Spoofs, Subversion & Suspicion

Alternative titles:

Lazarick's Liveness Lingo

Twisted Terminology Taxonomy

Voluntary Vocabulary Vexations

Where to start?

- This terminology is intertwined, so please be patient *(i.e. don't stone the messenger)*
- Let's start with some familiar examples, and look at their grouping titles
- Then we clarify between 'Subversive' and 'Suspicious'
- Some other familiar terms
- Lest we forget about testing terms

Table 1 Examples of Artificial and Human Subversive Presentation Characteristic Types

Artificial	*Complete artefact*	**gummy finger,** latex finger, photo of face, photo of iris, recording of voice, video of face, artificial hand, custom contact lens, **artificial/patterned contact lens**, facial mask (ski, theatrical, Halloween), opaque or theatrical contact lenses
	Partial artefact	glue on finger, **false facial hair,** cosmetics, removable implants, sunglasses
Human	*Lifeless*	cadaver part, **severed finger**/hand
	Altered	nose job, face lift, amputation, **mutilation**, surgical switching of fingerprints between hands and/or toes
	Non-Conformant	voice mimicry, hand shape control, **forged signature**, facial expression/extreme, tip or side of finger, falsetto voice
	Conformant	zero effort imposter attempt
	Coerced	unconscious, under duress, drugged

subversive presentation

presentation of an artefact or human characteristic to the biometric capture subsystem **with the intent** to interfere with or undermine the correct or intended policy of the biometric system.

artefact

artificial object(s) or characteristic(s) presenting a copy of biometric characteristics or synthetic pattern made to be presented to a biometric capture device with the aim of subverting the biometric system.

Some presentations can be <u>Suspicious</u> without being **Subversive** (top)

Some presentations can be **Subversive**, but *not be detectable* as being <u>Suspicious</u> *(bottom)*

<u>Suspicious</u> – from the capture system's viewpoint

<u>SUSPICIOUS</u>

<u>Artificial</u> (patterned contact lens – cosmetic only {no mal-intent})

<u>Altered</u> (accidental scar/burn,…)

<u>Non-conformant</u> (poor training, not attentive, careless)

SUBVERSIVE

<u>Artificial (with intent to defeat)</u>

<u>Lifeless</u>

<u>Altered (with intent to defeat)</u>

<u>Non-conformant (with intent to defeat)</u>

<u>Coercion (specific, detectable non-conformant)</u>

These security problems are detectable

Zero-effort imposter attempt (intending to defeat the system – by chance)
Coercion (with conformant presentation)

Subversive – from the test designer's viewpoint

NON-SUBVERSIVE – Good faith genuine presentation

Undetectable as Suspicious

It depends on your perspective…

<u>Suspicious presentation detection</u> (SPD) is the most comprehensive term (rather than artefact or liveness detection which are more commonly used). This takes the *biometric capture system* perspective.

