

Common Criteria Evaluations for the Biometrics Industry

Kathy Malnick

**Senior Manager
Criterion Independent Labs**

An initiative of the WVHTC Foundation



Presentation outline

- Common Criteria defined
- Common Criteria importance
- Evaluation process
- Biometric relevance
- Summary



Common Criteria defined

- A set of functional and assurance security requirements internationally developed to provide a common baseline
- ISO 15048
- Applied by accredited independent test labs (CCTLs) around the world
- The National Information Assurance Partnership (NIAP) is the governing body for all CCTLs in the U.S.
- Certificates issued by NIAP will be recognized around the world



Types of Common Criteria evaluations

- Categories of Evaluations



Protection
Profile

*Security
Target

Evaluation
Assurance
Levels
(EALs)

- * Typically as the first step in an EAL.

The meaning of an evaluation

- Not a claim of how good a product works.
- Is verification that the claims made in the ST were verified by an independent lab using proof supplied by the developer and tested by the lab.
- EAL4 with 2 claims in the ST does not equal an EAL4 with 10 claims in the ST
- Buyer beware!

Regulations in the United States

- **NSTISSP #11**
 - As of July 2002, all new IT product purchases for use in national security systems must be evaluated and validated under the Common Criteria.
- **DoD 8500.1 & DoD 8500.2**
 - “All IA ... components... incorporated into DoD information systems must comply with ... [NSTISSP #11] ...”
 - “... product validation will be maintained...”
 - ... restricts purchases, especially if an approved protection profile (PP) exists
- **National IA Acquisition Policy (DoD)**
 - Minimum EAL2 for products not yet evaluated



Common Criteria participating countries

- **Certificate producing countries**

- Australia
- New Zealand
- Canada
- France
- Germany
- United Kingdom
- United States

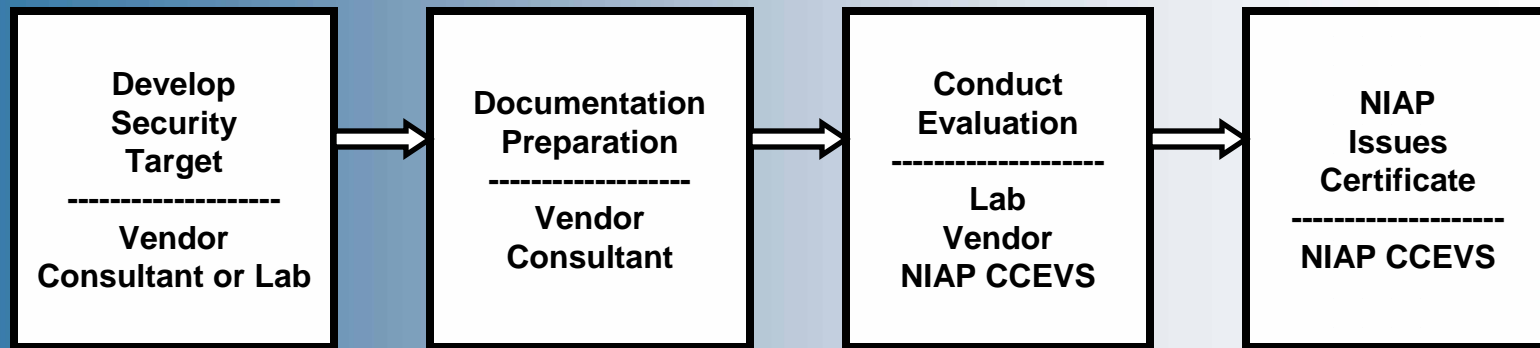
- **Certificate consuming countries**

- Austria
- Finland
- Greece
- Israel
- Italy
- Netherlands
- Norway
- Spain
- Sweden

Common Criteria importance

- **Why evaluate under CC?**
 - Government requirements
 - New Customers
 - International markets
 - Government agencies
 - Consumer confidence and vendor credibility
 - Independently-certified products
 - Internal benefits
 - Improved development processes
 - Improved delivery and installation process
 - Improved documentation

The evaluation process



- Work not necessarily performed by the CCTL:
 - Documentation preparation
 - Writing the Security Target
 - Other consulting

Required evaluation materials

- Security Target
- TOE (target of evaluation)
- Configuration Management documentation
- Functionality Specification
- High and low level design documentation
- User and Administrator's guides
- Life-cycle documentation
- Development tool documentation
- Security Policy model
- Correspondence analyses
- Installation and start-up procedures
- Delivery procedures

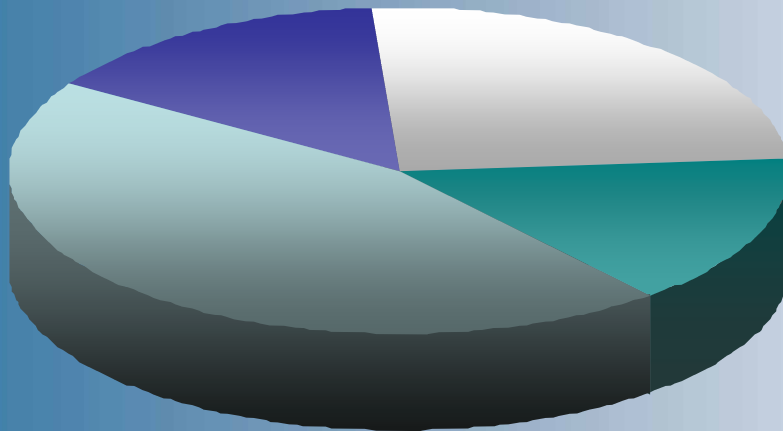
Results of the evaluation process

- Outcomes of Common Criteria Testing



- In U.S. this follows approval of lab test results
- Public posting of ST, validation report, and certificate

