Controlling Access: Methods, Problems, and Requirements

Ernst L. Leiss

Department of Computer Science

University of Houston

Support of this research under NSF grants DUE 0313880, SCI 0453498, and OISE 0519316 is acknowledged

Table of Contents

1. Introduction

Passwords: Text-based

Pro: Compact

On the order of tens of bytes

Easy to generate

Compliance with whatever rules are imposed is trivial

Unlimited number

With 26+26+10+10 (upper, lower, digits, special) characters, there are almost 20 septillion ($2 \cdot 10^{22}$) passwords with 8 to 12 characters

Easily replaced

Since they are easily generated, new ones are easily obtained

The access control is equally easily adjusted to a new password

Many schemes require periodic changes of passwords, some even employ one-time passwords

Con: Tenuous connection between user and password

The association between owner and password is artificial, unnatural

Non-uniqueness

The association between owner and password is non-unique: Different owners may use the same password, different passwords may be used by the same owner.

Biometric measurements: Signal-based

Pro: Intimately tied to on individual

- **Different individuals have different measurements**
- **Impossible to change the association between owner and measurement**

Unique

- **Ideally, no two individuals have the same measurement**

Con: Large amount of data to be captured and stored

- **On the order of hundreds of bytes to hundreds of kilo bytes**

Difficult to generate

- **Generally, require complicated data collection systems (more complex than a keyboard)**

Impossible to replace

- **Once “lost”, it is impossible to generate “new” biomeasurements**

Fundamental differences between text-based and signal-based information

Redundancy

Tolerance of errors

Size

2. Biometric Data

Fingerprints

- Old method for identifying persons (criminals)
- Generally assumed to be unique
- Not all individuals have suitable fingerprints
- Much fingerprint information is captured
- Only certain aspects (indicia) are extracted and used in the similarity test

Retina scans

- Based on the pattern of blood vessels in an individual's eye retina
- Generally considered to identify uniquely a given individual
- Is fairly intrusive (requiring close contact) and not commonly employed.

Iris scans

- Similar to retina scans; use the iris of the eye instead of the retina's blood vessel pattern Significantly less intrusive; can tolerate greater distance between user and apparatus
- Considered to identify uniquely individuals (even identical twins)
- Much information is captured and used in a similarity test whether there is a match

Hand geometry

Uses geometric aspects of the hand and physical characteristics of hand and fingers

Captures either several 2D images or a 3D image

Much information is captured (approximately one hundred different measurements)

Uniqueness is not entirely guaranteed – hand geometry is used to identify individuals drawn from a relatively small set (e. g., access control to a specific facility)

Face authentication

Oldest technology for identifying individuals – by humans!

Newest for computer-based authentication

Measures geometric facial structure (distance between eyes, nose, mouth, jaw, etc.), in 2D (not very reliable) or 3D

Measurements use either visible or infrared light (thermal imaging)

Supremely non-intrusive: the only biometric authentication approach that can be administered without knowledge and cooperation of the subject, at a distance

Much information is captured. The similarity test is complex.

DNA

The ultimate identifier (except for identical twins)

Obviously not useful for computer-based authentication (timeliness!)

Much information must be captured to carry out a similarity test.

Signature verification

Extends the classical signature approach (only final result, the signature)

Includes information captured during signing

pressure exerted, variation of the angle of pen to surface, speed of signing

Much information is captured for the similarity test between stored template of signature and captured measurements

Voice authentication

Employs specific characteristics of an individual's speech

The similarity condition is crucial because of the variability of a person's speech medical conditions (cold, asthma, etc.), fatigue

Stored template (voice sample) and captured voice require significant data storage

Keystroke dynamics

The mechanical way a user types text at a keyboard

Limited discriminative power of keystroke dynamics
(unlikely that millions of typists can be differentiated from each other)

Failure rate is larger than with other biometric methods

Much information must be captured and transmitted

Passwords require an identical match, biometric measurements must satisfy a similarity condition.

Problem: Interception of measured data may obliterate that person from the canon of acceptable users.

3. A Proposed Solution

Exploit the variations between different measurements of the same individual

For a transmission, store a hash of the measurements, say 100 bytes.

Any subsequent transmission is compared to each prior transmission (on the basis of the hashes):

A measurement is only acceptable if it is similar, but <u>not identical</u>.

Any exact match is considered an attempt of fraud (replaying a previously intercepted transmission)

Method requires little storage capacity

Amount of space stored per log-on is a parameter.

If too small, access is denied (collision); however, in this case a new attempt will be made by the user, and it is virtually impossible, given the characteristics of capturing data, that this new attempt (which produces a different measurement!) hashes to the same value.

Even if the hash is only 1 bit, the probability of detecting this is 50%.

