NIST

Strength of Function for Authenticators (SOFA):

Discussion Draft Overview

Elaine Newton, PhD

NIST

APPLIED CYBERSECURITY DIVISION

ACCESS MANAGEMENT • SECURITY & PRIVACY APPLICATIONS • EDUCATION & WORKFORCE DEVELOPMENT • NATIONAL CYBERSECURITY CENTER OF EXCELLENCE • TRUSTED IDENTITIES

Purpose & Scope of SOFA

- NIST is exploring a framework around **Strength of Function for Authenticators (SOFA)** 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

- Intended to be modality agnostic

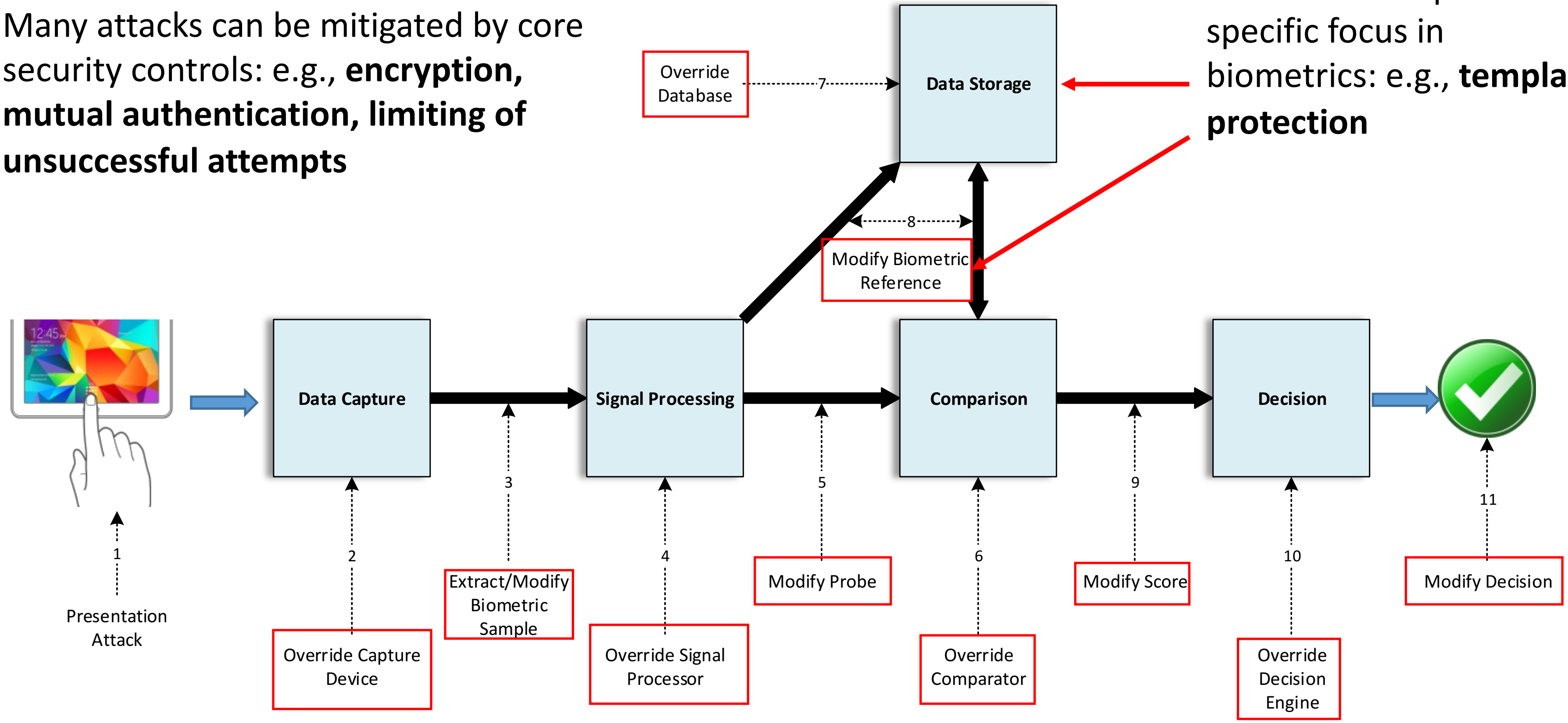
Problem Statement

- 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?

