

ISO/IEC 19989-3:2020 (E)

Information security — Criteria and methodology for security evaluation of biometric systems — Part 3: Presentation attack detection

Contents

	Foreword
	Introduction
1	Scope
2	Normative references
3	Terms and definitions
4	Abbreviated terms
5	General remark
6	Overview of PAD testing in Class ATE and Class AVA
6.1	Objectives and principles
6.1.1	Class ATE
6.1.2	Class AVA
6.2	PAIs used in testing activities
6.2.1	Class ATE
6.2.2	Class AVA
6.3	Testing activities
6.3.1	Class ATE
6.3.2	Class AVA
6.4	Criteria of pass/failure
7	Supplementary activities to ISO/IEC 18045 on tests (ATE)
7.1	Testing approach toward PAD
7.2	Metrics for PAD testing
7.2.1	General
7.2.2	Metrics used for PAD subsystem TOEs
7.2.3	Metrics used for data capture subsystem TOEs
7.2.4	Metrics used for other TOEs
7.3	Minimum test sizes and maximum error rates
8	Supplementary activities to ISO/IEC 18045 on vulnerability assessment (AVA)
8.1	Penetration testing using PAI variations
8.2	Potential vulnerabilities
8.3	Rating of vulnerabilities and TOE resistance
Annex A	(informative) Examples of calculations of attack potential
A.1	General
A.2	Example 1 — Simple system without presentation attack detection
A.3	Example 2 — Fingerprints with presentation attack detection
A.4	Example 3 — Fingerprints with advanced presentation attack detection
A.5	Example 4 — 3D Face with presentation attack detection and try counter
A.6	Example 5 — Wolf attack