AN EVALUATION OF PRESENTATION ATTACK DETECTION OF FINGERPRINT BIOMETRIC SYSTEMS APPLYING ISO/IEC 30107-3

Ines Goicoechea-Telleria, Belen Fernandez-Saavedra, Judith Liu-Jimenez, Raul Sanchez-Reillo

Carlos III University of Madrid, Spain

International Biometric Performance Conference 2016. Gaithersburg, MD.

Outline

- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

Outline

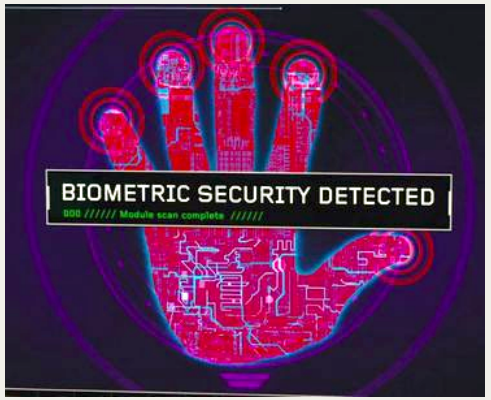
- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

Why, how, what was done?

- **WHY?**

iPhone 5S fingerprint sensor hacked by Germany's Chaos Computer Club

Biometrics are not safe, says famous hacker team who provide video showing how they could use a fake fingerprint to bypass phone's security lockscreen



- **HOW?**

Security evaluations (PAD)

ISO/IEC 30107-3 + Common Criteria

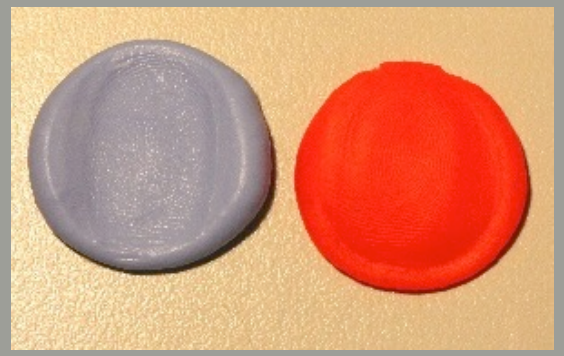
- **WHAT?**

Find vulnerabilities → experiment

Apply ISO/IEC 30107-3

Outline

- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

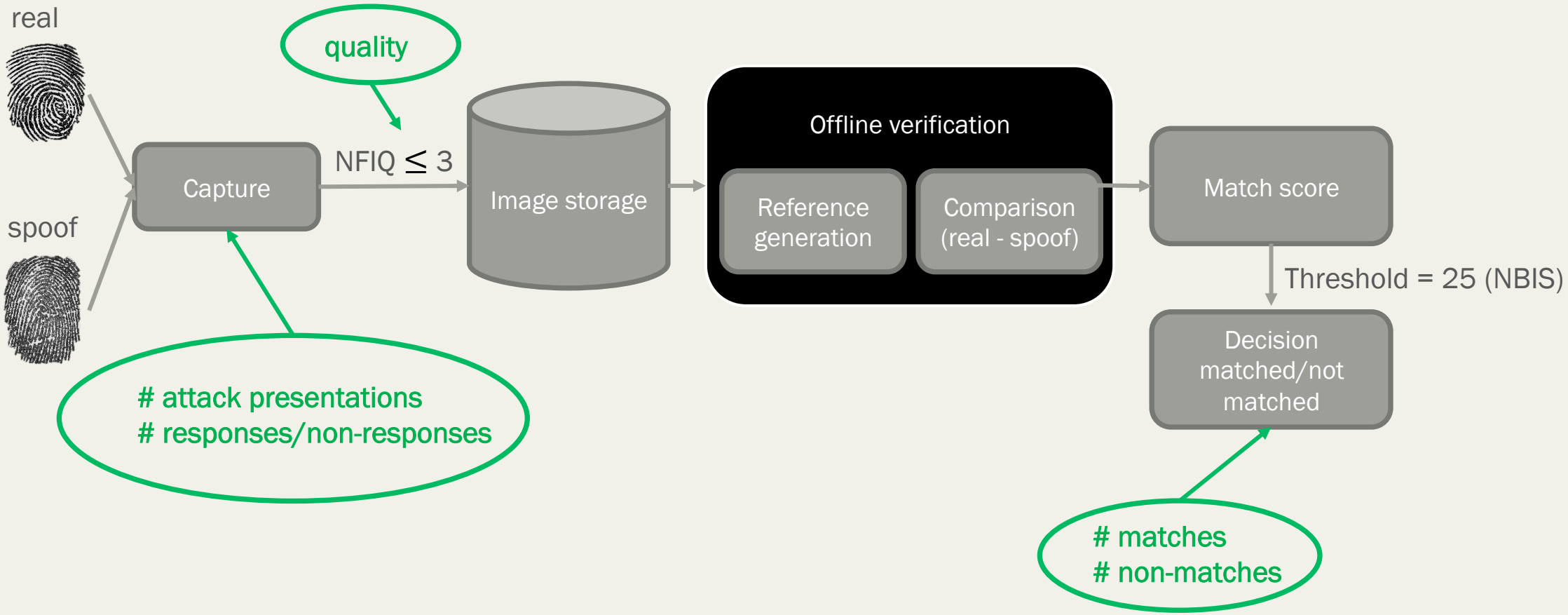


Experiment

- 4 sensors: 1 thermal, 2 capacitive, 1 optical
- 330 + 126 artefacts
- 36 real fingers, 6 capture subjects
- 4672 images
- Cooperative and non-cooperative attacks
- 10 artefact species: Play-Doh (x2), gelatine, latex, silicone, white glue, latex with graphite (x2), silicone with graphite (x2)

