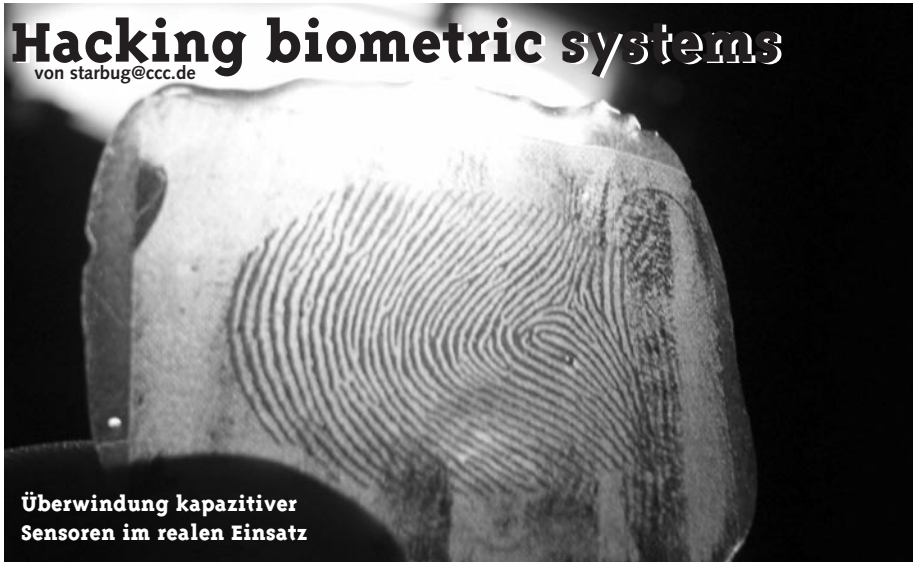
Hacking biometric systems

von starbug@ccc.de



Überwindung kapazitiver Sensoren im realen Einsatz

Nach dem c't Bericht zur Überwindbarkeit von verschiedenen biometrischen Systemen Mitte 2002 (http://www.heise.de/ct/02/11/114/) kam von einigen Seiten, der Vorwurf, dass es sich bei den Tests nur um Laborversuche gehandelt hätte. Vor allem die Firmen der getesteten Systeme meinten, dass solche Überwindungen in der Realität nicht durchführbar wären.

Da diese Feststellungen ja durchaus nicht von der Hand zu weisen waren lag der Fokus der weiteren Arbeiten darauf, die "Angriffe" auch in der Öffentlichkeit unbemerkt durchführen zu können. Die Erfolge sollen hier, am Beispiel eines erfolgreichen "Angriffs" auf das Bezahlsystem des Offiscom-Shops in Offenburg dargestellt werden.

Bezahler per Fingerabdruck im Officecom-Shop

Gestartet wurde der Einsatz des Fingerabdrucksystems "digiPROOF" Anfang 2003. Die Firma "it-werke" rüstete dazu den Officecom-Shop (http://www.officecom-shop.de/index1.php) mit einem kapazitiven Sensor aus. Mitmachen kann jeder, der ein eigenes Konto und ausreichend ausgeprägte Fingerabdruckmerkmale besitzt. Dazu füllt man lediglich ein Formular mit der eigenen Bankverbindung aus, beweist die eigene Identität anhand des Ausweises und lässt einen Finger in das System einlernen.

Will man einen Artikel kaufen, gibt man lediglich seinen Namen an und legt den Finger auf den Sensor. Der Betrag wird dann automatisch vom Konto abgebucht.

Szenarien des "Identitätsdiebstahls"

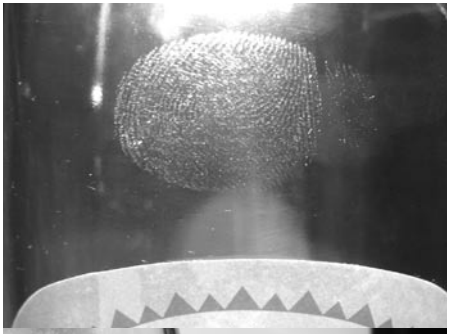
Beim Einsatz von biometrischen Systemen zur Authentifikation eines Bezahlvorgangs sind zwei Szenarien des "Identitätsdiebstahls" denkbar. Im ersten Fall stiehlt eine unberechtigte Person die Daten eines regulären Benutzers um so auf seine Kosten einzukaufen. Bei der anderen Möglichkeit arbeitet der berechtigte Benutzer mit und gibt freiwillig seine Daten der anderen Person weiter.

