A Systematic Process for Vulnerability Assessment of Biometric Systems at Borders

2017 BTI Performers' Meeting and Showcase

Washington, DC, December 4th 2017

UNC CHARLOTTE

BTI Institute

Project Team Profile

- PI(s) Name(s), University: Bojan Cukic, University of North Carolina at Charlotte
- Project Start Date: July 1, 2016
- Anticipated End Date: June 30, 2020
- Project personnel:
  - Emanuela Marasco; Senior Personnel
  - Mohammed Shehab, Siddarth Krishnan; Senior Personnel
  - Arunkumar Bagavathi, Pegah Karimi, Usman Rauf, Weitong Yin; Student Researchers

Problem Statement

- Biometrics and Identity management are critical technologies ensuring the integrity of immigration services.
  - Also a natural target for identity manipulation.
  - Threats to DHS systems have dimensions not accounted for in generic “liveness detection”.
  - *Attacks related to:*
    - *Presentation*.
    - *Workflow*

Hong Kong Polytechnic University Disguise and Makeup Faces Database

A surgically altered finger

UNC CHARLOTTE

BTI Institute

Beneficiary / End User Profile: Jobs

- Who are the beneficiaries / end-users of this research (the “jobs”)?
  - Biometric Technology Rallies
    - System evaluators
  - CBP risk analysts
  - CBPO Fraudulent Documents Analysis Unit
  - OBIM – Futures Identity

Beneficiary / End User Profile: Desired Gains

- What are the main outcomes and benefits that the end user desires (the “gains”)?
- Connect human factors motivating travelers, immigrants and refugees to identity concealment efforts;
- Understand and quantify misidentification and concealment risks.

Beneficiary / End User Profile: Pain Points

- Can identity be manipulated at a supervised immigration check point?
- Illegal immigrant used surgery to fake fingerprints and enter Japan.

- Age: 27 years old
- Gender: Female
- Nationality: Chinese
- Background: Arrested for faking a marriage license

1. She paid a plastic surgeon to surgically alter her fingerprints to evade detection. She paid about 15000$ for the fingerprint transplant surgery. Patches of skin from her thumbs and index fingers were removed and grafted onto the fingers of the opposite hand.
2. She passed through the checkpoint using fake fingerprints.
3. Rong's identity was not detected when she entered Japan illegally.

Collect money for transplant fingerprint surgery → **Pay a plastic surgeon** → **Get skin from fingers removed and grafted on the other hand** → **Pass through the checkpoint** → **Enter the country**

UNC CHARLOTTE

BTI Institute

Beneficiary / End User Profile: Pain Points (2)

- What are the main issues the capability/knowledge gap is causing (the end user “pains”)?
  - Lacking description of attack vectors or comprehensive processes to mitigate ID risks
    - Traveler, immigrant and refugee services
    - Connecting motivation, capabilities (technical and resources) and methods
    - Prioritizing defensive measures through risk assessment.

Products & Services

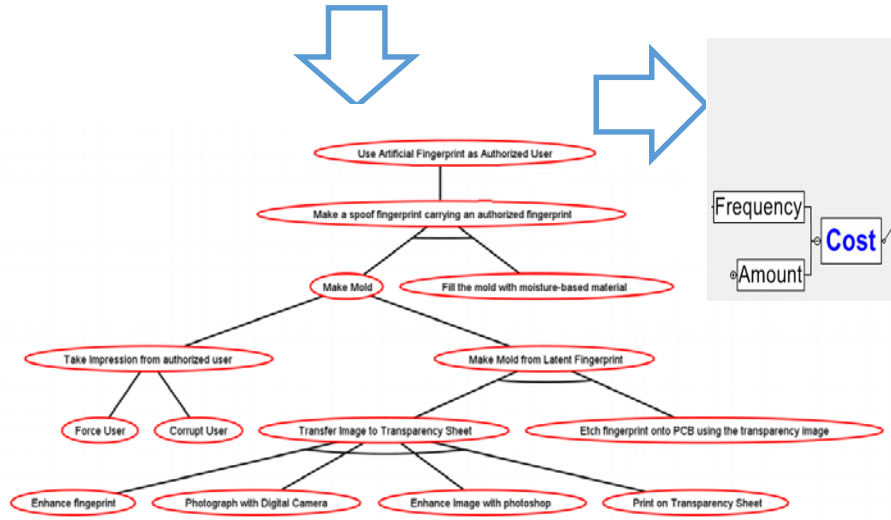
- What products & services are the outcomes of this research project?
  - Knowledge Products (completed):
    - Three technical reports related to motivation, techniques and attack vectors
    - Three papers published so far
  - Technologies (completed and in progress):
    - Abstraction / collection / classification of biometric attack vectors
  - Tools:
    - Risk assessment from attacked vectors
      - Tool created, but revealed a knowledge gap

