User Authentication

Simon Foley,
Department of Computer Science,
University College Cork
s.foley@cs.ucc.ie

October 5, 2015

User Authentication

A security policy is typically defined in terms of the users of the system. A (user) authentication mechanism is needed to counter the threat of one user masquerading as another.
An authentication mechanism requires a user to prove that they are who they claim to be. The proof can come from

- what the user knows (passwords, PINs, . . .)
- what the user has (a key, a badge, . . .)

- what the user is (fingerprint, retinal characteristics, . . .)


- where the user is (at a particular terminal, . . .)

Some Authentication Threats

Password guessing; Shoulder surfing; Eveasdropping on network traffic;

Poorly designed authentication mechanism;

Inconvenience: hard to remember passwords; have to carry physical authentication tokens; using same password for different accounts;

Denial of Service: attacker behavior (attempting to masquerade as target) results in account locked out.

Social Engineering; phishing;

physical keystroke loggers; login-spoof Trojan Horse program; pharming (redirecting website traffic to a bogus website).

KISMET

Something you know

Password Based Authentication

Most operating systems distinguish between different users and use password-based user authentication. A person proves that they are the user they claim to be by providing a secret password at login.

- ☐ do protect your password
- ☐ do use good password choices: don't use short words, words in a dictionary, your name, or anything that someone could guess.
- ☐ do change your password if you feel it has been violated
- ☐ don't share your password with anyone
- ☐ don't use anyone else's password
- ☐ don't work under anyone else's password
- ☐ don't leave passwords displayed on keyboards or monitors

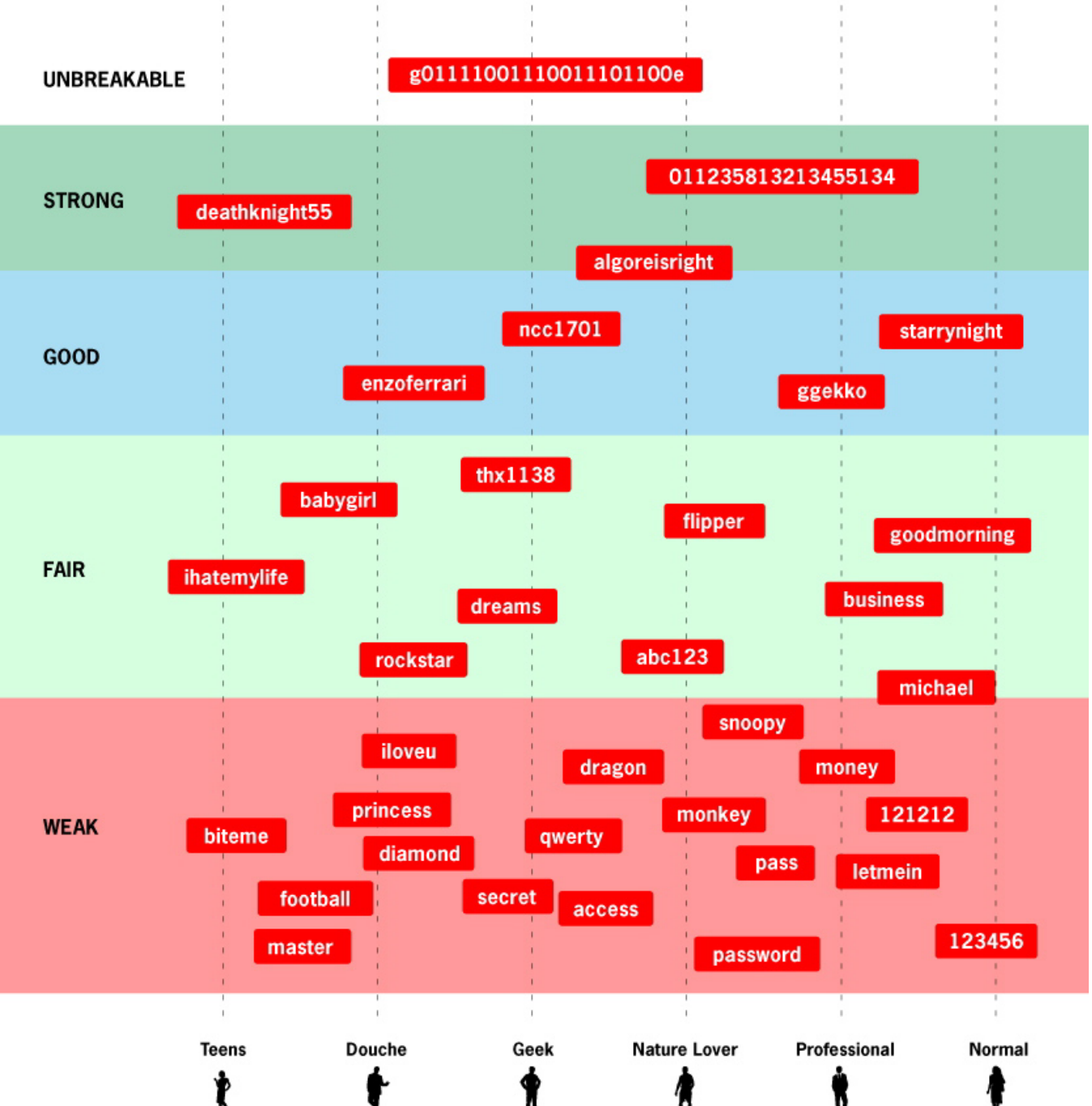
Use password-based authentication in combination with another authentication mechanism to counter threat of password guessing (multi-factor authentication).