Subversive presentation represents the *test designer's* perspective, when the intent of the presentation is to defeat the system.
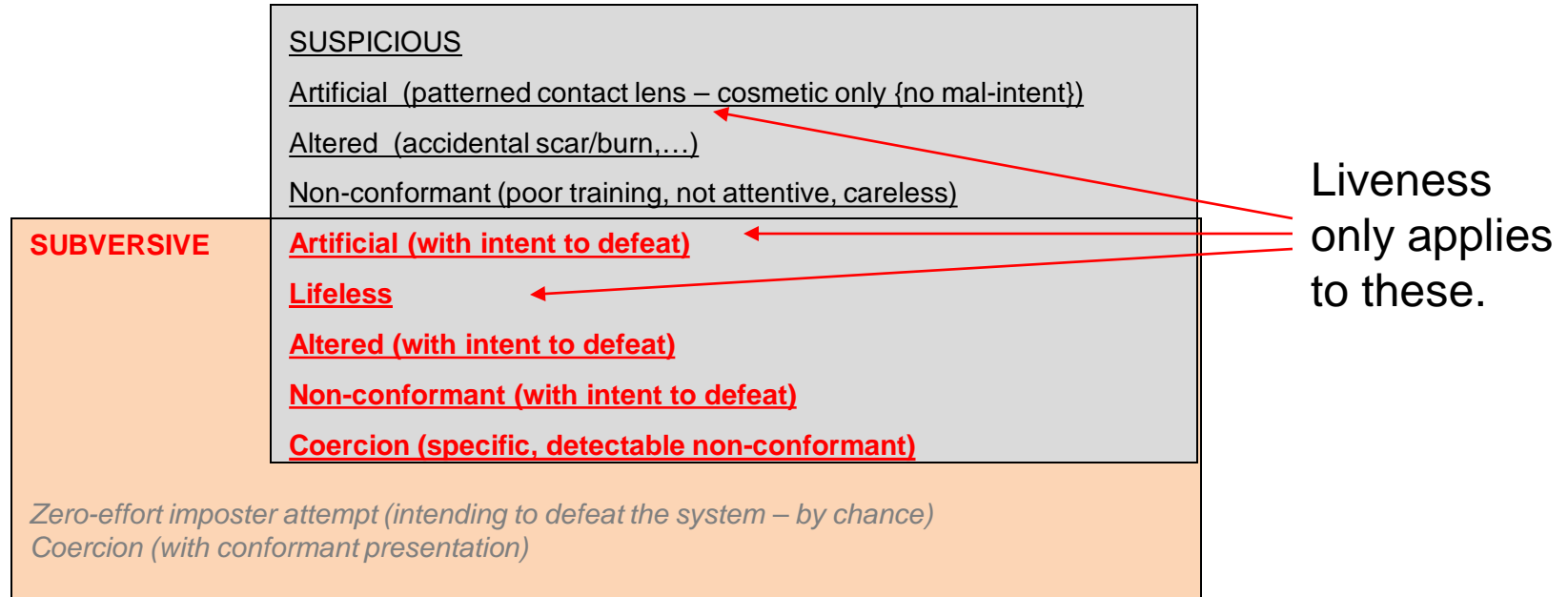
What about "spoof" and "liveness"?

Using the prior structure avoids dependence on these 2 terms, and their related "baggage"

For the record (WD3 includes):

- **spoof** - in the context of biometrics, to make a subversive presentation (with conscious effort).

- **liveness** - the quality or state of being alive, made evident by anatomical characteristics (e.g. skin or blood absorption of illumination), involuntary reactions or physiological functions (e.g. iris reaction to light, heart activity – pulse), or voluntary reactions or subject behaviors (e.g. squeezing together fingers in hand geometry or response to a directive cue).

Liveness detection

SUSPICIOUS

Artificial (patterned contact lens – cosmetic only {no mal-intent})

Altered (accidental scar/burn,…)

Non-conformant (poor training, not attentive, careless)

SUBVERSIVE

Artificial (with intent to defeat)

Lifeless

Altered (with intent to defeat)

Non-conformant (with intent to defeat)

Coercion (specific, detectable non-conformant)

Zero-effort imposter attempt (intending to defeat the system – by chance)
Coercion (with conformant presentation)

Liveness only applies to these.

- **liveness detection** - detection of anatomical characteristics or involuntary or voluntary reactions, in order to determine if a biometric sample is being captured from a living subject present at the point of capture.

{Note that liveness detection applies only to "lifeless" and in some instances "complete artefact" detection, but not other Suspicious Presentations}

Additional (but secondary) Concept

What is the role/purpose of the attacker?

- Impersonator *(synonym = impostor)*
  - "subversive biometric capture subject who attempts to be matched to someone else's biometric reference." [From ISO/IEC CD 2382.37]

- Identity Concealer
  - "subversive biometric capture subject who attempts to avoid being matched to their own biometric reference." [From ISO/IEC CD 2382.37]

Overall testing metric terms

Performance metrics

Successful cases:

- True suspicious Presentation Detection Rate (TSPDR): the proportion of subversive presentations correctly classified as being suspicious

- True Non-suspicious Presentation Detection Rate (TNSPDR): the proportion of non-subversive presentations correctly classified as being non-suspicious

Error cases:

- False Non-suspicious Presentation Detection Rate (FNSPDR): the proportion of subversive presentations incorrectly classified as being non-suspicious

- False suspicious Presentation Detection Rate (FSPDR): the proportion of non-subversive presentations incorrectly classified as being suspicious

Other more specific metrics also in WD3