Wider das unauslöschliche Siegel

Peter Bittner
peter@pbittner.de

Forum InformatikerInnen für Frieden
und gesellschaftliche Verantwortung
Köln

Ziel dieses Beitrages ist es, Strategien zur Überwindung biometrischer Verifikationen und Identifikationen darzustellen. Zur Überraschung vieler wird gezeigt, dass das Unterwandern, Hintergehen und Austricksen biometrischer Systeme überhaupt kein neues Phänomen ist.

Bereits 1907 beschreibt R. Austin Freeman in seinem Roman „The Red Thumb Mark" eine Hightech-Methode zur Herstellung einer Gelatinefolie mit einem „falschen" Fingerabdruck. Frappierend ist, dass mit der dort beschriebenen Methode noch heute (einige) optische Sensoren überwunden werden können. In den Geschichtsbüchern verschwunden sind die vielfältigen Versuche von Verbrechern der 30er und 40er Jahre, einem „Wiederauffinden" der Fingerabdrücke in der FBI-Fingerabdruckkartei zu entgehen. Der Autor hat sich auf den mühsamen Weg gemacht, die „alten Geschichten" zu recherchieren und mit den heutigen Strategien zu vergleichen. Neben dem Rückgriff auf die Geschichte und den aktuellen Stand der Technik wird aber auch auf filmische Thematisierungen der Überwindung aus verschiedenen Genres (u.a. dystopische Gesellschaftsentwürfe, Actionthriller, Agentenfilme, Science Fiction) Bezug genommen – immer mit dem Blick auf das vielleicht bald schon Mögliche.

Dem Autor geht es aber nicht um eine bloße Aneinanderreihung von Beobachtungen. Ziel ist es, eine Systematik der Überwindung vorzulegen.

Zunächst geht es um Mittel und Wege, eigene Spuren zu vermeiden oder zu beseitigen. Hernach stellt sich die Frage der gezielten – zeitlich befristeten oder persistenten – Elimination oder Veränderung des Merkmalsträgers zur Verschleierung eigener Spuren. Als Plagiate könnte man die Wiederverwendung vorhandener Spuren bezeichnen. Eine Latenzbildreaktivierung auf einem Sensor gehört in diese Kategorie. Verwirrung stiften Kontextwechsel, wenn „abnehmbare" Spuren an einem anderen Ort hinterlassen werden. Die damit verbundenen Verwirrungen beschreibt z.B. der Film „Fingerprints don't lie" aus den 50er Jahren. Unter dem Oberbegriff Ent-Eignung könnte man die Varianten zusammenfassen, bei denen der Merkmalsträger gewaltsam von Fremden genutzt wird. Prototypisch wären hier der bewusstlose Wachmann, dessen „berechtigender" Finger auf einen Sensor gelegt wird oder der Autofahrer, dem von Dieben ein Finger abgetrennt wurde, um die biometrische Wegfahrsperre zu überwinden. Weiters besteht die Möglichkeit von „echten" Vorlagen Attrappen herzustellen. Wege der technischen Reproduzierbarkeit kennen wir dank Freeman seit 1907, wie einfach die Reproduktion ist, haben

der Chaos Computer Club, aber auch japanische Forscher wie Matsumoto eindrucksvoll gezeigt. Schließlich bleibt der Weg des Transfers von Merkmalsträgern. Prototypisch seien hier Transplantationen von Fingern, Händen und Gesichtern genannt.

Dies sind alles „Angriffe von vorn“. Sehr gut vorstellbar sind auch Manipulationen der Datenbanken, in denen biometrische Rohdaten oder Templates abgespeichert sind (Backend-Angriff) oder Angriffe auf die Kommunikationsstrecken im System bzw. auf Systemkomponenten, z.B. durch Veränderung der Vergleichseinheit oder die Veränderung des Sensors.

Es stellt sich also nicht nur die Frage des „authentischen“ Nutzers. Die letzten Bemerkungen machen klar, dass man auch die Frage stellen muss, unter welchen Umständen ein „Nutzer“ überhaupt wissen kann, dass er es mit einem „authentischen“ Biometriesystem zu tun hat?