

Overview of the ISO/IEC 30107 Project

Anti-Spoofing and Liveness Detection Techniques

Elaine Newton, PhD
NIST

elaine.newton@nist.gov

1-301-975-2532



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

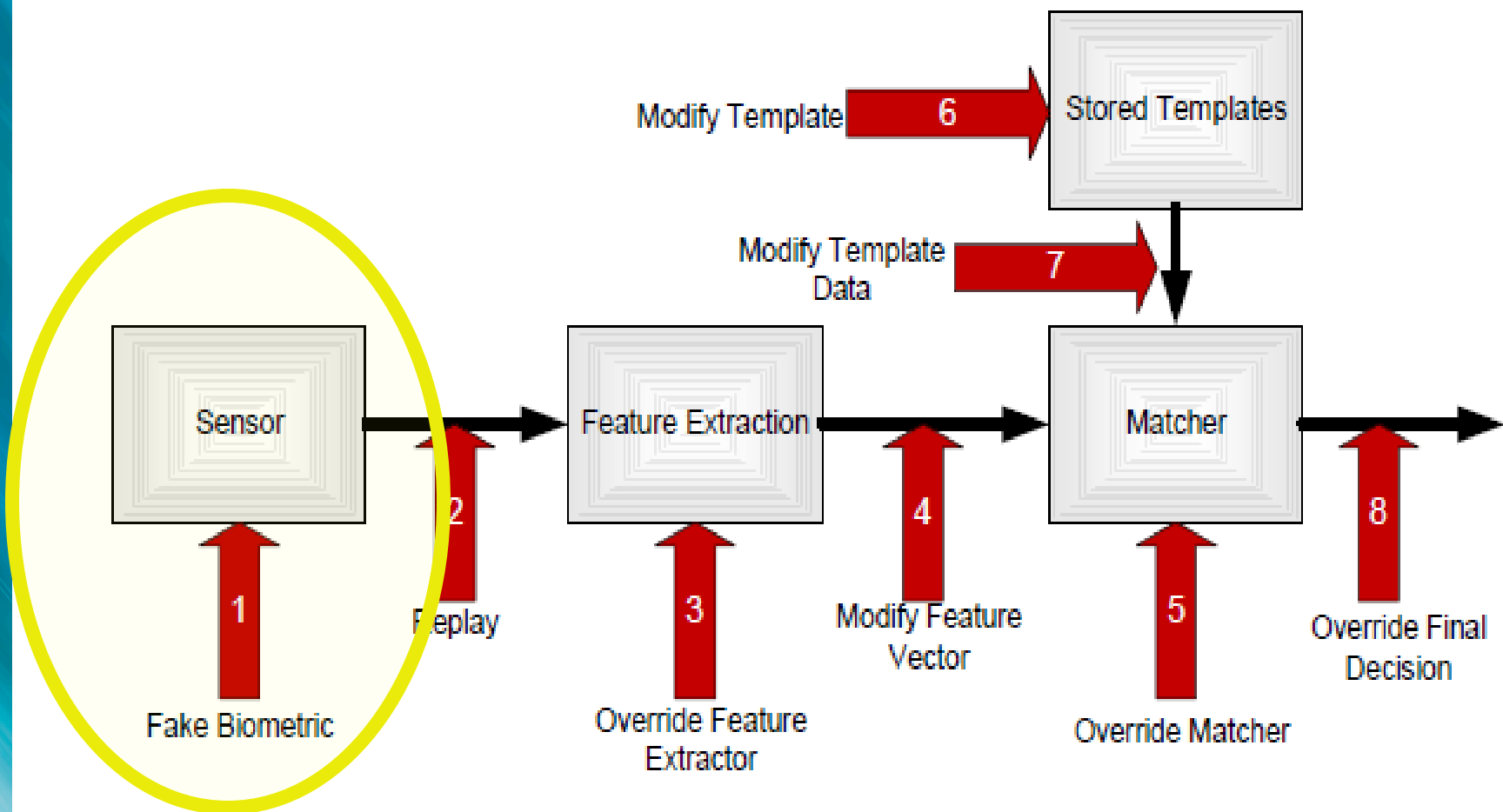


Figure by Nalini Ratha, IBM, 2001



We're not in Kansas anymore...

- Increasing use of online and mobile apps and need for more complex & secure ID management
 - Exemplified by the National Strategy for Trusted Identities in cyberspace, released April 2011
- Recognized need by groups of potential users:
 - Financial Services Technology Consortium
 - The Drug Enforcement Administration (DEA)
 - The US National Science and Technology Council report on the “The National Biometrics Challenge.”