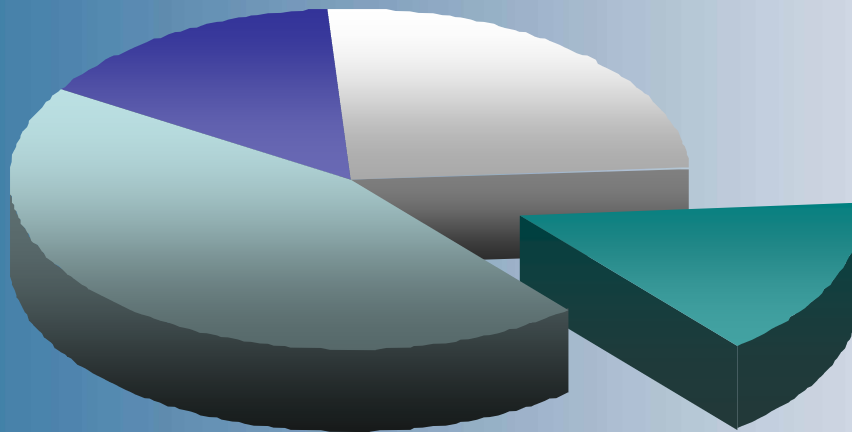
Testing of biometric attributes



- Technical Performance**
- Social Acceptance**
- Business Risk and Benefits**
- Trust of System Security**

Adapted from Biometric Testing Best Practices, Version 2.01

Common Criteria evaluations

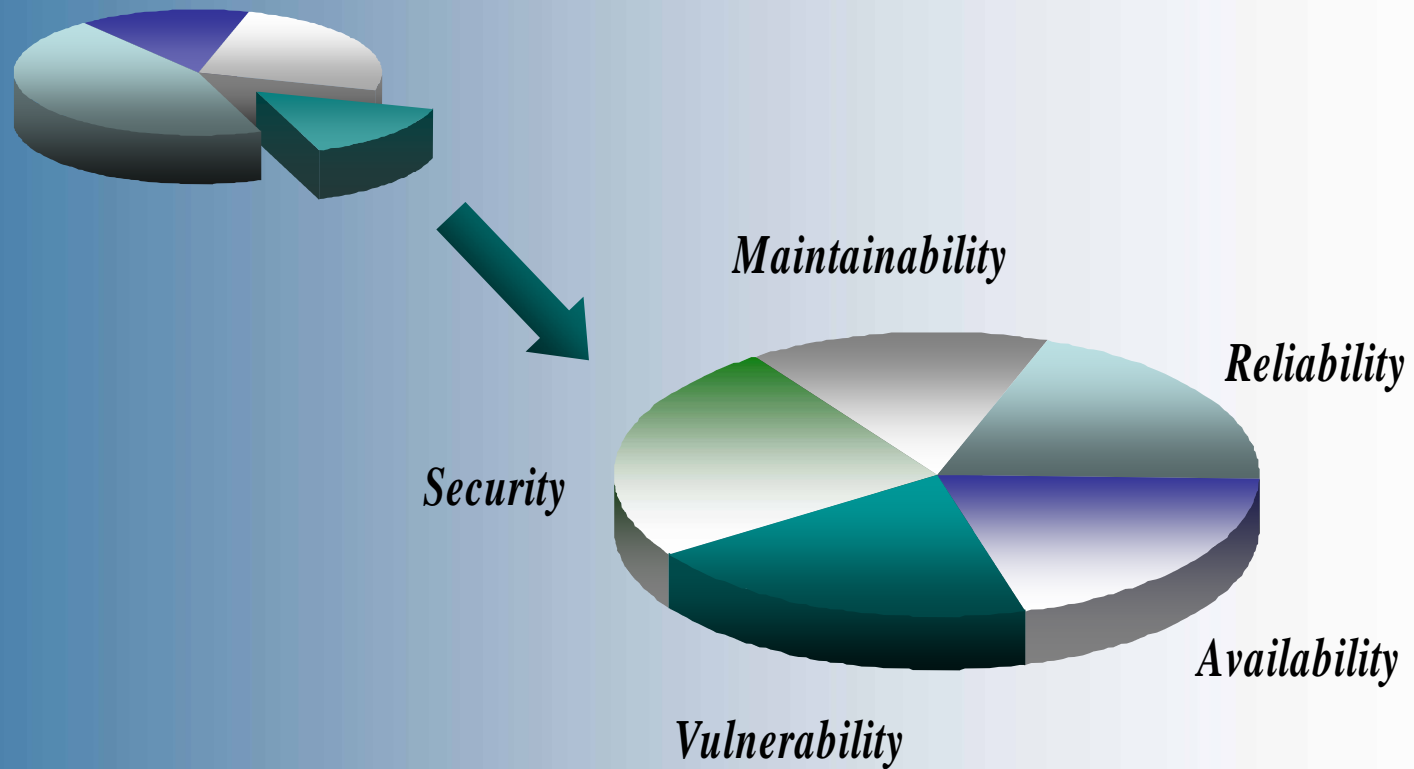


- **Technical Performance**
- **Social Acceptance**
- **Business Risk and Benefits**
- **Trust of System Security**