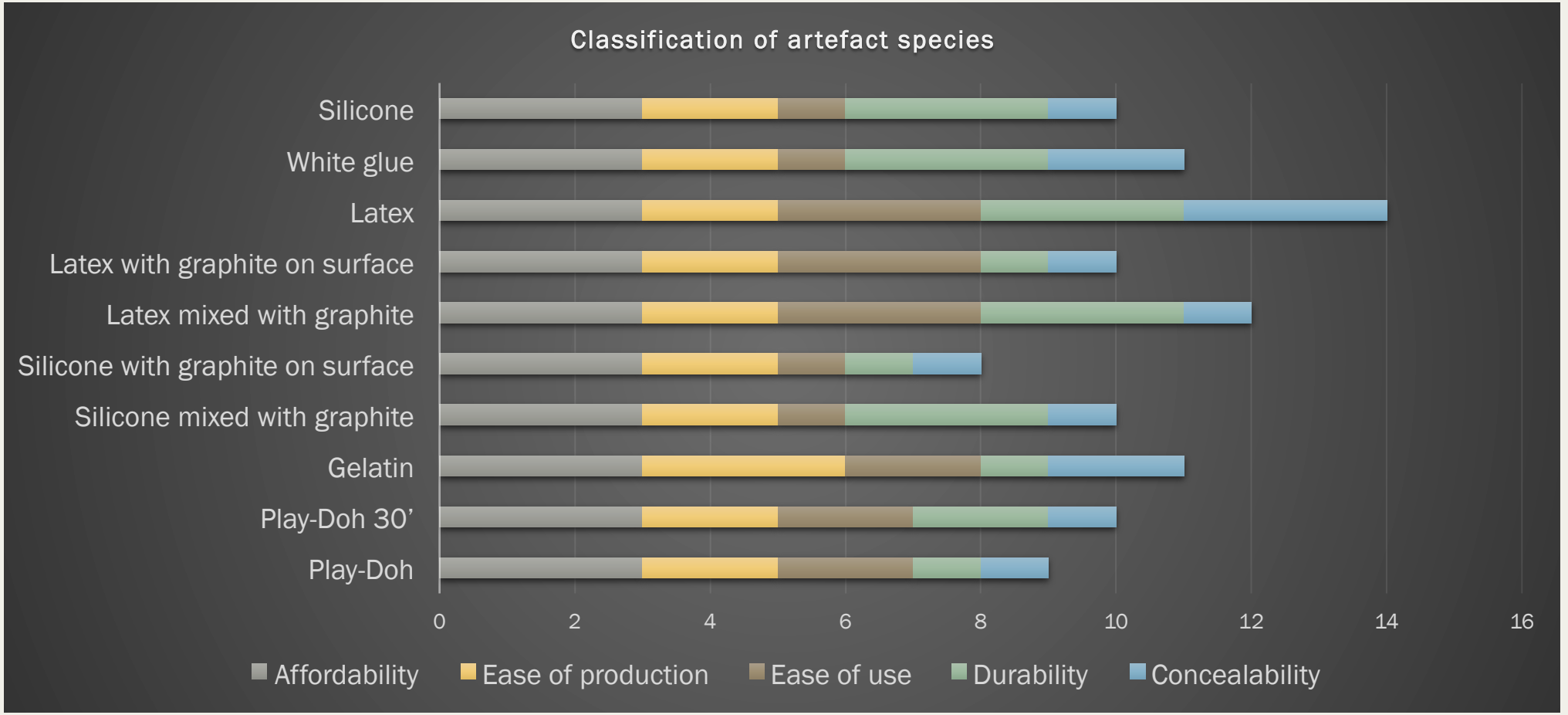
Experiment
Acquisition process

- If sensors respond → more artefacts



Experiment

Classification of artefact species



Outline

- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

Cooperative

Non-cooperative

Before

After

Applying ISO/IEC JTC1 – 30107-3

Artefacts

- Biometric impostor attacks
  - *Artefacts appear natural*
  - *Extractable features*

Select adequate materials for artefact species

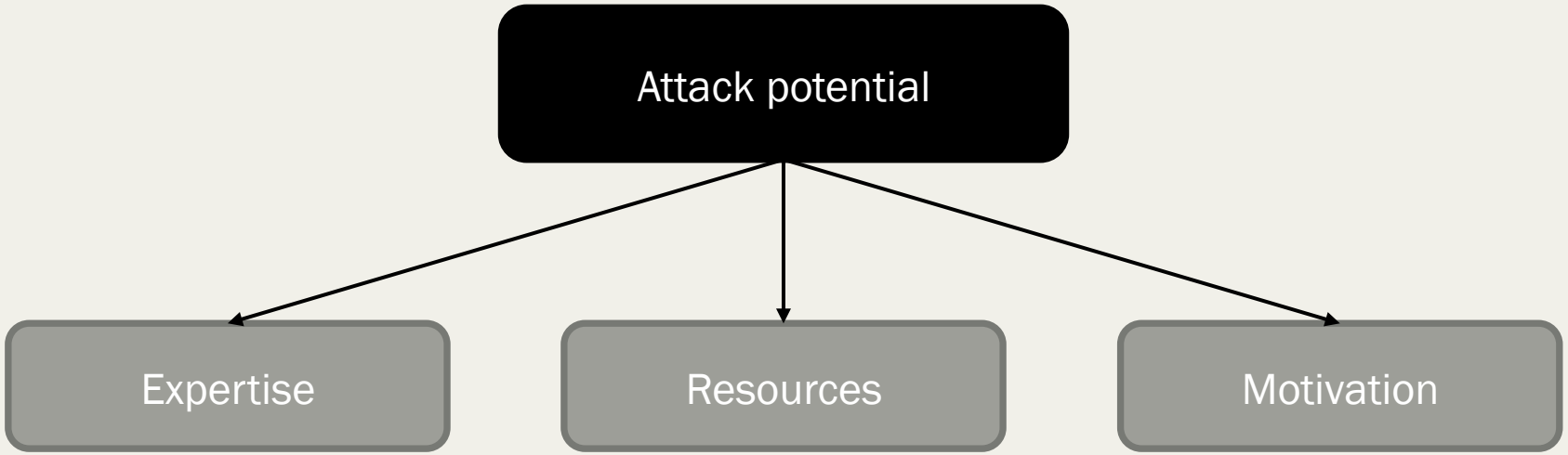
- Separation cooperative/non-cooperative attacks
- Attacker's expertise

