REMOTE IDENTIFY PROOFING WORKSHOP

REMOTE VIDEO IDENTIFICATION: ATTACKS AND FORESIGHT

The European Union Agency for Cybersecurity (ENISA) organized a one-day physical workshop[1] on 10th May 2023 in Amsterdam, dedicated to the topic "Remote Video Identification: Attacks and Foresight".

The workshop was attended by more than 100 participants. Guest speakers from EU Supervisory Bodies (SB), remote identity proofing solution vendors and testing laboratories experts presented the current landscape of threats and challenges and discussed possible solutions to them.

The workshop comes at a time of increasing concern and interest in the rapid evolution of (new) cyber attacks. ENISA is currently working on a study to address new developments in attacks, countermeasures, and good practices in remote identity proofing, which will complement two previous reports.

Key Takeaways

National implementations

Multiple remote identity proofing allowed by the same SB

Need of a harmonized regulatory framework regarding remote identity proofing testing and certification

Challenges to sectorial enforcement and supervision include the absence of legislation at national level and a skills gap

Innovative identification methods may be available in 2 years

Remote Identity Proofing Attacks

Deepfakes are a major concern

AI perceived as a game changer

Injection attacks introduce persistent threats to biometrics systems and are on the rise due to scalability

eIDAS 2.0 to provide high levels of assurance

Good Practices for Remote Identity proofing

A dynamic approach, rather than static, is needed for auditing purposes

Some good practices include risk management, security by design, regular pentesting, and use of combined human+machine defensive systems

Survey results

56% of respondents have experienced a Remote Identity Proofing attack in 2022

Generative AI deepfake presentation ranked as the most difficult attack to mitigate

Pentesting is perceived as the most effective control

Lack of harmonized regulatory framework is the main challenge

[1] https://www.enisa.europa.eu/events/remote-video-identification-attacks-and-foresight

WORKSHOP DETAILS

National implementations

During the first, “national implementations” section, the Supervisory Bodies presented the status of their national implementations and requirements for remote identity proofing, aligned to the eIDAS Regulation and the national legislation in place. Regarding the conformity assessment of these methods, it was highlighted that a conformity assessment report (CAR) which provides confirmation of equivalent assurance to physical presence (eIDAS par 24.1.d) is required. Also, it was emphasised that remote identity proofing is allowed only for short-term qualified certificates (“ad hoc” certificates) and cannot be used for issuing qualified website authentication certificates (QWAC).

Remote identity proofing is not recognised at national level in all Member States

One of the supervisory bodies presented its national certification scheme for remote identity proofing, aligned with the eIDAS regulation. Important aspects of this presentation were the assurance levels of the certification scheme and the rigorous risk analysis involved in designing the certification scheme to identify an exhaustive set of requirements to prioritize the criteria of the remote identity proofing methods.

The use of remote identity proofing in many sectors (eID & trust services, banking, mobility & healthcare) and the lack of national legislation, force the supervision to be made on a case-by-case basis. Moreover, the challenges for auditors and supervisory bodies are related to the lack of specific skills in the context of emerging threats targeting remote identity proofing processes.

Important views during these sections where the fact that a supervisory body allows two types of remote identity proofing to take place: video with identity proofing operator and the so called “innovative identification methods”, where an automated proofing procedure is followed). Innovative identification methods are not yet officially recognized at national level and are provisionally recognized, and it was pointed out that it may take up to two years for this recognition.

The goal of attackers is identity fraud. Attacks may be aimed at the biometrics, the ID document, the front-end, and/or the back-end

One of the issues mentioned multiple times was the capability to read the NFC chip of the national identification documents (identity, passport), since attacks against these documents are increasing. Document verification during remote identity proofing could provide adequate assurance when introducing NFC reading which is considered reliable for the next couple of years.

The main challenges identified were the need of a harmonized regulatory framework regarding remote identity proofing testing and certification, the continuous need to assess vendors and providers, the constant precedence that attackers have against defenders and the need to keep up with the technological and adversarial advancements.