Adapted from Biometric Testing Best Practices, Version 2.01

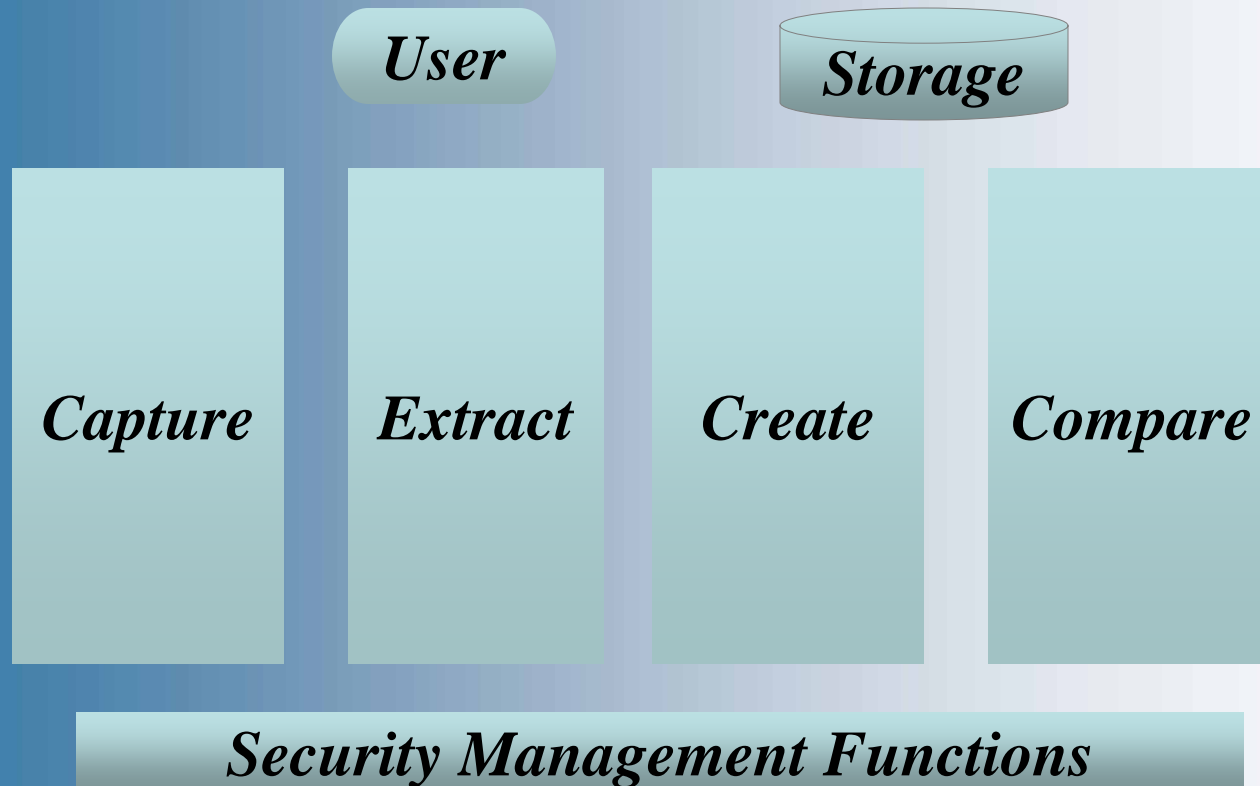
Common Criteria evaluations

- Technical Performance
- Social Acceptance
- Business Risk and Benefits
- Trust of System Security



