Importance of Open Discussion on Adversarial Analyses for Mobile Security Technologies
--- A Case Study for User Identification ---

14 May 2002

Tsutomu Matsumoto
Graduate School of Environment and Information Sciences
Yokohama National University
email: tsutomu@mlab.jks.ynu.ac.jp
Mobile Security Technologies

Security Architecture
Operating Systems Security
Software Tamper Resistance
Mobile Code Security
Physical Tamper Resistance
Communications Security
Cryptographic Protocol
User Identification

......
Security assessment of biometric user identification systems should be conducted not only for the accuracy of authentication, but also for security against fraud.

In this presentation we focus on Fingerprint Systems which may become widespread for Mobile Terminals.

Examine Adversarial Analysis as A Third Party

- Can we make artificial fingers that fool fingerprint systems?
- What are acceptance rates?
Fingerprint Systems

Typical structure of a fingerprint system

Types of sensors
- Optical sensors
- Capacitive sensors
- Thermal sensors, Ultrasound sensors, etc.

“Live and Well” Detection
A Risk Analysis for Fingerprint Systems

Attackers may present
1) the registered finger,
   by an armed criminal, under duress, or with a sleeping drug,
2) an unregistered finger (an imposter's finger),
   i.e., non-effort forgery,
3) a severed fingertip from the registered finger,
4) a genetic clone of the registered finger,
5) an artificial clone of the registered finger, and
6) the others,
   such as a well-known method as a “fault based attack.”
**Fraud with Artificial Fingers**

Part of patterns of dishonest acts with artificial fingers against a fingerprint system.

<table>
<thead>
<tr>
<th>Enrollment</th>
<th>Verification / Identification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>L(X)</td>
</tr>
<tr>
<td>L(X)</td>
<td>(1)</td>
</tr>
<tr>
<td>A(Y)</td>
<td>—</td>
</tr>
<tr>
<td>A(Z)</td>
<td>—</td>
</tr>
</tbody>
</table>

L(X): A Live Finger corresponding to Person X  
A(Y): An Artificial Finger corresponding to Person Y  
A(Z): An Artificial Finger corresponding to Nobody
Fraud with Artificial Fingers I

Enrollment

X
L(X)

Authentication

X or Y
A(X)

Y obtains A(X).

Distribution of A(X)s

A(X)s

Y
X
Fraud with Artificial Fingers II

X obtains A(Y).

X enrolls A(Y).

Authentication

Distribution of A(Y)s

X or Y

A(Y) or L(Y)
Fraud with Artificial Fingers III

Enrollment

Y makes A(X).

Authentication

Distribution of A(X)s

A(X)s
Mapping a Fingerprint onto Artificial Fingers

Fingerprint
e.g., Live Fingers, Generators, ...

Impression
e.g., Molds, Residual Fingerprints, ...

Artificial Finger
Known Results

Process 0

(1) Finger
(2) Mold
(3) Silicone Rubber Finger
Fact

Optical Sensor

Highlighted:
- Light Source
- Finger
- Detector

Legend:
- Often Accepts Silicone Rubber Fingers

Capacitive Sensor

Highlighted:
- Finger
- Array of Electrodes

Legend:
- Usually Rejects Silicone Rubber Fingers
Our Result

Process 1

(1) Finger
(2) Plastic Mold
(3) Gummy Finger
Recipe 1-1

Making an Artificial Finger directly from a Live Finger

Materials

Free molding plastic “FREEPLASTIC” by Daicel FineChem Ltd.

Solid gelatin sheet “GELATINE LEAF” by MARUHA CORP

Free molding plastic:
- Price: 350JPY/35grams

Solid gelatin sheet:
- Price: 200JPY/30grams
Recipe 1-2

Making an Artificial Finger directly from a Live Finger

How to make a mold

Put the plastic into hot water to soften it.

Press a live finger against it.

It takes around 10 minutes.

The mold
Recipe 1-3

Making an Artificial Finger directly from a Live Finger

Preparation of material

- A liquid in which immersed gelatin at 50 wt.%. Add boiling water (30cc) to solid gelatin (30g) in a bottle and mix up them. It takes around 20 minutes.
Recipe 1-4

Making an Artificial Finger directly from a Live Finger

How to make a gummy finger

Pour the liquid into the mold.

Put it into a refrigerator to cool.

It takes around 10 minutes.

The gummy finger
Similarity with Live Fingers

The photomicrographs of fingers

(a) Live Finger  
(b) Silicone Finger  
(c) Gummy Finger
Captured images with the device C (an optical sensor).

