Security and Privacy Challenges of Biometric Authentication for Online Transactions

Elaine Newton, PhD
NIST
Information Technology Laboratory,
Computer Security Division
elaine.newton@nist.gov
1-301-975-2532

Remote Authentication in the Federal Government

- OMB Memo 04-04
  - Describes 4 assurance levels, with qualitative degrees of confidence in the asserted identity's validity:
    - Level 1 = Little or no confidence
    - Level 2 = Some confidence
    - Level 3: High confidence
    - Level 4: Very high confidence
- NIST Special Publication 800-63
  - Technical requirements for remote authentication over an open network in response to OMB 04-04

NIST SP 800-63 (E-authentication Guidance)

- Adopted by non-USG orgs and an international standard project is based on 800-63.
  - – NIST (E. McCallister) is the lead editor, ISO/IEC Project 29115
- Levels 3 and 4 require two-factor authentication
- Biometrics not included in authentication protocols in this guidance

Outlook for Identity Management

- WH Initiative on the National Strategy for Trusted Identities in Cyberspace (NSTIC)
  - Aims to improve the security of online transactions of consumers (e.g. online banking)
    - Remote access for more services, available anytime, anywhere
    - Risk-based choices of factors and methods
    - Open standards, interoperable platforms

Authentication Use Case Comparison

For law enforcement, immigration, etc.

- Enrollment and subsequent recognition attempts
  - highly controlled
  - Supervised / Attended
- Successful recognition
  - Answers the question, “Has this person been previously encountered?”
  - Is a unique pattern

For online transactions, e.g. banking, health, etc.

- Enrollment
  - Less controlled
  - Probably not in person
- Subsequent recognition attempts
  - Unattended
- Successful recognition
  - Answers the question, “How confident am I that this is the actual claimant?”
  - Is a tamper-proof rendering of a distinctive pattern