Applying ISO/IEC JTC1 – 30107-3
Process-dependent evaluation factors

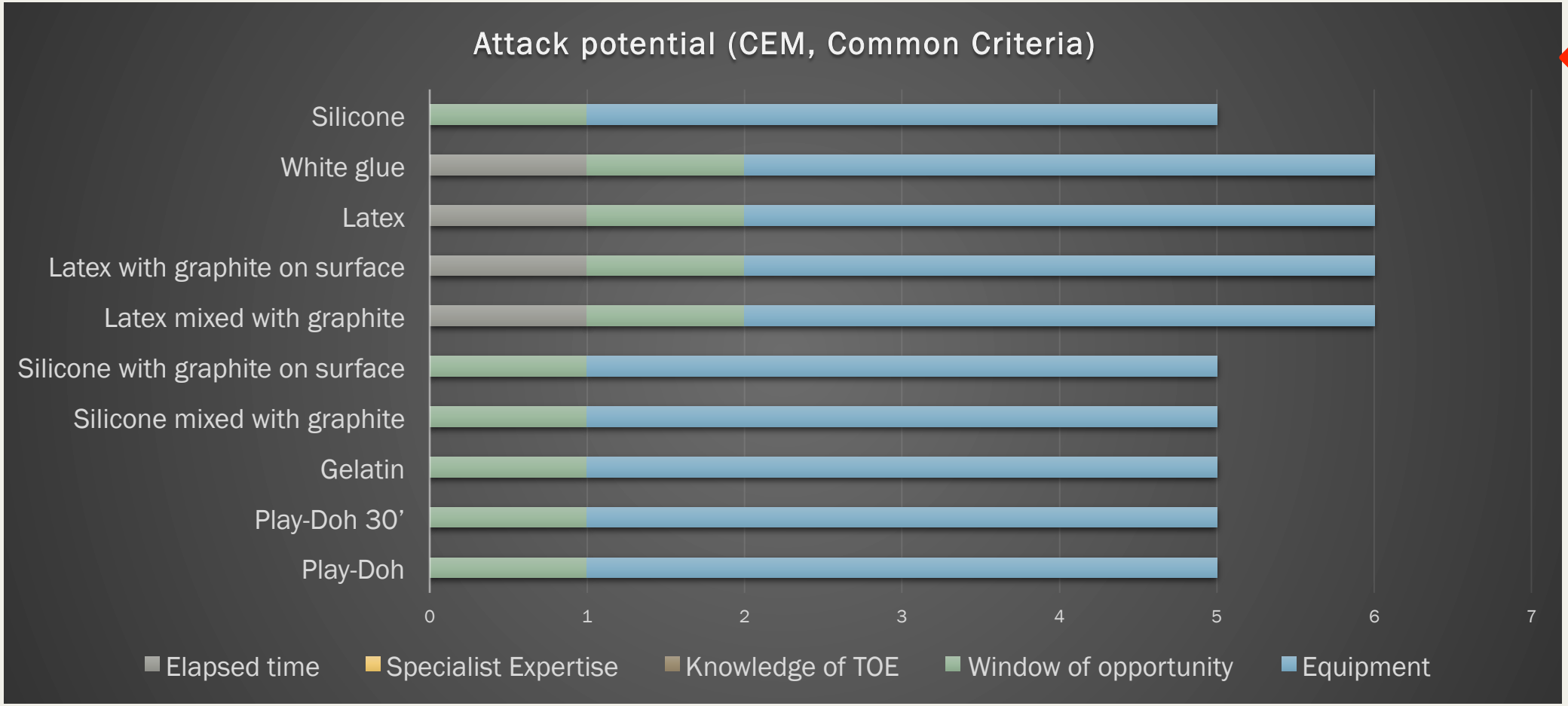
- Enrolment
  - *Quality thresholds*
  - *Presentation policy (operator oversight)*

- Verification
  - *Usually no operator oversight*
  - *In this case -> no quality threshold*

Applying ISO/IEC JTC1 – 30107-3
Attack Potential

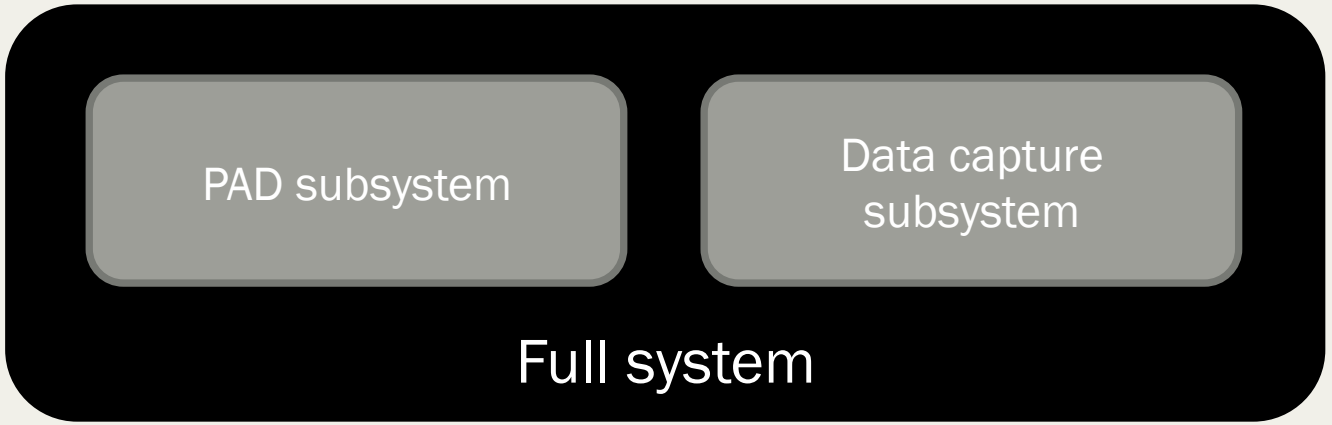


Applying ISO/IEC JTC1 – 30107-3
Attack Potential



Basic

Applying ISO/IEC JTC1 – 30107-3
Level of evaluator's access



This case: gray box
(response/non response, quality, reference matching)

Applying ISO/IEC JTC1 – 30107-3
Metrics

Attack Presentation Non-Response Rate

Data capture APNRR = *AP that cause no response/total AP*

Attack Presentation Non-Capture Rate

APNCR = *AP with low quality/total AP*

Attack Presentation Match Rate

APMR= *AP that match reference/total AP*

Attack Presentation Non-Match Rate

APNMR= *AP that do not match reference/ total AP*

Applying ISO/IEC JTC1 – 30107-3
Required reporting metrics

System	Metric	Presentation type	Reported?
Data capture subsystem	APCER	Attack	✗ - no access to PAD subsystem
	BPCER	*Bona fide*	✗ - no access
	APNRR	Attack	✓
	BPNRR	*Bona fide*	✗ – no access
	APNCR	Attack	✓
Comparison subsystem (verification)	FNMR/FMR	*Bona fide*	✗ - no access
	APMR	Attack	✓
	Full system processing duration	Attack or *bona fide*	✗ – capture and verification done separately