Code breaking

How secure is your password

Tested using Gmail password strengh meter

CXO
www.cxo.eu.com



Passwords: It should be something that only you know

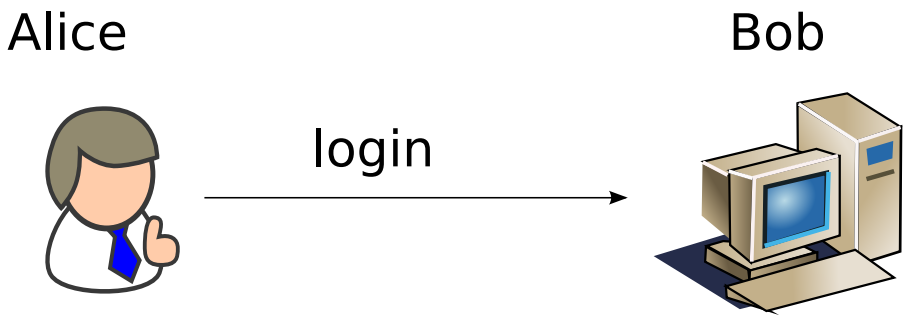
Maybe the attacker cannot guess the password, but can exploit the security controls in order to reveal the password/permit access.

Some systems use secret questions to permit user reset a (forgotten) password. Perhaps the attacker can figure out your postal code, your date of birth, you mother's maiden name and clicks on `forgot password` for your email address. Used to hack Paris Hilton's T-mobile account, Sarah Palin's Yahoo email account.


Sarah Palin's E-Mail Hacked: How It Was Done
http://www.huffingtonpost.com
Sarah Palin's E-Mail Hacked: How It Was Done
Huffington Post | Danny Shea | September 18, 2008 04:08 PM
Read More: Sarah Palin, Sarah Palin Email, Sarah Palin Email Hacked, Sarah Palin Hacked, Sarah Palin Password, Media News
Show your support.
Buzz this article up.
Share
Print
Comments
Wired reported Thursday how Sarah Palin's email got hacked — a simple trip through Yahoo's "Forgot My Password" function:
A person claiming to be the hacker who obtained access to Alaska Gov. Sarah Palin's private Yahoo e-mail on Tuesday has posted a supposed first-person account of the hack, revealing the relatively simple steps he says he took to crack the private e-mail of the Republican vice-presidential candidate.
The story was briefly posted Wednesday to the 4chan forum where the hack first surfaced. Bloggers have connected the handle of the poster, "Rubico," to an e-mail address, and tentatively identified the owner as a college student in Tennessee.
Threat Level was unable to reach the student by phone because his number is unlisted. A person who identified himself as the student's father, when reached at home, said he could not talk about the matter and would have no comment. The father is a Democratic state representative in Tennessee.

