Strength of Authentication for Biometrics: An Evaluation Framework

Elaine Newton, NIST

Colin Soutar, Deloitte & Touche LLP

Agenda

- **Background on the Advanced Identity Workshop:**
  Applying Measurement Science in the Identity Ecosystem
- **Purpose & Scope**
- **Approach:**
  - **Problem Statement**
  - **System Attack Analysis**
  - **Zero Information Attack**
  - **Consider an Additional Factor: Effort**
  - **Incorporating Effort**
  - **Strength of Function for Authenticators (SOFA)**
  - **Ultimate Goal: Comparing & Combining Authentication Technologies**

Background on the Advanced Identity Workshop: Applying Measurement Science In the Identity Ecosystem

- January 12-13th @ Gaithersburg
- Focus on quantifying strength of function to enable risk based decisions
- Three focus areas:
  1. Strength of Authentication
  2. Strength of Proofing
  3. Attribute Confidence
- Strength of Authentication will focus initially on measuring the strength of **Biometric Authentication Systems**
- The overall goal of this area is to reach the point where the strength of authentication mechanisms can be **measured**, **compared**, and eventually **combined**
- Why start with biometrics? Growing availability and use.

Purpose & Scope

- Produce a framework for measuring and evaluating the strength of a biometric authentication system that enables:
  - Greater understanding of how much trust can be placed in solutions
  - Better alignment of solutions with assessed risks
- Focus is on positive authentication and one-to-one matching:
  - Does not address watch-list applications
  - Does not deal with situations where users are avoiding identification
- Intended to be modality agnostic
- Framework will be released as a report from NIST, but may be used as contribution to a standards development effort
- Framework will be open for public comment throughout its development