Biometric Security Issues

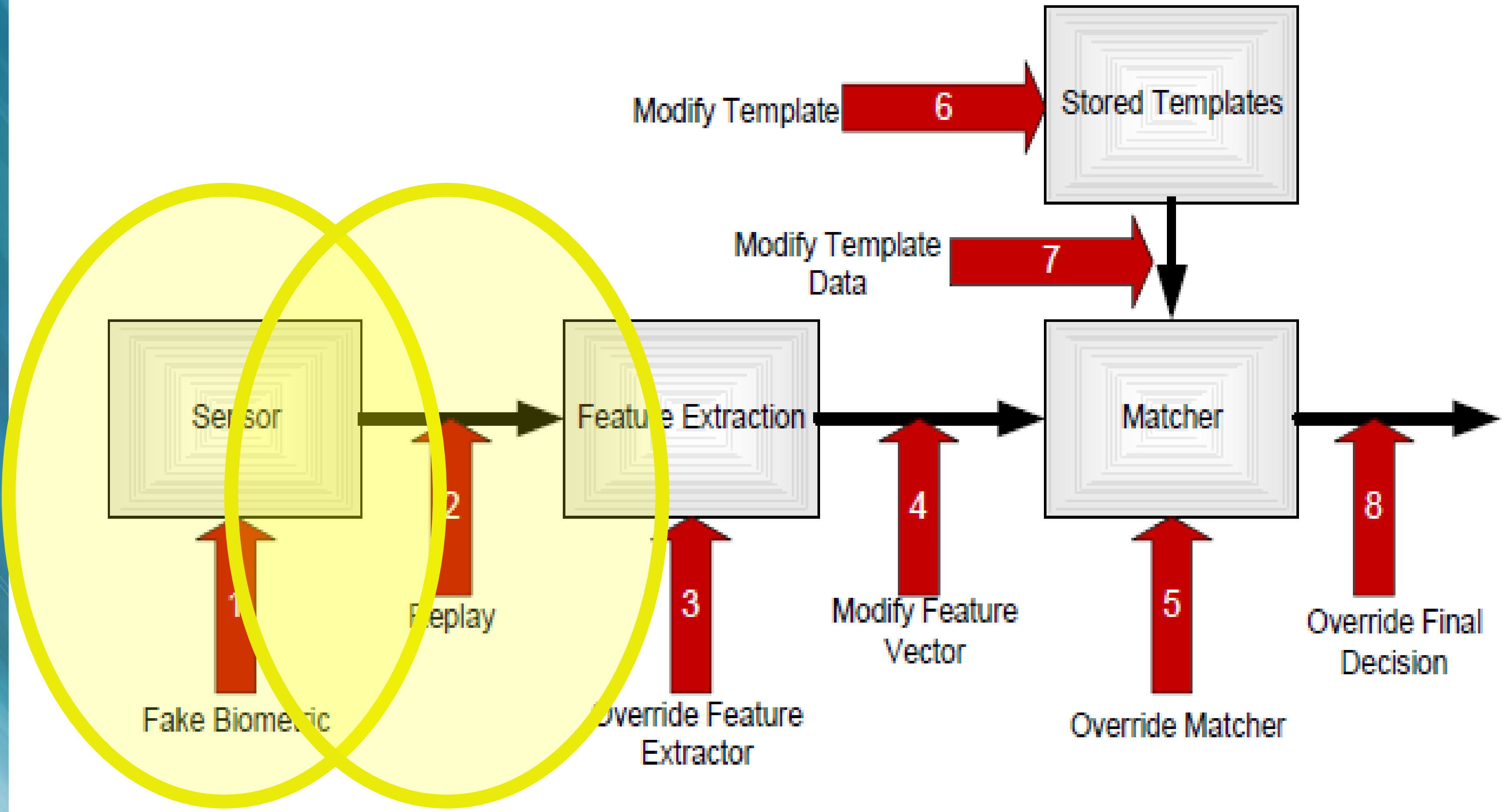


Figure by Nalini Ratha, IBM

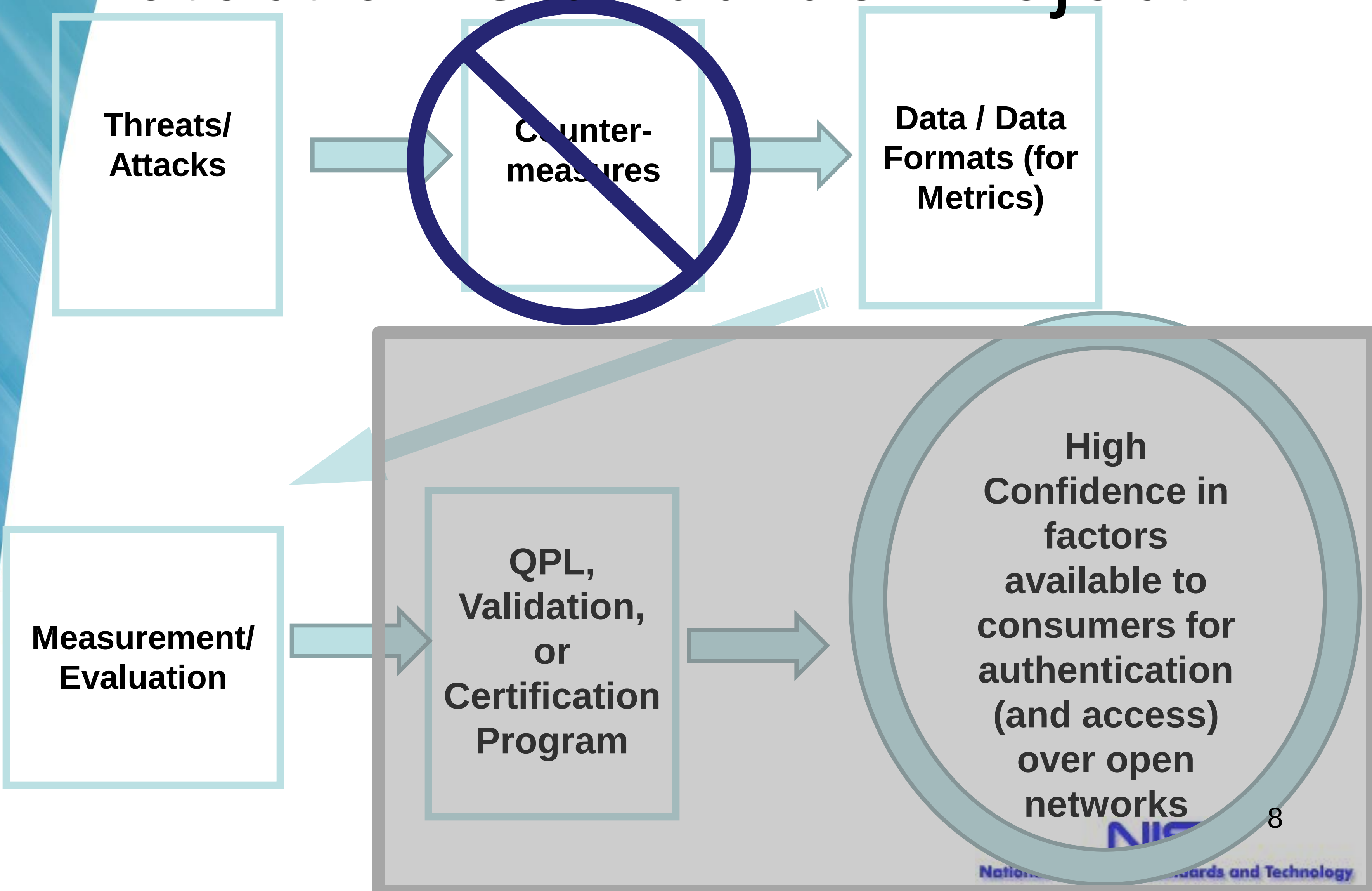
Focus Areas

1) Artefact/Liveness Detection
   - New Project in ISO/IEC JTC1 SC37: 30107

2) Biometric Template Protection

3) Web Services
   - To be covered by Kevin Mangold in the next talk