Rubber Hose Cryptanalysis

User Authentication Protocols



Alice must prove to Bob that she knows some secret.

Secrets should be secured. For example, Bob stores $h(secret)$, or Bob's operating system provides protection of secret.

Alice does not want to reveal her secret in public (eavesdropping attack).

If the authentication-interaction is always the same then a replay attack is possible.

A one-time password scheme is intended to ensure that each authentication-interaction between Alice and Bob is different and that an attacker should not be able to deduce the next interaction from past interactions.

Challenge Response Protocols

Alice (user) shares a secret key K_{AB} with Bob (workstation).

$$\begin{aligned} \text{Msg1}: \quad & A \rightarrow B: \quad userid \\ \text{Msg2}: \quad & B \rightarrow A: \quad challenge \\ \text{Msg3}: \quad & A \rightarrow B: \quad \{challenge\}_{K_{AB}} \end{aligned}$$

where $\{X\}_K$ represents encryption of X and provides secrecy and integrity; for example, AES CBC encryption of X and its message digest.

Bob issues a different ('fresh') challenge for every login session.

Resilient to shoulder-surfer at terminal and eavesdropper if over network.

Alice can calculate her response using a Challenge Response Calculator.

- Tamper-resistant, with embedded secret key K_{AB}.
- Alice enters PIN and challenge; $\{challenge\}_{K_{AB}}$ is calculated/displayed.
- Activated by PIN; three incorrect PINs and device disabled.

Authentication Token based Protocols

Use the current time as a challenge.

This challenge-response calculator does not have a key pad, but has an internal clock and a simple display of the current response which changes every 20 seconds, for example, a simplified protocol:

$$\text{Msg1}: \quad A \rightarrow B: \quad userid, \{userid, time\}_{K_{AB}}$$

Bob decrypts the message and if the time is recent then Alice is authenticated. Alice may also be required to provide a password to help to counter threat from loss of the calculator.

Clock on token must be synchronized with clock on server/workstation.

Challenge Response Tokens

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

RSA SecurID SID800

RSA SecurID SD520

BlackBerry with
RSA SecurID software token

Challenge Response Protocols: Managing Secret Keys

Given the previous protocol, Bob will need to store a copy of each user's secret key K_{AB}.

He could, instead, use/manage one master secret K that only he knows, and compute

$$K_{AB} = \{\texttt{"Alice@cs.ucc.ie"}\}_K$$

Bob must explicitly store/protect this secret properly (he can't store $h(K)$).

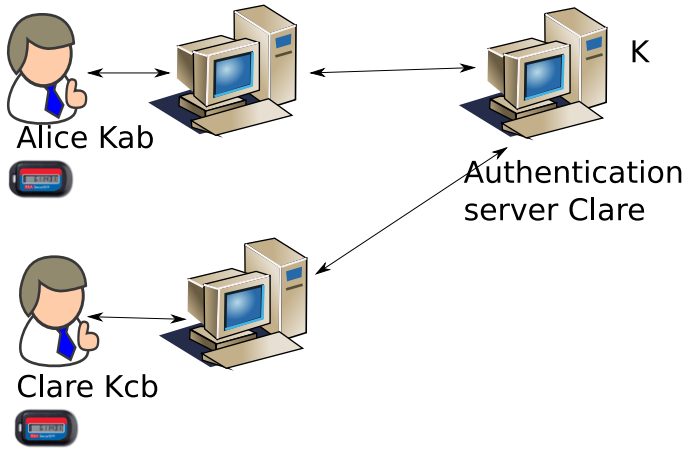
However, many different users may wish to login to many different workstation/systems.

