Security Evaluation of Vascular Biometrics

4th May, 2016.

Akira Otsuka, Tetsushi Ohki
AIST, Japan

How to evaluate the Security of Biometrics

Two Standards

Common Criteria

- 5 levels of Attack Potential (AP)
  Basic, Enhanced-Basic, Moderate, High, Beyond High
- Tester makes the best efforts to attack the TOE
  If no attack is found within the given AP,
  TOE is considered secure against any attack below AP.

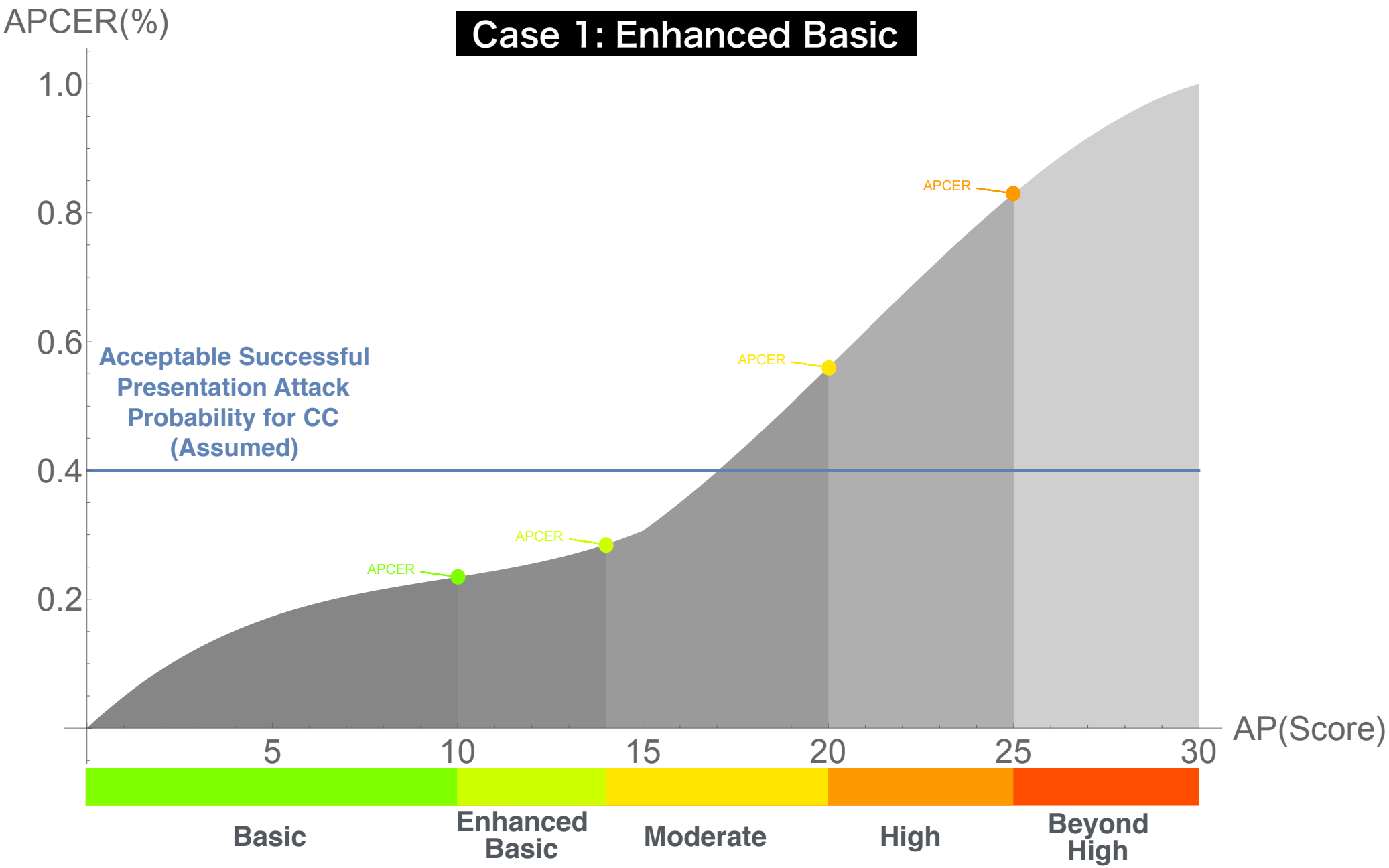
ISO/IEC 30107, "Biometric Presentation Attack Detection"