Approach

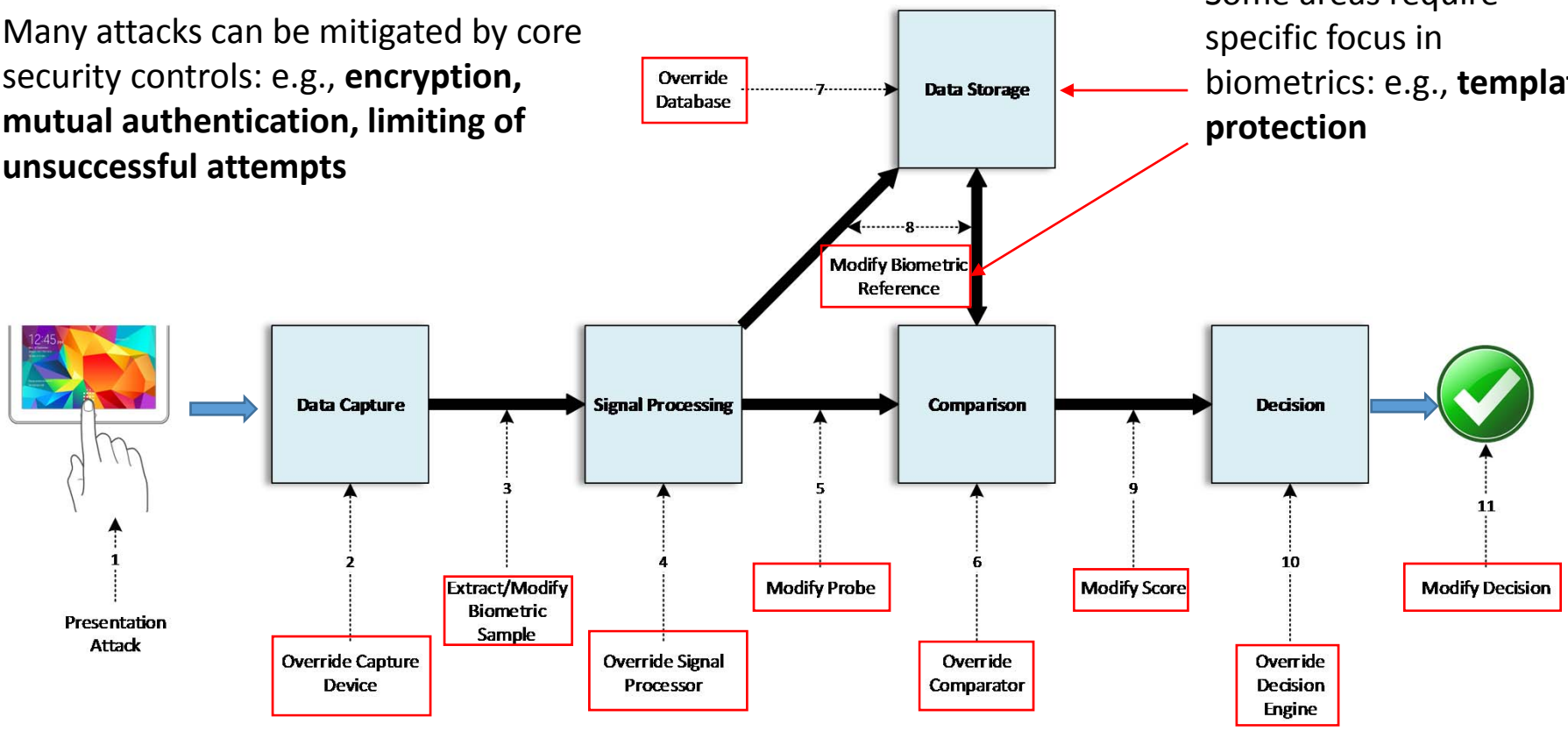
Problem Statement

- Starting point: What generally accepted measurements exist around "strength" of authenticators?
  - Entropy and the strength of passwords/key length
  - Strength of Function: Common Criteria
- How can we compare strength of biometric authentication mechanisms to each other, and to other types of mechanisms?
  - Can we create a comparable measure in biometrics to entropy or strength of function?
- Can we establish a general framework for comparing different mechanisms?
  - SOFA = Strength of Function for Authenticators

System and Attack Analysis

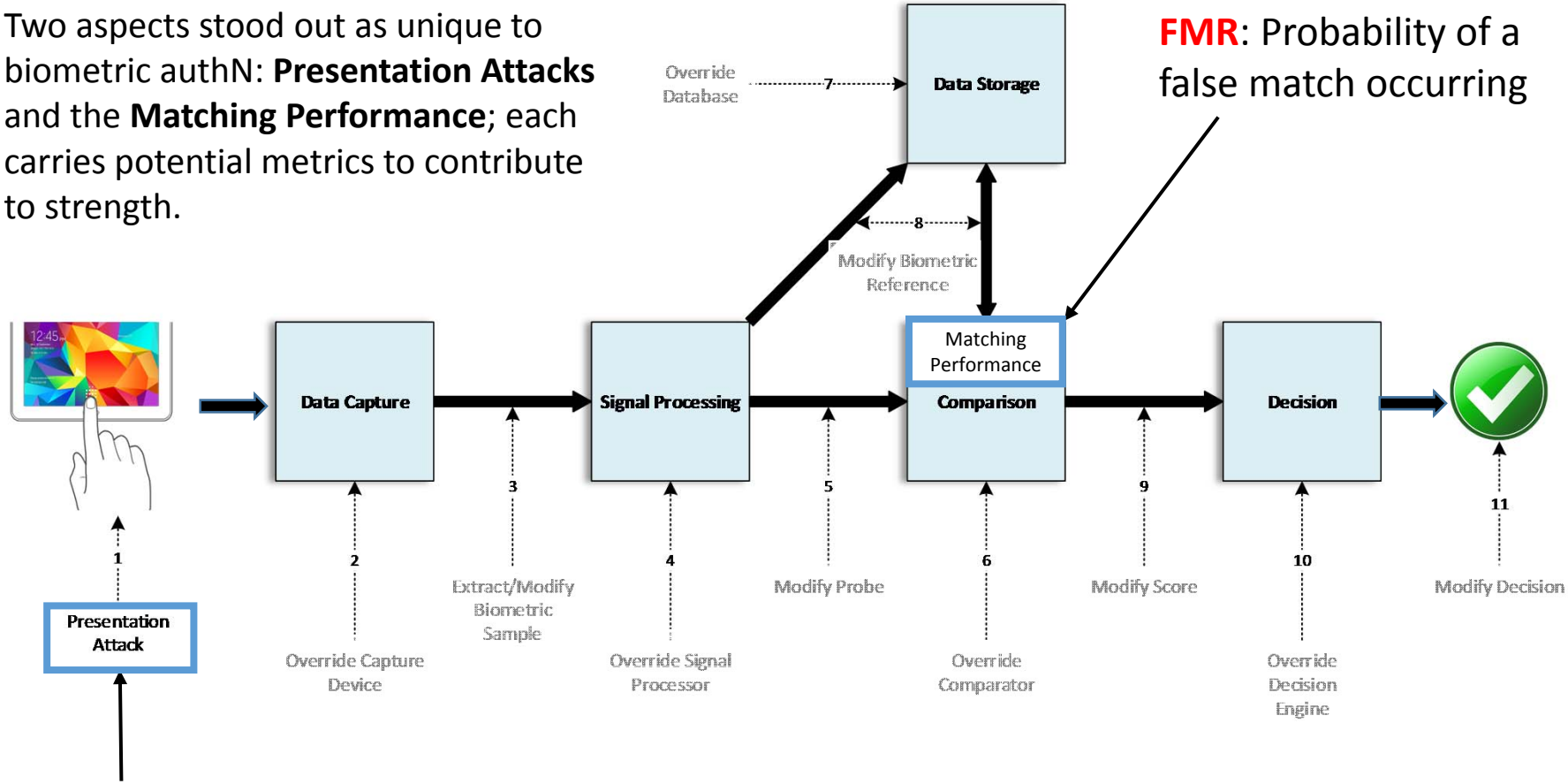
Many attacks can be mitigated by core security controls: e.g., **encryption, mutual authentication, limiting of unsuccessful attempts**

