

Principles of Protection
Renewable | Revocable

Template Protection Testing

IBPC Satellite II Workshop
Gaithersburg, MD
05 March 10

Point of Contact: Elaine.Newton@nist.gov

Identity Management Systems Program Manager
NIST Information Technology Laboratory

iTL



**V.I.P.- Diplomáticos
Tripulación
V.I.P.-Diplomatics - Crews**



Objectives

- Long-term
 - To support the development of biometrics as a suitable authentication factor for large-scale systems, across multiple domains
- Short-term
 - To determine the set of measures that define template protection functionality
 - To determine how to use available resources to test and report an evaluation of these metrics

REV-X ?

Agenda (1 of 3)

- Welcome and Introductions
- Template Protection Background – “Security and Privacy in Biometric Systems - The purpose of Biometric Encryption,” Tom Kevenaar, priv - ID
- NIST’s Cryptographic Module Validation Program, Randall Easter (CMVP Director)

Agenda (2 of 3)

- Panel on Testing of Template Protection Schemes
 - Panelists:
 - Terry Boulton, UCCS
 - Christoph Busch, Fraunhofer
 - Jean - Christophe Fondeur, Sagem
 - Tom Kevenaar, priv - ID
 - Nalini Ratha, IBM
 - Xuebing Zhou, Fraunhofer

Agenda (3 of 3)

- ISO 24745 Biometric Template Protection – Christoph Busch, Fraunhofer
- Twiki Set - up – Ross Micheals, NIST



Panel on Testing and Metrics

Testing Principles

Testing should be performed...

- by an independent party.
- on a sequestered dataset.
- on a dataset that is the appropriate size for error rates being tested.

Results should be made public.

NIST Biometric Testing/Data

- Fingerprint
 - Ongoing Proprietary Fingerprint Test (PFT) and MINEX (MINutiae EXchange) testing using various databases of 120K+ subjects
 - Software development kit (SDKs) –based testing
- Face
 - Data from grand challenges and vendor tests
 - DOS Database of 37K subjects
 - Algorithm-based testing
- Iris
 - Data from grand challenges and vendor tests
 - Algorithm-based testing

Potential Participant Variations:

- What barriers prevent entry into current evaluations?
 - E.g. “Two images are needed to create an enrollment template.”
 - Are they common v. specific to a solution?
- What available public data might work for testing?
 - E.g. SD 29 – 2 rolled and 2 flat images per finger, 216 subjects
- What other departures from current testing protocols may be of interest for template protection?

NIST Special Pub 800-63

- Technical requirements for remote authentication over an open network in response to OMB 04-04
- Four Assurance Levels, ranging from low or no confidence (1) to very high confidence (4) in the claimant's identity
- Biometrics not included in authentication protocols in this guidance
- Adopted by non-USG orgs and in the process of being standardized internationally

Passwords v. Biometric Data

- P: Known only to the end-user
- B: Potentially known by anyone who can encounter the individual in-person or virtually