- Attack Presentation Classification Error Rate

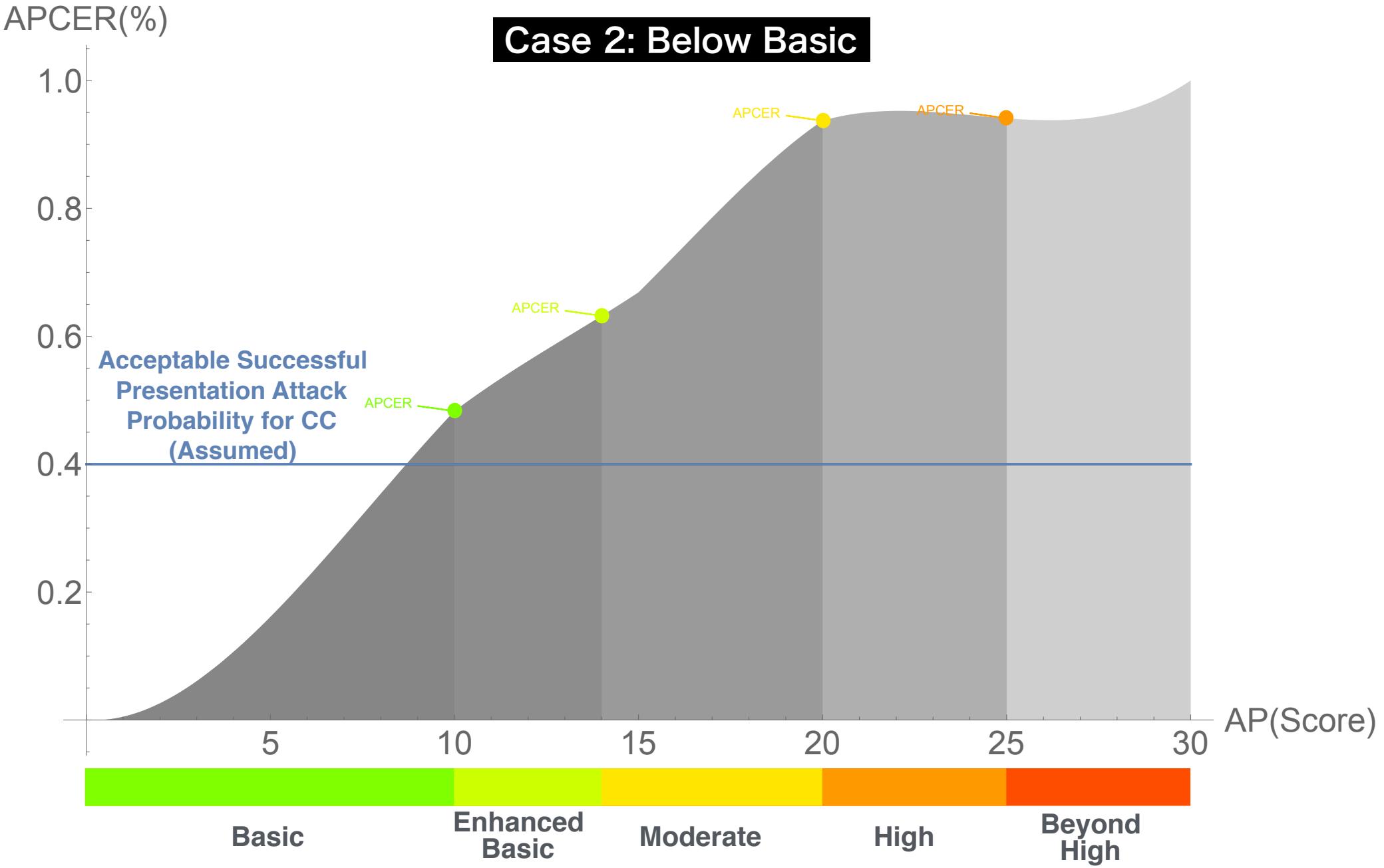
$$\mathrm{APCER}_{\mathrm{AP}} = \max_{\mathrm{PAIS} \in \mathcal{A}^{\mathrm{AP}}} \frac{1}{N_{\mathrm{PAIS}}} \sum_{i=1}^{N_{\mathrm{PAIS}}} (1 - \mathrm{Res}_i)$$

PAIS: Presentation Attack Instrument Species
$\mathcal{A}_{\mathrm{AP}}$: a subset of PAI species with attack potential at or below AP

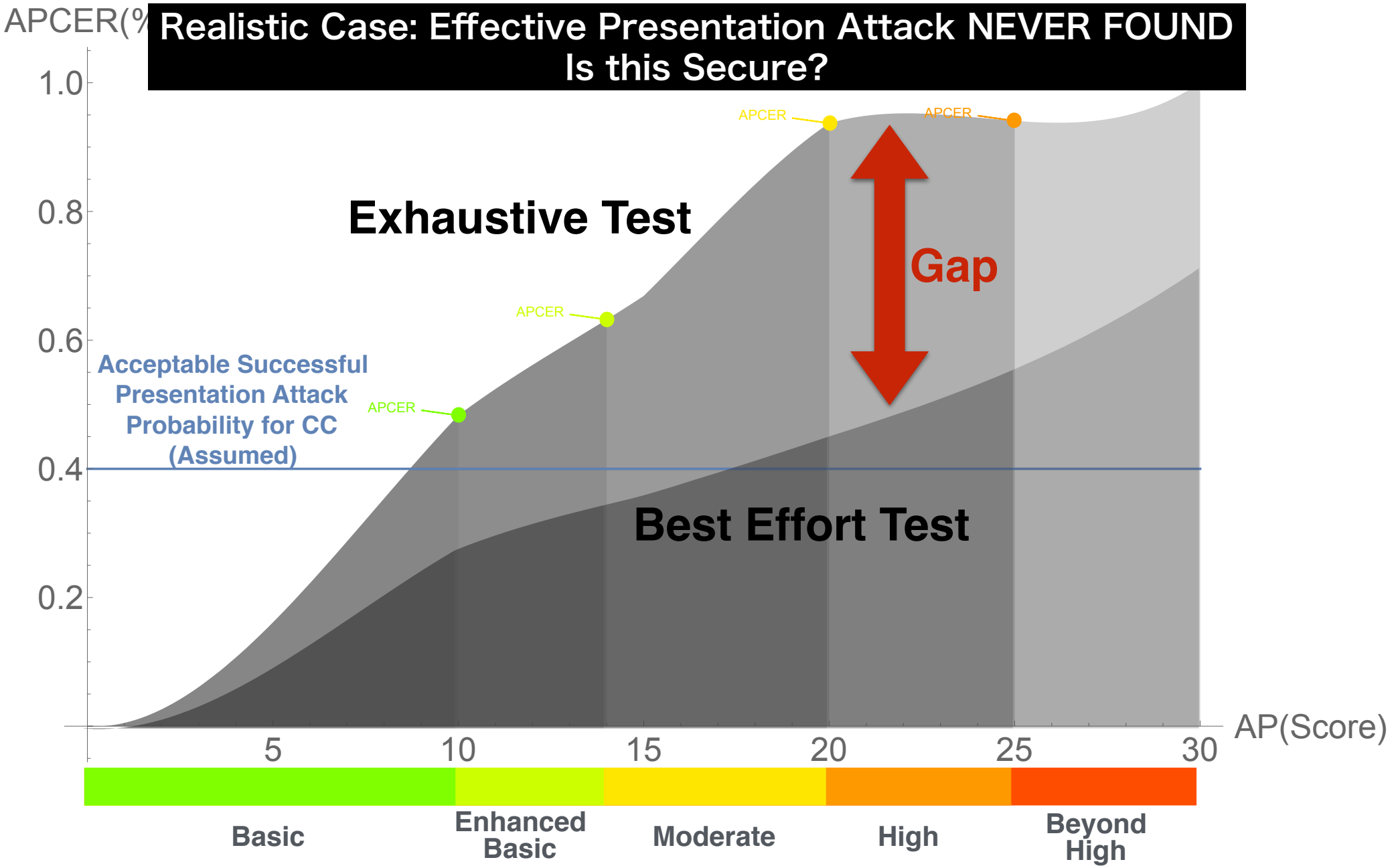
Relation between AP and APCER(1)