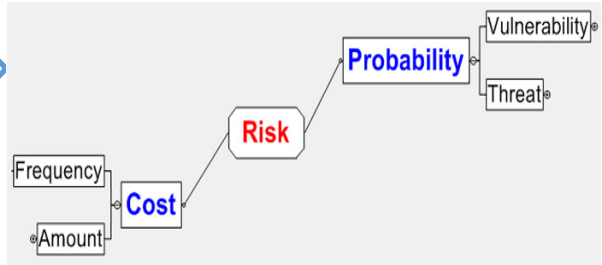
Gains Created: Example

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.

- **Security cards – parse the content**
  - Adversary's Motivations, Adversary's Resources, and Adversary's Methods





- **Risk Assessment**
- **Attack Representation: trees, graphs**

UNC CHARLOTTE

BTI Institute

Gains Created

- What are the gains achieved and how are they measured?
  - 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, cyber intrusions (ID manipulation), motivation, expertise, passport fraud)
    - Need coordination and integration of concerns.

Pains Alleviated

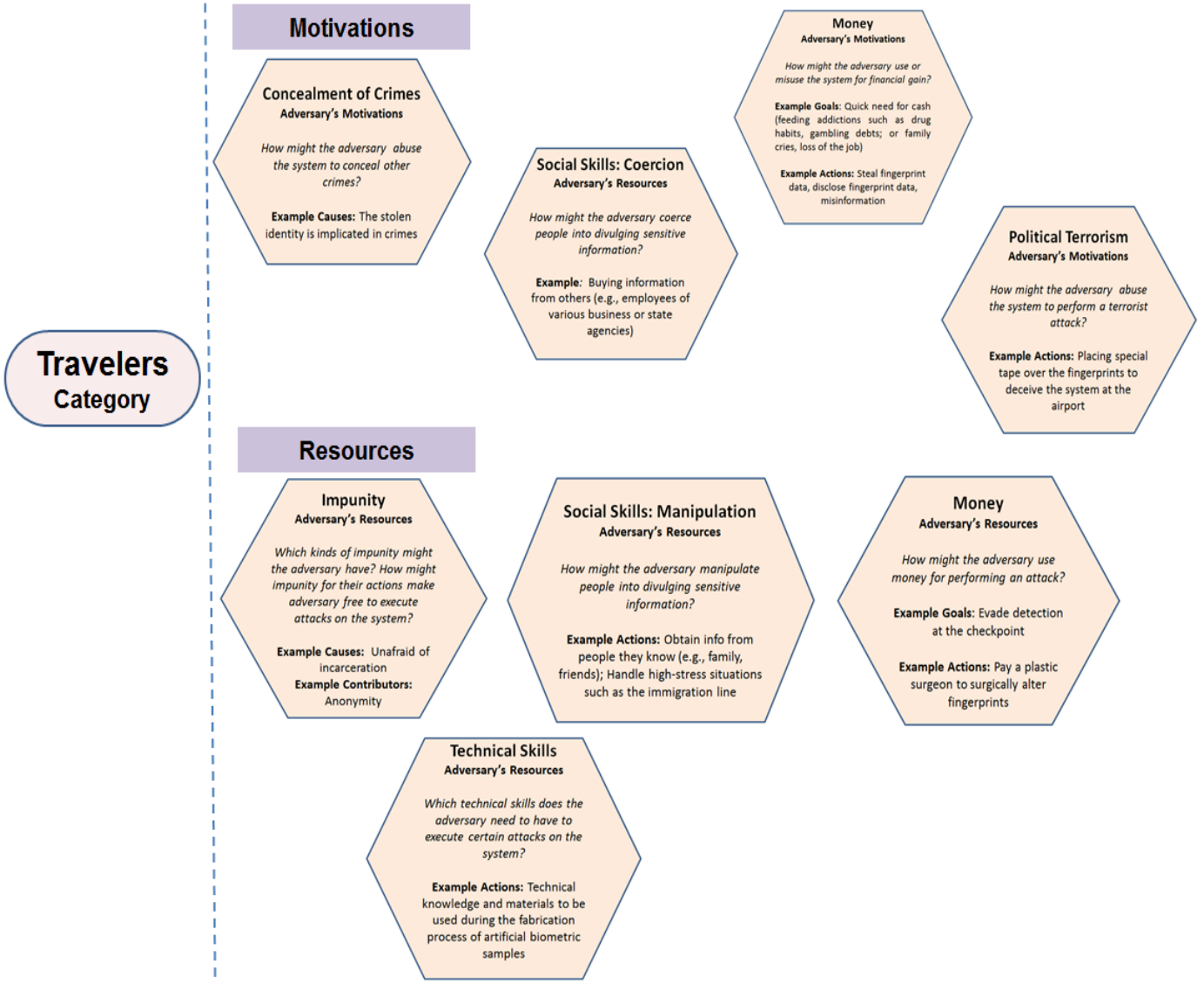
- What are the pains alleviated and how are they measured?
  - Identification of common biometric attack vectors through a systematic methodology that describes biometric / process vulnerabilities and attack opportunities.
    - Stories can be properly documented and analyzed.
  - Metrics: deliver at least one attack scenario for each of the populations of interest (travelers, immigrants, refugee management)
    - Delivered at least two in each category
  - Tool support for the analysis process:
    - http://securitycardsforreview.njs.jelastic.vps-host.net/
    - Risk assessment from attack trees

