Salting Passwords and Biometrics

20 May 2026
Lecture 8

Some Slides Credit: Steve Zdancewic (UPenn)

Topics for Today

- Password storage
- Password alternatives

How does the system store them?

- Is the password file readable by the OS?
  - Then if I break the OS…
- Can privileged users see the file?
  - … and make copies
- Is the file backed up somewhere
  - … insecure?
- Is the file/password in plaintext somewhere in memory?
  - Core dump or memory scan (Windows)
- Fool the user
  - A program that masquerades as the authentication program

- Similar problems for database Username / Password tables

Counter-hacks

Control-Alt-Del for logging in

- Establishes a "trusted path" in hardware
- Prevents trojan horses from intercepting passwords

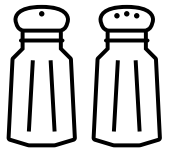
Slow down / restrict number of tries

- Make guessing take too long
- e.g. 3 tries and you're blocked for 30 seconds

Encrypt the password file and hash the passwords

- System admin doesn’t know the password!
- Use one way hashes or encryptions on the passwords
- “Salt" - to prevent duplicate passwords showing as duplicate codes

Add Salt

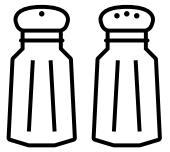


- "Salt" the passwords by adding random bits.
  - Decreases the likelihood that two identical passwords will appear as identical entries in the password file.
- 12 bit salt results in 4,096 versions of each password.
- Unix: `/etc/passwd` entry:

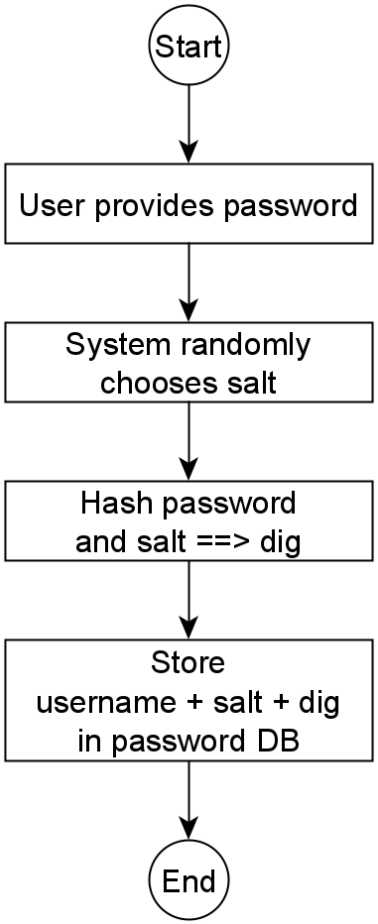
user_id	$salt_u$	$Hash(salt_u + passwd_u)$	…

- Modern implementations of Unix/Linux use so-called *shadow* password files `/etc/shadow` that aren't world readable.
- Most use longer salts now too (48 bits to 128 bits)

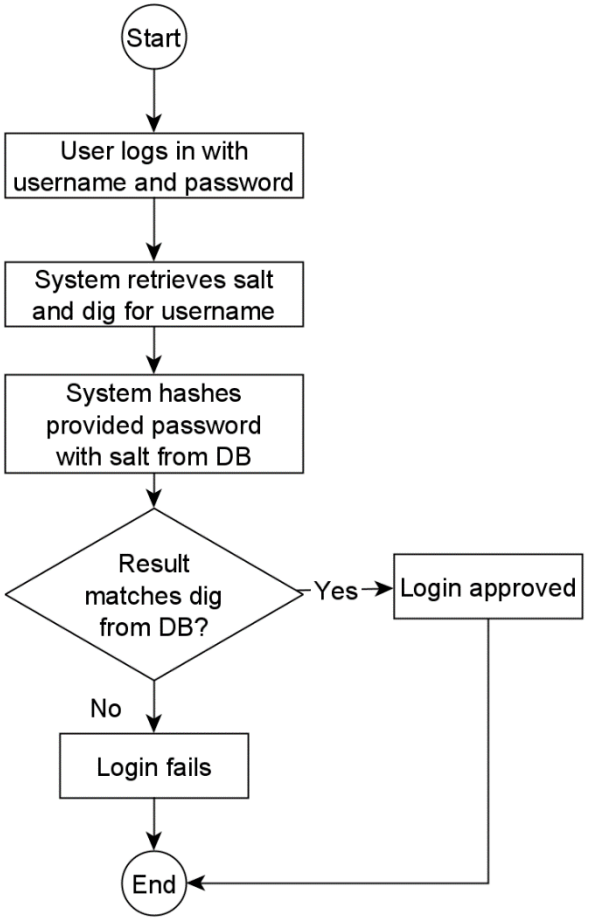
Using Salt



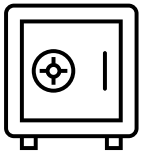
Registration



Login



Password File Hardening



- What if an attacker steals the password file (or database table)?
  - Simple hashes of passwords can be attacked using Rainbow Tables (precomputed hash chains)