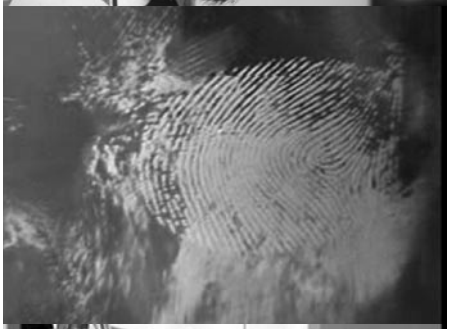
Szenario 1: Zur Durchführung benötigt man sowohl den Namen eines regulären Benutzers als auch einen Fingerabdruck des zur Verifikation verwendeten Fingerabdruckes. Den Namen und den verwendeten Finger erhält man am einfachsten bei der Überwachung eines Bezahlvorganges. Abdrücke von Fingern mit ausreichend guter Qualität hinterlässt man täglich bis zu 25 mal (http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf). Guckt euch nur mal eure Türklinke an oder den Hochglanzumschlag einer Zeitschrift, welche ihr freundlicherweise kurzzeitig gehalten habt, während ich mir die Schuhe zubinden musste...

Szenario 2: Dieses hat den Vorteil, dass man sich die Suche nach einem Benutzer und die Suche nach Fingerabdrucken erspart. Allerdings steht man hier dann dem Problem gegenüber, dem Ladenbesitzer und eventuell der Polizei erklären zu müssen, dass man an diesem Tag mit Sicherheit nicht einkaufen war. Ein gut gewähltes Alibi sollte aber Beweis genug sein.

Überwindung

Geht man vom ersten Szenario aus, ist es nötig, die hinterlassenen Fingerabdrücke sichtbar zu machen um



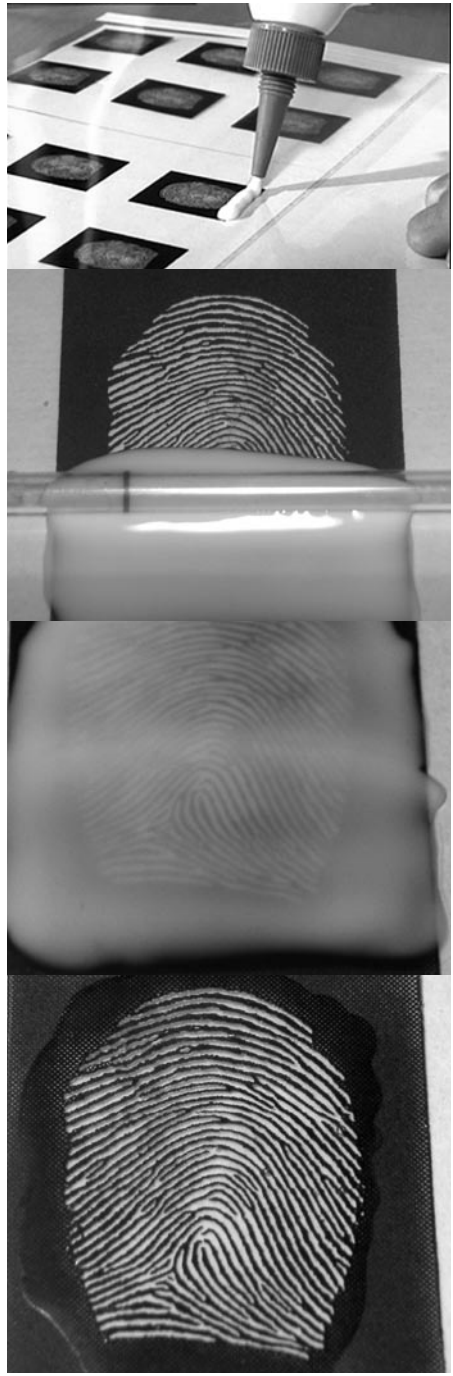


sie weiterverarbeiten zu können. Muss die Abnahme vor Ort (z.B. an einer Türklinke) geschehen, sollte man ein Verfahren wählen, das möglichst schnell den Abdruck sichtbar macht. Hierfür eignet sich das, aus der Polizeiarbeit bekannte, Bestäuben des Abdrucks mit Grafitstaub, Ruß oder anderen Farbpigmenten. Dabei bringt man neben dem Abdruck eine ausreichend große Menge Pigmente auf und streicht diese mit einem sehr feinen buschigen Pinsel vorsichtig über die Fettrückstände. Sind alle Teile gleichmäßig bedeckt nimmt man den Abdruck mit einem Stück durchsichtigem Klebeband ab. Gerüchteweise gibt es auch gewisse Inhaltsstoffe von Spülmitteln (Fit) die mit dem Fett eine Verbindung eingehen und durch UV-Bestrahlung sichtbar werden. Wenn jemand da mehr weiß, wäre ich für einen Hinweis dankbar.