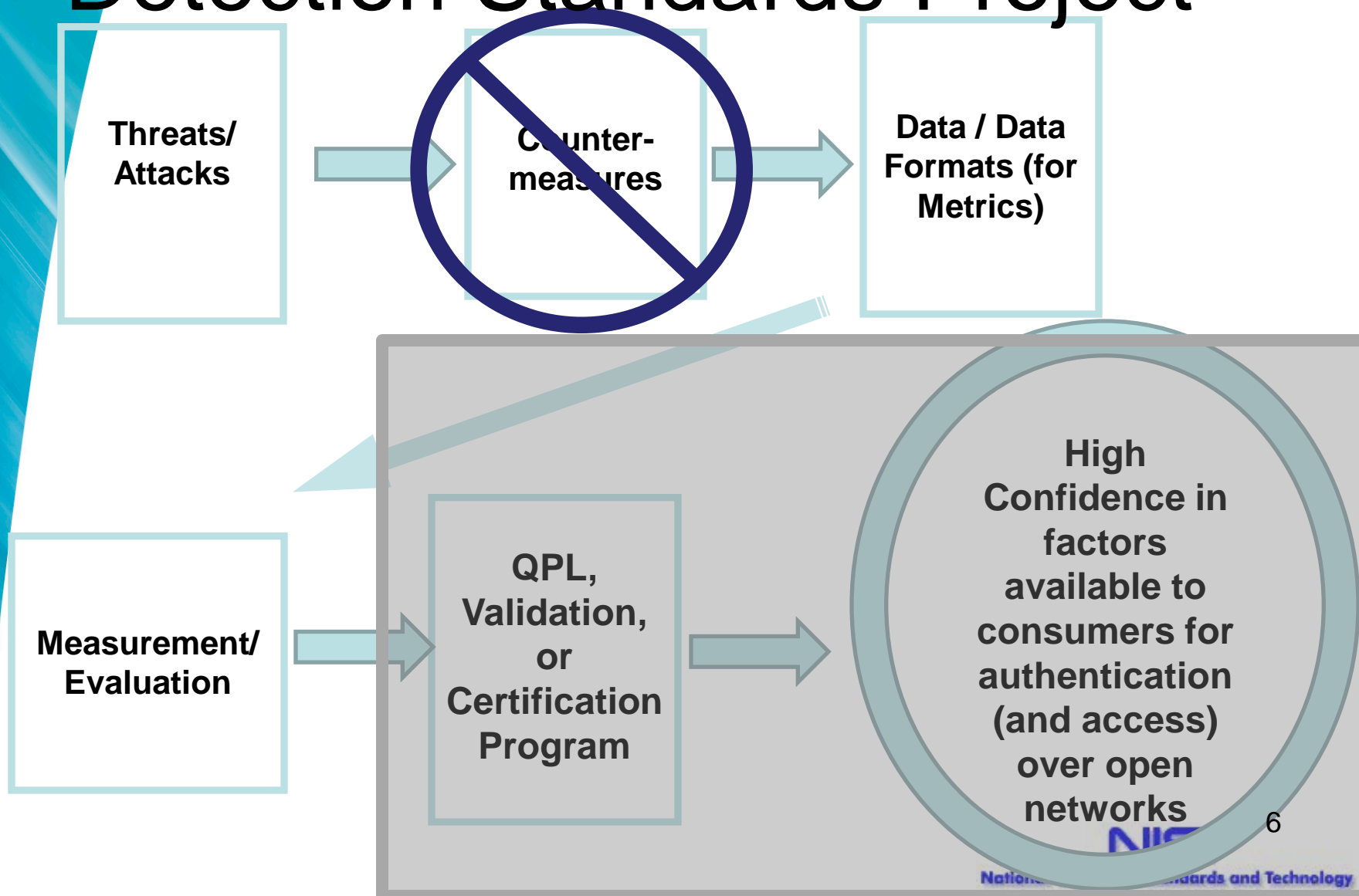


Remote Authentication in the US Federal Government

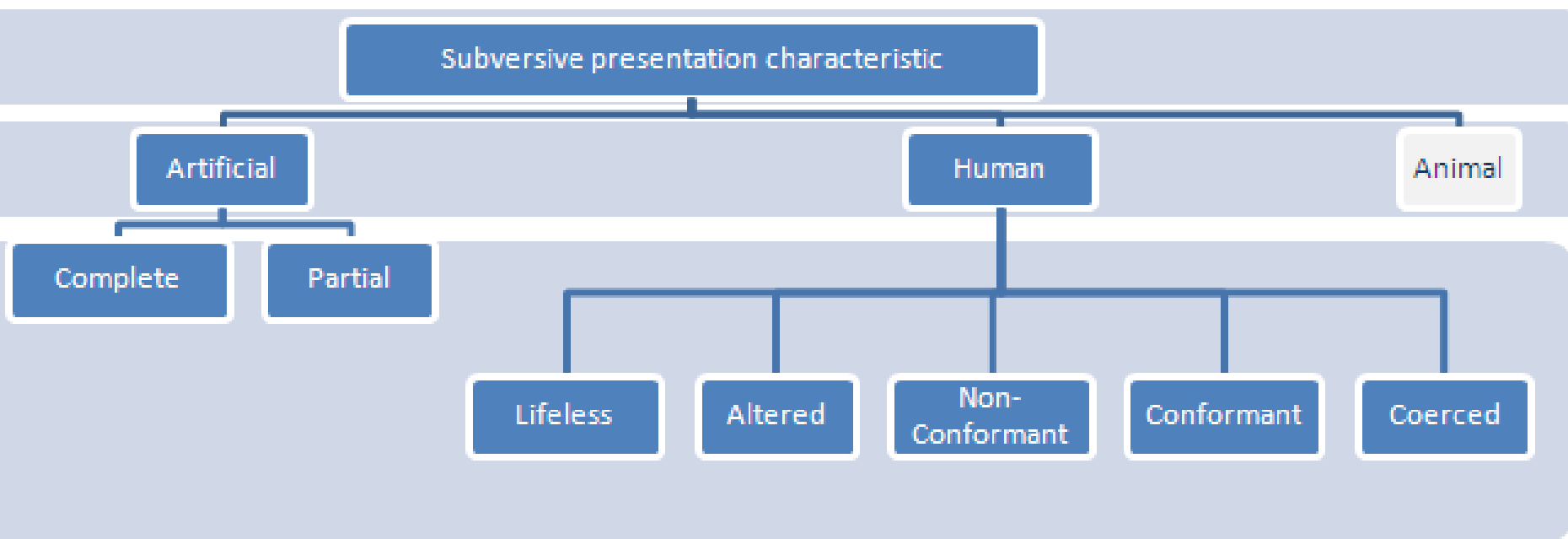
- NIST Special Pub 800-63-1 provides technical requirements for remote authentication over an open network
- Four Assurance Levels, ranging from low or no confidence (1) to very high confidence (4) in the claimant's identity
- Framework is based on secrets; Biometrics are not included in authentication protocols in this guidance.
- Adopted outside of the USG and in the final stages of being standardized in ISO/IEC JTC 1 SC 27 and ITU-T SG17 (jointly)



Anti-Spoofing/Liveness Detection Standards Project



Types of Biometric “Spoofing”*



From the 3rd Working Draft of IS Project 30107

Types of Detection

<i>Through a biometric system</i>	Artefact Detection
	Liveness Detection
	Challenge-Response
	Alteration Detection
	Non-conformance Detection
	Coercion Detection
	Obscuration Detection
<i>Through system security policies</i>	Failed attempt detection
	Geographic
	Temporal

From the 3rd Working Draft of IS Project 30107

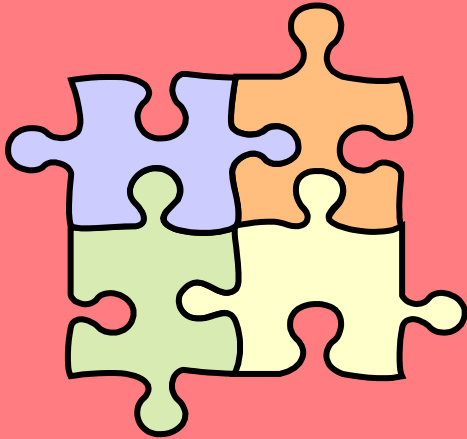
Examples of Data Fields for Detecting Suspicious Presentations*

- Is there a local check for SPD (yes/no)?
- The local SPD decision (pass/fail)