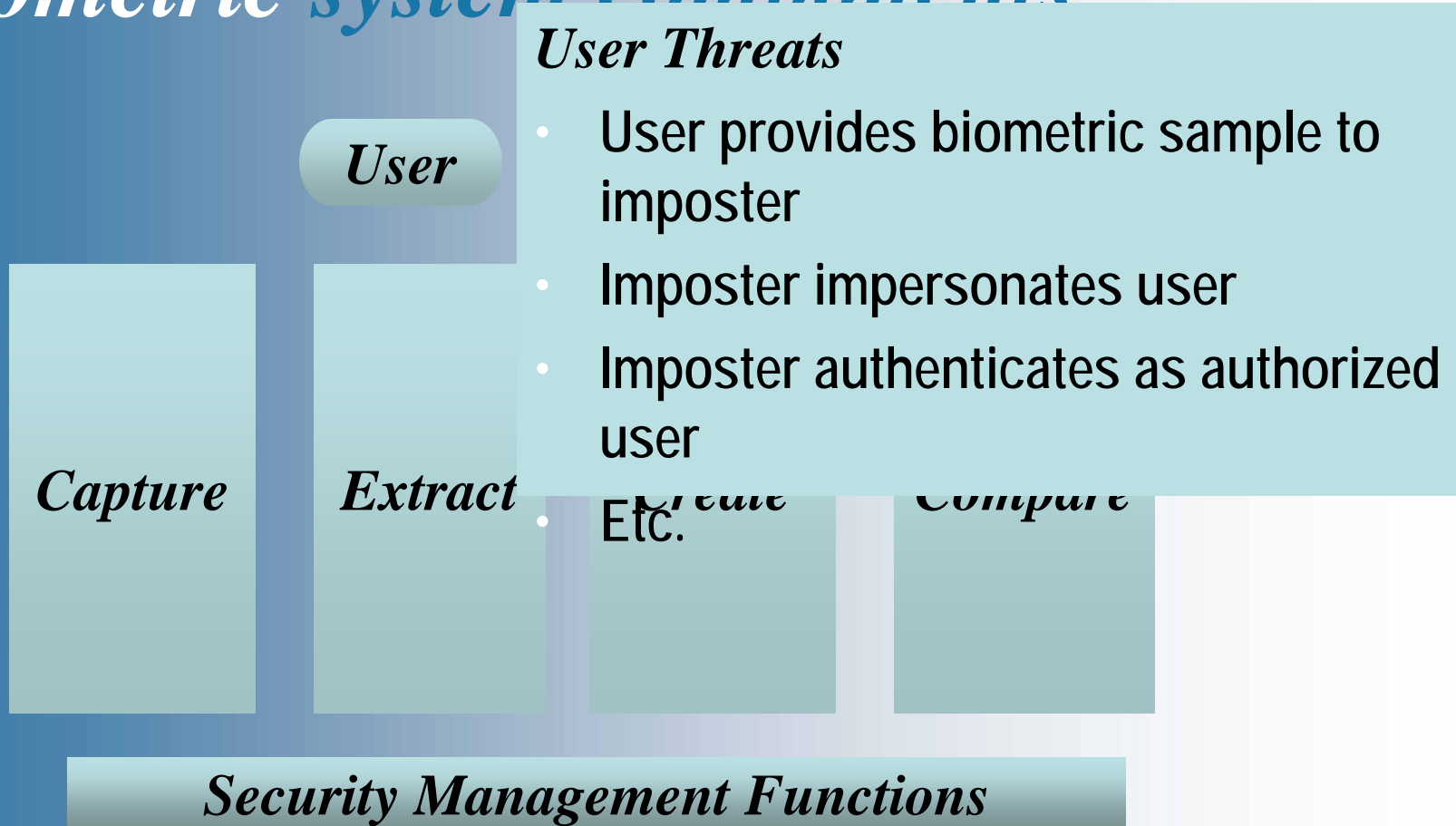
Adapted from Biometric Testing Best Practices, Version 2.01

Biometric system components



Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric system components



Adapted from Biometric Evaluation Methodology, Version 1.0

Storage Threats

- **Template Storage Threats**
 - Imposter steals template
 - Attacker modifies or deletes template
- **Template Retrieval Threats**
 - Imposter intercepts template during transmission to/from storage
- **Etc.**