Hat man ausreichend Zeit den Abdruck sichtbar zu machen, bietet sich der Einsatz von Cyanoacrylat, einem Hauptbestandteil von Sekundenkleber, an. Von diesem bringt man eine kleine Menge in einen Flaschenverschluss oder eine Überraschungseihälfte und stülpt das Ganze über den Abdruck. Das ausgasende Cyanoacrylat reagiert mit den Fettrückständen des Fingerabdrucks zu einer festen weißen Substanz. Durch Erwärmen kann man das Ausgasen beschleunigen, so dass auch hier nach ca. 10 min ein deutliches Fingerbild zu sehen ist. Die so oder mittels aufgepinselter Pigmente sichtbar gemachten Abdrücke werden mit einer Kamera oder einem Scanner digitalisiert und grafisch nachbearbeitet. Neben einigen automatischen Bearbeitungsschritten (Anpassen von Kontrast und Threshold) müssen manche Fingerlinien von Hand nachgezeichnet werden. Es ist daher ratsam, mehrere Abdrücke zu haben, um schlecht abgebildete Teile ersetzen zu können. Eine Software, wie sie benutzt wird, um Panoramafotos zusammenzustellen könnte hierbei hilfreich sein.

Die aufbereiteten Fingerbilder werden dann in eine 3D-Form überführt. Sie dient als Grundlage für die Herstellung der Attrappen. In den wenigen existierenden Publikationen zu dem Thema wird Gelatine als Attrappenmaterial und fotostrukturierbare Leiterplatten als Form verwendet. Da deren Bearbeitung, insbesondere der Ätzschritt, aber sehr aufwendig sind wurde nach Alternativen gesucht. Dabei stellte sich heraus, dass der Toner eines Fotokopierers auf einer Folie eine ausreichende Dicke besitzt, um für die Abformung genutzt zu werden. Auch die Gelatine besitzt einige negative Eigenschaften. In dünnen Schichten ist sie nicht besonders widerstandsfähig und trocknet sehr schnell aus. Außerdem muss sie zum Abformen unter Temperatureinfluss verflüssigt werden. Hier hat sich nach längeren Experimenten eine gut zu verarbeitende, stabile und billige Alternative ergeben: "Ponal" Holzleim.

Er trocknet nicht aus und ist auch sonst deutlich widerstandsfähiger. So kann man den Finger mit der angeklebten Attrappe weiterhin normal benutzen ohne den Abdruck zu beschädigen. Zur besseren Verarbeitbarkeit



und Erhöhung des Feuchtigkeitsgehalts kann man dem Holzleim eine kleine Menge Glycerin zusetzen. Gut durchmischt wird die Masse in einer dünnen Schicht auf die Form gerakelt, so dass nach dem Aushärten des Klebers (ca. zwei Stunden) eine Fingerabdruckattrappe von nur ca. 0,2 mm Dicke bleibt. Zum Ankleben dieser eignet sich wasserunlöslicher Maskenkleber von "Mastix" recht gut. Da die Sorte für medizinische Anwednungen extrem teuer ist, kann die alkoholbasierte verwendet werden. Allerdings beginnt der Alkohol den Holzleim nach ca. zwei Stunden zu zersetzen. Das sollte aber für die normale Anwendung nicht relevant sein.

Konsequenzen für den Einsatz von Fingerabdrucksystemen

Wie dem Artikel zu entnehmen ist, ist es möglich Attrappen von Fingerabdrücken mit sehr geringem Aufwand und einfachsten technischen und finanziellen Mitteln herzustellen und sie unbemerkt einzusetzen. Auch überwachte Szenarien bieten so gut wie keinen Schutz, da die Attrappen weitgehend unsichtbar sind. Anders als beim Zutritt zum Zoo von Hannover oder beim Bezahlen im Heilbronner Biergarten kann im Officecom Shop großer finanzieller Schaden angerichtet werden. Der Kunde oder Ladenbesitzer kann sehr schnell mehrere 1000 Euro verlieren.

Aber auch die Aufnahme von Fingerabdrücken in internationale Reisedokumente ist mit Blick auf diesen Artikel als überaus fragwürdig einzuschätzen. Die versprochene zusätzliche Sicherheit bei der Identitätsüberprüfung von Einreisenden existiert kaum. Auch weiterhin können Personen mit gestohlenen oder geliehenen Dokumenten einreisen, selbst wenn ihre Abdrücke in irgendwelchen Täterdatenbanken vorliegen. Da die Aufnahme zusätzlicher biometrischer Daten in Reisedokumente augenscheinlich so gut wie keinen Nutzen hat, im Gegenzug aber datenschutzrechtlich überaus bedenklich ist und außerdem mit sehr hohen Kosten zu rechnen ist sollte das Projekt nochmals kritisch begutachtet werden!