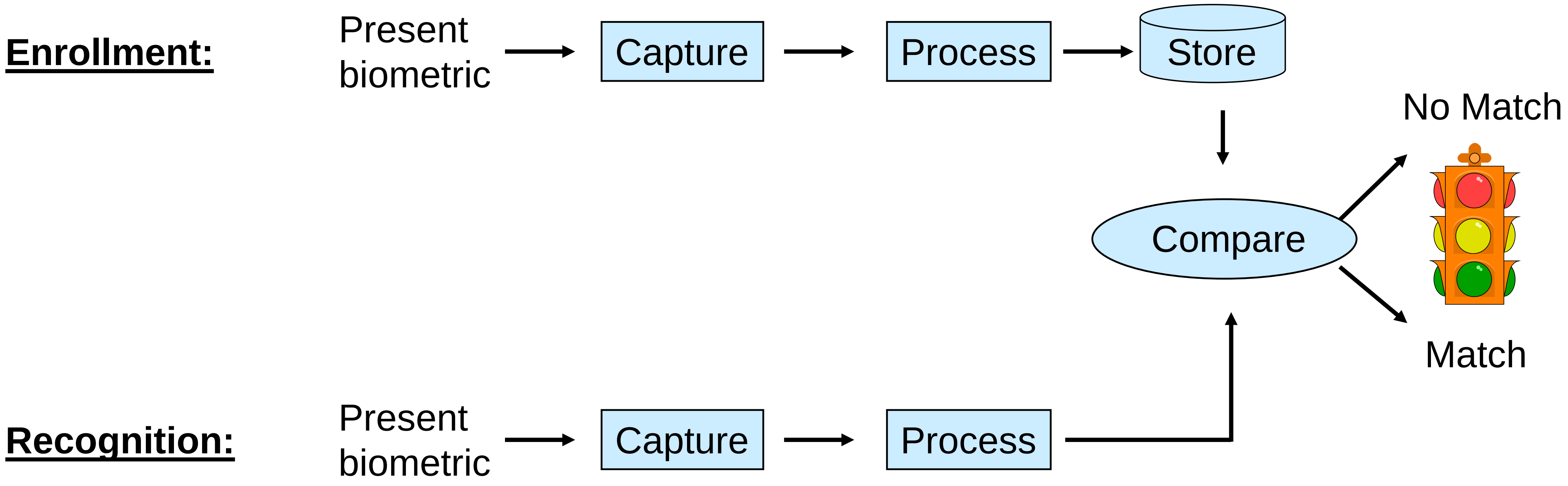
Biometric Authentication
Introduction

C. Tilton, CSRA

12 Jan 2015

Biometric process



Enrollment:

Present biometric → Capture → Process → Store

Recognition:

Present biometric → Capture → Process

Compare

No Match

Match

Basic processes

- Enrollment
  - Adding a biometric identifier (reference) to the database
- Verification (1:1)
  - Matching against a single record
  - Answers “Am I whom I claim to be?”
- Identification (1:N)
  - Matching against all records in the database
  - Answers “Who am I?”
- 1:few

Biometrics are probabilistic

Challenges

- Biometric samples different for each capture
- User behaviour always has impact (e.g. rotation, translation, distortion)
- Matching is a ***measure of similarity of collected samples***

False Match Rate (FMR)

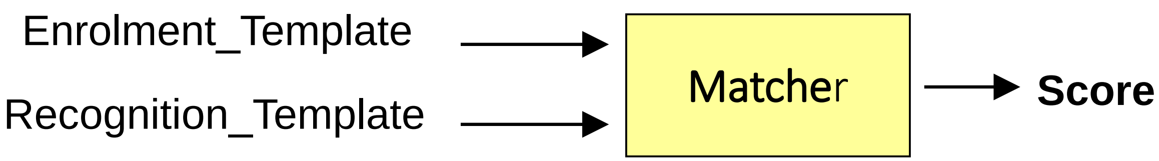
- Probability that single impostor attempt is incorrectly accepted as genuine match

False Non-Match Rate (FNMR)