Applying ISO/IEC JTC1 – 30107-3
Other reporting metrics

Item	Value	Comments
Capture subjects	6	4 male, 2 female
Sources for artefacts	36	Index, middle finger and thumb from both hands
Artefacts	330 + 126	Not included in 30107-3, addition by the evaluator. Thermal and capacitive + optical.
Artefact species	10	Silicone, silicone with graphite (mixed and on surface), latex, latex with graphite (mixed and on surface), Play-Doh (fresh and a bit dry), gelatine, latex and white glue
Artefact series	-	Out of each mold one artefact was made for each species
Detected AP (total, by capture subject, by artefact species, by artefact series)	* - * -	* Reported later
Non-detected AP (total, by capture subject, by artefact species, by artefact series)	* - * -	* Reported later
Detected normal presentations	-	Not reported – additional evaluation needed
Non-detected normal presentations	-	Not reported – additional evaluation needed
Alterations/modifications to artefact creation	-	There were no alterations to artefact creation. A different evaluation should be performed for this end.
Configuration of PAD systems under test	NBIS, threshold = 25	Set from previous performance evaluation, same sensors
Presentation attack resistance	Reported before	
Attack potential	Reported before	
Description of IUT (sensors)	1 therm., 2 cap., 1 opt.	Manufacturers and models are confidential