System and Attack Analysis

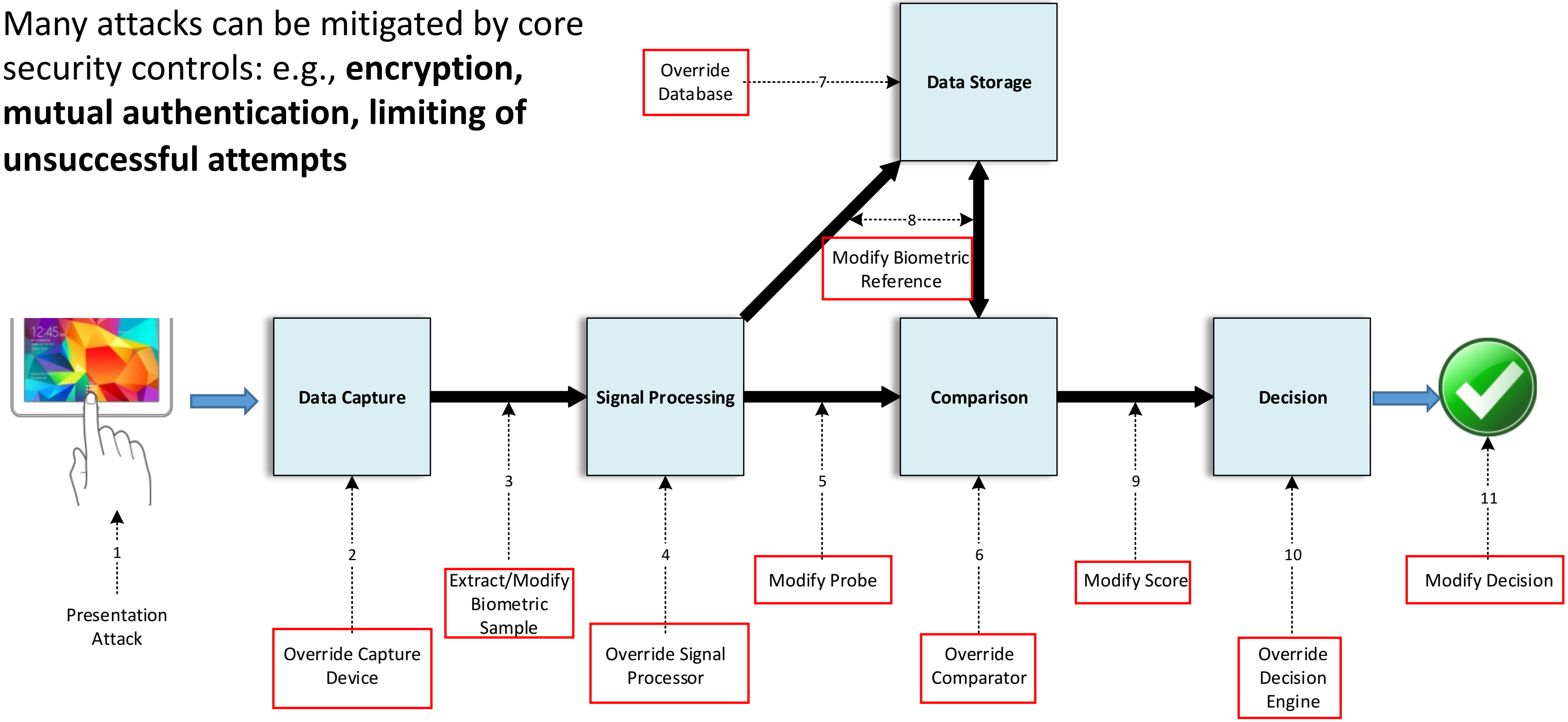
Many attacks can be mitigated by core security controls: e.g., **encryption, mutual authentication, limiting of unsuccessful attempts**

