Soft Biometrics and Continuous Authentication

DR. TERENCE SIM
SCHOOL OF COMPUTING
NATIONAL UNIVERSITY OF SINGAPORE
Brief Bio

- Associate Professor & Vice Dean
- Research: face recognition, biometrics, computational photography
- PhD from CMU, MSc from Stanford, SB from MIT
- Google “Terence Sim”, or tsim@comp.nus.edu.sg
Traditional authentication: one-time
Session hijacking

System still thinks legitimate user is there!
Solution: continuous authentication
R Janakiraman, S Kumar, S Zhang, T Sim 2005

- Using Continuous Face Verification to Improve Desktop Security
INTRODUCTION
Challenges
#1: Must be done passively

- Asking for PIN repeatedly causes frustration
- Biometrics is best suited for this
#2: Have minimal overhead

• Usability & energy issues
#3: Achieve low error rates

- High FAR: imposter easily takes over
- High FRR: re-login needed, user is inconvenienced
- Time must be taken into account
  - FAR & FRR not enough;
  - new performance metric needed
#4: Provide Authentication Certainty at all times

- Certainty that the legitimate user is still present
- Even when user provides no biometric signals
CRITERIA
Observations over time

BIOMETRIC

Face

Fingerprint

t1  t2  t3  t4

time

a  b  c

d  e  f  g
#1: Account for reliability of different modalities

- Fingerprint considered more reliable than face
- Thus must affect the authentication decision more than face
#2: Older observations must be discounted to reflect the increasing uncertainty of the continued presence of the legitimate user.

- The longer the elapsed time, the more uncertain is the continued presence of the user.
#3: It must be possible to determine authentication certainty at any point in time, even when there is no observations in one or more modalities

- At any time, the system must be able to check if the legitimate user is still present.
CRITERIA
Mouse with fingerprint sensor
Mouse with fingerprint sensor
System Architecture

KDM+pam

User ok/not ok (actually delay jiffies)

If user ok, continue with system call without delay.

If user not ok, freeze/delay process.
Probabilistic Approach

• The Integrator computes a probabilistic estimate of user presence, $P_{safe}$.

• The OS is tuned with a threshold for verification, $T_{safe}$.
  • If $P_{safe} < T_{safe}$, then user deemed absent.

• OS processes belonging to the user’s *interactive* session are *suspended* or *delayed* as a function of $(P_{safe} - T_{safe}, syscall)$.
Hidden Markov Model
HMM States

Safe

Attacked

$p$: prob. of remaining in Safe state at next time instant.

User still present at console.

User is absent, or Imposter has hijacked console.
Bayesian Inference

- Let \( z_t \) be a biometric observation (face or fingerprint) at time \( t \).
- Let \( x_t \) be the state at time \( t \).

Given the current and past observations, what is the most likely current state?

Bayesian inference: select the larger of
\[
P(x_t=\text{Safe} \mid z_1, z_2, \ldots z_t) \quad \text{and} \quad P(x_t=\text{Attacked} \mid z_1, z_2, \ldots z_t)
\]
Bayesian Inference

- $$P(x_t | z_1, ..., z_t)$$ is efficiently computed in terms of
- $$P(z_t | x_t)$$: prob. of getting current observation given current state
- $$P(x_t | x_{t-1})$$: transition probabilities
- $$P(x_{t-1} | z_1, ..., z_{t-1})$$: previous state given previous observations (recursion)

Upon initial login,
- $$t=0$$, and $$P(x_0=\text{Safe}) = 1$$
Face Biometric

- We use a Bayesian classifier.
- From 500 training face images of legitimate user, and 1200 images of other people (imposter), we learn:

\[ P(y | \text{user}) \quad P(y | \text{imposter}) \]
Face Biometric

- Note that
  - $P(z_t \mid x_t = \text{Safe})$ is just $P(y \mid \text{user})$
  - $P(z_t \mid x_t = \text{Attacked})$ is just $P(y \mid \text{imposter})$
Fingerprint Biometric

- Also Bayesian classifier.
- Vendor’s proprietary algorithm matches 2 fingerprint images.
  - Outputs a matching score, $s$
- From training images, we learn:
  - $P(s \mid \text{user})$ and $P(s \mid \text{imposter})$
- Which become
  - $P(z_t \mid x_t = \text{Safe})$ and $P(z_t \mid x_t = \text{Attacked})$ respectively
Further Comments

- \( P_{safe} = P(x_t=\text{Safe} \mid z_1, \ldots, z_t) \)

- We can compute \( P_{safe} \) anytime.
  - If no observation at time \( t \), then use most recent observation: \( P_{safe} = P(x_t=\text{Safe} \mid z_1, \ldots, z_{t-1}) \)
  - But decay transition probability \( p \) by time lapse.
    \[ p = e^{k\Delta t} \]
  - This reflects increasing uncertainty about presence of user when no observations available.
Further Comments

• In theory, we want the larger of
  \[ P(x_t=\text{Safe} \mid z_1, \ldots, z_t) \quad \text{and} \quad P(x_t=\text{Attacked} \mid z_1, \ldots, z_t) \]

• Equivalent to: \( P_{\text{safe}} > 0.5 \)

• But in practice, we use \( P_{\text{safe}} > T_{\text{safe}} \)
  • More flexible: different \( T_{\text{safe}} \) for different process actions (e.g. reads vs. writes)
  • Avoids “close call” cases when both probabilities almost equal.