Anti-Spoofing/Liveness Detection Standards Project



Threats/ Attacks

Counter- measures

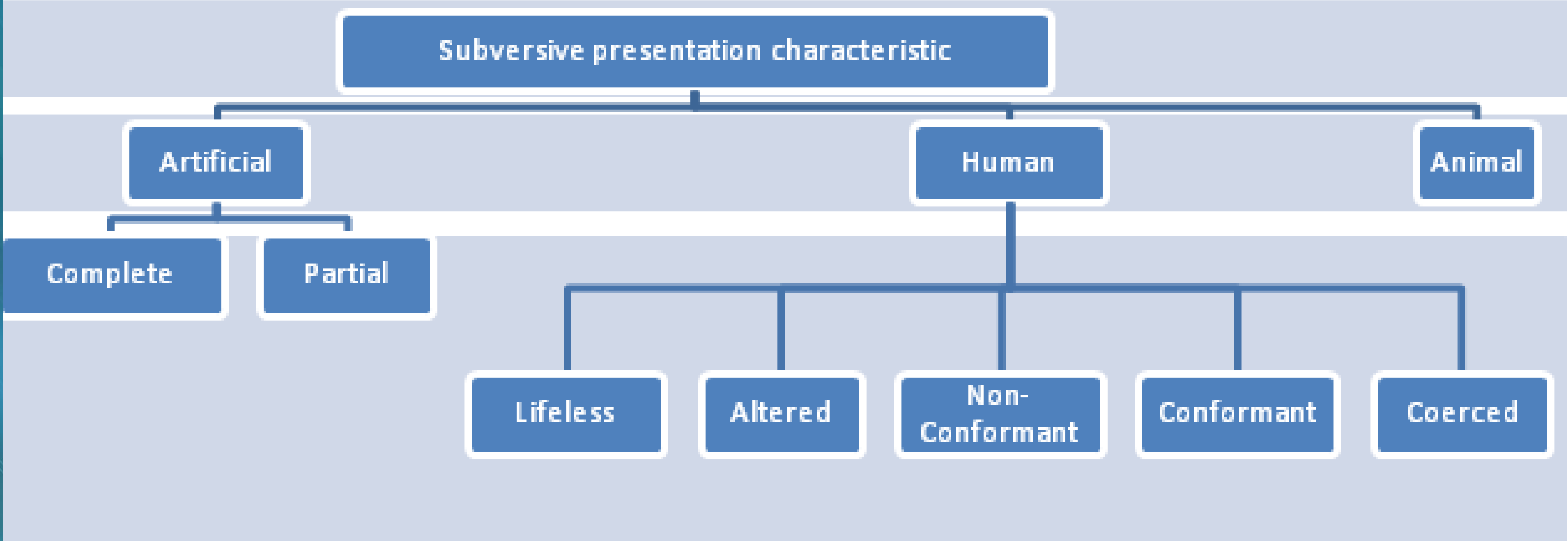
Data / Data Formats (for Metrics)

Measurement/ Evaluation

QPL, Validation, or Certification Program

High Confidence in factors available to consumers for authentication (and access) over open networks

Types of Biometric “Spoofing”