Some areas require specific focus in biometrics: e.g., **template protection**



System and Attack Analysis: Biometric Specific

Two aspects stood out as unique to biometric authN: **Presentation Attacks** and the **Matching Performance**; each carries potential metrics to contribute to strength.



FMR: Probability of a false match occurring

PAD Error Rate: Probability of a successful presentation attack

Approach

- Isolate the aspects of biometric technologies that can be quantified
- Assume a baseline of “cyber hygiene”
- Inherent biometric strength
  - “Zero information” attacks,
    i.e., the attacker doesn’t have the PIN or biometric pattern
  - “Targeted” attacks
- Additional controls (e.g., limiting failed attempts) may be layered on top of the quantified strength to improve the overall security of a system
- What are the relevant factors for the framework?

Zero Information Attack

Factors: FMR and PADER

False Match Rate (FMR)

- Proportion of impostor attempt samples falsely declared to match the compared template
- Empirically determined
- Combination of
  - Inherent discrimination
  - signal fidelity; sensor performance; processing and matching capabilities

Presentation Attack Detection Error Rate (PADER)

- Proportion of presentation attacks incorrectly classified as bona fide presentations at the PAD subsystem in a specific scenario*
- Error rates and testing being developed in ISO/IEC 30107-3 and FIDO Alliance
- Testing standards and procedures may address…
  - Type of attacks used
  - Number of attempts
  - Types of tests: verifying vendor claims, or full statistical significance trials?

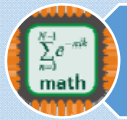
Hypothesis—FMR and PADER can be combined to produce a measure that can be compared to a password's entropy.

Assumption—FMR and PADER are independent of one another.

* This is very similar to the APCER measure used in the draft of ISO/IEC CD 30107-3