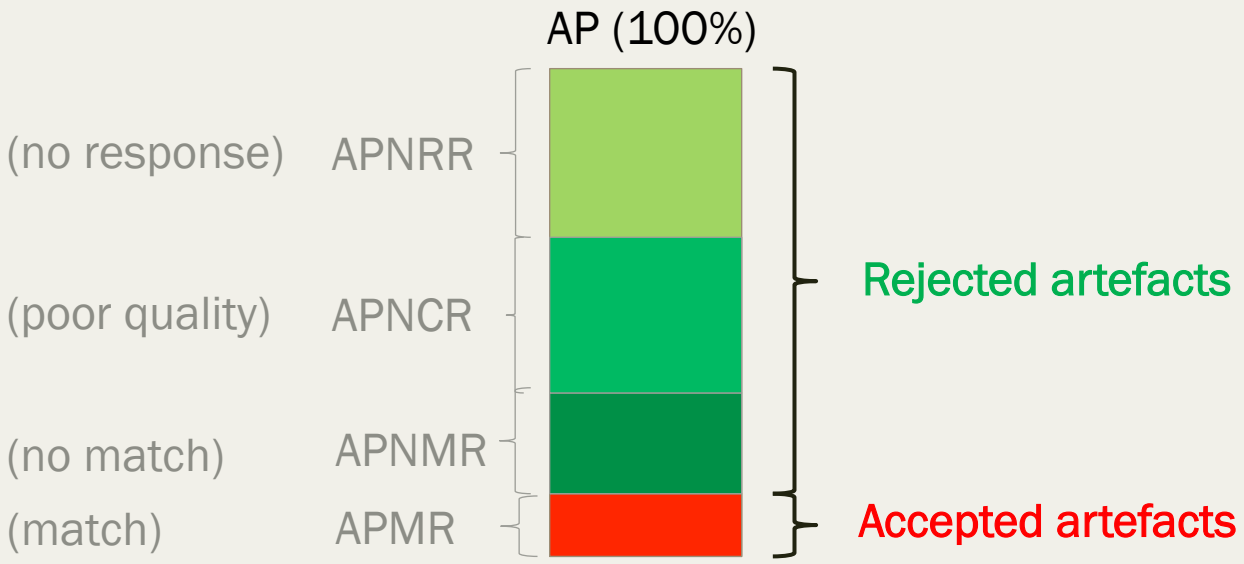
Outline

- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

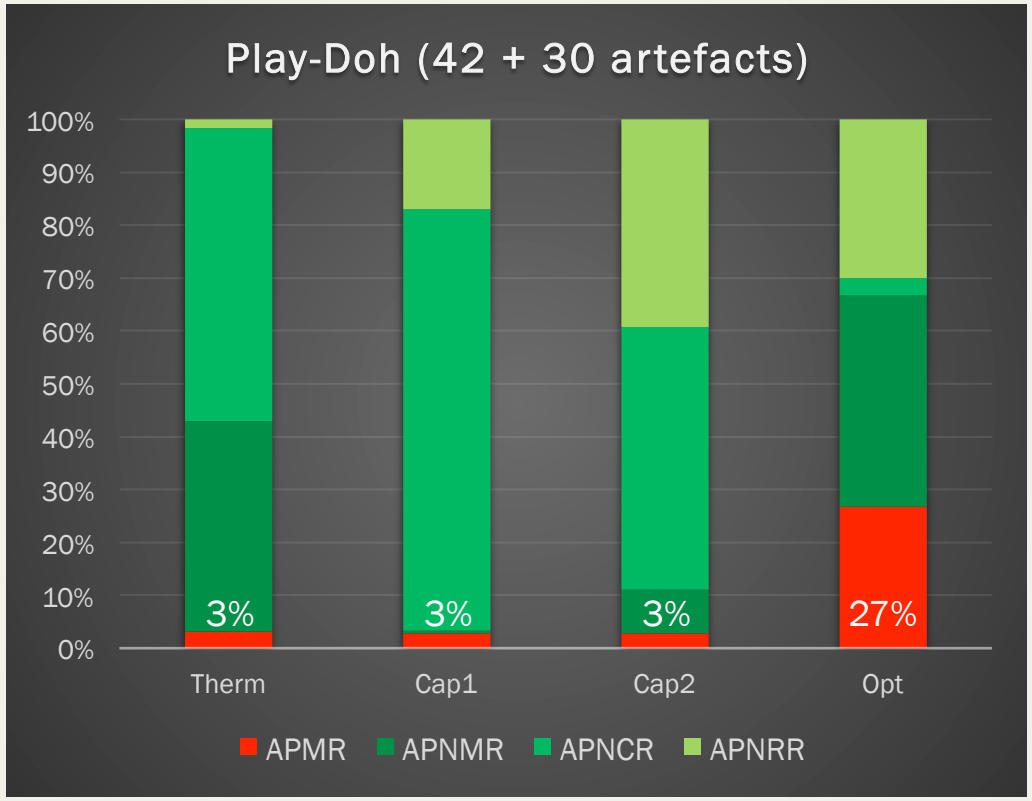
Results reporting

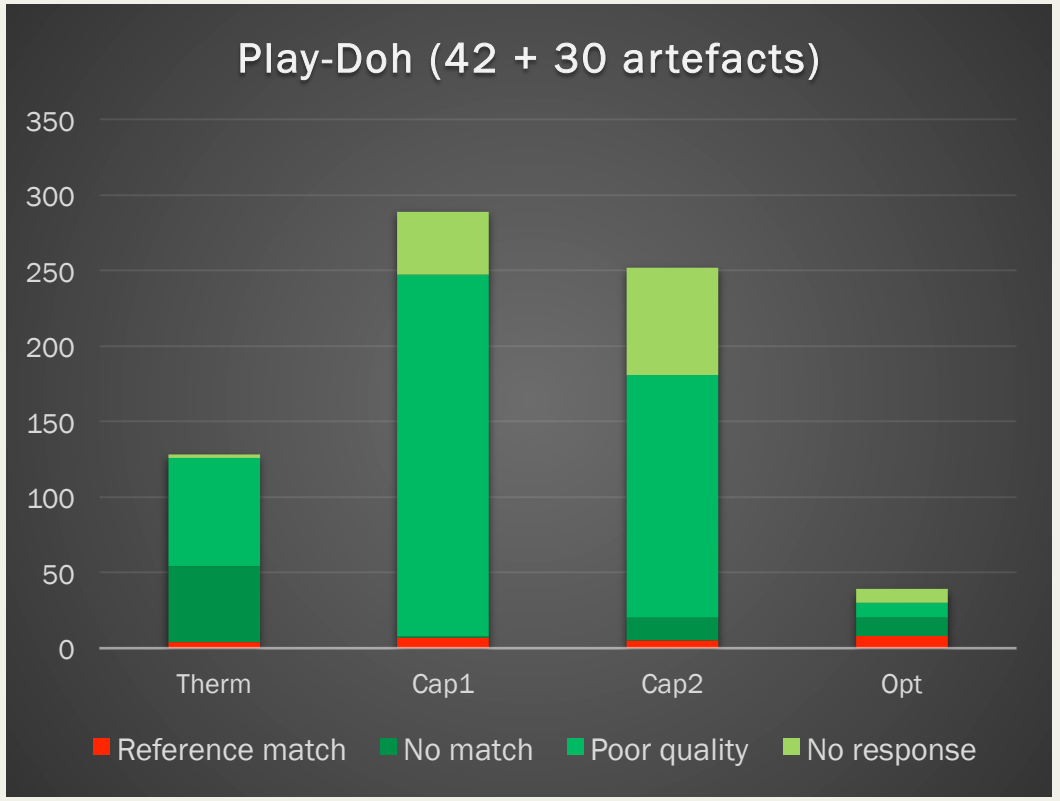
- Attack Presentations = rejected artefacts + accepted artefacts