- Probability that a single genuine attempt fails to match

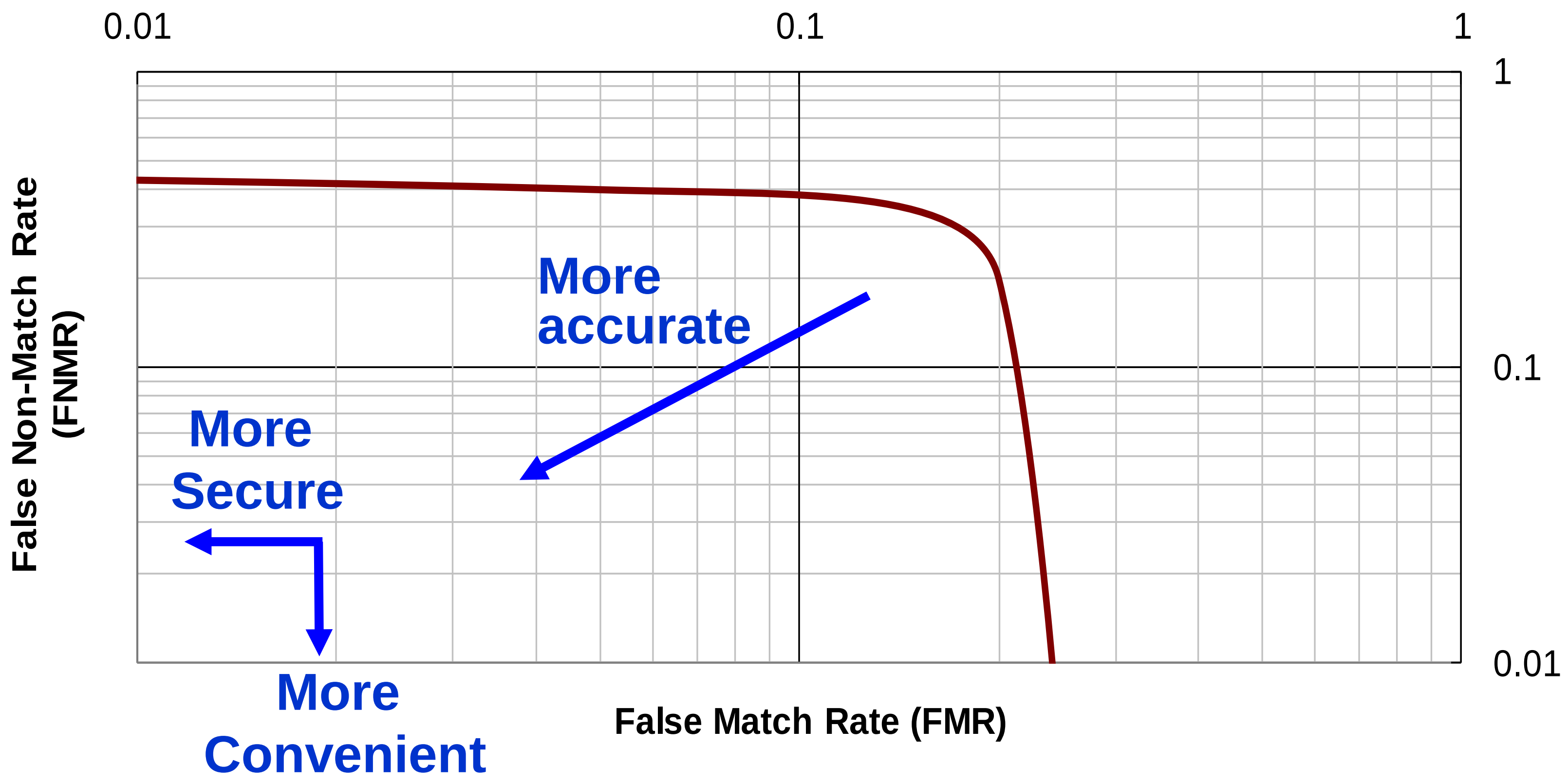
Each matcher score corresponds to a (FMR, FNMR) pair

- Security-convenience trade off
- Ability to set the desired "operating point"



NOTE: FAR/FRR are system level equivalents.

Detection Error Tradeoff (DET) Curve



* When the Y-axis is True Accept Rate (TAR = 1-FNMR), this becomes a Receiver Operating Characteristic (ROC) curve.