Subversive presentation characteristic

Artificial

Human

Animal

Complete

Partial

Lifeless

Altered

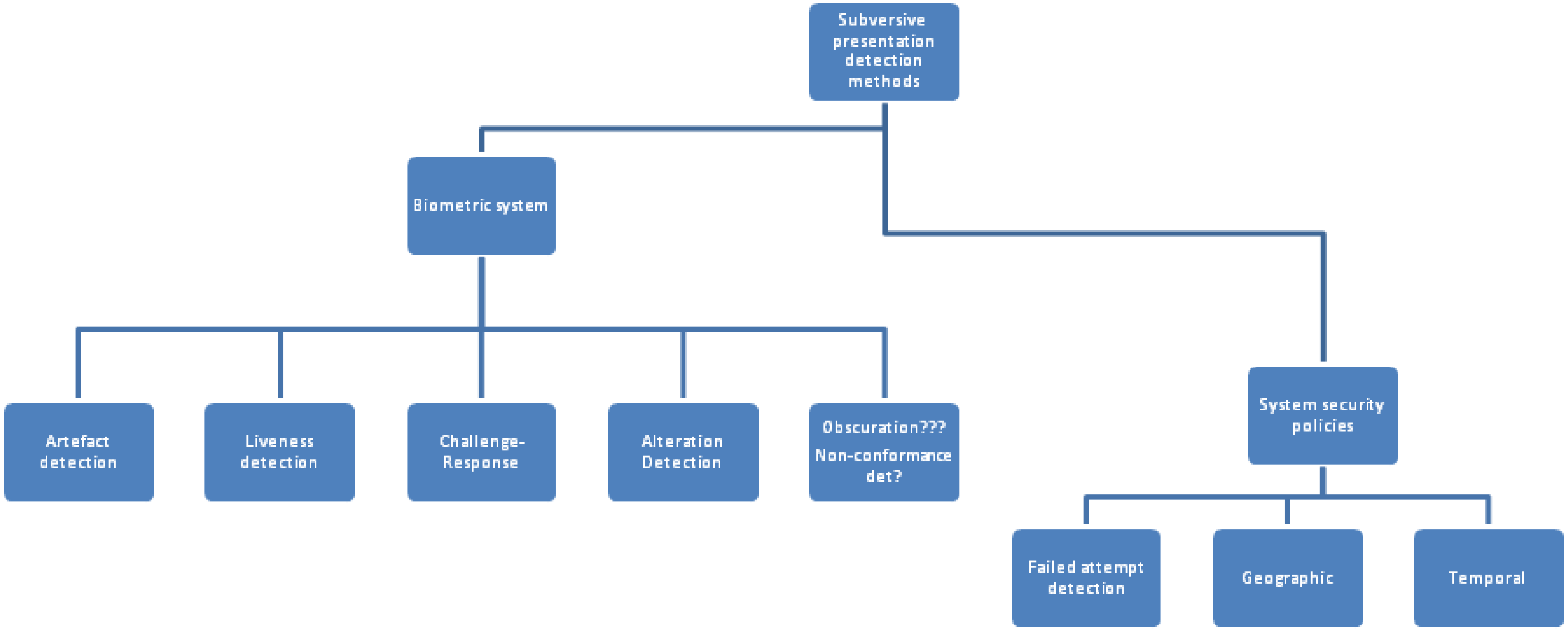
Non-Conformant

Conformant

Coerced

From the 2nd Working Draft of IS Project 30107

Types of Detection



Subversive presentation detection methods

Biometric system

Artefact detection

Liveness detection

Challenge-Response

Alteration Detection

Obscuration???

Non-conformance det?

System security policies

Failed attempt detection

Geographic

Temporal

From the 2nd Working Draft of IS Project 30107

Data Fields for Detecting Subversive Presentations*

a) whether the capture device provides artefact/liveness detection [locally, where a one indicates the existence of artefact/liveness detection (one-byte-block)];

b) the generic [or normalized] artefact/liveness detection threshold used in capture (i.e. the sensitivity level at the time of the presentation) (one-byte-block);

c) the technique-specific artefact/liveness detection threshold used in capture (i.e. the sensitivity level at the time of the presentation) (one-byte-block);

**From the 2nd Working Draft of IS Project 30107*

Data Fields for Detecting Subversive Presentations* (cont.)

d) a local decision on aretefact/liveness detection, where a zero indicates failure to pass aretefact/liveness detection (one-byte block);

e) a confidence score between 0 and 100, where higher values indicate higher likelihood of a live (or non-spoofed) sample, or a value of 255 indicating failure to compute (one-byte block);

f) technique specific data (1 byte) and their units (1 byte) (two-byte block); and/or

g) the level of supervision / surveillance during capture [denoted by the number for the condition in Table 3 (one-byte-block)].

In addition to: vendor ID, algorithm ID, and sensor ID.

How to Participate in the Development of 30107

- In the US, interested parties should join INCITS M1
  - http://standards.incits.org/a/public/group/m1

- In other countries, interested parties should participate in their country's Technical Advisory Group (TAG) to ISO/IEC JTC1 SC37

Biometric Template Protection

Methods for protecting biometric data from misuse, such as linking data subjects' records across databases and impersonation

- Need for metrics to evaluate algorithms incorporating both the security properties and accuracy
  - Biometric Performance
  - De-Identification
  - Irreversibility
  - Others

http://collaborate.nist.gov/twiki-secbiotemp/

Multi-Factor Authentication (MFA) Initiative

- Supported by the Comprehensive National Cybersecurity Initiative (CNCI)
  - Objective:

    To improve cyber security through strengthening authentication assurance by
    - Advancing multi-factor authentication
    - Shifting the predominance of the username-password paradigm for online transactions
    - Addressing major gaps for remote authentication for higher risk online transactions

Thank you

Questions?

Elaine Newton, PhD

elaine.newton@nist.gov

1-301-975-2532