APNRR + APNCR + APNMR | APMR

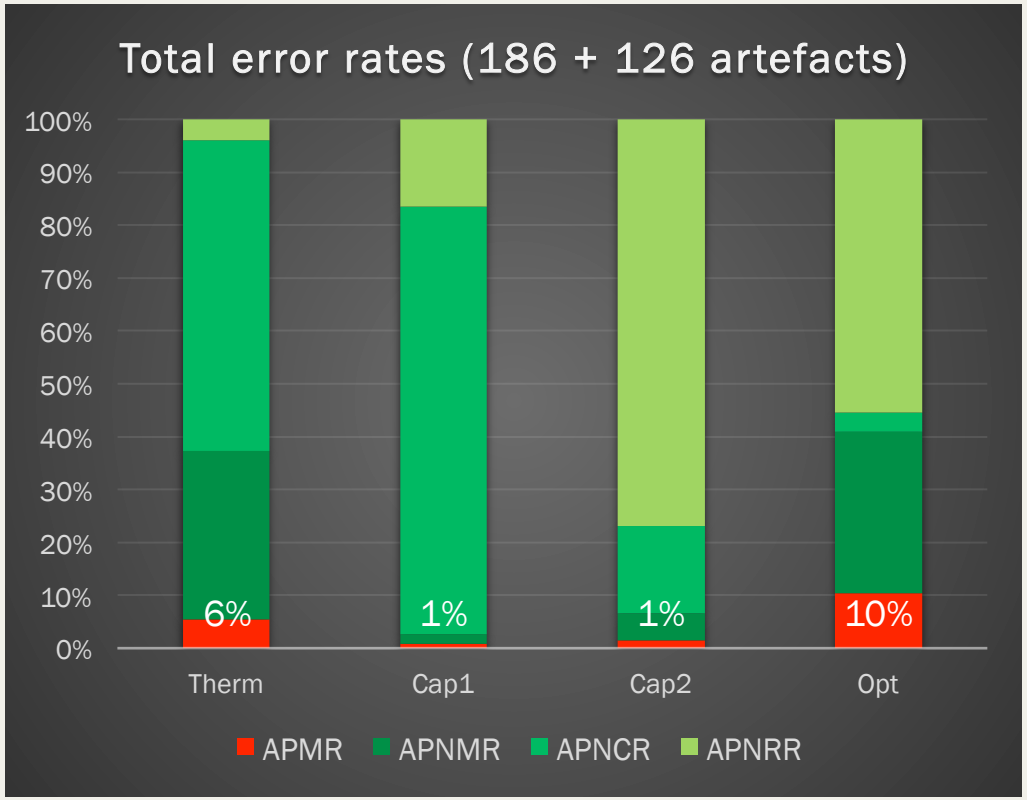


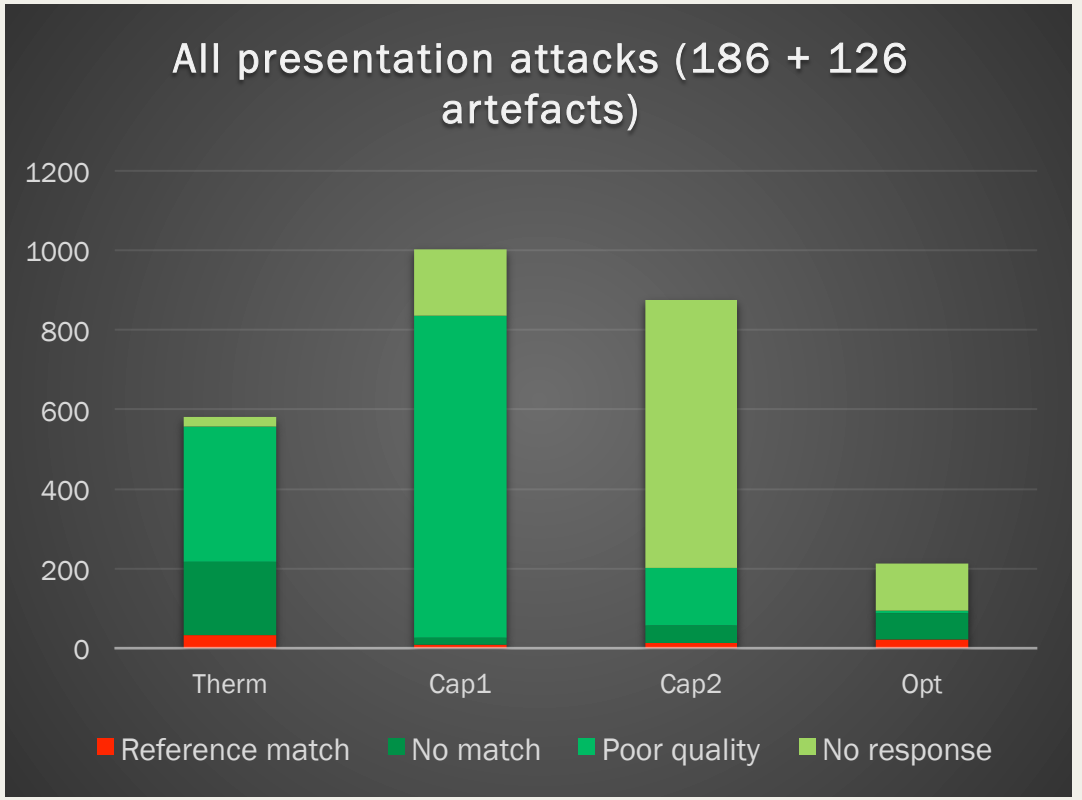
Results reporting
Cooperative attacks





Results reporting
(All) Cooperative attacks





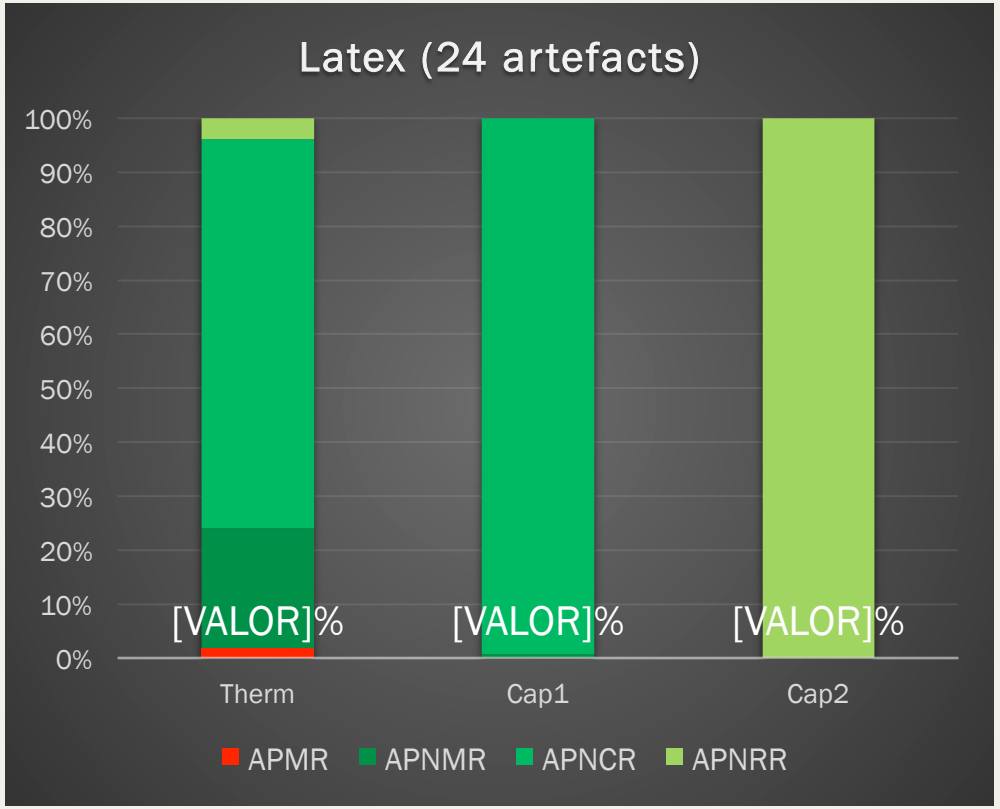
Results reporting

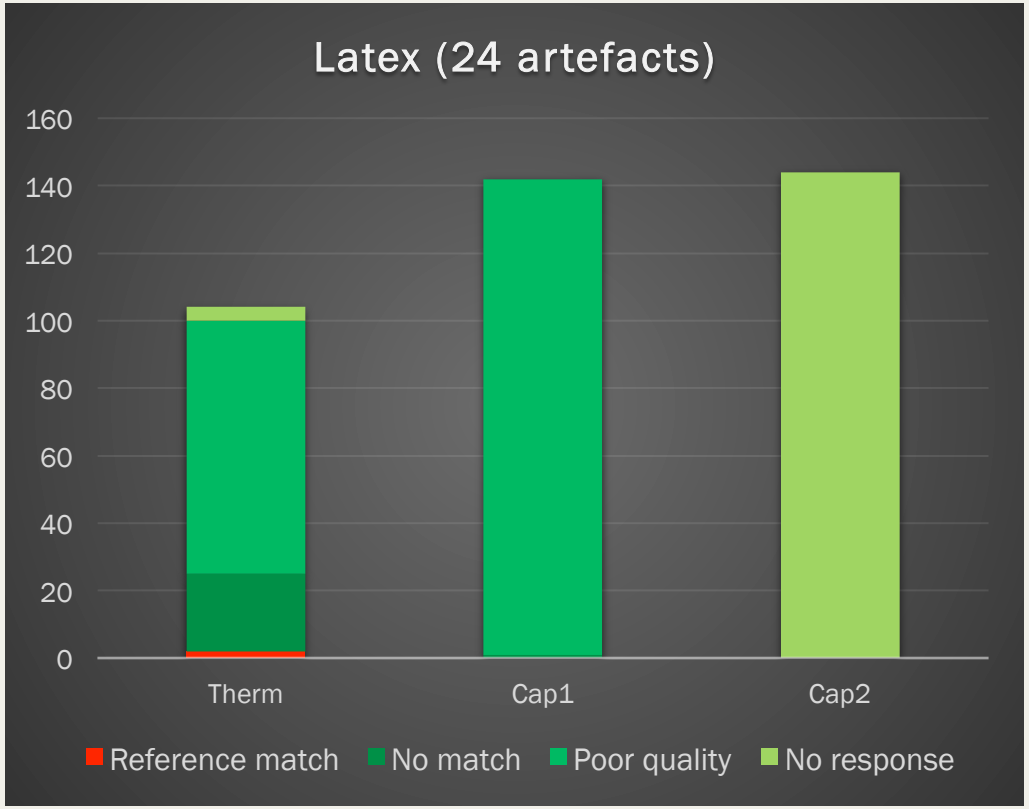
Cooperative attacks

	Silicone				Gelatine				Latex				Latex + graphite				Latex + graphite surface			
Sensor	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt
Artef		6		6		36		30		12		30		12		6		36		12
AP	25	36	36	6	114	130	102	32	47	72	72	31	52	72	72	6	108	214	190	36
Resp	25	24	0	6	114	130	62	28	47	66	0	29	52	72	0	6	101	156	4	0
NFIQ>3	17	36	36	1	95	120	82	7	29	72	72	2	39	72	72	3	59	212	189	36
APNRR	0%	33%	100%	0%	0%	0%	39%	13%	0%	8%	100%	6%	0%	0%	100%	0%	6%	27%	98%	100%
APNCR	68%	67%	0%	17%	83%	92%	41%	9%	62%	92%	0%	0%	75%	100%	0%	50%	48%	72%	2%	0%