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



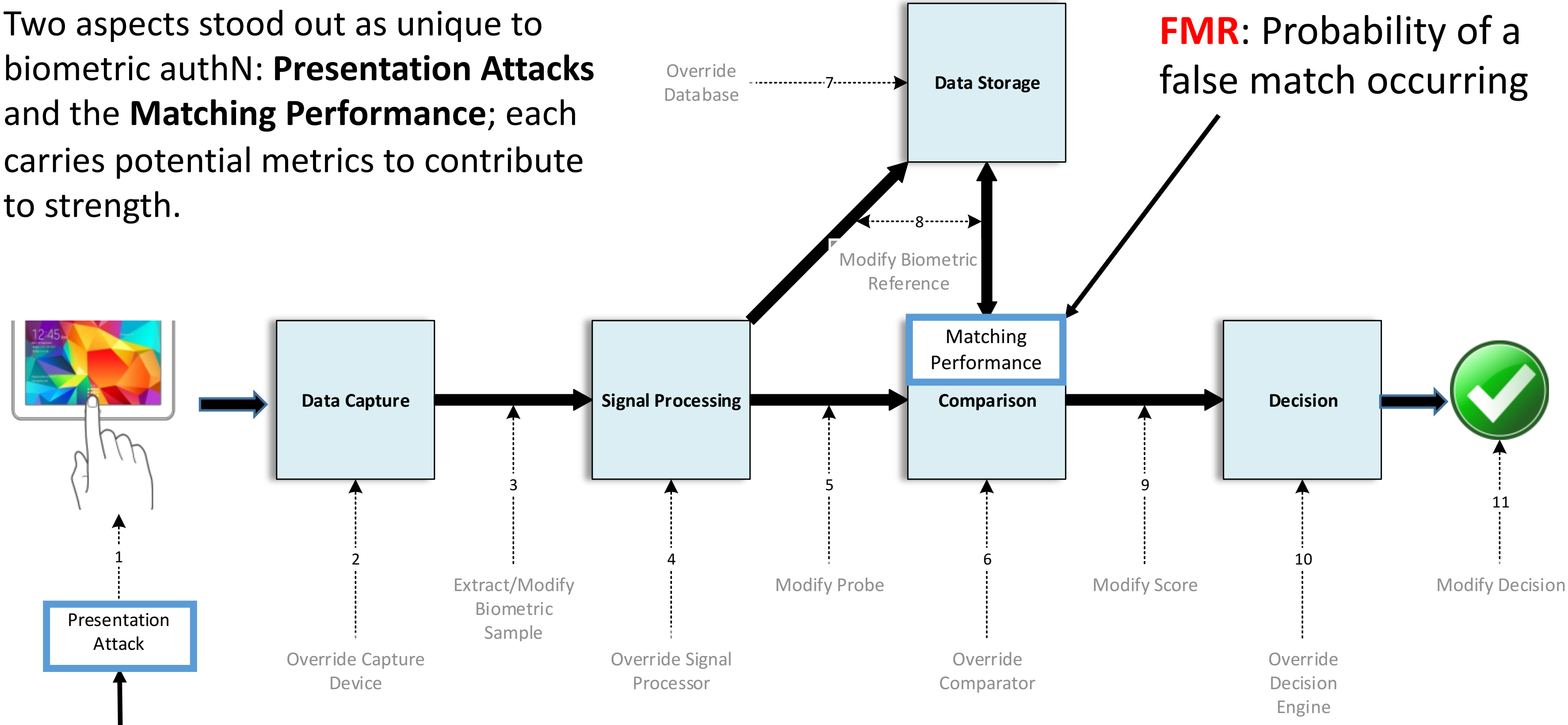
Recommendation 1:
Use baseline security to mitigate most attacks

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



Recommendation 2: Analyze and quantify factors specific to biometric systems.