- A score between 0 and 100 provided by the spoof detection mechanism, with lower scores being indicative of spoofed samples
- technique specific data and their units;
- level of supervision / surveillance during capture (qualitative categories)

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

Topics for Discussion

Terms & Concepts



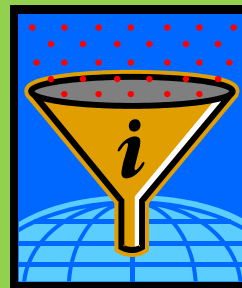
Metrics for Recognition Decisions



Testing Principles



Evaluation Metrics



Up Next...

- Rick Lazarick, CSC, Co-editor of ISO/IEC 30107
 - Spoofs, Subversion & Suspicion: Terms and Concepts
- Stephanie Schuckers, Clarkson University, and Arun Ross, West Virginia University
 - Error rate metrics proposed for detection of suspicious presentations to biometric authentication systems.
- Ralph Breithaupt, BSI
 - Need and perspectives to realize liveness detection
- Axel Munde, BSI
 - How can artifact detection complement common criteria and other security assessments of authentication systems



How to Participate in the Development of 30107

- In the US, interested parties participate through INCITS M1
 - <http://standards.incits.org/a/public/group/m1>
- In other countries, interested parties participate in their country's Technical Advisory Group (TAG) to ISO/IEC JTC1 SC37

Thank you & Safe Travels

Elaine Newton, PhD

elaine.newton@nist.gov

1-301-975-2532