Relation between AP and APCER(2)



A Gap between Theory and Practice

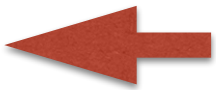


How to close the GAP?

Sensor-independent Security Evaluation

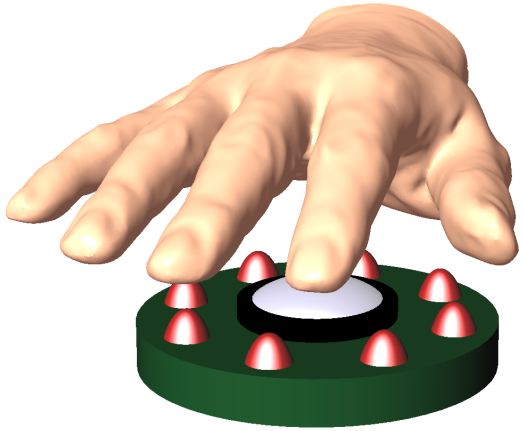
- Same test set can apply many TOE's (Ideally)
- That's good, but…
  - "Universal" attack instruments (applicable to many TOE's) are hard to produce in many cases
    — Palm vein vs Finger vein / Front vs Side finger vein

Sensor-dependent Security Evaluation

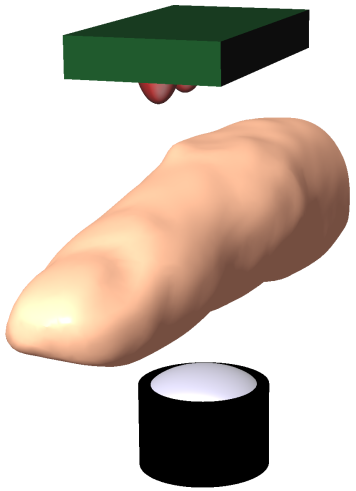


- Provide (as much as possible) internal specification of TOE to test labs. Test labs will create(or provided) Simulated Sensor/Algorithm:
  - Sensor Specification — **Simulated Sensor**
  - Algorithm Specification — **Simulated Algorithm**
- Create "**good attack instruments**" based on simulated sensor.

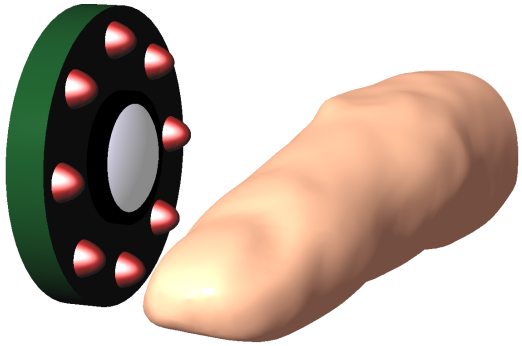
Variety of Vascular Biometrics



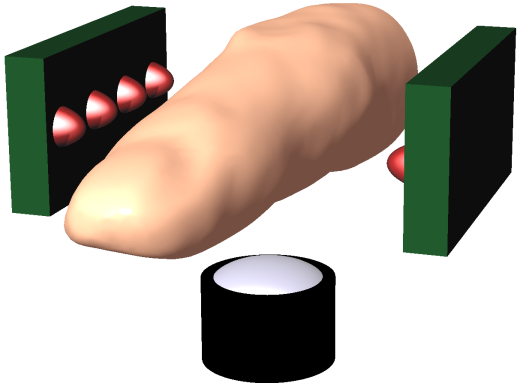
(I) Palm Vein Scanner
Reflective



(II) Font Finger Vein Scanner
Direct Transmissive



(III) Side Finger Vein Scanner
Reflective



(IV) Front Finger Vein Scanner
Indirect Transmissive

Sensor-dependent Security Evaluation

$\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$: Presentation Attack Instruments (PAI) sepcies