- Harden the password file: Make the password + salt → code calculation hard:
  - Old: Encrypt with DES using password and salt 25 times
  - Newer: 5,000 rounds of SHA-2 on the password and salt
    - Minimum 1,000 rounds

- More rounds and large salt make Rainbow Tables unfeasible
- Also make guessing attacks longer

- Read more: `crypt()`, PBKDF2, John the Ripper (https://www.openwall.com/john/)

NYTimes Breach Lessons

SECURITY

The New York Times source code leaked by a 4chan user

An anonymous user has published a torrent file with 270GB worth of data.

by Alex Ivanovs June 8, 2024

Here are some other findings we can confirm:

- The leak does have the original source code of the game Wordle, which the Times acquired in 2022.
- The leak includes a WordPress database of 1,500 *NY Times Education* site users. The database contains names and surnames, email addresses, and hashed passwords.
- Several folders contain internal communications from Slack channels.
- Many exposed authentication methods exist, including authentication URLs and their respective passwords, secret keys, and API tokens. The majority are well protected, but plenty of such secrets need immediate attention. We have also seen private user keys used for authentication.

https://stackdiary.com/the-new-york-times-source-code-leaked-by-a-4chan-user/

Dropbox too

https://sign.dropbox.com/blog/a-recent-security-incident-involving-dropbox-sign

Blog / **Product news**

A recent security incident involving Dropbox Sign

Dropbox Sign

by Dropbox Sign team

May 1, 2024 • 6 minute read

On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed Dropbox Sign customer information. We believe that this incident was isolated to Dropbox Sign infrastructure, and did not impact any other Dropbox products. We're in the process of reaching out to all users impacted by this incident who need to take action, with step-by-step instructions on how to further protect their data. Our security team also reset users' passwords, logged users out of any devices they had connected to Dropbox Sign, and is coordinating the rotation of all API keys and OAuth tokens. Please read on for additional details and an FAQ.

On April 24th, we became aware of unauthorized access to the Dropbox Sign (formerly HelloSign) production environment. Upon further investigation, we discovered that a threat actor had accessed data including Dropbox Sign customer information such as email addresses, usernames, phone numbers and hashed passwords, in addition to general account settings and certain authentication information such as API keys, OAuth tokens, and multi-factor authentication.

