



Cabinet of expertise covering technologies, standards and European policies within the digital security and the Cyber security



Technology Evaluation Laboratory (Biometrics and Security)

« How to evaluate biometric injection attack within remote Identity Proofing solutions? »

May, Tuesday 2nd Munich

Confidential – Copyrights CLR Labs 2019

Ad Usque Fidelis
Cabinet Louis Reynaud



Some existing biometric certification schemes

- Biometric attacks

- ISO/IEC 30107 (PAD only)



- French ANSSI PVID



- ETSI TS 119 461



- Performances

- ISO/IEC 19795



New threat: biometric data injection attacks

- Described for the first time by French ANSSI in PVID certification scheme
- Also introduced by ETSI in TS 119 461
- Performed thanks to IT penetration testing technique



Why is it not an IT problem ?

- On face recognition, injection attacks can be made with:
 - Virtual cameras
 - Overwriting camera images
- Mobile apps and web apps **can't be considered as trusted environments**. Nowadays architectures do not allow us to identify images from a unique camera.
- Countermeasures to this new threat **must rely on biometric aspect**. IT security features (e.g, code obfuscation, virtual camera detection, root detection) are not sufficient.



Identity Proofing Solutions : impact of this new threat

- Based on web app or mobile app which are vulnerable against injection and presentation attacks.
- Today: security highly based on PAD subsystems. **PAD won't detect injection attacks as there is no artifact.**
- A.N.S.S.I. decided to add human operator in their referential as no automatic solution is able to detect deepfake like one presented in previous slide.
- **Injection attacks ≠ deepfake.** If a system does not implement randomness, a simple photo injected will fool it.



Conclusion

- The main threat against identity proofing is injection attacks as presentation attack detection is pretty mature. Note that this threat do not only concern biometrics but also ID documents...
- There is a real need to develop biometric data injection attack detection systems to protect remote biometric systems.
- CLR Labs is editor of a new standard (TS) at CEN about biometric data injection attack detection.