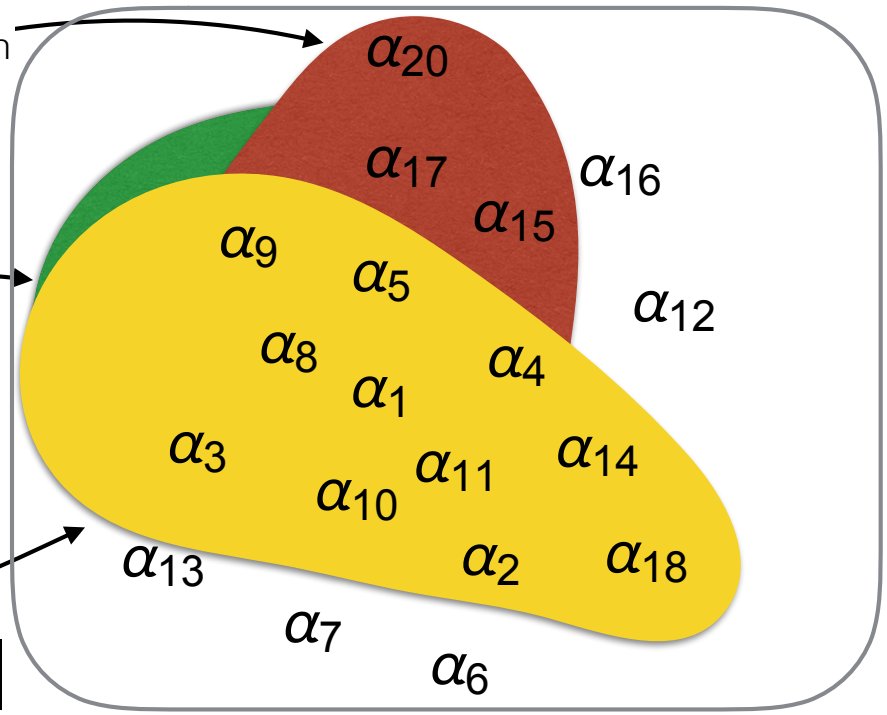
PAI species α_i is indistinguishable from Bona Fide presentation by a sensor if and only if

$$\mathrm{APCER}_{\alpha_i} + \mathrm{BPCER} \approx 1$$

Divide and Conquer

In a case TOE consists of …

TOE
- NIR Image Sensor → A_{NIR} NIR absorption
- Conductive Sensor → A_{Cond} conductive
- Blood Flow Sensor → A_{Blood} internal motion