APNMR	24%	0%	0%	50%	15%	8%	16%	50%	32%	0%	0%	94%	25%	0%	0%	33%	41%	1%	1%	0%
APMR	8%	0%	0%	33%	2%	0%	4%	28%	6%	0%	0%	0%	0%	0%	0%	17%	5%	0%	0%	0%

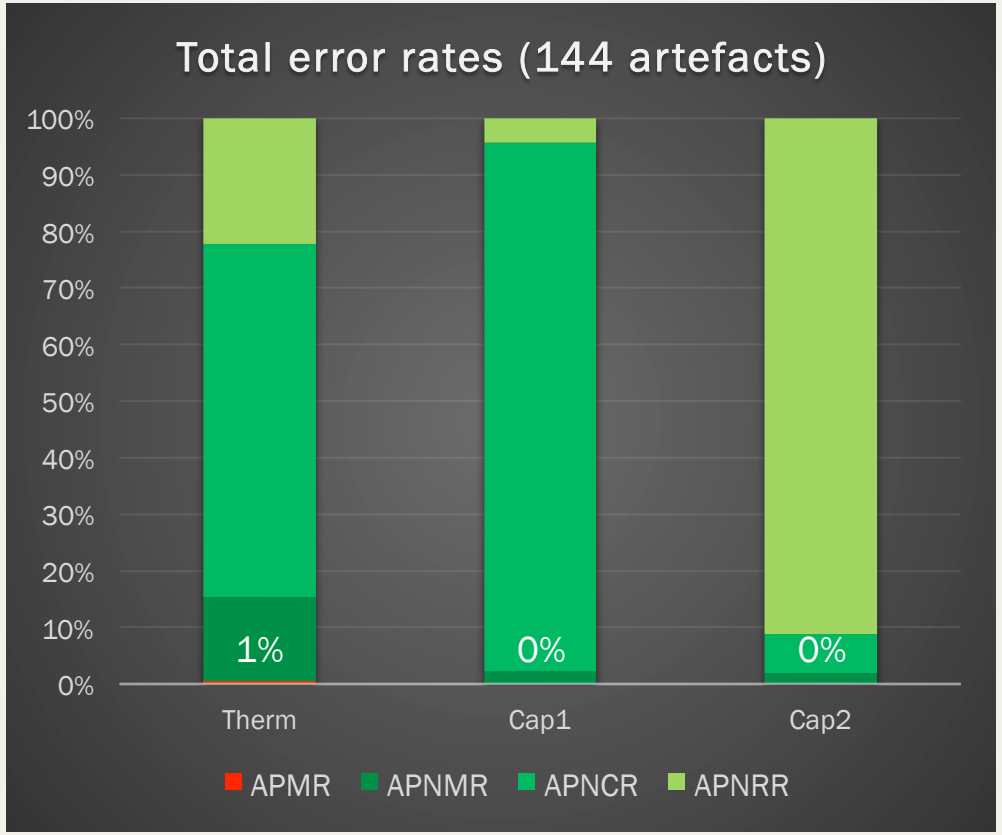
	Silicone + graphite				Silicone + graphite surface				Play-Doh				Play-Doh after 30 minutes				White glue			
Sensor	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt	Ther	Cap1	Cap2	Opt
Artef		12		6		12		6		42		30		12		0		6		0
AP	37	66	96	36	24	34	33	36	126	247	181	30	27	97	56	-	20	33	36	-
Resp	23	60	0	5	24	24	0	0	124	205	110	21	27	65	26	-	20	33	0	-
NFIQ>3	22	66	96	31	17	33	33	36	72	239	161	10	4	95	39	-	10	30	36	-
APNRR	38%	9%	100%	86%	0%	29%	100%	100%	2%	17%	39%	30%	0%	33%	54%	-	0%	0%	100%	-
APNCR	22%	91%	0%	0%	71%	68%	0%	0%	56%	80%	50%	3%	15%	65%	16%	-	50%	91%	0%	-
APNMR	24%	0%	0%	8%	17%	3%	0%	0%	40%	0%	8%	40%	74%	1%	23%		30%	9%	0%	
APMR	16%	0%	0%	6%	13%	0%	0%	0%	3%	3%	3%	27%	11%	1%	7%	-	20%	0%	0%	-