Verification is fast

In contrast to the similarity condition (which is usually quite slow), the test for equality can be done using binary search.

4. The "Sniff and Suppress" Attack

The previous scheme safeguards against simple intercepts

It does not protect against the "sniff and suppress" attack

Action: The attacker monitors the communication between capturing device and central database system and suppresses and stores a legitimate transmission of biometric measurements B.

Results:

For the legitimate user: One access validation request fails. The legitimate user will usually repeat the request.

For the attacker: The data B are known to have not been used. Therefore, they constitute a valid access request which is guaranteed to be successful. (Works once, cannot be repeated.)

5. Resulting Requirements

What is needed to prevent the sniff and suppress attack?

Systems with synchronization

Use time to avoid this attack: Impose tight time limits to prevent the attacker from completing the attack in a timely fashion.
Sufficient for secure transmission: simple intercepts are defeated by the previous method.
Requires significant hardware support (usually not present since the capturing devices are very simple)

Systems without synchronization

Requires a multi-pass protocol: Hand-shake in which the capturing device must request a unique item from the central database system that must be incorporated into the transmission of the biometric data.

Possible protocol:

D: Capturing device
CS: Central storage site
U: User attempting to obtain access using the biometric measurements BU

Prior to transmission, D and CS have agreed on an encryption key K.

D requests a unique encryption key KU used only for this access request of U.
K is used to encrypt this exchange.
D encrypts BU using key KU and sends this to CS.
CS Verifies that this process was completed within the time limits and complies with all requirements.

Comment: Protects against simple intercept and sniff and suppress.

Requires significant processing power at device – not available with current devices

Conclusion

The currently available and used biometric stand-alone devices are inherently unsuitable for authentication of individuals if data are transmitted over an insecure channel.

This applies in particular if the data are transmitted over the Internet.

6. Improved Password Schemes

Recap:

1. Something you are

e.g., biometric data

2. Something you have

e.g., dongle, smart card

3. Something you know

e.g., password

Add: Something you know how to do

Iterated Password Schemes

Several passwords in sequence

However, no acknowledgment occurs until the very end:

User	System
pw_1 <cr>	
pw_2 <cr>	
…	
pw_n <cr>	accepts or rejects access request

Difference between acknowledged and unacknowledged scheme:

Assume breaking a password of length ℓ requires time C^ℓ for some constant $C>1$

$C^{\ell_1} + C^{\ell_2} + C^{\ell_3} + \ldots + C^{\ell_n}$ vs. $C^{\ell_1+\ell_2+\ell_3+\ldots+\ell_n}$

Knowing how to produce

Start with an easily remembered pass-word or pass-phrase P
Apply a function f to P which produces a string of length h: f(P)
Select a position i in f(P) and extract a total of m characters starting at that position

Examples of f:

encryption function
hash function (MD5, SHA-512)

Selection process:

positions i, i+1, …, i+m-1
positions i, 2i mod(h), 3i mod (h), … mi mod(h)

Defeats attacks of type Narayan and Shmatikov who argued in a recent paper that
”as long as passwords remain human-memorable, they are vulnerable to ‘smart-dictionary’ attacks even when the space of potential passwords is large”

Implementation considerations

Unacknowledged iterated scheme

No architectural changes required

Memorizable process for obtaining a strong password

Requires the ability to call a strong encryption or hash function before logging on, in a secure environment (e.g., no spyware)

7. Secure Vestibules

Guarding against Key Stroke Capturing

Key stroke capturing devices record user input, they do not record screens transmitted.

Display a translation table and have the user input the randomized password.

Example:

Display:

A	B	C	D	E	F	G	H	I	J	L	K	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	1	2	3	4	5	6	7	8	9	0
0	Z	1	Y	2	X	3	W	V	4	U	T	5	9	A	C	B	6	D	E	F	G	H	8	M	N	L	K	J	I	7	O	P	Q	R	S

Password: `PASSWORD`

Input by user: `C0DDHA6Y`

Screen capturing

- **Screens would have to be captured at least once per second**
- **480x640 color pixels or almost 1 MB**
- **8 hours of screen shots == Over 25 GB per day**

Key stroke capturing

- **No more than 100 words per minute**
- **Say each word requires 30 bytes**
- **Less than 1.5 MB for eight hours of continuous typing**

Difference: Over four orders of magnitude

Thus: infeasible for this type of interceptor to store and later transmit or deliver a day’s (or a week’s, or a month’s!) worth of data

8. Conclusion

Controlling access remotely is difficult

Biometric measurements must be protected to a much greater extent than passwords

Current capturing devices for biometric measurements are too primitive to be safe for remote use

Should revisit password generating schemes in order to obtain the advantages of passwords as well as the strength of biometric schemes