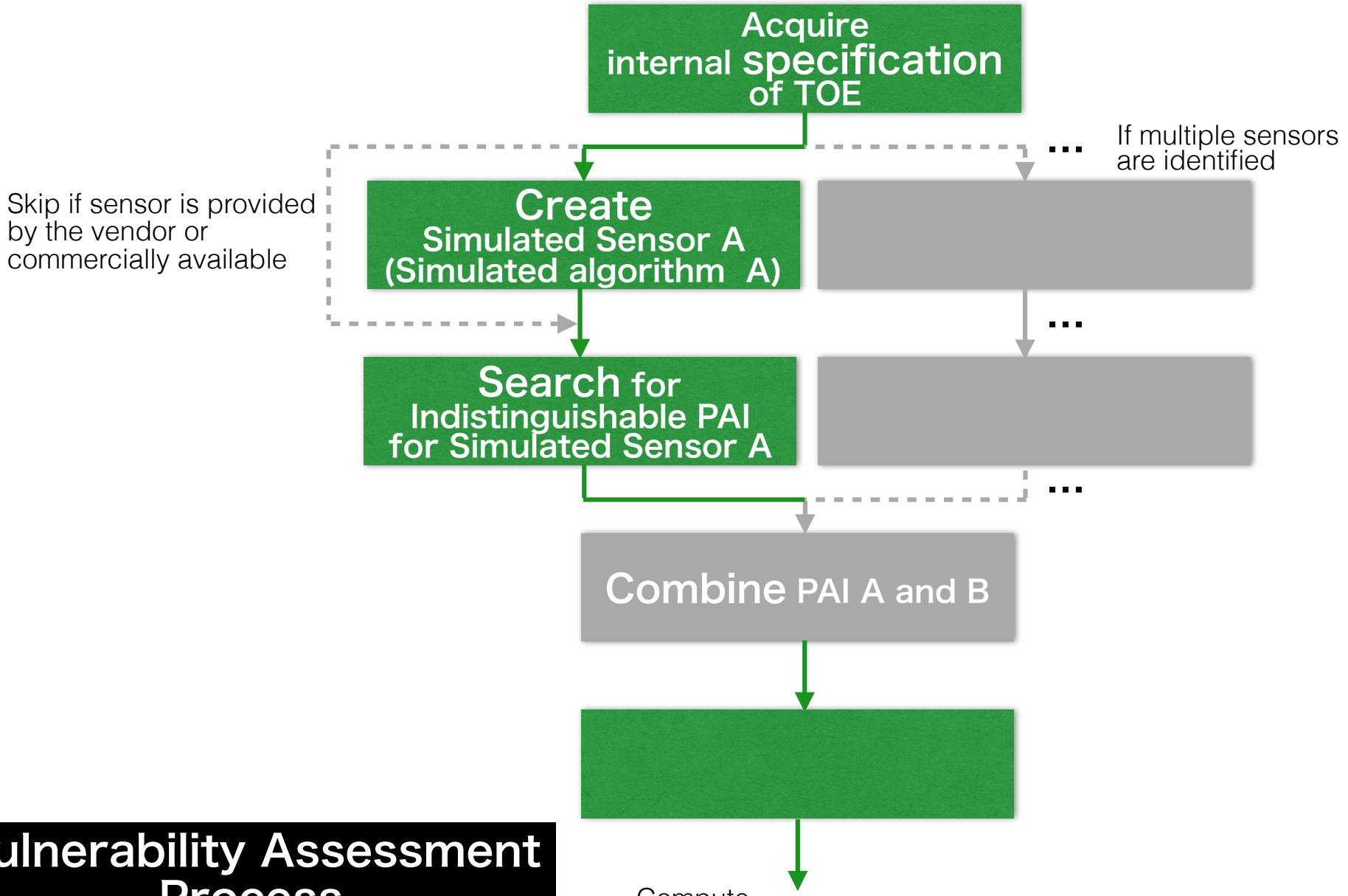


Arithmetics on Indistinguishable Sets

Set of PAIs on each sensor narrows down the set of PAI on TOE

$$A_{\mathrm{TOE}} \supseteq A_{\mathrm{NIR}} \cap A_{\mathrm{Cond}} \cap A_{\mathrm{Blood}}$$

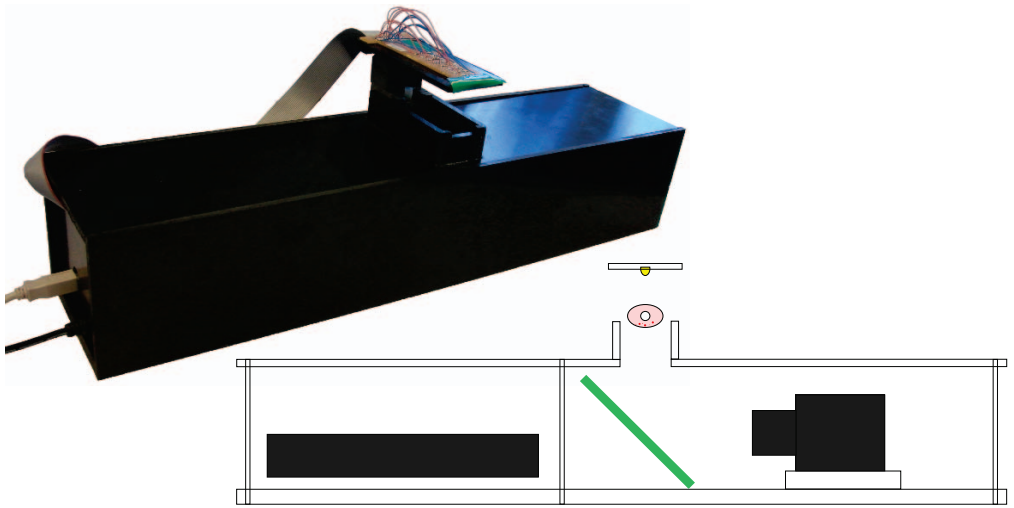
Sensor-dependent Security Evaluation



Vulnerability Assessment Process

Preliminary Experiment

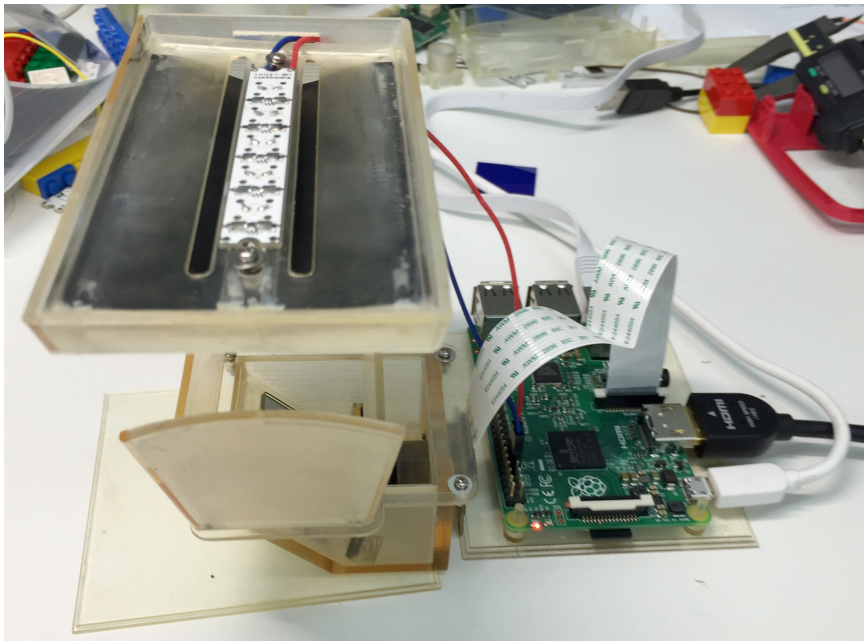
Example TOE



[TV13] Finger Vein Sensor

Source) Ton, Bram T., and Raymond NJ Veldhuis. A high quality finger vascular pattern dataset collected using a custom designed capturing device. Biometrics (ICB), 2013 International Conference on. IEEE, 2013.