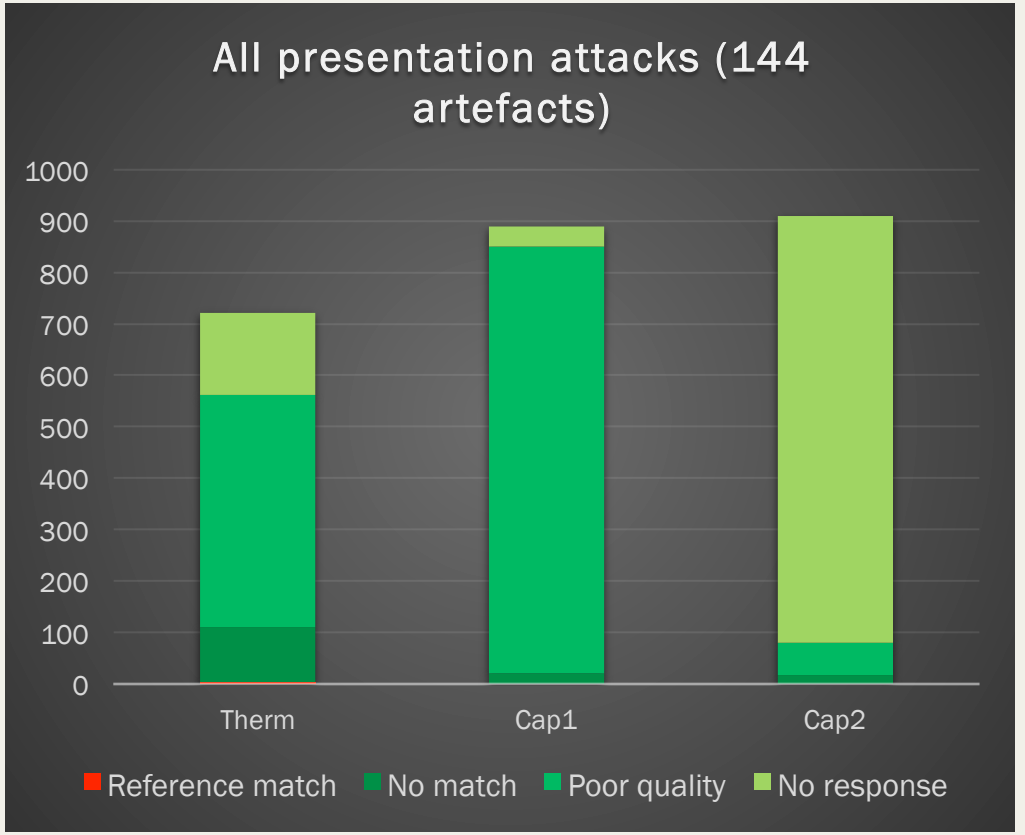
Results reporting
Non-cooperative attacks





Results reporting
(All) Non-cooperative attacks





Results reporting

Non-cooperative attacks

	Silicone			Gelatine			Latex			Latex + graphite			Latex + graphite surface		
Sensor	Ther	Cap1	Cap2	Ther	Cap1	Cap2	Ther	Cap1	Cap2	Ther	Cap1	Cap2	Ther	Cap1	Cap2
Artef.		24			30			24			6			6	
AP	110	138	174	161	218	196	104	142	144	36	32	36	36	36	36
Resp.	106	138	0	136	206	73	100	142	0	0	32	0	0	36	0
NFIQ > 3	90	138	174	123	209	179	79	141	144	36	30	36	36	36	36
APNRR	4%	0%	100%	16%	6%	63%	4%	0%	100%	100%	0%	100%	100%	0%	100%
APNCR	78%	100%	0%	61%	90%	29%	72%	99%	0%	0%	94%	0%	0%	100%	0%
APNMR	17%	0%	0%	24%	4%	9%	22%	1%	0%	0%	6%	0%	0%	0%	0%
APMR	1%	0%	0%	0%	0%	0%	2%	0%	0%	0%	0%	0%	0%	0%	0%

	Silicone + graphite			Silicone + graphite surface			Play-Doh			White glue		
Sensor	Ther	Cap1	Cap2	Ther	Cap1	Cap2	Ther	Cap1	Cap2	Ther	Cap1	Cap2
Artef.		6			24			18			6	
AP	36	36	36	139	144	144	77	107	107	23	36	36
Resp.	0	36	0	124	132	0	77	93	7	19	36	0
NFIQ > 3	36	36	36	135	143	144	60	101	107	17	35	36
APNRR	100%	0%	100%	11%	8%	100%	0%	13%	93%	17%	0%	100%
APNCR	0%	100%	0%	86%	91%	0%	78%	81%	7%	57%	97%	0%
APNMR	0%	0%	0%	3%	1%	0%	21%	6%	0%	26%	3%	0%
APMR	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%

Outline

- Why, how, what was done?
- Experiment
- Applying ISO/IEC JTC1 – 30107-3 to the experiment
- Results reporting
- Lessons learned

Lessons learned

- Compare security evaluations
- Attack Potential difficult to measure, should be more specific
- 2 side-by-side graphs (rates, quantities)
- Environmental conditions should be reported
- Give image examples of artefacts and captured samples

References

- ISO / IECJTC 1 / SC37, “CD 30107-3, Biometric presentation attack detection — Part 3: Testing and reporting,” 2016.
- Common Criteria, “Common Methodology for Information Technology Security Evaluation methodology September 2012 Revision 4 Foreword,” *Ccmb-2012-09-004*, no. September, p. 433, 2012.
- T. van der Putte and J. Keuning, “Biometrical fingerprint recognition: don’t get your fingers burned,” *Smart card Res. Adv. Appl. IFIP TC8/WG8. 8 Fourth Work. Conf. Smart Card Res. Adv. Appl. Sept. 20-22, 2000, Bristol, United Kingdom*, vol. 31, no. 0, p. 16, 2000.
- L. Thalheim, J. Krissler, and P.-M. Ziegler, “Body Check: Biometrics Defeated,” 2002. [Online]. Available: http://www.pcmag.com/article2/0,2817,13919,00.asp.
- S. a C. Schuckers, “Spoofing and Anti-Spoofing Measures,” *Inf. Secur. Tech. Rep.*, vol. 7, no. 4, pp. 56–62, 2002.
- J. Galbally, J. Fierrez, J. Rodriguez-Gonzalez, F. Alonso-Fernández, J. Ortega-Garcia, and M. Tapiador, “On the Vulnerability of Fingerprint Verification Systems to Fake Fingerprints Attacks,” 2006.
- A. Choiniere and T. Lubysheva, *Novetta - Protecting against Fingerprint Vulnerabilities when Deploying Biometric Systems*. 2015.

Thank you!

Extra info

Material	Elapsed time	Specialist Expertise	Knowledge of TOE	Window of opportunity	Equipment	Total	Attack potential	Attack resistance
Play-Doh	0	0	0	1	4	5	Basic	No rating
Play-Doh 30’	0	0	0	1	4	5	Basic	No rating
Gelatin	0	0	0	1	4	5	Basic	No rating
Silicone mixed with graphite	0	0	0	1	4	5	Basic	No rating
Silicone with graphite on surface	0	0	0	1	4	5	Basic	No rating
Latex mixed with graphite	1	0	0	1	4	6	Basic	No rating
Latex with graphite on surface	1	0	0	1	4	6	Basic	No rating
Latex	1	0	0	1	4	6	Basic	No rating
White glue	1	0	0	1	4	6	Basic	No rating
Silicone	0	0	0	1	4	5	Basic	No rating

Extra info
Enrolment process

- Transaction 1:

Capture (3 attempts)

NFIQ ≤ 3

Image storage

- Transaction 2:

Capture (3 attempts)

NFIQ ≤ 3

Image storage

Comparison

Finger enrolled