Key Accomplishments - Example

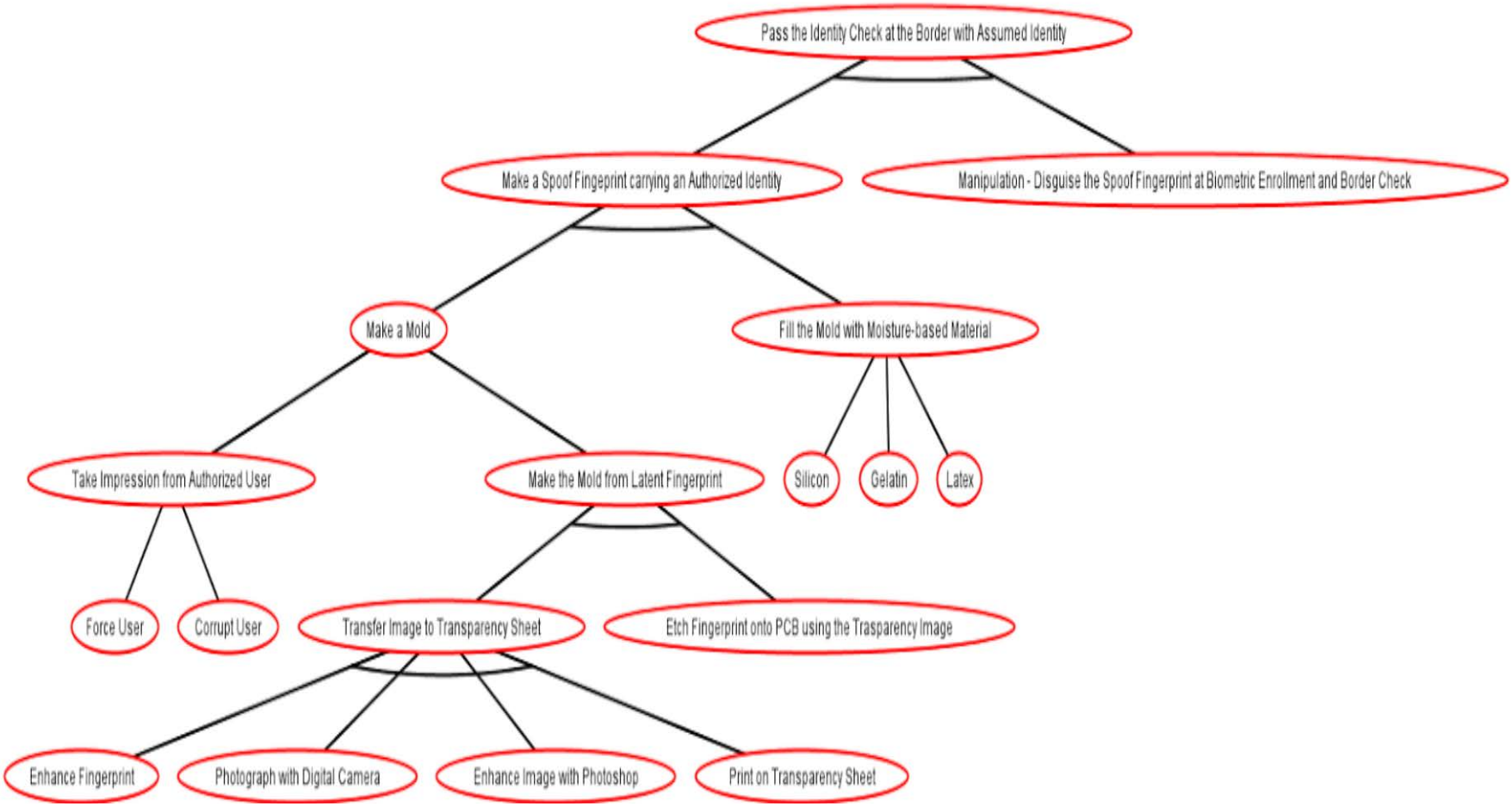
STORY:

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.

UNC CHARLOTTE



Achievements: Travelers – the attack tree



UNC CHARLOTTE

BTI Institute

Key Achievements: Immigrant population

STORY:

Miriam obtained F1 visa to study in the US. She arrived to her University using F1 visa and requested that her boyfriend / fiancé be issued F2 visa. Background check determined he served military service in a company associated with Iranian Republican Guard. His visa was denied. Miriam left the university, supposedly because of her boyfriend, and lost F1 visa. Instead of going back to Iran, she went see her uncle in California. While there, she overstayed her visa. She tried to pay individuals to impersonate her while exiting the US.

UNC CHARLOTTE

Motivation

Access or Convenience

How might the adversary abuse the system for life of convenience?

Example Actions: Obtaining admission to US University without intention to pursue a degree.

Motivation

Malice or Revenge

How might the adversary abuse the system to exact revenge?

Example Actions: With the dream of life in US threatened, revenge through an adversarial action

Resources

Impunity

How to achieve the goal without risking fines or incarceration?

Example Actions: Pay someone to exit US as her. Access to passport falsification service.

Resources

Inside knowledge

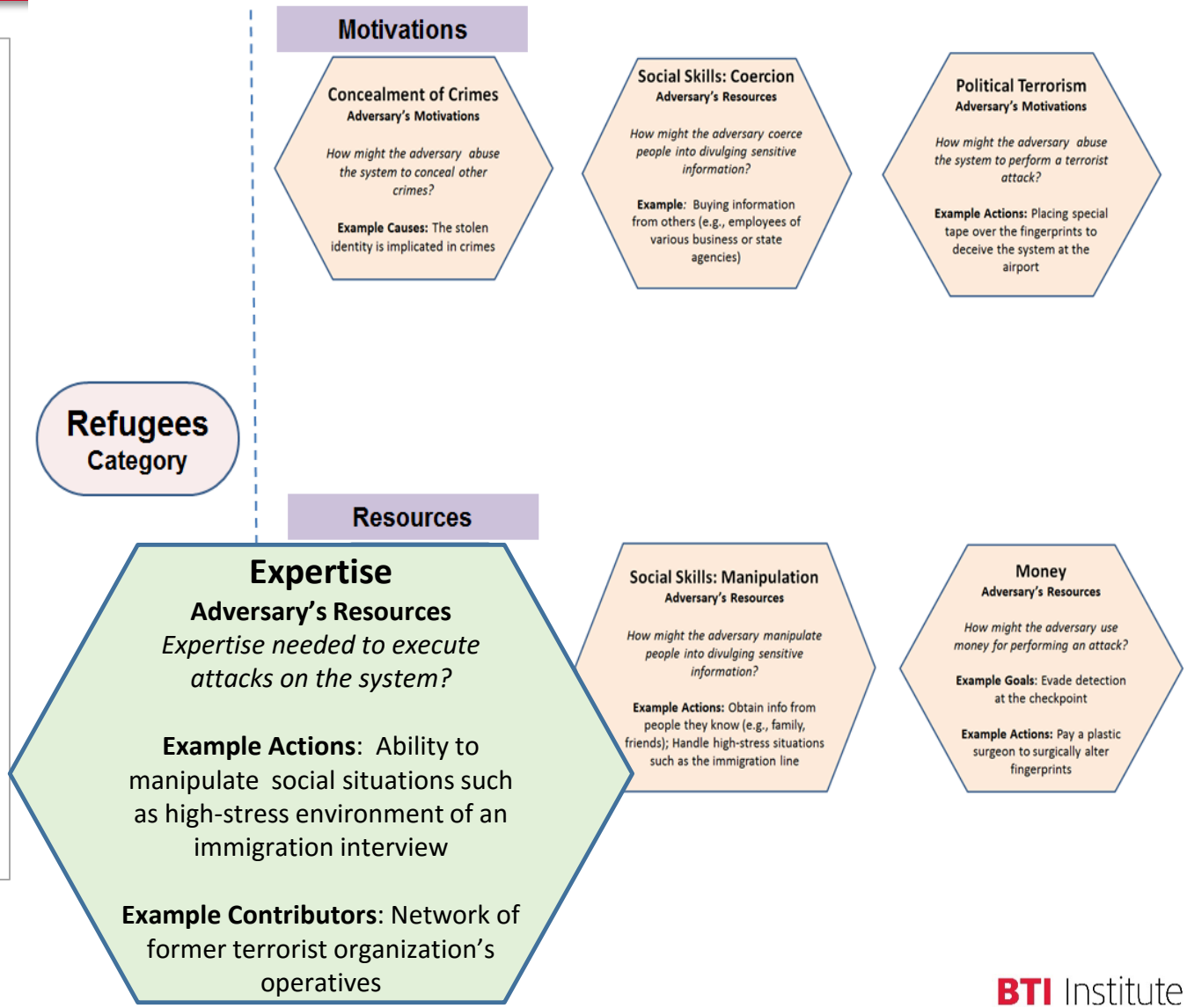
What kind of insider information an adversary needs to succeed?

