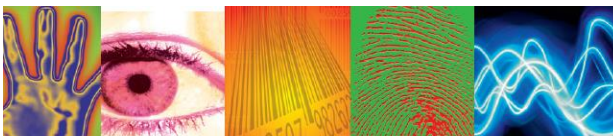


Biometric Vulnerability Assessment Checklist

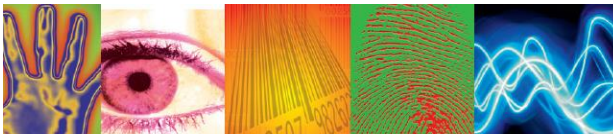
The Biometrics Institute has put together this checklist to help guide members, in particular users and integrators, to address vulnerability assessments in biometrics.

A vulnerability is the susceptibility of any system to internal or external attack. It deals with how difficult it is for a determined attacker to trick the system into misclassifying their identity. It is different from accuracy, which is focused on the chance of misclassification from a random person rather than attempting to fool the system.

Whilst a security vulnerability can include any aspect of the overall system, biometric vulnerabilities focus on those aspects relevant just to biometric applications. This includes for instance the use of fake biometric artefacts, for example masks, or weakness in biometric template storage or vulnerabilities in matching algorithms.

We have consulted our experts to suggest a few questions you may want to consider when planning or implementing a biometric system from the perspective of vulnerability.

- ☐ What are the likely potential vulnerabilities for your technology? (e.g. masks, fake fingers, stolen biometric templates)
- ☐ Do you have a risk management plan, and does it include the potential for biometric vulnerabilities?
- ☐ Are you aware of the difference between a standard false accept rate and the chance of a biometric vulnerability?
- ☐ What vulnerability-related documentation exists for your biometric system?
- ☐ Are there any configuration options for the vulnerability detection?
- ☐ Will there be tradeoffs in performance using the vulnerability detection?
- ☐ How is a potential vulnerability notified?
- ☐ What types of conditions might create a false vulnerability alert?
- ☐ Do you have a plan in your enrolment or verification workflow that supports the detection of potential attacks?
- ☐ What mitigations can be established to protect against vulnerabilities?
- ☐ How will you conduct an assessment of biometric vulnerability issues? (i.e. using internal or external resources)



Further reading

Biometrics Institute Top 10 Vulnerability Questions

Biometrics Institute Presentation attack detection and liveness guiding document

Biometric presentation attack detection series

- ISO/IEC 30107-1:2016 - Information technology – Biometric presentation attack detection – Part 1: Framework

  ISO/IEC 30107-2:2017 – Information technology – Biometric presentation attack detection – Part 2: Data formats

- ISO/IEC 30107-3:2017 – Information technology – Biometric presentation attack detection – Part 3: Testing and reporting

- ISO/IEC 30107-4 Information technology – Biometric presentation attack detection – Part 4: Profile for testing of mobile devices

Contact

This checklist was compiled by the Biometrics Institute Security and Integrity Expert Group.
If you have any questions or comments about this document, please email manager@biometricsinstitute.org.

Disclaimer

The Biometrics Institute provides guiding material as a tool to help its members conduct due diligence. While the institute has used reasonable care to ensure the accuracy of the material, due to the content and variable inputs during and after the process of implementing biometrics, the institute cannot be held accountable for outcomes or compliance. The material has been prepared for informational purposes only and is not intended to provide legal or compliance advice. Organisations should consult industry experts should they require advice on the technical, legal or compliance aspects of the material.

Last updated: August 2020