Storing (and managing/protecting) a copy K on every system is a security risk.

Challenge Response Protocols: Authentication Servers

A common strategy is to use a special secure (hardened) server that provides a dedicated *authentication service*.

The master key K is stored only on this system and the server is referred to by all other systems when a user logs-in.



Communication to authentication server must be secure.

The Kerberos protocol is an example of the exchanges necessary between the workstations and the authentication server.

TECHNOLOGY | JUNE 7, 2011

Security 'Tokens' Take Hit

RSA Offers to Replace Nearly All of Its SecurIDs in Use or Provide Monitoring

By SIOBHAN GORMAN And SHARA TIBKEN

RSA Security is offering to provide security monitoring or replace its well-known SecurID tokens—devices used by millions of corporate workers to securely log on to their computers—"for virtually every customer we have," the company's Chairman Art Coviello said in an interview.

In a letter to customers Monday, the EMC Corp. unit openly acknowledged for the first time that intruders had breached its security systems at defense contractor Lockheed Martin Corp. using data stolen from RSA.

Something you are

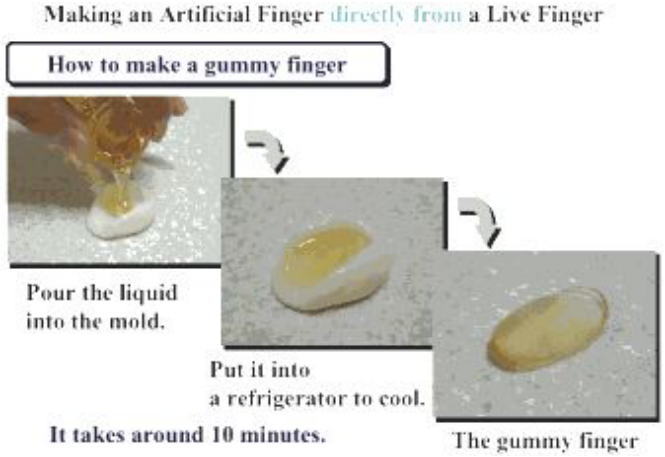
Biometric Based Authentication: Something you are

Biological characteristics may identify a person: facial, fingerprint, iris, keystroke dynamics, gait, voice, palm, ear, ...

Ensure the mechanism is fit for purpose and rely on multiple and different authentication mechanisms (Belt and Braces).