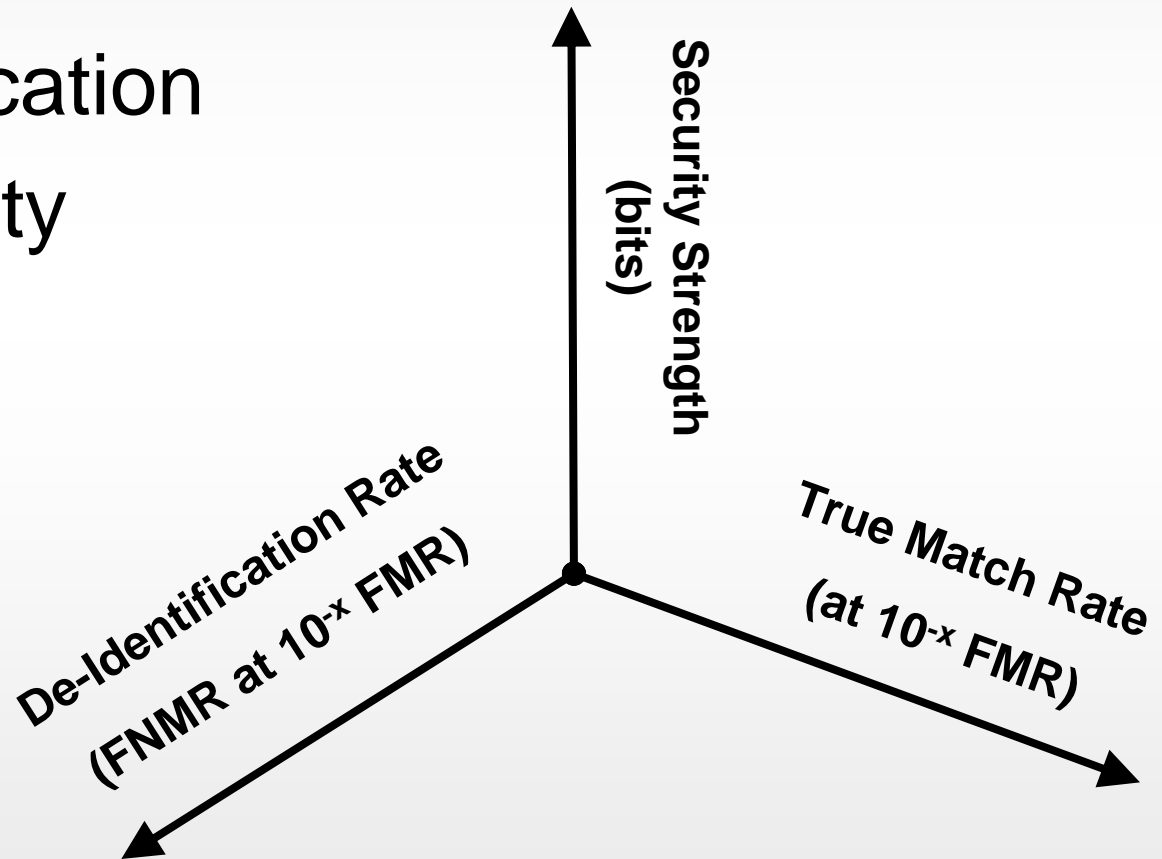
- P: Deterministic
- B: Probabilistic

- P: Can be (easily) changed if compromised and periodically renewed to mitigate risk
 - Can be lengthened to increase security
- B: A pattern with some degree of robustness over time that can be used to distinguish individuals

- P: Many possibilities for users to choose different credentials for different domains, which could be randomly generated or otherwise have no personally identifying information
- B: A presentation of the same biometrics for any application, and many can be used for identification

What should be measured?

- Biometric Performance
- De-Identification
- Irreversibility
- Others?



Measurements

- Could be jointly or severally required and/or tested
- Could be mapped to the Assurance Levels in NIST SP 800-63 (AL 1 through 4)



Discussion

Agenda (3 of 3)

- ISO 24745 Biometric Template Protection – Christoph Busch, Fraunhofer
- Twiki Set - up – Ross Micheals, NIST

Thank you

- Image Attribution for Slide 2

- Lounge web surfer = <http://www.free-stockphotos.com/images/woman-working-at-lobby.jpg>
- Kitchen web surfer = http://www.stockvault.net/Human_activity_g23-Laptop_girl_p9853.html
- War zone = http://www.stockvault.net/Tools_weapons_g51-Army_at_war_p8462.html
- Laptop And Mobile Phone = <http://www.free-stockphotos.com/images/laptop-with-mobile-phone.jpg>
- E-commerce = <http://www.free-stockphotos.com/images/online-shopping.jpg>
- US Senate entrance = <http://www.everystockphoto.com/photo.php?imageId=2456738>
- ATM = <http://www.everystockphoto.com/photo.php?imageId=2610700>
- Rescue workers = <http://www.everystockphoto.com/photo.php?imageId=2723279>
- Land/Car Passport Check = <http://www.everystockphoto.com/photo.php?imageId=2535743>
- US VISIT = <http://www.everystockphoto.com/photo.php?imageId=3411527>
- Frankfurt Iris Check = <http://www.everystockphoto.com/photo.php?imageId=1182105>
- Cuba Passport control = <http://www.everystockphoto.com/photo.php?imageId=2651417>