Remote Identity Proofing Attacks

During the section on “remote identity proofing attacks”, one of the remote identity proofing solution vendors reported that only 0.3% of all identifications are detected as attacks, 75% of which are presentation attacks, and of those presentation attacks, 50% are pictures (photos). Presentations attacks based on “deepfakes pose a big challenge. The suggestions were not to rely on biometrics solely, but also to add another trusted factor (e.g. passport), utilize up-to-date Presentation Attack Detection (PAD) software, include human operators in the presentation attack detection processes, avoid solely rely on a certification but employ external penetration testing by accredited labs and, to detect and block spoofed or emulated devices.

AI is a game changer

Throughout the workshop it was evident that artificial intelligence (AI) is rapidly evolving to a key element in the context of remote identity proofing, both in offensive and defensive aspects. The evolution of AI and machine learning technologies is a game changer, as it allows attackers to produce easily, ultra-realistic photo and video artifacts, which makes the detection of fake image or video of a person presented during a remote identity proofing session quite complex. Of course, automatic, AI-powered detection solutions are already available and constantly evolving to effectively spot fake artifacts but a hybrid approach where an AI-assisted decision is verified by a human operator, was mentioned multiple times as a more effective measure.

It was interesting that video injection attacks (e.g. web browser on computer, web browser on mobile, mobile app) have shown a 149% increase in the second half in comparison to the first half of 2022. There are currently more than 80 tools for face swapping and face swap injection attacks show a 295% increase during the same period. The main difference between presentation attacks and injection attacks is that the latter do not require the construction of physical artifacts/presentations and they rely on different techniques which require new approaches for the proper detection and mitigation. Injection attacks are considered the way to introduce persistent threats to biometric systems, they can be automated and performed in a scripted way without much of human involvement, and they are cheaper to launch than presentation attacks. This proves the scalability of injection attacks and the rapid evolution of attacks based on generative adversarial networks and synthetic imagery.

Human operator remains a key role and constant training is required

Good Practices for Remote Identity Proofing

During the third section on “good practices for remote identity proofing”, standardization and regulatory bodies, conformity assessment bodies and biometrics testing laboratories presented their views and provided insights and recommendations.

Regarding audit practices, it was explained that the currently static approach in auditing should be shifted to a dynamic one, since today’s challenges require a dynamic process where core elements are constantly changing and that a quality - security - assurance management triptych is required.

According to a testing lab representative, some good practices for operating a remote identity proofing system include: a clear business model, compliance with regulations and standards, defense against fake IDs, biometrics presentation and injection attacks, implementation of cybersecurity hygiene and good practices and the application of risk management, security by design, penetration testing, audits and annual reassessments.

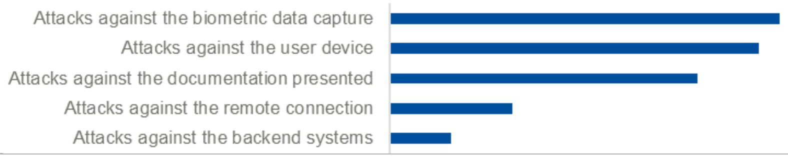
Serious need for a harmonized landscape

More than five years of research are needed to identify effective countermeasures for injection attacks. Fully automatic remote identity proofing systems are not enough for critical use cases; combination of automatic and human methods is key supported by continuous training of operators. Finally, during the panel discussion, it was highlighted that a high assurance level will be set by the revised eIDAS Regulation (eIDAS 2.0) and the need for a common regulatory landscape was underlined repeatedly.

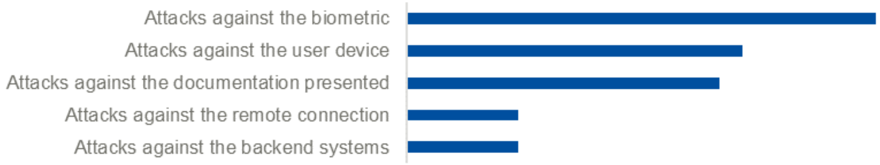
The presenters agreed that a Conformity Assessment Report for a remote ID process/solution/method, issued by a Conformity Assessment Body should be considered sufficient, which will attest that the assessed identity proofing method has equivalent assurance to physical presence (art. 24 par.1d eIDAS Regulation), special technical and personal requirements have been checked and resilience tests have been conducted.