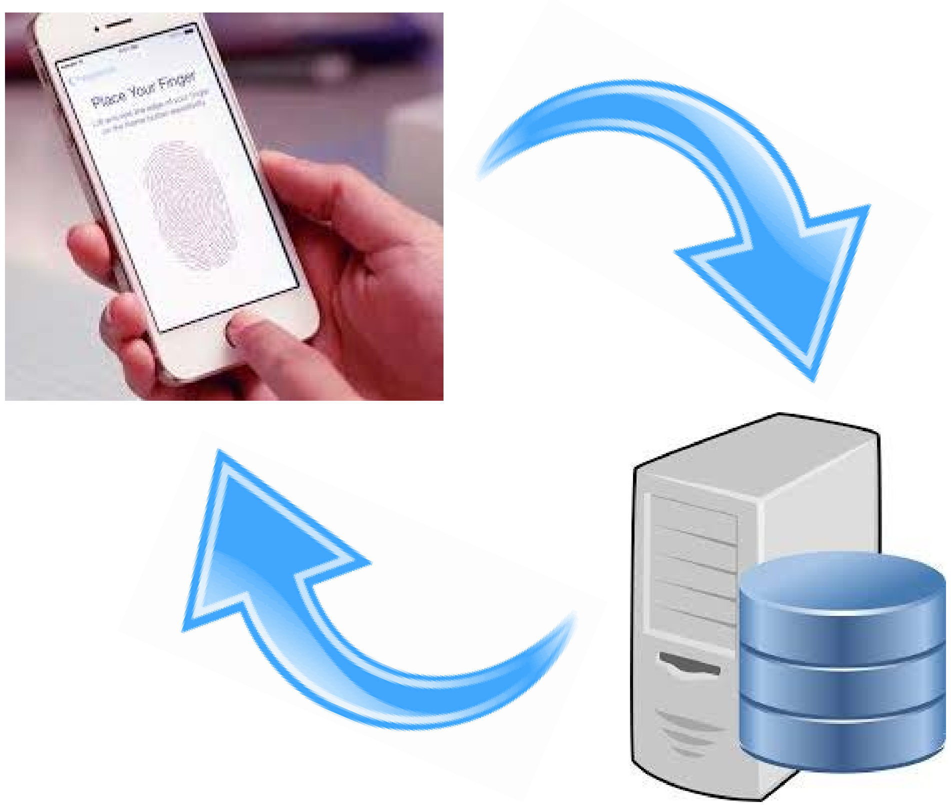
Biometric system architecture decisions

Most common architectures are:

Store and match on server

Store and match on client

(including workstation, device, physical token,...)

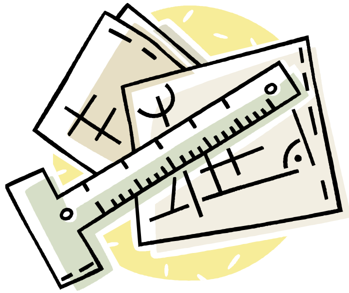


Other architectures may exist.

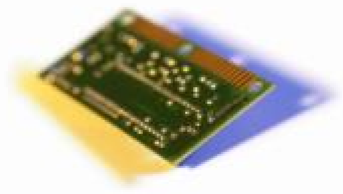
Why does where matter?

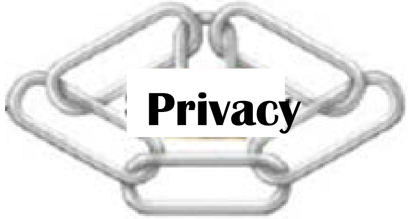
Affects:

Design



Component Selection





Speed

Vulnerability Points

Connectivity Requirements

Example: Store on server, match on server

One of most used architectures

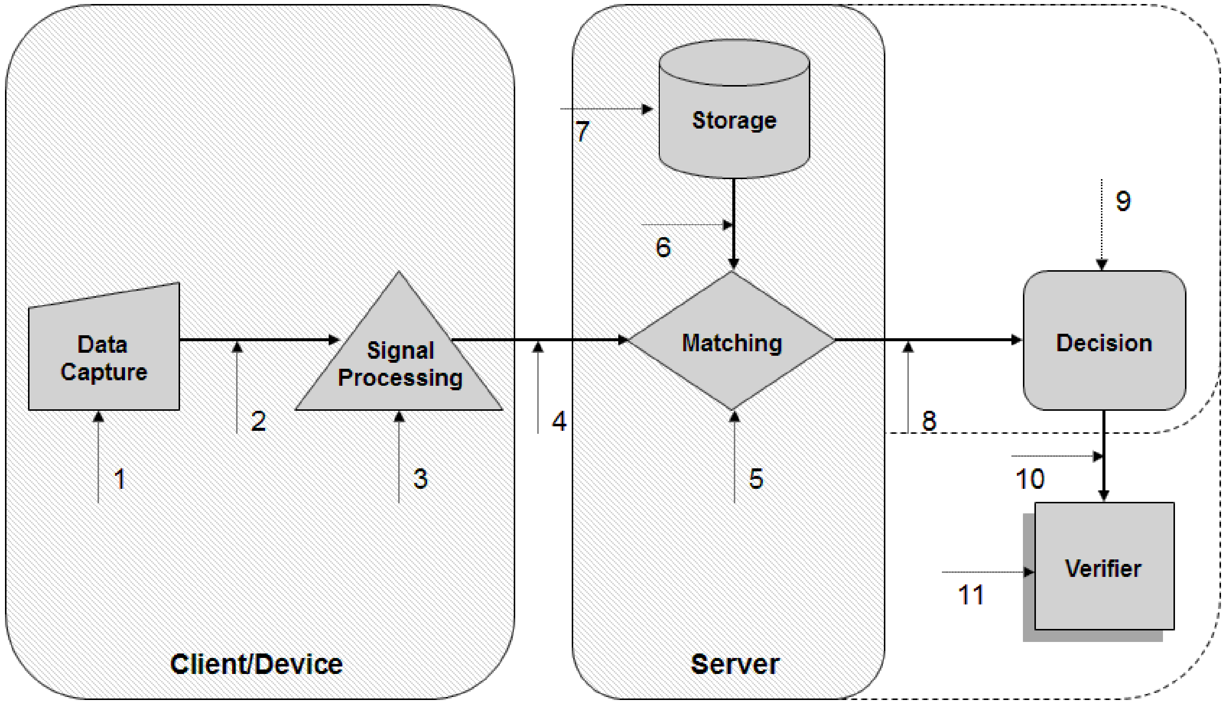
Lends itself to a network environment

Co-location of storage/matching

Example: Web services

Potential vulnerabilities:

- Transfer of live sample to server
- Database compromise



This architecture stores biometric templates on a server and requires that live samples be submitted back to the server in order for the matching process to occur. Once a match or no match result has been determined, the result is then sent to the verifier and the appropriate actions take place.

Example: Store on device, match on device

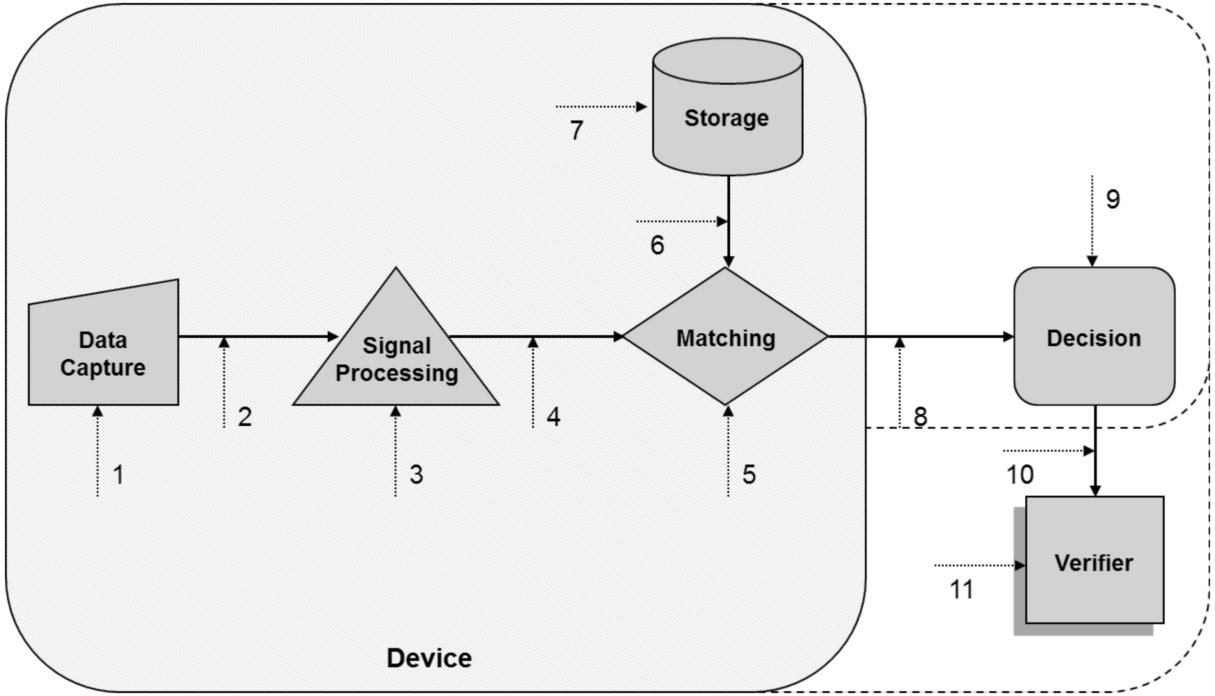
Device: “self-contained” biometric sensor unit, smart phone