Example Actions: Studied US immigration processes., befriended a DHS employee.

Achievements: Refugee management

STORY:

Nizar is a refugee from Syria who had been living in an area occupied by a terrorist organization. Nizar and his family were surviving by creating supplies used for terrorist activities. Nizar may have worked in a lab operated by the terrorist organization. The lab has been taken over by the Iraqi forces and fingerprints were lifted from the lab surfaces. Nizar and his family managed to escape and are now applying for refugee status in US.

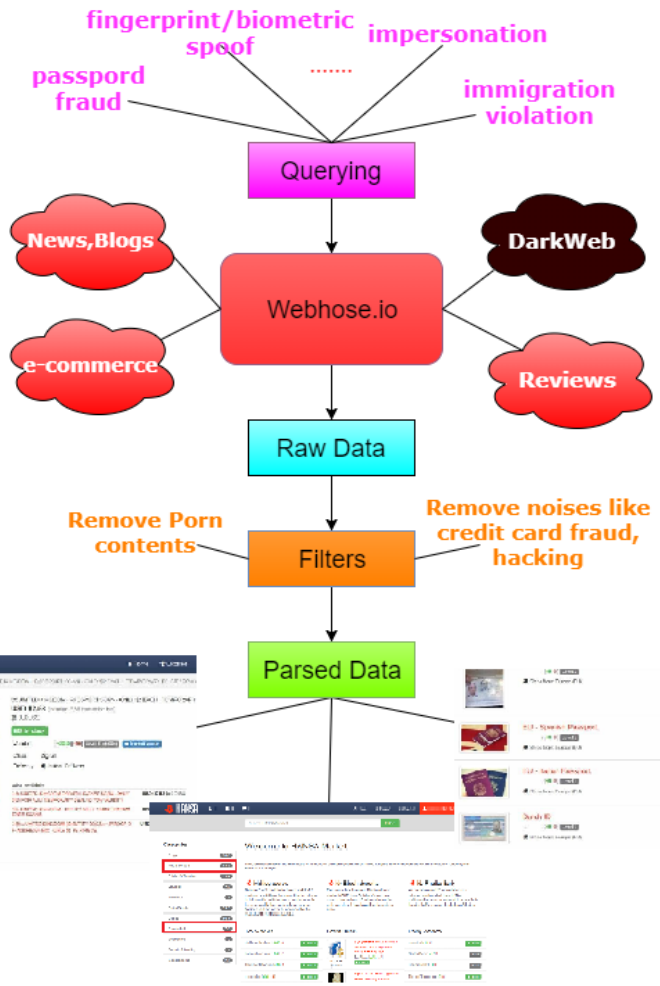


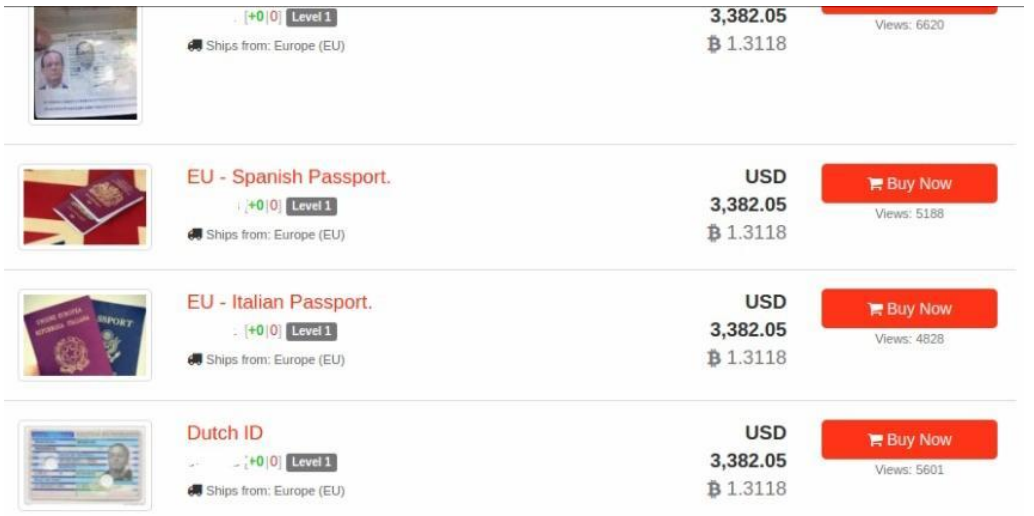
UNC CHARLOTTE

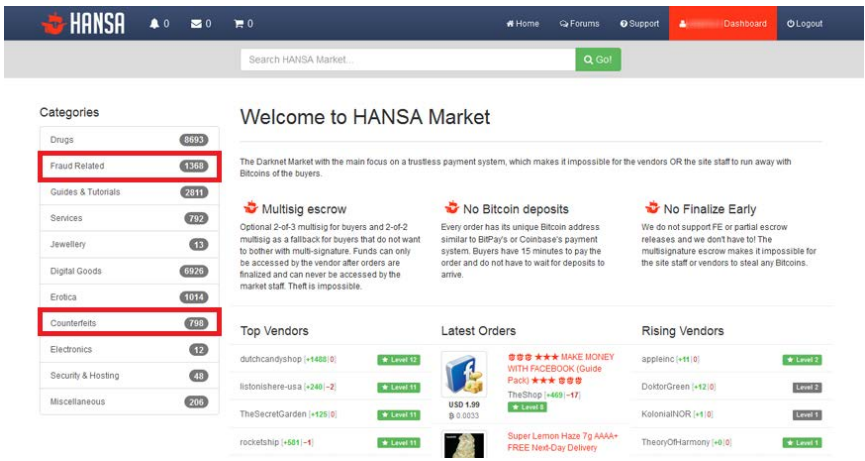
BTI Institute

Achievements: Barriers to Risk Assessment

- Querying dark web for ID manipulation offers







Transition Pathways, Engagement

- How will the work reach the end-user? What is the proposed transition pathway?
  - Notional transition plan developed, being discussed with the Project Champion.
    - Major product is not a tool, but a methodology, which may affect organization and workflows.
    - No IP planned.
  - Engagement discussions initiated at this meeting
    - Opportunities for planning test scenarios in upcoming Biometric Technology Rallies.

Transition Challenges

- What does the project team perceive to be the challenges they will face in the near and long term going forward?
  - Discussions related to potentially sensitive information create communication barriers.
  - Transitioning a methodology, rather than IP, with many “process touch points” may require complex coordination efforts.

Next steps

- Current and future tasks
  - Exploring Dark Web for ID misrepresentation services and tools
    - Understanding availability, cost of acquisition, effectiveness
  - Reanalyzing exposed processes and systems.
- Examining attack vector representation and scope
  - Current information indicates that biometric attacks are likely to be part of broader manipulations (documents, fake IDs)
  - Better understanding of availability and support for identity obfuscation will help risk estimates.
  - Exploration of the effectiveness of defense mechanisms.

Acknowledgment and Disclaimer

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.

UNC CHARLOTTE

BTI Institute