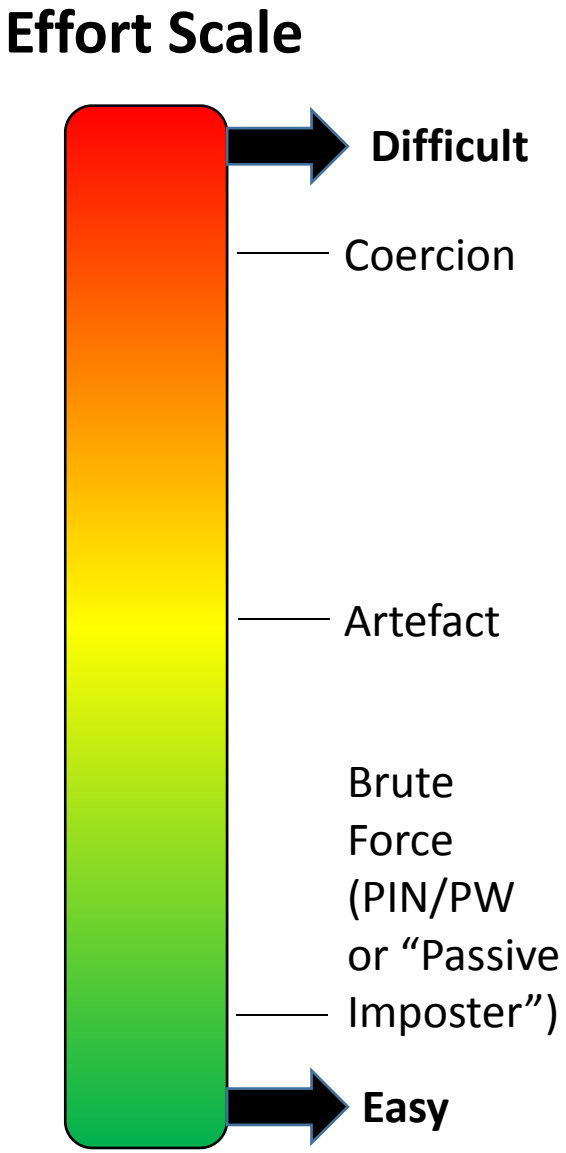
Consider an Additional Factor: Effort

- To understand the inherent strength of a biometric system, more than PADER and FMR are required—effort should also be considered

	Password/Pin	Biometrics
Zero Info.	 Length and complexity	 Sample size and complexity  Access to sensor/device  Computational complexity of matching
Targeted	 Shoulder surf  Notepads	 Retrieve biometric  Create artefact

Incorporating Effort

- Effort = Level of effort required to attack specific components of an authentication system.
  - Focuses on the point of input or sensor
  - Requires qualitative assessment and comparison of attacks extending across systems
  - The time, knowledge, and resources required for an attack may contribute to the effort
  - Consequences may also be considered
- Many factors could be incorporated into effort: further exploration required



Strength of Function for Authenticators (SOFA)

Inherent Strength

- Incorporating the FMR, PAD, and effort into a single measure of strength could look something like this:

$$SOFA_{Zero\ Info}\ (Biometrics) \quad \alpha \quad \frac{Effort}{FMR \times PADER}$$

- In the case of targeted attacks, the measure of strength may look like:

$$SOFA_{Targeted}\ (Biometrics) \quad \alpha \quad \frac{Effort}{(1 - FNMR) \times PADER}$$

Ultimate Goal: Comparing & Combining Authentication Technologies

- Goal is to move towards developing metrics that can be compared and combined to better understand authentication systems
- Ultimately, we would be able to determine the same type of measure for most authentication systems

$$SOFA_{Zero\ Info}\ (Biometrics) \quad \alpha \quad \frac{Effort}{FMR \times PADER}$$

$$SOFA_{Zero\ Info}\ (PIN/PW) \quad \alpha \quad Effort \times N^{L}$$

For PIN/PW, N is the number of possible symbols and L is the length of the string of the set of N symbols.

Next Steps

- NIST will produce an initial draft document
- Using short, open public comment periods the document will be iteratively reviewed and updated based on community feedback
- NIST will finalize the document and identify the most appropriate venue to forward additional work
- Your feedback is welcomed and encouraged through the entire process! Please send comments to (sofa@nist.gov) or through the comment mechanism during the iterative public review periods

References

- M1.4 AHGBEA – *Study Report on Biometrics in E-Authentication*
- OASIS – *Analysis of Methods of Trust Elevation Version 1.0* (2013) and *Electronic Identity Credential Trust Elevation Framework Version 1.0* (2014)
- ISO 19092:2008 - *Financial services -- Biometrics -- Security framework*
- ISO/IEC 30107-1:2016 - *Information technology -- Biometric presentation attack detection -- Part 1: Framework*
- Committee Draft of ISO/IEC 30107-3 - *Information technology -- Biometric presentation attack detection -- Part 3: Testing and Reporting*
- ISO/IEC 24745:2011 - *Information technology -- Security techniques -- Biometric information protection*
- ISO/IEC 19792:2009 - *Information technology -- Security techniques -- Security evaluation of biometrics*
- "Measuring Strength of Authentication" - *Workshop: Applying Measurement Science in the Identity Ecosystem*
- *http://www.commoncriteriaportal.org/*

Contributors

NIST

Elaine Newton, PhD
- National Institute of Standards and Technology
- enewton@nist.gov

Kevin Mangold
- National Institute of Standards and Technology
- kevin.mangold@nist.gov

Paul Grassi
- National Institute of Standards and Technology
- paul.grassi@nist.gov

Contract support to NIST

Colin Soutar, PhD
- Deloitte & Touche LLP Cyber Risk Services
- csoutar@deloitte.com

Ryan Galluzzo
- Deloitte & Touche LLP Cyber Risk Services
- rgalluzzo@deloitte.com

Raj Dinh
- Deloitte & Touche LLP Cyber Risk Services
- abdinh@deloitte.com

Special guest contributions to NIST

Cathy Tilton
- CSRA Inc.
- cathy.tilton@csra.com