Match can result in the release of a cryptographic token

Example: PACS, FIDO

Potential vulnerabilities:

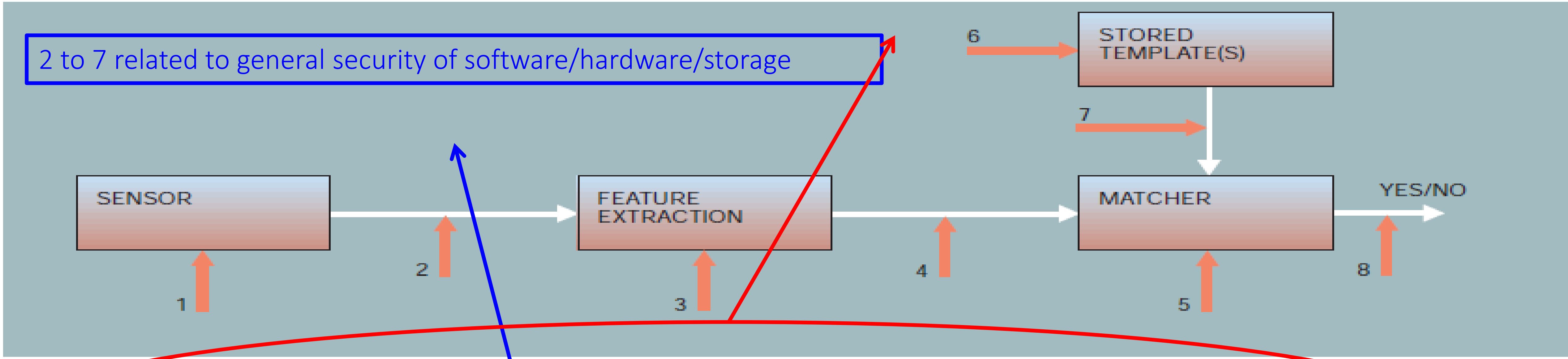
- Integrity of device (tamper resistance, certification)
- Transmission of results



This architecture stores biometric templates on an authentication device and requires that live samples be matched on that device. Once a match or no match result has been determined, the device sends the appropriate signal to the mechanism it is securing.

Biometric Security—Attack Examples

1 & 6 relate to vulnerabilities that are specific to biometrics



2 to 7 related to general security of software/hardware/storage

1. Presentation attacks
2. Replay attacks
3. Overriding feature extraction
4. Tampering with feature sets
5. Corrupting the matcher
6. Tampering with stored templates
7. Attacking channel-stored templates & matcher
8. Overriding final decision

Ratha et al, Enhancing security and privacy in biometrics-based authentication systems, 2001

The big 7 challenges

Integrity -vs- Secrecy

Compromise

Revocation

Sensor Spoofing/Liveness Detection

Entropy/Strength-of-Function

Peer Review Methods

Privacy Considerations

Let the fun begin!

Advanced Identity Workshop:

Attribute Confidence Metadata & Scoring Framework

January 13, 2016

Panelists

Darran Rolls

CTO

SailPoint Technologies

Gerry Gebel

Axiomatics America

Robin Wilton

Technical Outreach Director, Identity and Privacy

Internet Society

Ryan Disraeli

Co-founder

Telesign

Whitepaper

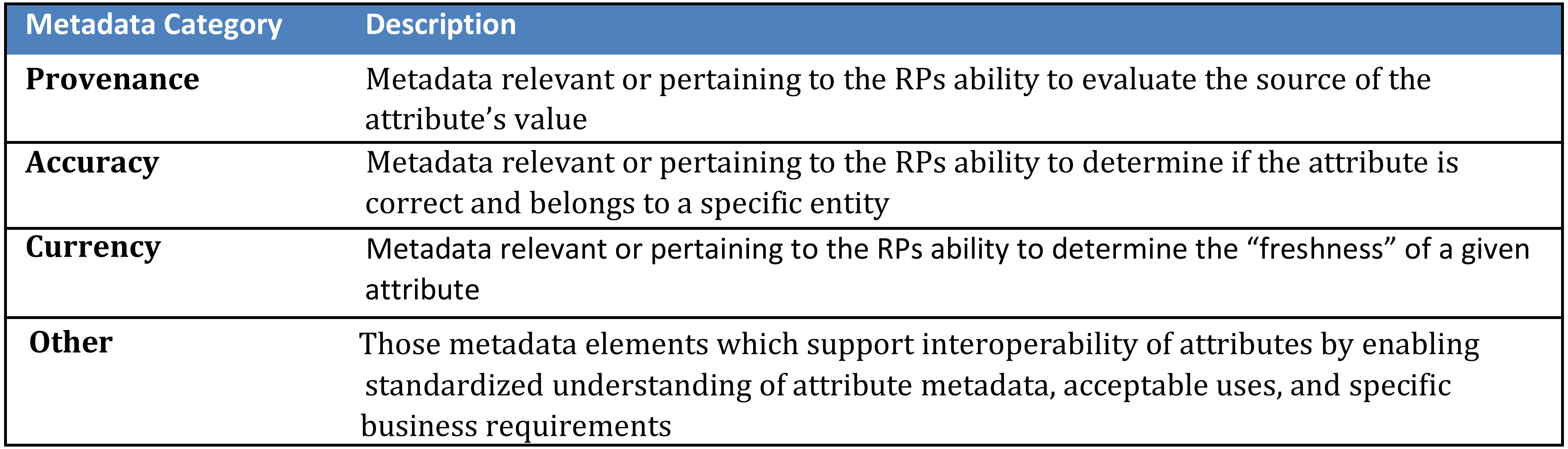
Attribute Metadata and Confidence Scoring

Discussion Draft: Version 1, December 2015

http://www.nist.gov/nstic/NSTIC-attribute-confidence-metadata-discussion-draft.pdf

What are a few real-world usage scenarios from a business and user’s perspective?

Metadata



Metadata Category	Description
Provenance	Metadata relevant or pertaining to the RPs ability to evaluate the source of the attribute's value
Accuracy	Metadata relevant or pertaining to the RPs ability to determine if the attribute is correct and belongs to a specific entity
Currency	Metadata relevant or pertaining to the RPs ability to determine the "freshness" of a given attribute
Other	Those metadata elements which support interoperability of attributes by enabling standardized understanding of attribute metadata, acceptable uses, and specific business requirements

NIST proposes an initial set of 13 metadata elements:

five in the *provenance* category, two in the *accuracy* category, and three each in the *currency* and *other* categories

Metadata	Description + Value
Verifier	The entity that verified the attributes value.
Verification Method	The method by which the attribute value was verified as being true and belonging to a specific individual.
Last Update	The date and time when the attribute was last updated. This metadata is used to derive the age of the attribute.
Update Frequency	The frequency the Attribute Provider (AP) will refresh the attribute.
Update Frequency	The frequency the Attribute Provider (AP) will refresh the attribute.
Expiration Date	The date an attribute's value is considered to be no longer valid for its defined use.
Origin	The entity that issues or creates the initial attribute value.
Provider	The entity that is providing the attribute.
Provider Signature	Properly formatted digital signature of the organization providing the attribute.
Origin Signature	Properly formatted digital signature of the organization that issued of created the attribute value.
Pedigree	Description of the attribute's relationship to the authoritative source of the value.
Individual Consent	Captures whether the user has consented to providing the attribute.
Description	A description of the attribute.
Acceptable Uses	A description of the acceptable business uses to which the attribute can be applied.

Confidence Scores

Scoring based on standardized metadata would involve the assigning of numeric values to metadata values.

For example, when assigning scores to verification method, the acceptable values of {not verified, record verification, in-person verification, in-person with record verification}, could equate to ordinal values (i.e., 1, 2, 3, and 4), respectively, or scalar values (e.g., 0, 0.2, 0.8, 1)

- *page 8*

Overall Confidence Scores

Aggregate Score

Origin Score + Provider Score + Pedigree Score +

Verifier Score + Verification Method Score + …

Category Score

Accuracy Score, Provenance Score, Currency Score

Weighted Aggregate

a(Origin Score) + b(Provider Score) + c(Pedigree Score) +

d(Verifier Score) + e(Verification Method Score) + …

Weakest Link

Min{Origin, Provider, Pedigree, Verifier, Verification Method, …}

Past, Present and Future