Simulated Sensor

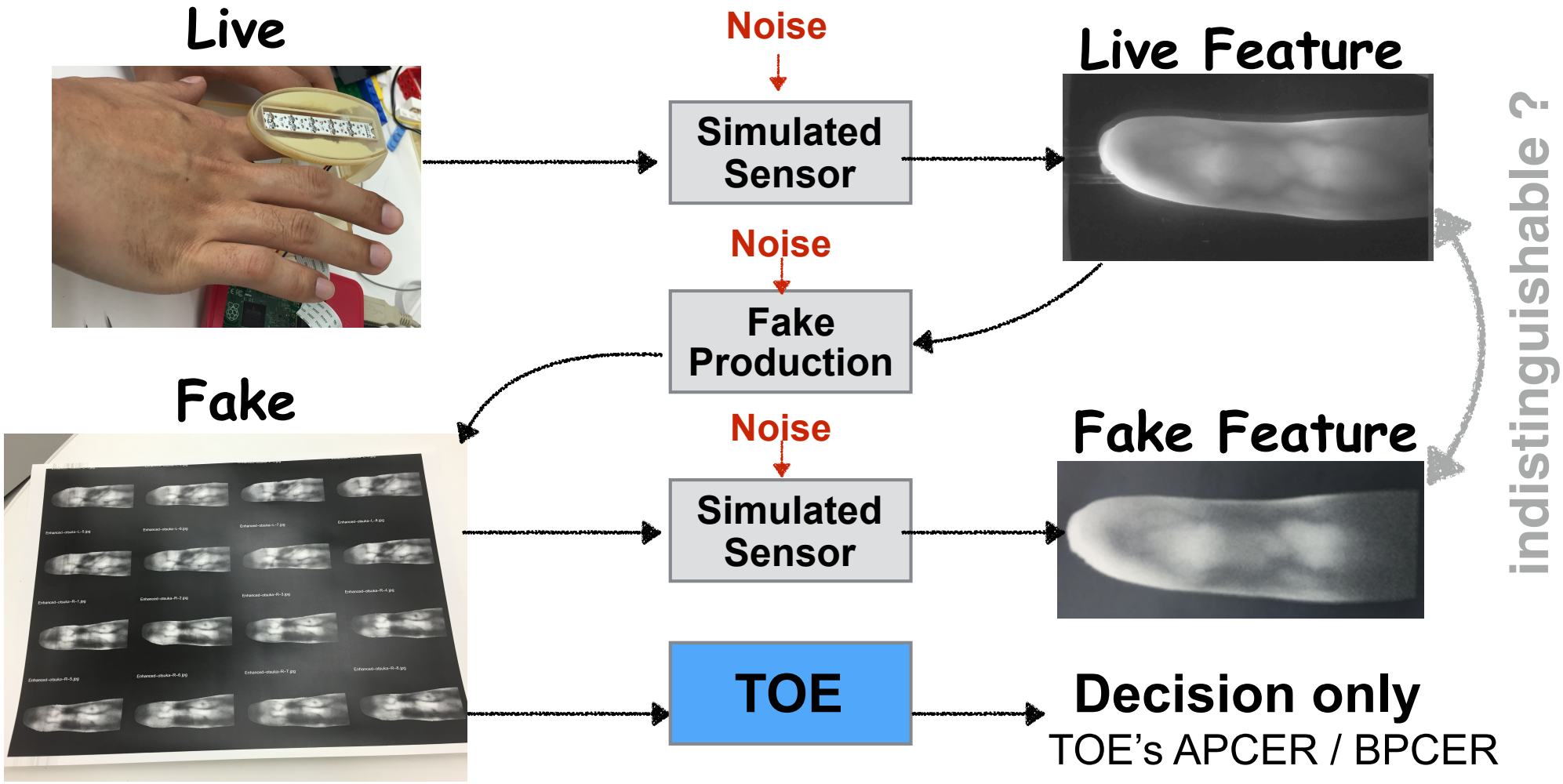


e) AIST

	Example TOE	Simulated Sensor
Image Sensor	C-Cam Tech. BCi5 1280x1024	OmniVision OV5647 2592x1944
NIR Filter	B+W 093 IR filter 800nm - 930nm band-pass filter	Asahi Spectra M.C. 850/12nm φ25 850nm-centered band-pass filter
Light Source	850nm Oslam SFH4550 x 8 LED Adaptive Intensity Control	850nm Oslam SFH4550 x 5 LED Non-adaptive Intensity Control
Algorithm	bob.fingervein*	bob.fingervein*

*) idiap, available at https://github.com/bioidiap/bob.fingervein

Quality Control of Fake Samples

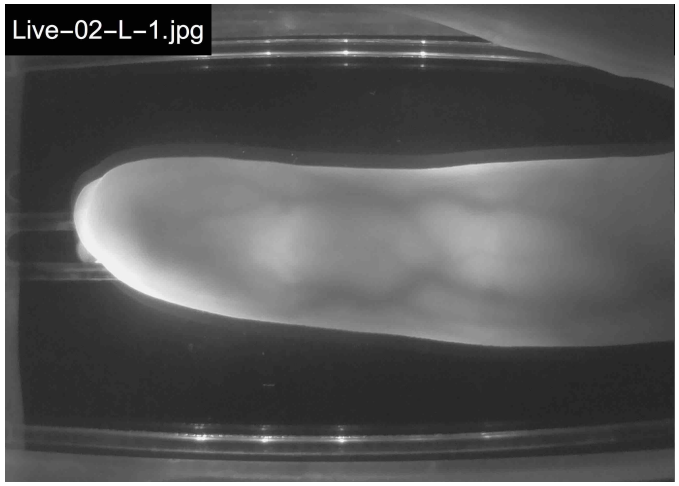


Control : Improve Sensor and Fake Production until Fake is indistinguishable from Live on the Simulated Sensor