Components



Create

Compare

Security Management Functions

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric system components

User

Storage

Capture

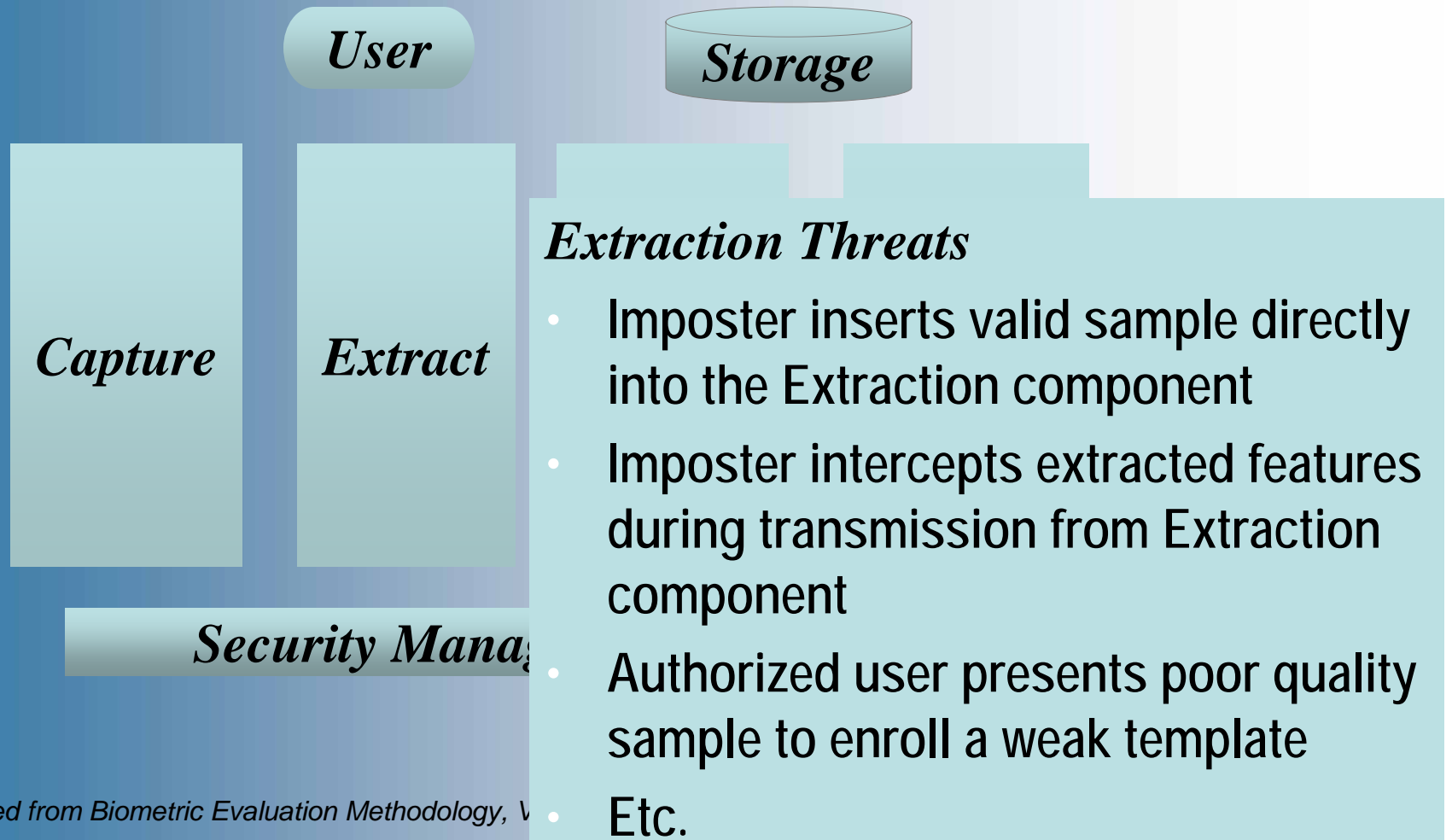
Capture Threats

- Imposter utilizes residual image to impersonate a valid user
- Imposter presents artificial biometric sample
- Imposter bypasses the Capture system
- Etc.

Sec

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric system components



Adapted from Biometric Evaluation Methodology, V

Biometric system components

User

Storage

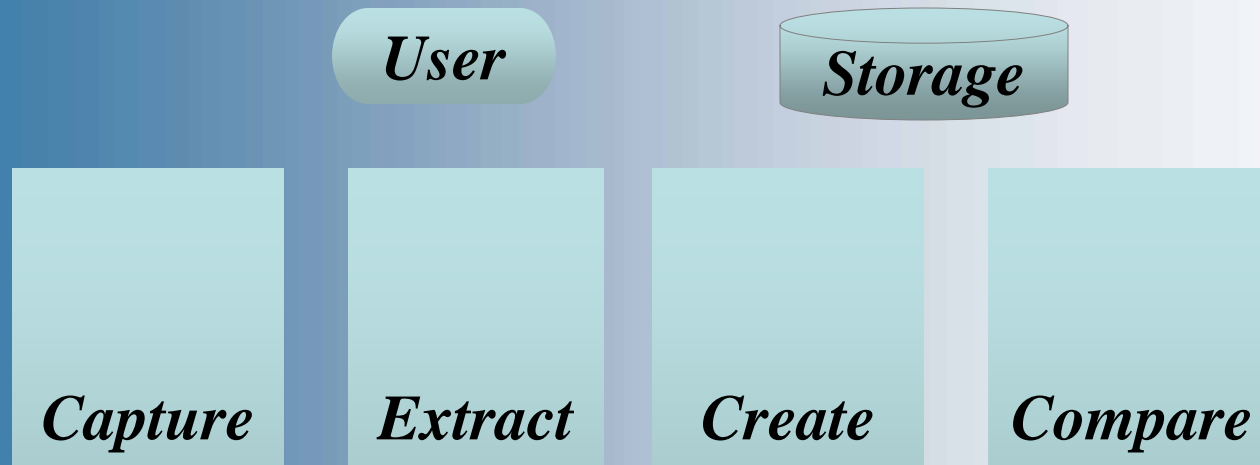
Compare

Creation Threats

- Unauthorized user is enrolled
 - Administrator error
 - Authorized user template intercepted and replaced with imposter during enrollment
- Etc.