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

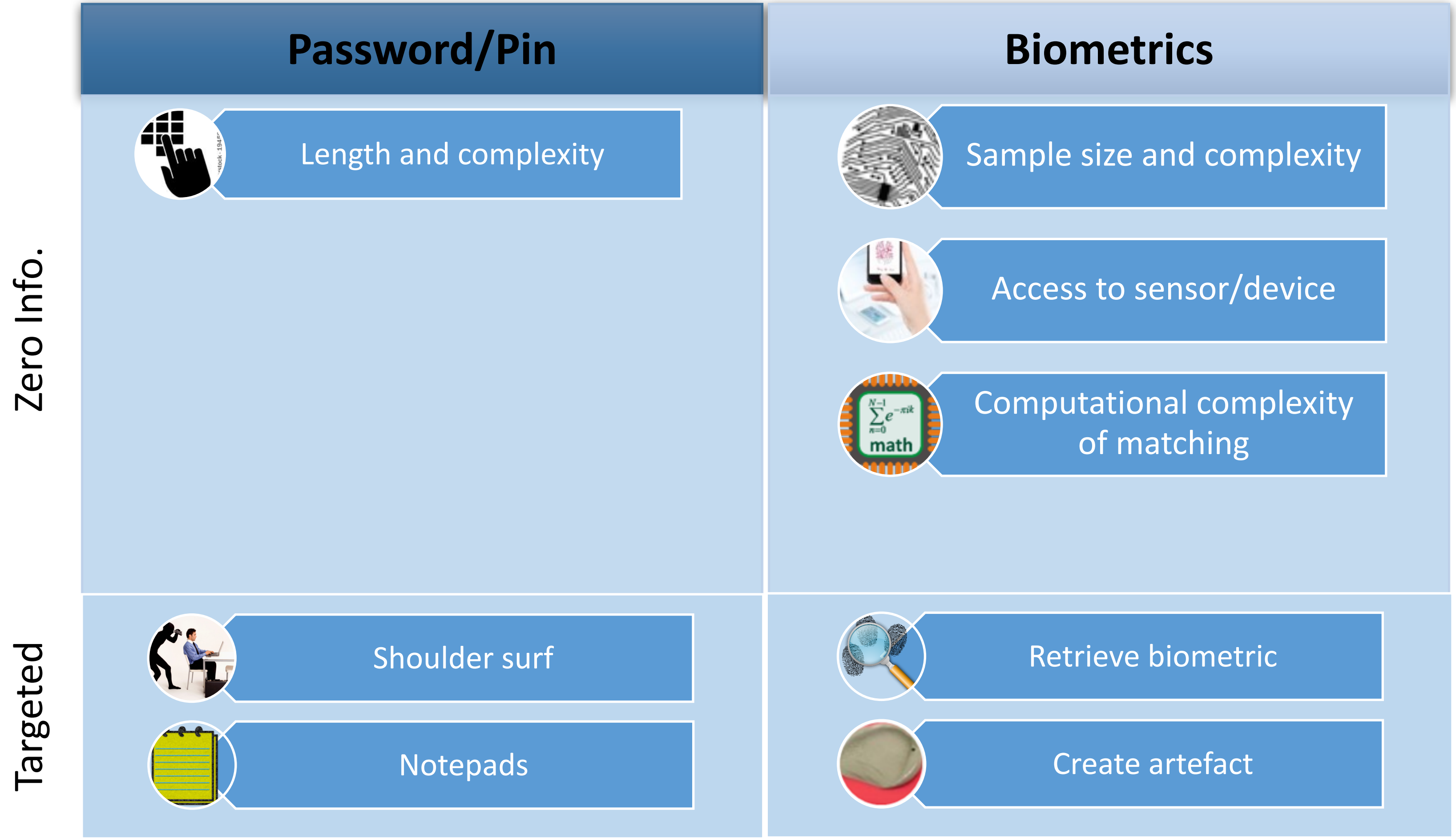
Biometric Strength and Factors for Consideration

- There are **three components** specific to biometrics that are relevant for consideration when determining the ability of a system to defend against attacks

False Match Rate (FMR)	Presentation Attack Error Rate (PADER)	Level of Effort
- Empirically determined - Combination of inherent discrimination and signal fidelity, senor performance, processing, and matching capabilities	- 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	- Focuses on the point of an input or sensor - The time, knowledge, and resources required for an attack may contribute to effort - Consequences may also be considered
FMR and PADER can be combined to produce a measure that can be compared to a password's entropy		

Zero-Information and Targeted Attacks

- “Zero-information” and “targeted” attacks should be considered, as both scenarios may affect Effort, as well as PADER and FMR.