• Math details in paper.
Evaluation
Other Fusion Methods

Temporal-first
Other Fusion Methods

Modality-first

BIOMETRIC

Face

Fingerprint

$P_{safe}$

t1, t2, t3, t4

d, e, f, g

y1, y2
Naïve Integration

- Idea: use the most reliable modality available at any time instant.
- Since fingerprint more reliable than face, use it whenever available.
- Else use face.
- If no modality available, use the previous one, but decay it appropriately.
Reliability
Experiment: Legitimate User

- Indiv. Probabilities sporadic $\Rightarrow$ significant FAR/FRR for any threshold $T_{safe}$
- FAR = security breach!
- FRR = inconvenience
- Holistic Fusion closest to ideal.
- Abrupt drop in Temporal-first, Modality-first curves.
Experiment: Imposter

- Imposter hijacks session at time = 38s
- Detect by change in slope.
- Holistic Fusion and Naïve Integration detects hijacking sooner than others (time = 43s).
Experiment: Partial Impersonation

- Successfully faked fingerprint, but not face.
- This is easily detected by Holistic and Naïve, but not by others.
$P_{safe}$ for different tasks
Usability test

• 58 people to perform different tasks
Usability test

- CBAS verifies users at a low FRR, and low FAR.
- Surprising result: (a) no statistical evidence to show that CBAS overhead affects task efficiency; (b) system performance degradation was imperceptible by users.
- Many users felt uncomfortable being “watched” by webcam. Discreet placement may solve this.
- A biometric solution for continuous authentication is practical and usable.
- Multi-core processors will further reduce the overhead.
New Performance Metric

- **Time to Correct Reject (TCR)**
- The interval between the start of the first action taken by the imposter to the time instant that the system decides to (correctly) reject him.
- Ideally, TCR = 0.
  - Practically, TCR < W (minimum time for the imposter to damage the system, eg. To type “rm –rf *”)
  - As long as TCR < W, system integrity is assured
New Performance Metric

- **Probability of Time to Correct Reject (PTCR)**
- The probability that TCR is less than W
- Ideally, PTCR = 1.
  - Practically, PTCR < 1 may be tolerable
  - This means that sometimes, the system can take longer than W seconds to correctly reject an imposter.
  - If system always fails to correctly reject, then PTCR = 0 for all W
- PTCR is analogous to FAR
New Performance Metric

• **Usability**

• the fraction of the total time that the user is granted access to the protected resource
  • eg. User logs in for a total duration of $T$, but system sometimes rejects user
  • Let $t$ be the total time user is accepted
  • Then Usability = $t / T$

• Ideally, Usability = 1.
  • Usability is analogous to FRR
New Performance Metric

- Usability-Security Characteristic Curve (USC)
- Plot of Usability vs PTCR
- Analogous to ROC curve
USC curve for our system
Soft Biometric Traits for Continuous User Authentication

Koichiro Niinuma, Unsang Park, Member, IEEE, and Anil K. Jain, Fellow, IEEE
Soft biometrics: Definition

- those characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals under normal circumstance
  - e.g. gender, clothes color
System

- Hard biometric: face recognition (eigenface)
- Soft biometric: face color histogram, clothes color histogram
4 modes

Initial login authentication (Mode I)
- Conventional authentication
- Face detection
  - Body localization
  - Template registration

Continuous authentication (Mode II)
- Face and body identification
- Face recognition
- Calculation of $S_{cont}$
- NO
- $S_{cont} < t_{cont}$?
- YES

Enrollment template update (Mode III)
- Illumination change?
- NO
- YES
  - Template Update

Re-login authentication (Mode IV)
- Face detection
  - Body localization
  - Template generation
  - Identification (Face + Histograms)
- NO
- User returns back?
- YES
## Hard vs Soft biometrics

<table>
<thead>
<tr>
<th></th>
<th>Hard biometrics</th>
<th>Soft biometrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidence of decision with each observation</td>
<td>High to medium</td>
<td>Medium to low</td>
</tr>
<tr>
<td>Frequency of observation</td>
<td>Medium to low</td>
<td>High</td>
</tr>
<tr>
<td>Pre-registration</td>
<td>Required</td>
<td>Not required</td>
</tr>
<tr>
<td>$\Omega_{\text{intra}}$ and $\Omega_{\text{inter}}$</td>
<td>Available</td>
<td>Not available</td>
</tr>
</tbody>
</table>
Coping with illum change
Coping with illum change

Fig. 18. Example 2 of similarity score versus time graphs with and without enrollment update. (a) Without enrollment update. (b) With enrollment update.
Fig. 20. Example results of relogin authentication experiments. (a) Authentic user; (b) authentic user walks away; (c) imposter user; (d) imposter user walks away; and (e) authentic user returns.
Evaluation
Smartphones

• New opportunity for Continuous Authentication
• Rich sensors:
Possible biometrics

• Face: gender, identity, age, race, expression
• Iris?
• Voice
• Gait
• Keystroke dynamics (touch)
• Fingerprint
• Location
• Wifi signature
• Cellular signature
Energy usage is critical!
• Most research use touch dynamics
• Multimodal biometrics will be more useful
• Computational efficiency not yet considered
• Possibility for forensics use
References