Biometric based mechanisms are not always accurate

- Fingerprint readers may be fooled: Gummi Bear attack,



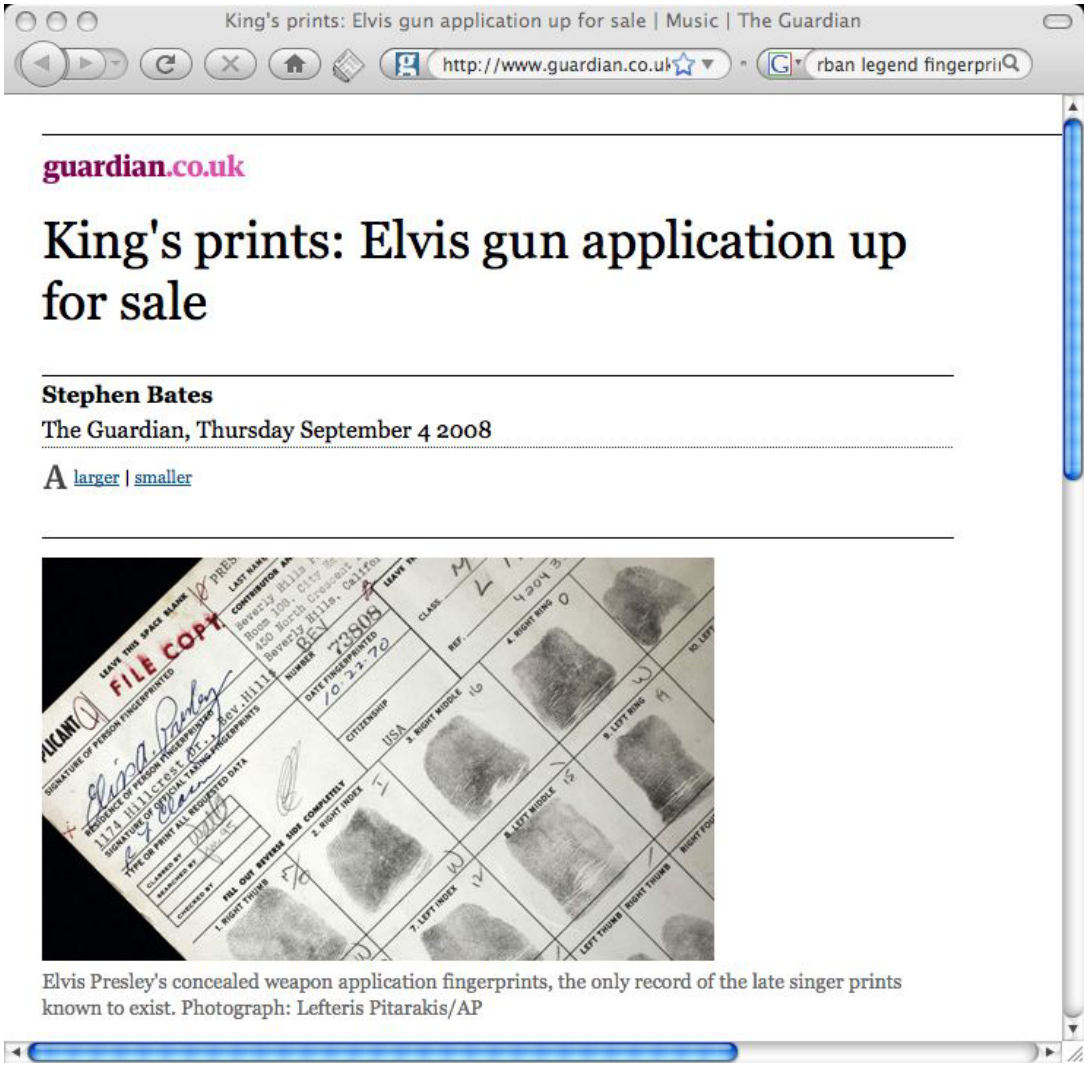
. . .

- Test for liveness: 'Wesley Snipes' attack (Demolition Man),

. . .

- Once a biometric is lost it is lost forever.

Elvis' Fingerprints for Sale

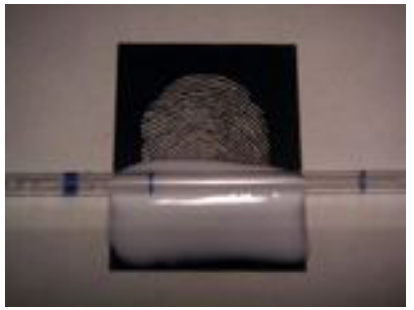


Faking a Fingerprint [from www.ccc.de]










Once a Biometric is lost, its breached for ever

https://www.washingtonpost.com/news/the-switch/wp/2015/09/23/opm-now-says-more-than-five-million-fingerprints-compromised-in-breach

Biometric Based Authentication: False Accept Rate (FAR)

Inaccuracies in the operation of biometric device may lead to vulnerabilities.

FAR is the likelihood of incorrectly matching a fingerprint comparison. For example, $FAR = 0.001$ means one false accept in 1,000 comparisons.

Using biometric to authenticate a claimed identity:

- At login, Alice presents her userid and swipes her finger on the fingerprint reader.
- The login process looks up Alice's biometric data from its biometric database and compares it against the fingerprint provided.
- The chance of of false accept is given by FAR of device.

