German TTT Biometrics Working Group Meeting on September 21st, 2016

The spring meeting of the German Biometrics Working Group was hosted by Fraunhofer IGD (https://www.igd.fraunhofer.de/) and took place on September 21st, 2016. The meeting with 53 participants featured numerous reports on biometric applications and most recent research results.

The event was introduced by Christoph Busch, who presented the Center for Research in Security and Privacy (CRISP). In addition, he announced several forthcoming events, including the European Biometrics Research and Industry Awards, and a Special Issue in Datenschutz und Datensicherheit (DuD) on biometrics.

Frank Smith (ENLETS Mobile) reported on mobile biometric solutions for law enforcement. He noted that, given the current trend in which mobile devices are overtaking the market, and foreseeable even more when 5G arrives, mobile id is becoming of special relevance. Not only through smart cards but also using smartphones, via applications such Apple TouchID or ApplePay, or the NFC reader for the passport. Law enforcement hence aims to protect (e.g., from spoofing attacks) and serve the public. He presented two particular case studies, namely:

- Immigration enforcement (illegal entry/working). At present 2 fingerprints are used for identification purposes. The QuickCheck program (2002) was replaced by RapID (2010), and a new program will be launched in the near future.
- MEOS (Mobiel effectiever op straat, Netherlands), used by operational front-line police. Officers were part of the design team. It includes ANPR (automatic number plate recognition) and fingerprints.

Both projects have received a fantastic feedback from FBI, Sweden or Accenture. Therefore, a progressive deployment is planned, reaching over 25K devices.

Ole Tom Seierstad (Microsoft Norway) presented biometrics in Windows 10. In particular, how biometric information is used to identify the subjects, and more importantly, protected, by Microsoft Windows Hello. Recognition is based on iris, using the Intel Real Sense Camera, which incorporates a 3D capture device, depth and infra-red sensors, as well as a visible spectrum camera. Easy sign-in also includes fingerprints, and both characteristics can be used on the smartphone under the same framework. Biometric data is protected through a secure hardware, which grants device integrity and includes a TPM to protect critical secrets. More specifically, biometric data is stored encrypted in the Virtual Secure Storage area, which cannot be accessed by any other application, only through the TPM. He highlighted that all devices run the same framework, and that Microsoft also features an integrated browser: Windows Edge. If Windows Hello is enabled, you can also verify the id for other applications such as online shopping. In addition, he run two demos on the smartphone and the laptop to show the new Windows functionalities. He finally added that, if there is an Intel Real Sense camera on the laptop, face verification will be possible as well. In terms of standardized secure methods, he remarked that Microsoft is part of the FIDO alliance.

Gemma Galdon Clavell (eticas Research & Consulting, Spain) addressed the problem of how EU IT systems grant fundamental rights in biometric deployments for border control, visa and asylum seekers. She started by pointing out the lack of assessment on the ground. To palliate this fact, surveys with staff, applicants, BCP (Border Crossing Point) staff were carried out, as well as interviews with experts and right-holders. In addition, observations were made on the ground. Those reports showed several deficiencies, such as the need for moisturizers or wipe towels for fingerprint acquisition, or problems with the handicapped. All these facts result in a need to take into account other factors from a policy perspective, not only technology, before deploying automatic biometric verification systems. In addition, there is no perception of the added value of biometrics by the BCP staff – training is necessary. Another common perception is that machines are less discriminative than body guards, and hence the latter are preferred by citizens in many cases.

Christophe Remillet (One Visage, Switzerland) reported on 3D facial authentication technologies. He started with some figures of the market: there are +18 billion connected devices, +1.8 billion smartphones (December 2015). He also highlighted that Cyber-crime is exploding ($430 billion cost of cyber-crimes, huge compared to $160 billion for natural disasters, +429 million ids exposed in 2015). And over 30% transactions are rejected due to two-step authentication (e.g., PIN never arrived). Identity management is thus key to many tasks. In that regard, six challenges have been identified with customers: user-experience, security, data privacy, architecture, universality and cost. And it is hard to reach a compromise.

In his application (SelfiePass), the smartphone is regarded as the new security token, and the FIDO UAF protocol, secure containers and encryption are used to provide security and privacy protection. Face 3D is used for verification, and a demo was run during the report. Risk assessment is carried out testing spoofing attacks in collaboration with IDIAP, and a new anti-spoofing algorithm will be added to the application.

Artem Kukharenko (N-Tech.Lab) presented their results on face recognition and the Megaface competition. He started introducing the LFW face dataset, which includes 13K photos from 5K people. Given the almost perfect accuracy reached, new datasets are needed, such as the Megaface challenge (1M ids), in which more than 100 teams were enrolled. The N-Tech.Lab achieved the best results (rank 1 73.30% accuracy, better than Google's FaceNet) using deep learning with the AlexNet architecture. 20M phace photos were used for training during 3 weeks on 3 GPUs NVidia Titan Black. Face occlusions were also studied and he highlighted that the obtained feature vectors of 16 floats can be used to classify other soft-biometrics such as gender (SVM 99.5% acc for 1K). Furthermore, the net was proved to outperform humans in a large scale recognition problem. He also presented FindFace.ru, a Russian social net with 250M photos. You can look for people similar to a given photo, using publicly available images. This is useful for applications such as looking for lost relatives, or for criminals. Finally, when asked "What's different from Google deep learning?" he answered that that was a difficult question, since Google's architecture is not fully known. NTechLAB main advantage is the fast training, which allowed multiple training and optimization of their 10 layer network.

The day concluded with some updates from Christoph Busch (CRISP), who summarized the main standardization efforts in the field of biometrics, including the new framework for biometric sample quality assessment (ISO/IEC 29794-1), the publicly available Harmonized Biometric Vocabulary (ISO/IEC 2382-37), the NFIQ2 toolkit and the recent ISO/IEC IS 30107-1:2016 framework for Presentation Attack Detection (PAD).

Slides of the meeting are available at: http://eab.org/events/program/105

The next meeting will take place in Berlin on December 13, 2016.
The agenda will be announced at: http://eab.org/events/program/127