actions

Biometric system components

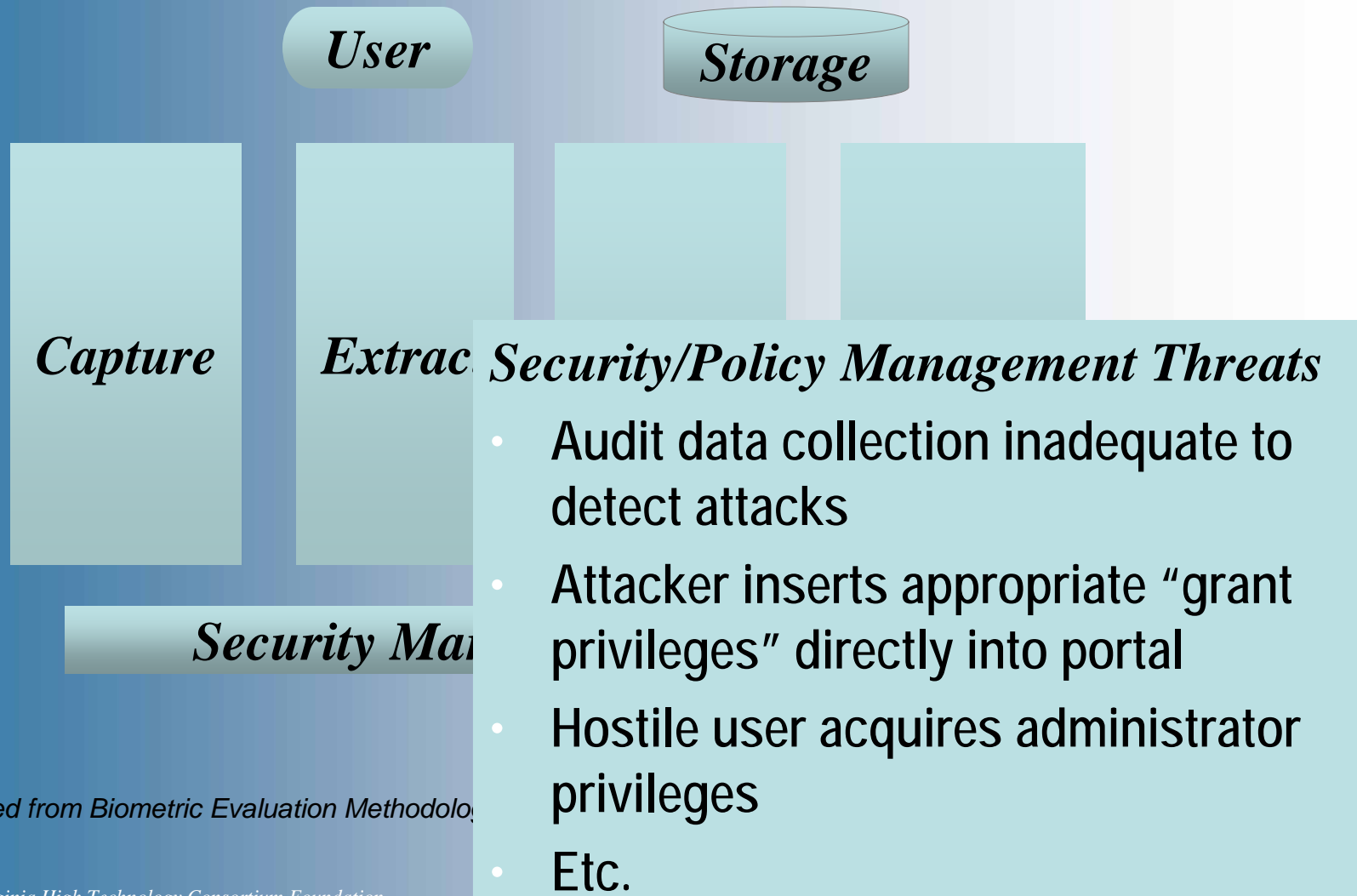


Comparison Threats

- Imposter inserts extracted features directly into the Comparison component
- Etc.

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric system components



Adapted from Biometric Evaluation Methodology

Biometric system concerns and threats

- **Threats to hardware components**
 - Attacker tampers, modifies, bypasses or deactivates
 - Attacker exploits design flaws
- **Threats to software/firmware components**
 - Attacker exploits algorithm quirk or failure mode
 - Attacker introduces virus into the system
- **Threats to all connections (including network threats)**
 - Imposter intercepts sample or template during transmission between components
- **Etc.**

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric evaluations

- **Development documentation**
 - Consider use of biometric standards
- **Guidance documentation**
 - Consider how privacy issues are documented
 - Consider how environmental factors are documented
 - Consider how threshold settings are described and documented

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric evaluations

- **Testing**
 - Requires performance testing
 - Requires verification of environmental “configuration”
- **Vulnerability Assessment**
 - Misuse: Consider system modes and environmental documentation
 - Strength of Function: Consider FAR and FRR in correct identification of user
 - Vulnerability Analysis: Consider vulnerabilities particular to biometric systems

Adapted from Biometric Evaluation Methodology, Version 1.0

Biometric protection profiles

- *Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 0.8, June 8 2003*
 - Status: Draft form; comments were due by August 24, 2003
 - Addresses: verification versus identification for Basic Robustness environments
 - No protection afforded to the biometrics package by the TOE
 - Protection must be provided by the IT environment
 - Developers can claim PP conformance if product only operates in verification mode
 - Developers can claim conformance to 2 PPs if product operates in verification mode and identification mode