For example, the Silex-combo mini fingerprint reader has a FAR of 0.00001, meaning 1 in 100,000 chance of authenticating Eve as Alice.

Biometric Based Identification: False Accept Rate FAR_{system}

It is important to distinguish the difference between using the biometric to authenticate a claimed identity versus using it to identify a person.

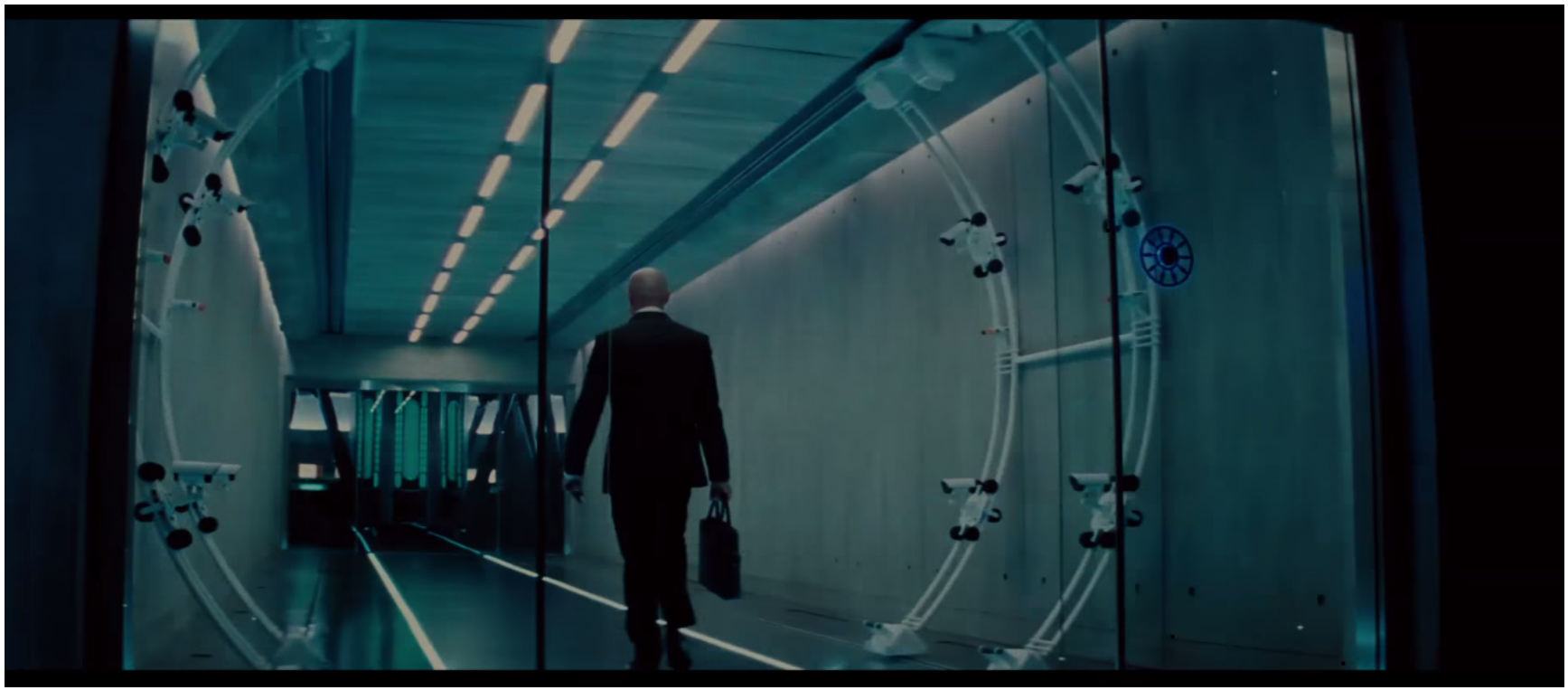
Given a database of N biometrics (eg fingerprints) and suppose we are checking a user (fingerprint) that is *not* in the database.