(a) Live Finger   (b) Silicone Finger   (c) Gummy Finger

Captured images with the device H (a capacitive sensor).

(a) Live Finger   (b) Gummy Finger
Experiments

Subjects: five persons whose ages are from 20’s to 40’s

Fingerprint systems: 11 types

We attempted one-to-one verification 100 times counting the number of times that it accepts a finger presented.

Types of experiments

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Enrollment</th>
<th>Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type 1</td>
<td>Live Finger</td>
<td>Live Finger</td>
</tr>
<tr>
<td>Type 2</td>
<td>Live Finger</td>
<td>Gummy Finger</td>
</tr>
<tr>
<td>Type 3</td>
<td>Gummy Finger</td>
<td>Live Finger</td>
</tr>
<tr>
<td>Type 4</td>
<td>Gummy Finger</td>
<td>Gummy Finger</td>
</tr>
</tbody>
</table>
## The List of Fingerprint Devices

<table>
<thead>
<tr>
<th>Manufacturer / Selling Agency</th>
<th>Product Name</th>
<th>Type</th>
<th>Product Number</th>
<th>Sensor</th>
<th>Live and Well Detection</th>
<th>Manufacturer / Selling Agency</th>
<th>Product Name (Application)</th>
<th>Comparison Levels</th>
<th>Methods for Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device A</strong></td>
<td>Compaq Computer Corporation</td>
<td>Compaq Stand-Alone Fingerprint Identification Unit</td>
<td>DFR1-200 E03811US001</td>
<td>Optical Sensor</td>
<td>unknown</td>
<td>Compaq Computer Corporation</td>
<td>Fingerprint Identification Technology Software version 1.1</td>
<td>1 through 3</td>
<td>Minutiae Matching</td>
</tr>
<tr>
<td><strong>Device B</strong></td>
<td>MITSUBISHI ELECTRIC CORPORATION</td>
<td>Fingerprint Recognizer</td>
<td>FPR-DTmkII 003136</td>
<td>Optical Sensor</td>
<td>unknown</td>
<td>Sumikin Izumi Computer Service co. Ltd.</td>
<td>SecFP V1.11</td>
<td>Fixed</td>
<td>Minutiae Matching</td>
</tr>
<tr>
<td><strong>Device C</strong></td>
<td>NEC Corporation</td>
<td>Fingerprint Identification Unit (Prism)</td>
<td>N7950-41 9Y00003</td>
<td>Optical Sensor</td>
<td>unknown</td>
<td>NEC Corporation</td>
<td>Basic Utilities for Fingerprint Identification</td>
<td>Fixed</td>
<td>Minutiae Matching (Minutiae and Relation)</td>
</tr>
<tr>
<td><strong>Device D</strong></td>
<td>OMRON Corporation</td>
<td>FingerPrint Recognition Sensor</td>
<td>FPS-1000 90500854</td>
<td>Optical Sensor</td>
<td>unknown</td>
<td>OMRON Corporation</td>
<td>“YUBI PASS” U are U3 Fingerprint Verification Software</td>
<td>Fixed</td>
<td>Minutiae Matching</td>
</tr>
<tr>
<td><strong>Device E</strong></td>
<td>Sony Corporation</td>
<td>Sony Fingerprint Identification Unit</td>
<td>FIU-002-F11 00709</td>
<td>Optical Sensor</td>
<td>Live Finger detection</td>
<td>TSUBASA SYSTEM CO.,LTD.</td>
<td>Fingerprint Identification Unit Windows 95 Interactive Demo Version 1.0 Build 13</td>
<td>1 through 5</td>
<td>Pattern matching</td>
</tr>
<tr>
<td><strong>Device F</strong></td>
<td>FUJITSU LIMITED</td>
<td>Fingsensor</td>
<td>FS-200U 00AA000257</td>
<td>Capacitive Sensor</td>
<td>unknown</td>
<td>FUJITSU LIMITED</td>
<td>Logon for Fingsensor V1.0 for Windows 95/98</td>
<td>Fixed</td>
<td>Minutiae Matching (Correlation)</td>
</tr>
<tr>
<td><strong>Device G</strong></td>
<td>NEC Corporation</td>
<td>FingerPrint Identification Unit (Serial)</td>
<td>PK-FP002 0300529S</td>
<td>Capacitive Sensor</td>
<td>unknown</td>
<td>NEC Corporation</td>
<td>Basic Utilities for Fingerprint Identification</td>
<td>Fixed</td>
<td>Minutiae Matching (Minutiae and Relation)</td>
</tr>
<tr>
<td><strong>Device H</strong></td>
<td>Siemens AG (Infineon Technologies AG)</td>
<td>FingerTIP3 EVALUATION KIT</td>
<td>C98451-D6100-A900-4</td>
<td>Capacitive Sensor</td>
<td>unknown</td>
<td>Siemens AG (Infineon Technologies AG)</td>
<td>FingerTIP3 Software Development Kit (SDK) Version: V0.90, Beta 3 “Demo Program”</td>
<td>Fixed</td>
<td>Minutiae matching</td>
</tr>
<tr>
<td><strong>Device I</strong></td>
<td>Sony Corporation</td>
<td>Sony Fingerprint Identification Unit</td>
<td>FIU-710 3000398</td>
<td>Capacitive Sensor</td>
<td>Live Finger detection</td>
<td>Systemneeds Inc.</td>
<td>Systemneeds Inc.</td>
<td>1 through 5</td>
<td>Pattern matching</td>
</tr>
<tr>
<td><strong>Device J</strong></td>
<td>Secugen</td>
<td>EyeD mouse II</td>
<td>SMB-800</td>
<td>unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Device K</strong></td>
<td>Ethentica</td>
<td>ethentication MS 3000 PC Card</td>
<td>MS 3000</td>
<td>unknown</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Experimental Results