Biometric protection profiles

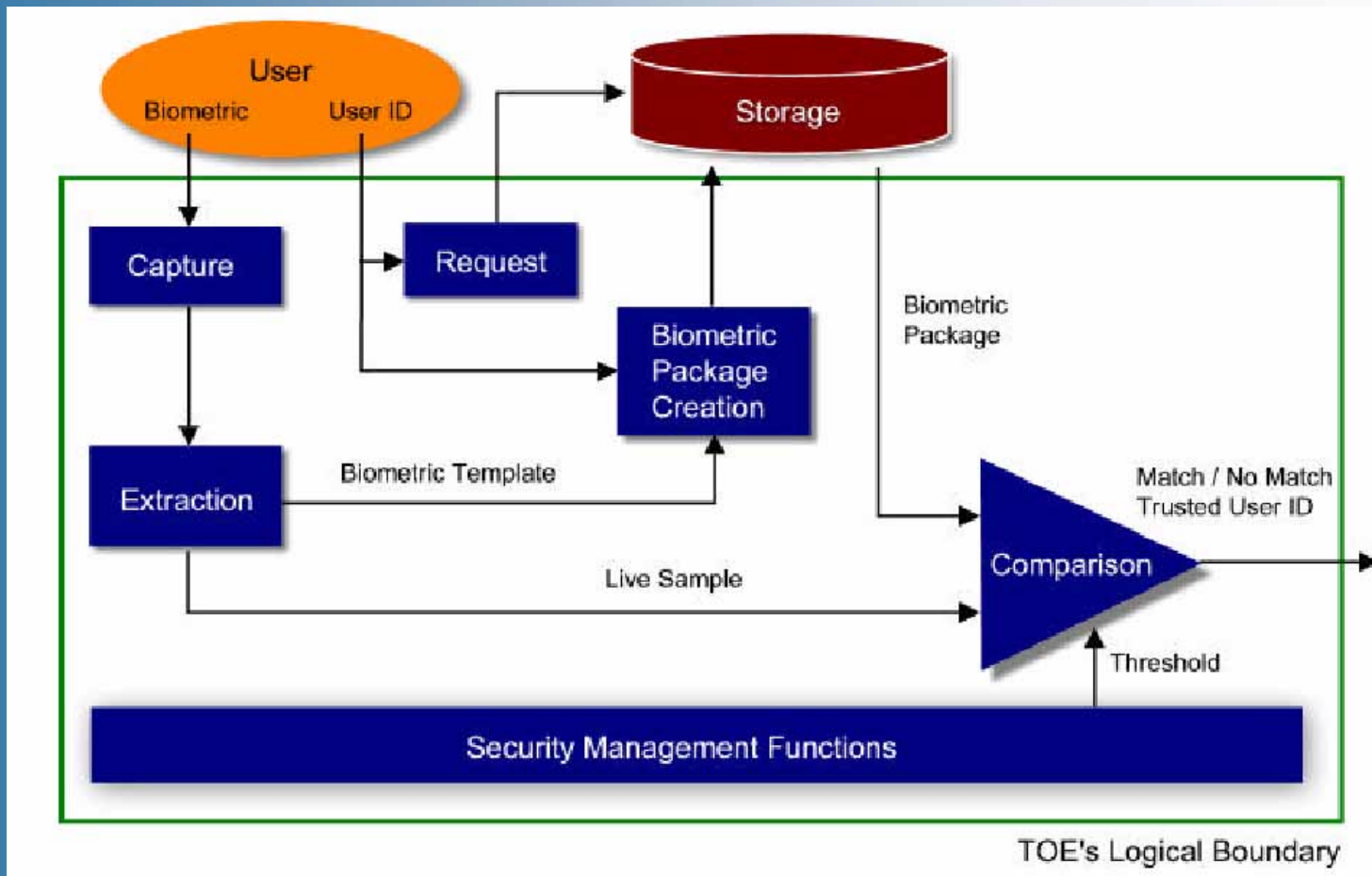


Figure from Draft Biometric Verification Mode Protection Profile for Basic Robustness Environments, Version 0.8

Biometric protection profiles

- *Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 0.5, December 12, 2002*
 - Status: In evaluation
 - Addresses: verification versus identification for Medium Robustness environments
 - Requires cryptography to protect biometrics packages
 - Does not rely on the environment to address threats or enforce security policies
 - More stringent assurance requirements than the basic robustness PP
 - Same conformance claims as Basic PP