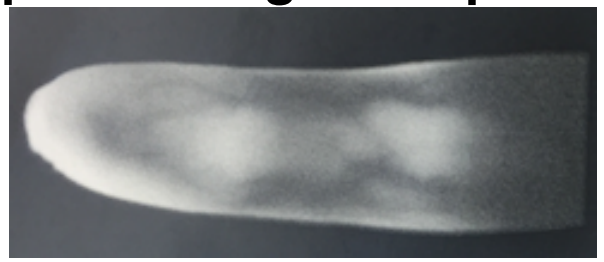
$$\mathrm{APCER}_{\mathrm{FAKE}} + \mathrm{BPCER}_{\mathrm{LIVE}} \approx 1$$

Fake Production

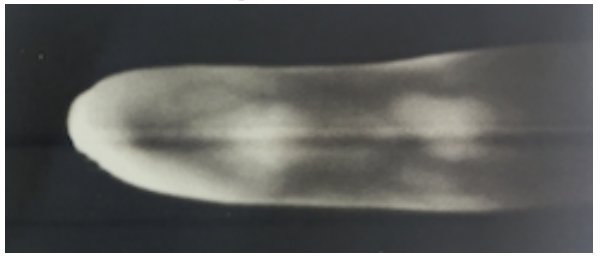
Live Sample



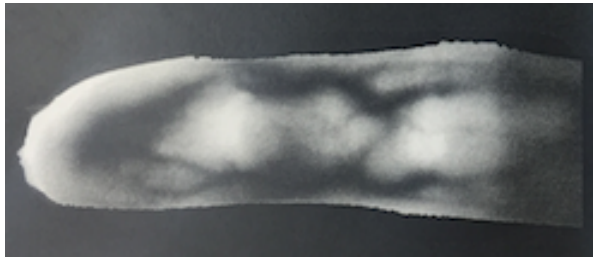
(A) Paper / Histogram Equalization



(B) OHP / Histogram Equalization



(C) Paper / PSF Deconvolution



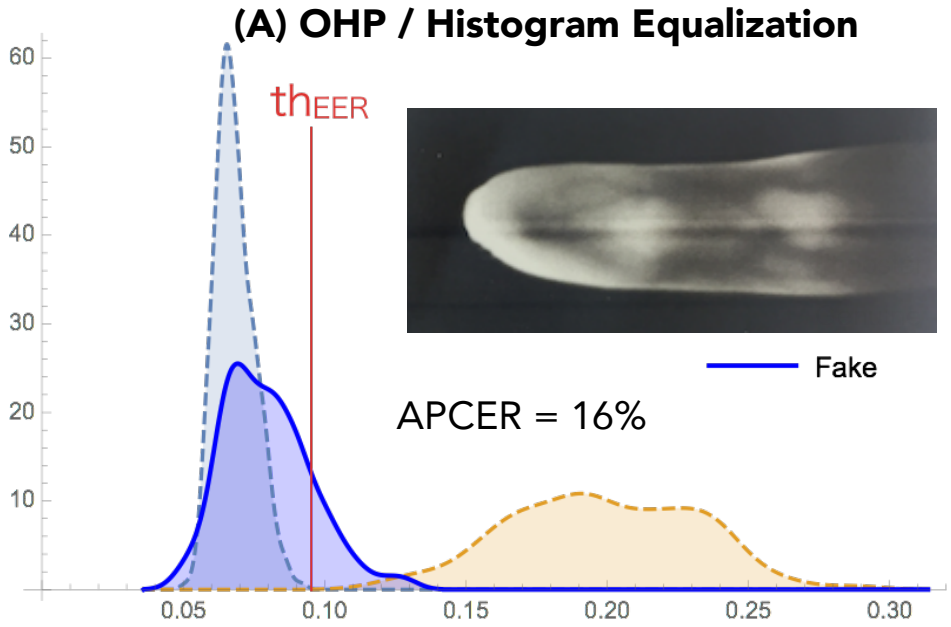
(D) OHP / PSF Deconvolution

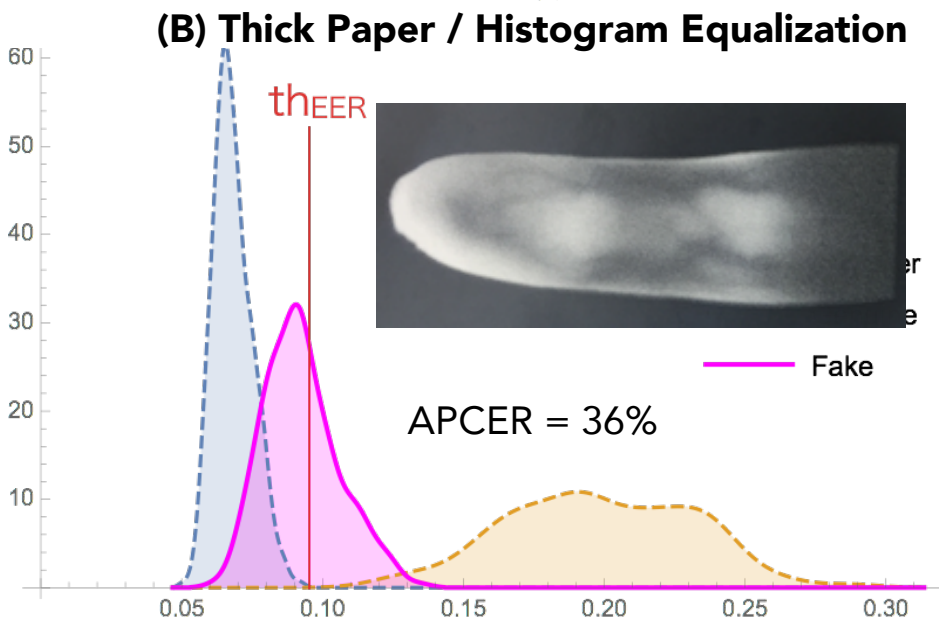
Material	/	Image Process
OHP Thick Paper	×	Histogram Equalization PSF Deconvolution