Making an Artificial Finger directly from a Live Finger

The Number of Acceptance (times/100 attempts)

- L - L
- L - A
- A - L
- A - A

Yokohama Nat. Univ. Matsumoto Laboratory
Our Result

Process 2

(1) Residual Fingerprint
(2) Digital Image Data
(3) Printed Circuit Board
(4) Gummy Finger
Recipe 2-1
Making an Artificial Finger from a Residual Fingerprint

Materials

A photosensitive coated Printed Circuit Board (PCB)  
“10K” by Sanhayato Co., Ltd.  

Solid gelatin sheet  
“GELATINE LEAF”  
by MARUHA CORP

320JPY/sheet

200JPY/30grams
Recipe 2-2

**Residual Fingerprint**

- Enhancing
- Capturing
- Image Processing

**Fingerprint Image**

- Printing
- Mask
- Exposing
- Developing
- Etching
- Mold

**Digital Microscope**

- KEYENCE VH6300: 900k pixels

**Inkjet Printer**

- Canon BJ-F800: 1200x600dpi

**Adobe Photoshop 6.0**

- Cyanoacrylate Adhesive
- Transparent Film
- Photosensitive Coated PCB
- UV light

**Yokohama Nat. Univ. Matsumoto Laboratory**
Recipe 2-3

An Enhanced Fingerprint

A Fingerprint Image

A Mask with Fingerprint Images
Recipe 2-4

Gelatin Liquid

Drip the liquid onto the mold.

Put this mold into a refrigerator to cool, and then peel carefully.
The Mold and the Gummy Finger

Mold: 70JPY/piece
(Ten molds can be obtained in the PCB.)

Gummy Finger: 50JPY/piece
Resolution of Fingerprint Images

Pores can be observed.

Enhanced Fingerprint

Captured Fingerprint Image of the Gummy Finger with the device H (a capacitive sensor)
Experimental Results

from Residual Fingerprints (for 1 subject)
## Characteristics of Gummy Fingers

<table>
<thead>
<tr>
<th></th>
<th>Moisture</th>
<th>Electric Resistance</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Live Finger</strong></td>
<td>16%</td>
<td>16 Mohms/cm</td>
</tr>
<tr>
<td><strong>Gummy Finger</strong></td>
<td>23%</td>
<td>20 Mohms/cm</td>
</tr>
<tr>
<td><strong>Silicone Finger</strong></td>
<td>impossible to measure</td>
<td>impossible to measure</td>
</tr>
</tbody>
</table>

The compliance was also examined for live and *gummy* fingers.
Conclusions

- There can be various dishonest acts using artificial fingers against the fingerprint systems.

- Gummy fingers, which are easy to make with cheap, easily obtainable tools and materials, can be accepted by 11 types of fingerprint systems.

- The experimental study on the gummy fingers will have considerable impact on security assessment of fingerprint systems.

- Manufacturers, vendors, and users of biometric systems should carefully examine security of their system against artificial clones.

- How to treat such information should be an important issue.
• **Paper:**