Biometric protection profiles

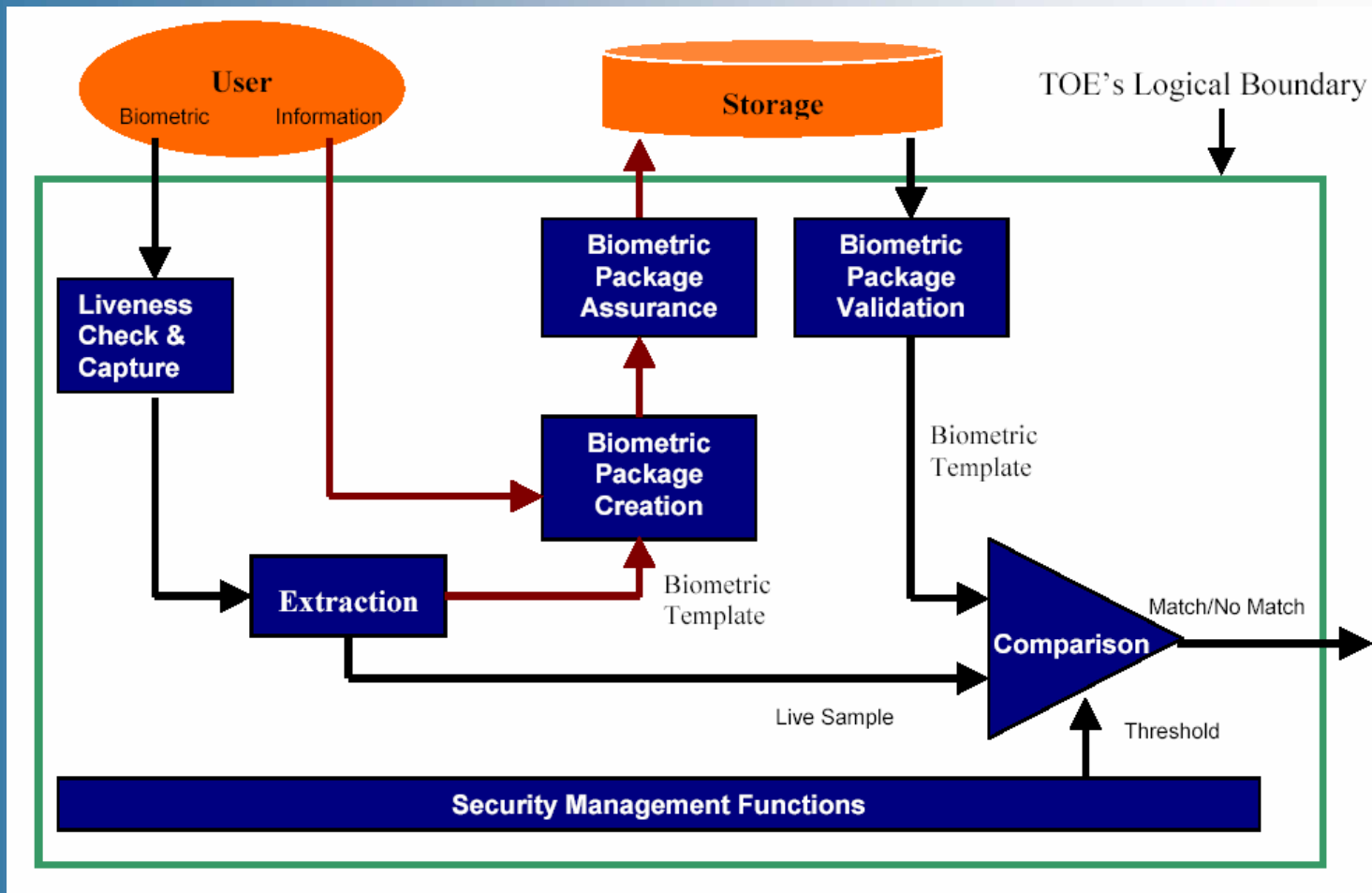


Figure from Draft Biometric Verification Mode Protection Profile for Medium Robustness Environments, Version 0.5

Biometric evaluations

- **Challenges**
 - Specific threats and vulnerabilities
 - Similar biometrics
 - Statistical performance tests
 - Test population
 - Environmental factors
 - Privacy issues



Summary

- The Common Criteria are an international set of evaluation criteria
- The Common Criteria are important in the U.S. because the DoD and other agencies are requiring evaluations for many purchases
- The Common Criteria are important in the international community because evaluation certificates received from any lab are recognized worldwide
- The Common Criteria can be applied to biometric products taking into account the unique challenges of biometric technology



Additional information

- International Common Criteria website:
<http://www.commoncriteria.org>
- United States Common Criteria website:
<http://www.niap.nist.gov/cc-scheme>
- Biometrics Evaluation Methodology document:
<http://www.cesg.gov.uk/site/ast/index.cfm?menuSelected=4&displayPage=4>

Contact

Kathy Malnick
Senior Manager

contact@criterionlabs.org

(304) 368-4516

(877) 408-5767

www.criterionlabs.org



An Initiative of the WVHTC Foundation

This slide intentionally left blank

Backup Slides

Selecting an EAL for a product

- Value of the assets
- Risk of the assets being compromised
- Current state of practice
- Development, evaluation and maintenance costs
- Resources of “adversaries”
- Functional requirement dependencies
- Security Objectives

Common Criteria Evaluations

Evaluation Materials from the vendor

EAL1 Evaluation – “basic” level of assurance

Security Target

Target of Evaluation (TOE) suitable for testing; TOE = all or part of a product

Administrator Guidance

Secure installation, generation, and start-up procedures

Functional Specification

User Guidance

Correspondence Analysis between the TOE summary specification and the functional specification



Common Criteria Evaluations

Evaluation Materials from the vendor

EAL2 Evaluation –

“low to moderate” level of assurance

Same as EAL1, plus:

Configuration management documentation

Delivery documentation

High-level design

Test documentation

Correspondence analysis between the functional specification and the high-level design

Test coverage evidence

Test procedures

Test coverage analysis

Strength of TOE Security Function analysis

Vulnerability analysis

Strength of function (SOF) claims analysis



Common Criteria Evaluations

Evaluation Materials from the vendor

EAL3 Evaluation – “moderate” level of assurance

Same as EAL2, plus

Development security documentation

Depth of testing analysis



Common Criteria Evaluations

Evaluation Materials from the vendor

EAL4 Evaluation – “moderate to high” level of assurance

Same as EAL3, plus:

Low-level design

Subset of implementation representation

Correspondence analysis between high-level and low-level design

Correspondence analysis between low-level design and the subset of implementation representation

TOE security policy model

Life cycle definition

Life cycle definition documentation

Development tool documentation

Misuse analysis of the guidance



Common Criteria Evaluations

Evaluation Steps

EAL2 (est. 4-6 months @ 2 evaluators and part of technical lead)	
Step	# of sub-steps
Evaluation Input Task	2
Evaluation of the Security Target (ST)	78
Evaluation of the configuration management	7
Evaluation of the delivery and operation documents	5
Evaluation of the development documents	20
Evaluation of the guidance documents	14
Evaluation of the tests	12
Testing	11
Evaluation of the vulnerability assessment	18
Evaluation Output Task	2
TOTAL	159



Common Criteria Evaluations

Evaluation Steps

EAL4 (est.10-12 months @ 2 evaluators and part of technical lead)

Step	# of sub-steps
Evaluation Input Task	2
Evaluation of the Security Target (ST)	78
Evaluation of the configuration management	26
Evaluation of the delivery and operation documents	7
Evaluation of the development documents	49
Evaluation of the guidance documents	14
Evaluation of the life cycle support	9
Evaluation of the tests	20
Testing	11
Evaluation of the vulnerability assessment	34
Evaluation Output Task	2
TOTAL	242

