State-of-the-Art in Biometrics for Multi-Factor Authentication in a Federative Context

Martijn Oostdijk[1], Arnout van Velzen[1],
Joost van Dijk[2], Arnout Terpstra[2]

[1] InnoValor, P.O. Box 321, 7500AH, Enschede, The Netherlands
{martijn.oostdijk, arnout.vanvelzen}@innovalor.nl

[2] SURFnet, P.O. Box 19035, 3511EP, Utrecht, The Netherlands
{joost.vandijk, arnout.terpstra}@surfnet.nl

Keywords: biometric authentication, multi-factor authentication, identity federations

Biometrics have been a promising technology for authentication for a long time, yet have not seen large scale adoption. The advantages of biometrics or "something-you-are" are clear when compared to traditional "something-you-know" and "something-you-have" authentication factors, such as passwords and smartcards respectively. For example, users are always in the possession of a biometric authentication token. Yet, the technology also faces some challenges. One of these challenges is the cost associated with introducing the technology to a mass audience. With the advent of smartphone and other mass market mobile devices equipped with sensors suitable for biometric capturing (camera, microphone, fingerprint sensor, heart monitor) this shortcoming appears to have been almost solved for some modi. In addition, multi-factor authentication itself has received increased attention lately as witnessed by the emergence of standards such as FIDO. These recent trends urged the Dutch NREN SURFnet to assess the current state-of-the-art of biometric authentication with a focus on use-cases within an NREN federative context, as a precursor to a proof-of-concept.

Comparing the different biometric modi is not trivial. There are innumerous biometric modi, of which fingerprint, face, iris, retina, and voice are probably the most well-known for authentication. The state-of-the-art scan that was conducted in the current study firstly presents a long list of all known biometric technologies for authentication based on desk research. This list ranged from the above mentioned traditional physiologic and behavioral modi to exotic modi such as butt impression and otoacoustic emission. A short list of most suitable technologies was then composed and reviewed by various experts in the field. The short list contains the following modi: *fingerprint*, *iris*, *retina*, *finger vein*, *eye vein*, *face*, *heart rate*, *voice*, *handwritten signature*, *user interaction*, and *gesture*. The state-of-the-art scan applied five key criteria on which the different technologies were scored. These criteria are: *performance*, *security*, *universality*, *user friendliness*, and *fit-for-purpose in a federative setting*, which will be explained in more detail in the remainder of this paper.

The performance of different biometric technologies has been compared in the past, both by the independent research community and by technology vendors in large scale tests (e.g. the so-called "grand challenge" tests as organized by NIST). In such tests biometric technologies are compared on performance metrics such as false acceptance rate, false rejection rate, failure to enroll, etc. Recent developments embed the biometric sensors for the traditional modi in consumer hardware devices (e.g. Apple's Touch ID) and also introduce new modi like finger vein pattern, eye vein recognition, heart rate, and various behavior based

technologies. Commercial vendors nowadays appear to be more protective of their intellectual property. This makes it harder to compare the performance of new biometric technologies.

The security of biometric technologies depends on the ability to keep adversaries from spoofing the sensor. Liveness detection may help to mitigate the risks associated with the former challenge.

The universality of biometric technologies is affected by the availability of the technology. The inclusion of a suitable sensor in a mass market electronic product, especially when that product is mobile and strongly bound to the end-user, makes it very likely that a large audience of students and staff-members will be able to access the particular technology. Contrarily, the need for dedicated (and often costly) additional hardware has a negative impact on the universality criterion. Also, universality is determined by the biometric technology functioning properly under different circumstances and over time.

The user friendliness of biometric technologies is influenced by the intrusiveness of the biometric mode and the complexity and effort of use. For instance, for retina scanning the camera needs to be very close to the user's eye. Also, the time it takes to perform a scan during enrollment and authentication influences the user friendliness of the solution.

The fit-for-purpose of biometric technologies depends on how well the technology integrates within the existing authentication infrastructure. Consider, for example, the characteristics of the user base and authentication process, scalability of the solution, or business case. The architecture of the federation also influences this criterion. Within an identity federation the responsibility for authentication is delegated to the identity provider, so that so-called continuous authentication is less obvious. Some biometric technologies require a tighter integration of the authentication process and the service provider. This especially holds true for technologies that rely on user behavior rather than physiological features such as user interaction, gesture recognition, heart rate recognition, etc. Another important factor to fit-for-purpose is the maturity of the technology and market; experimental technology or a few small vendors may adversely affect the decision to adopt biometric authentication solutions.

After applying the criteria to the list of biometric technologies, the solutions that appeared to be most promising for second factor authentication within an NREN's identity federation are: firstly, fingerprint recognition using either a specialized sensor (as is becoming increasingly common on high-end smartphones), or using the device camera, is a safe choice in terms of performance, universality, and convenience, yet has some issues with security (spoofability). Secondly, eye vein recognition is a reliable solution, although it is patented by a single vendor, hence objective assessment of this technology proved difficult. Thirdly, facial recognition using the generic device camera is a good option, yet performance is sub-optimal. The other technologies either have poor performance, require dedicated hardware, are not sufficiently mature, or require tight and continuous integration with the service provider.

On a final note, comparing biometrics is notoriously complicated, in part because much depends on the properties of specific solutions and vendors. Aside from the five key criteria discussed above, important characteristics to assess are existing user base of the particular solution, compliancy to technological standards such as FIDO, template protection and other security features, and agreement with privacy regulation.

SURFnet plans to conduct a proof-of-concept with academic institutions in the first quarter of 2016, based on the above state-of-the-art study. Early results of this PoC are intended to be presented at TNC 2016 in conjunction with the results outlined here.

About the authors:

- Martijn Oostdijk works as a Senior Advisor and Software Architect at InnoValor and combines a background in hard security with a broad interest in Identity, Privacy & Trust related topics.
- Arnout van Velzen is a Junior Consultant at InnoValor in the areas of identity and access management, privacy and cybersecurity.
- Arnout Terpstra is working at SURFnet as a Product Manager Trust & Identity. He spends half of his time working on daily administrative tasks for several services and products related to SURFconext. The other half of his time is spent on innovation activities, such as examining what impact the changes in the world of Identity Management have for SURFnet and SURFconext.
- Joost van Dijk is technical product manager at SURFnet. He works on innovation projects in the area of Security, Privacy, and Trust.