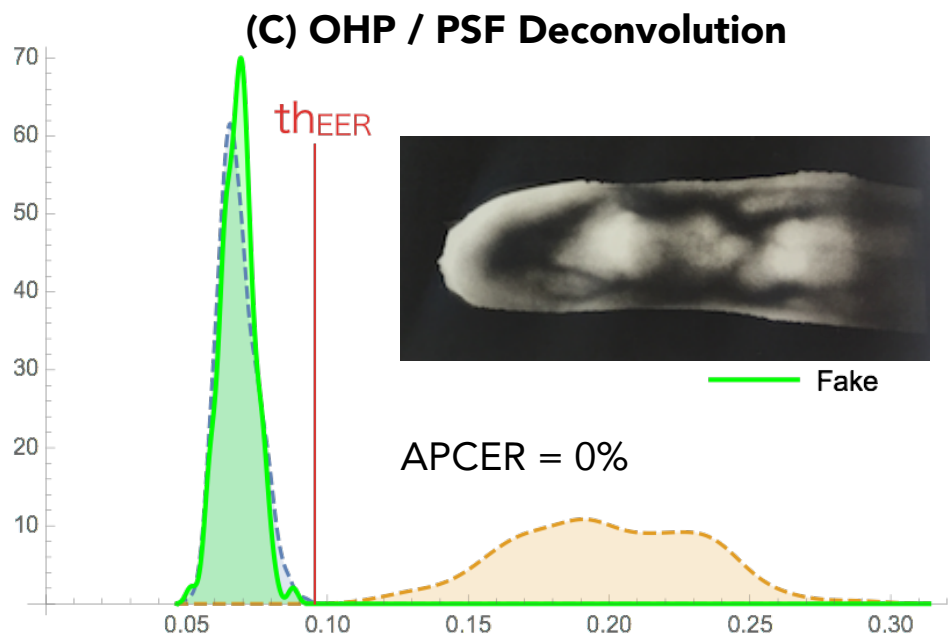
Preliminary Experiment details

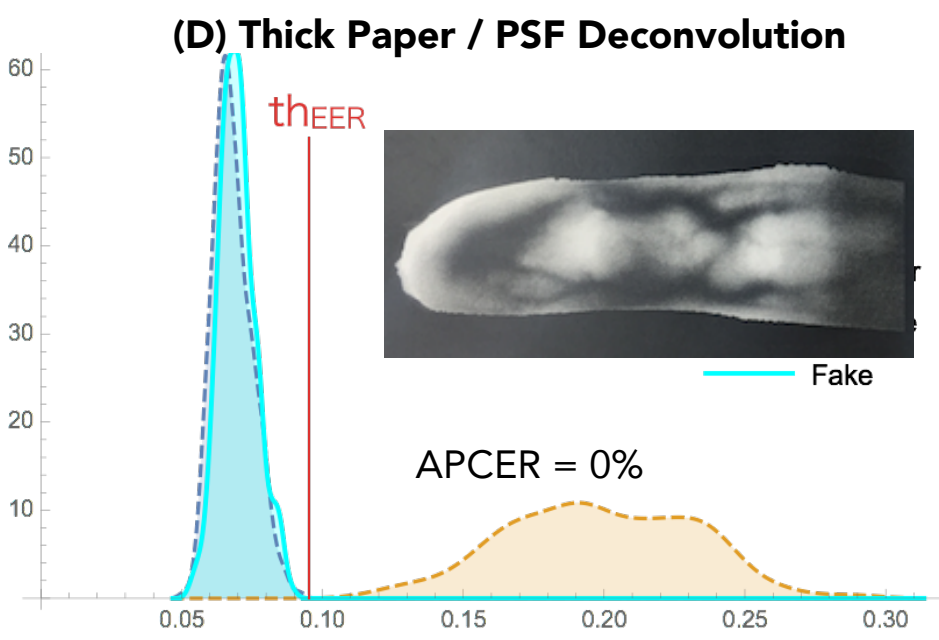
Biometric Samples	
Sensor	Original NIR Sensor (Type II: Front Transmissive Vein Scanner)
Number of Subjects	2
Number of Samples	Left and Right Index Finger x 8 samples each 1 as Gallery, 7 for Probe
Spoof Production	
Material	OHP (for Laser Printer), Thick Paper (Thickness 175μm, Weight 158g/m^2)
Image Enhancement	CLAHE (Contrast Limited Adaptive Histogram Equalization), PSF Deconvolution (Wiener Deconvolution of Point Spread Func.)
Verification	
Algorithm	bob.fingervein (Algorithm [Miura2005])
Verification Count	Live-Live Genuine: 224 pairs Live-Live Imposter: 768 pairs Fake-Live Genuine: 224 pairs

Preliminary Experiment Result









Conclusion

- In **Sensor-independent Security Evaluation** (Toolkit),
  - “Universal“ presentation attack instruments (applicable to many sensors) are hard to produce especially in vascular biometrics.
- Introduced **Sensor-dependent Security Evaluation**
  Test labs are provided (as much as possible) internal specification of TOE.
  Test labs will create(or provided) **Simulated Sensor/Algorithm**
  - **Quality control** of Presentation Attack Instruments
  - **Narrow down** the (infinitely many) set of PAIs to the (small) set of the most effective PAIs.
- Shown the preliminary experimental results
  - **Quality measurement** improves the quality of PAIs.