- chance of no-match on first test is $(1 - FAR)$,
- chance of no-match after two tests is $(1 - FAR)^2$,
- ...
- chance of no-match after N^{th} test is $(1 - FAR)^N$.

Thus, the chance of a false accept when testing against entire database (N tests, $FAR = 0.0001$) is $FAR_{system} = 1 - (1 - FAR)^N) \approx N \times FAR$ (if FAR is small).

- $N = 100$ then $FAR_{system} = 0.095$
- $N = 1,000$ then $FAR_{system} = 0.63$
- $N = 10,000$ then $FAR_{system} = 0.99995$

Anyone watch Mission Impossible 7?



Was this use of a gait biometric effective?

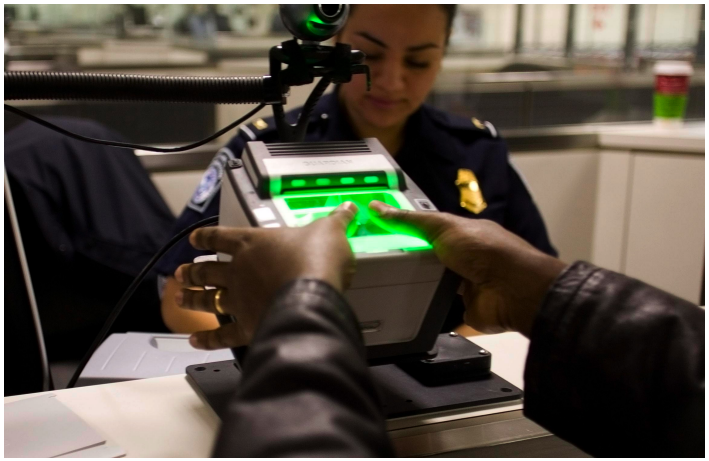
Social media

Primary Facebook photos visible to all by default *"Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings."*

How many use their real name and photo as primary profile picture?

Facebook's DeepFace system has a FAR of 0.03 [unconfirmed] which roughly matches accuracy of a human.

Biometric Based Identification: US-VISIT programme and FAR_{system}



The US-VISIT programme checks the fingerprints of arriving visitors against a database of blacklisted individuals.

With 6,000,000 blacklisted individuals in the database, the FAR_{system} in 2004 was 0.0031, that is, approximately one in every 333 visitors is flagged (based on a scan of two fingerprints).

FAR_{system} was recently improved by scanning all fingers/thumbs.

Biometric Based Identification and the Birthday Paradox

Recall the birthday paradox: the probability that k people have a different birthday is is less than 0.5 if $k > \sqrt{365} \approx 23$.

A similar result can be derived if we consider the probability of people having non-distinct fingerprints. Intuitively, the probability that k people will all have distinct fingerprints is less that 0.5 if $k > \sqrt{1/FAR_{system}}$.

For example, suppose we wanted to build a biometric database that *uniquely* identifies students in UCC. Suppose $FAR_{system} = 0.000001$, then over a 50% chance of a false match by the time we'd registered only $k = 1000$ students!

Hard to achieve high accuracy when using a fingerprint reader alone as a means of identification.

Biometrics can be useful to help authenticate a claimed identity.

Avoid using a biometric system to identify a person.


THIS WORKSTATION IS STILL LOGGED IN TO THE NETWORK.
IT'S TIME TO TEACH SOMEONE A LESSON ABOUT SECURITY.
I'LL JUST GO IN HERE AND . . .
WARNING! WARNING! IDIOT ALERT!
GAAA!!!
ACTIVATING DEFENSIVE WEDGIE SYSTEM.
I HAVE TO GO. SOME IDIOT VIOLATED MY PERIMETER.
BEEP BEEP
PLEASE MAKE IT STOP.
THEN HOW WOULD YOU LEARN?
E-mail: SCOTTADAMS@AOL.COM
© 2009 Scott Adams, Inc./Dist. by UFS, Inc.
www.dilbert.com

Social Engineering