SHORT AFTER-EVENT SURVEY FINDINGS

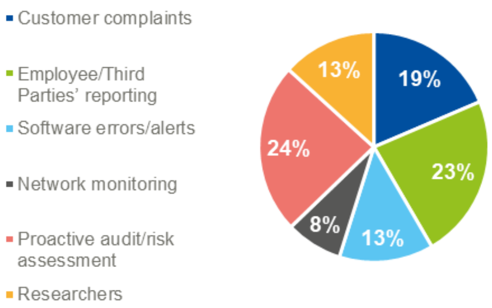
Most Vulnerable attack areas



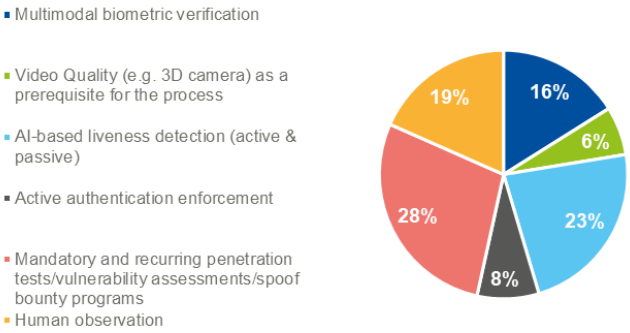
Attacks increased in the last year



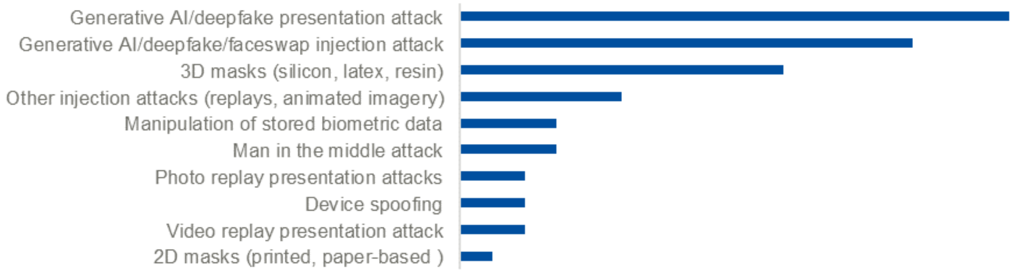
Channels used to identify/detect attacks



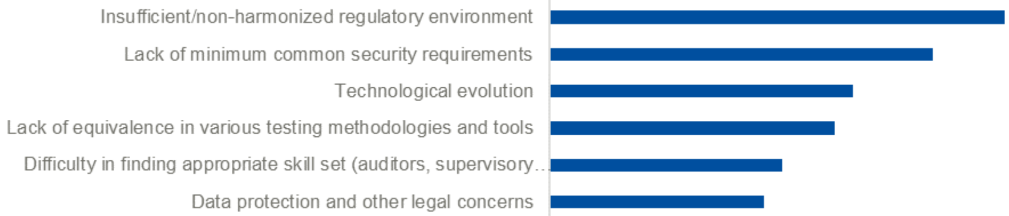
Most effective controls to provide higher assurance for the security of the process



Attacks harder to mitigate



Main challenges



Further Input

- Governments need to invest on testing labs (public & private), so technologies can be evaluated before regulations. This would be a continuous/recurring operation, not static
- The regulatory environment should allow private and public testing labs to use forged identification documents for testing purposes
- Statistics on incidents would be great for awareness and becoming aware of best practices
- Companies operating in multiple countries face major challenges among the differences in national acceptance under article 24.1.d of eIDAS
- It would be helpful if remote identity verification methods had similar interoperability as the Notified eIDs, whose LoA is recognized across member states and not subject to national law