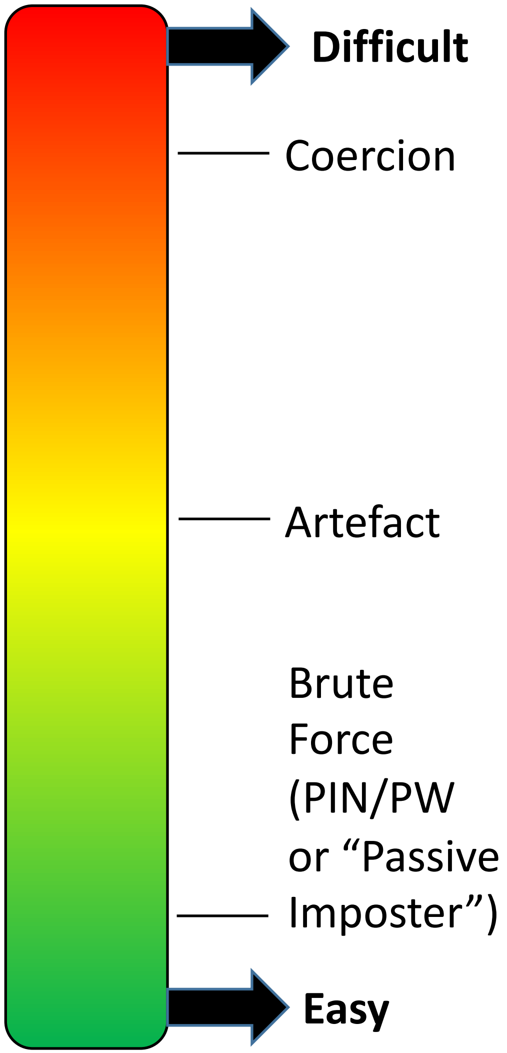


	Password/Pin	Biometrics
Zero Info.	Length and complexity	Sample size and complexity Access to sensor/device Computational complexity of matching
Targeted	Shoulder surf Notepads	Retrieve biometric Create artefact

Recommendation 3: Differentiate Attack types and Incorporate 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

Effort Scale



Recommendation 4:
Quantify SOFA for Zero Information Attacks

- 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

$$\text{SOFA}_{\text{Zero Info}}\,(\text{Biometrics}) \quad \alpha \quad \frac{\text{Effort}}{\text{FMR x PADER}}$$

$$\text{SOFA}_{\text{Zero Info}}\,(\text{PIN/PW}) \quad \alpha \quad \text{Effort} \;\; \text{x} \;\; N^{L}$$

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

Recommendation 5: Strength of Function for Authenticators-Biometrics (SOFA-B)

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

$$\mathrm{SOFA}_{\mathrm{ZeroInfo}}(\mathrm{Biometrics}) = \min\left(\frac{\mathrm{Effort}_{material}}{\mathrm{FMR}\text{ x }PADER_{material}}\right)$$

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

$$\mathrm{SOFA}_{\mathrm{Targeted}}(\mathrm{Biometrics}) = \min\left(\frac{\mathrm{Effort}_{material}}{(1-\mathrm{FNMR})\text{ x }PADER_{material}}\right)$$

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

Next Steps

- We want your feedback:
  - The SOFA-B discussion draft document is available at:

  https://pages.nist.gov/SOFA/

  [This is case-sensitive.]

  - Please provide comments and proposed changes via GitHub or to (sofa@nist.gov).

Thank you!

Q&A