute: A DHS Center of Excellence led by the University of Houston, and includes support for the project "A Systematic Process for Vulnerability Assessment of Biometric Systems at Borders" awarded to the University of North Carolina at Charlotte. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

BTI Institute
Borders • Trade • Immigration
A Department of Homeland Security Center of Excellence