Appendix 3

INVENTORY OF ATTACKS

TABLE OF CONTENTS

FRUSTRATION OF ENROLLMENT AND VERIFICATION

In case of a genuine rejection, a subject may nevertheless claim to be falsely rejected. The relevant biometric feature may be mutilated or manipulated in order frustrate the verification process. Subjects may refuse to cooperate during enrollment and verification thus frustrating the verification process.

In all these cases, a subject can enforce to pass through the fall back procedure. A relatively weak fall back procedure is an attractive alternative for frauds.

SPOOFING OF BIOMETRIC FEATURES

Masks, lenses and thin films

Spoof life biometric feature: in case of iris recognition, lenses may be used; in case of finger recognition, thin rubber or silicon; in case of face recognition, heavy make up or masks

Gelatin copies of biometric features defeat liveness detection

'A study on the performance evaluation of the liveness detection for various fingerprint systems' [26] shows that gelatin copies of fingerprints can easily mislead verification units. If immediately used or until 24 hours later, the optical sensor is (almost) 100% spoofed; the capacitive sensor is spoofed almost 95%. If immediately used the tactile sensor is spoofed 90%; the thermal sensor 40%. After 24 hours, the tactile sensor is spoofed 70%, the thermal sensor 60%. The thermal sensor seems relatively successful in detecting gelatin forgery, but it is not clear what bandwidth was allowed. Generally, a large bandwidth will be imperative due to the conditions of verification on airports and offices, people walking in when its freezing outdoors. This might render a thermal sensor useless.

Collect fingerprints and make your own copy

In "Biometrical Fingerprint Recognition: Don't get your fingers burnt" [38] Ton van der Putte and Jeroen Keuning describe the limited effect of countermeasures against the use of artificial biometric features. They mention a couple of risks because of the fact that using artificial biometric features is relatively easy and successful:

- A fingerprint from someone who is granted access can be intercepted
- People handling transactions can claim to be framed by someone intercepting their fingerprint; and
- People can even cooperate with intercepting or copying their fingerprint and at the same time claim that they are framed.

The authors subsequently state that fingerprint systems are the only type where the biometric features can be stolen without the owner noticing it or reasonably being able to revert it. Although this risk is not limited to fingerprints (optician, mini-camera's), but nevertheless I think they make a point. The authors conclude that for this reason, comparing all biometric verification possibilities, fingerprint scanners are the least secure means of verification.

Spoof live biometric features and eat the evidence

In "Impact of Artificial 'Gummy' Fingers on Fingerprint Systems" [35] Tsumoto Matsumoto and others describe in detail the possibilities open to those using gummy and gelatin fingers. As an additional illustration of the fact that spoofing of biometric features is difficult to detect, I quote Bruce Schneier [36], who says: "Gummy fingers can even fool sensors being watched by guards. Simply form the gelatin finger over your own. This lets you hide as you press your own finger onto the sensor. After it lets you in, you can eat the evidence".

LAMBS AND GOATS

Lambs

The application of biometric technology might bring look alike fraud on a higher level [10]. Impostors might try to obtain the ID of a so called *lamb*, an individual whose biometric feature is weak in the sense that on verification it has a relative high probability of matching to someone else's biometric feature. Successful application of *lamb* biometric features in spoofing life or stored biometric features is a risk to be considered.

Goats

A goat is the logical counterpart of a lamb. The biometric feature of a goat is beyond the range allowed by the system and may consequently be falsely rejected by the system. Depending on the number of goats, the false rejections may lead to complaints and a loss of confidence from the side of the public.

Virtual lambs and goats

An analysis performed by the 'Nederlands Forensisch Instituut' (Dutch Forensic Institute) [12] shows that a biometric template of an iris can be changed in such a way that more than two persons are accepted by the system. They do not mention how many people exactly, and out of which group (composition and size) these three or more people were chosen (I assume they weren't a set of triplets). In other words, they created what I would like to call a 'virtual lamb' i.e. a forged stored biometric feature that will lead two acceptance if compared with more than one live biometric feature. The question is whether this deficiency also applies to a biometric feature stored as a digital image and other biometric features like fingerprints and faces. In addition, as there is only one supplier for iris recognition technology, it is not clear whether the algorithm used influences this problem.
Furthermore, they found lenses with which they successfully mislead the system. The resulting hamming distance was between 250 and 320 but the system did not come up with the warning 'no living eye'.

MANIPULATION OF OPERATING POINT

The report of the Ministry of the Interior and Kingdom Affairs [8] points out that systems can be configured to produce a lower FAR at the cost of a higher FRR and vice versa. The specific setting of the system performance is called the operating point. The report points to the fact that manipulation of the operating point makes the system vulnerable and biometric systems should therefore store and analyze information about (potential) intrusion or misuse of system settings.

In my opinion, the measures proposed here are insufficient to protect the system against attacks. In order to create a secure system, the operating point should be fixed, automated or centrally managed. If not, quick and dirty or corrupt employees might make a mess.