Also a Bank

https://thecyberexpress.com/alleged-ecb-data-breach-claimed-by-intelbroker/

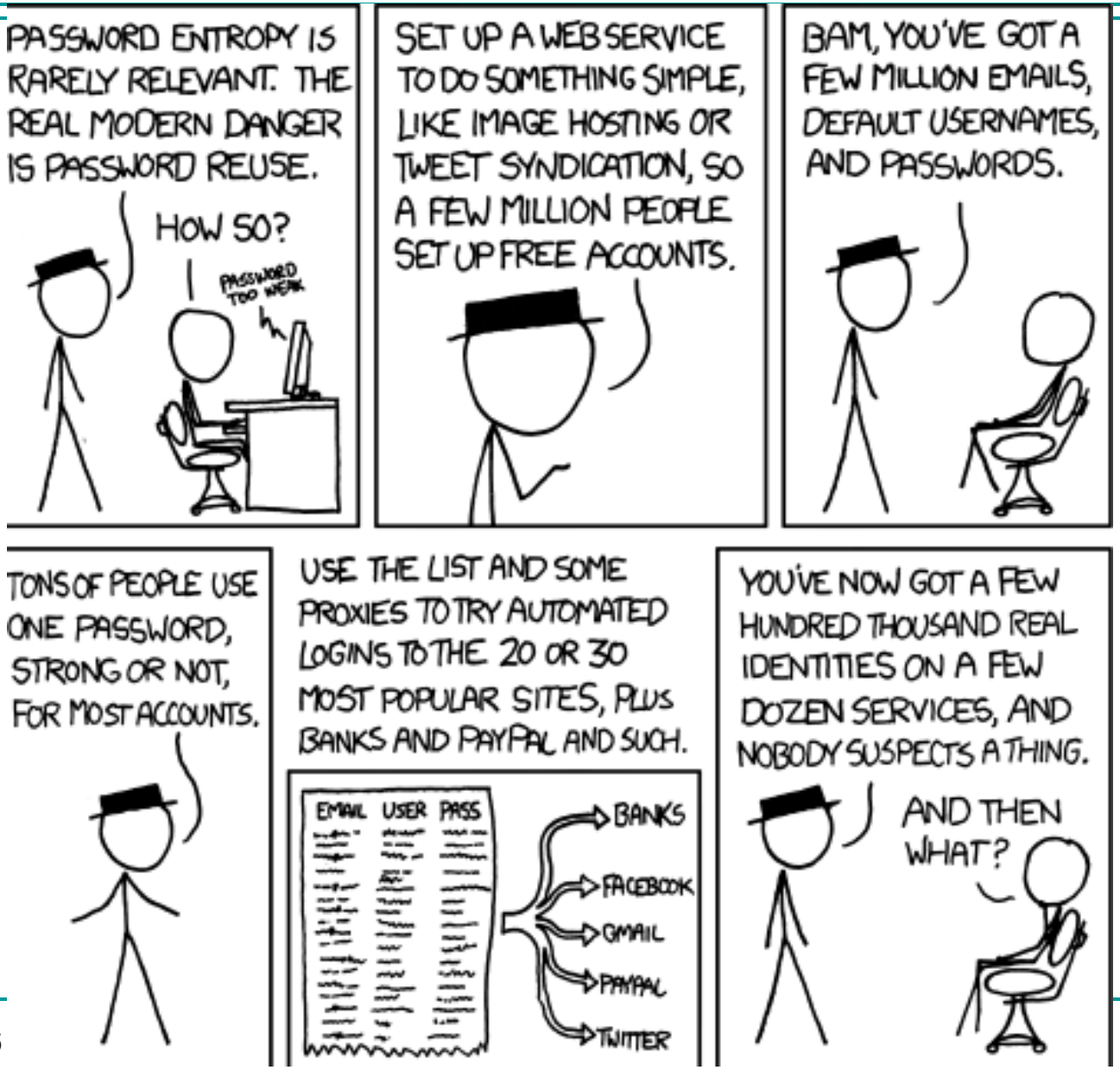
Home » Firewall Daily » Dark Web News » 'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)

'IntelBroker' Claims Access to Database Belonging to England and Wales Cricket Board (ECB)

The dataset contained various user account information, such as email addresses, hashed passwords, and dates of registration and last login.

by Ashish Khaitan — March 26th, 2024

Password Reuse



Source: xkcd.com

Password Reuse: Problem

2011 Study:

- 49% of users on one site reused the password on a different site
- Makes it worse if the site uses email address as login
- Bad if you use the same user name on multiple sites

2015 Study (Harris Interactive)

- 59% of consumers reuse passwords

2017 Survey (Digital Guardian):

- 60% of consumers reuse passwords

Password Reuse: Problem

- Recent(ish) news:

2 April 2014:

- Ars Technica reports 158,000 passwords from Boxee.tv (Israeli startup) published

15 June 2015:

- LastPass password vault website hacked, password hints, salts, and authentication hashes stolen.

7 Jan 2023:

- Israeli researcher reports leak of 235m email addresses linked to Twitter accounts

From the past year or so

cybernews

Home » Security

RockYou2024: 10 billion passwords leaked in the largest compilation of all time

Last updated: 4 July 2024 6

Vilius Petkauskas, Deputy Editor

ssues VentureBeat Subscribe GamesB

e Security Data Infrastructure Automation Enterprise Analytics More

Report: Hackers leaked over 721 million passwords in 2022

Tim Keary
@tim_keary

March 14, 2023 3:00 AM

From the past year or so

cybernews® News ▾ Editorial Security Privacy Crypto Tech Resources ▾ Tools ▾ Reviews ▾

If you purchase via links on our site, we may receive **affiliate commissions**.

Home » News

Outdated password exposed Poland's military secrets

Updated on: 12 May 2023

Vilius Petkauskas, Senior Journalist

Home > News > Security > NortonLifeLock warns that hackers breached Password Manager accounts

NortonLifeLock warns that hackers breached Password Manager accounts

By **Bill Toulas**

January 13, 2023 11:47 AM 7

Password Reuse Solutions

Don’t use the same login or passwords for multiple websites

Single Sign On systems (OAuth, Kerberos)

Host proof password management tools

Passwordless Future

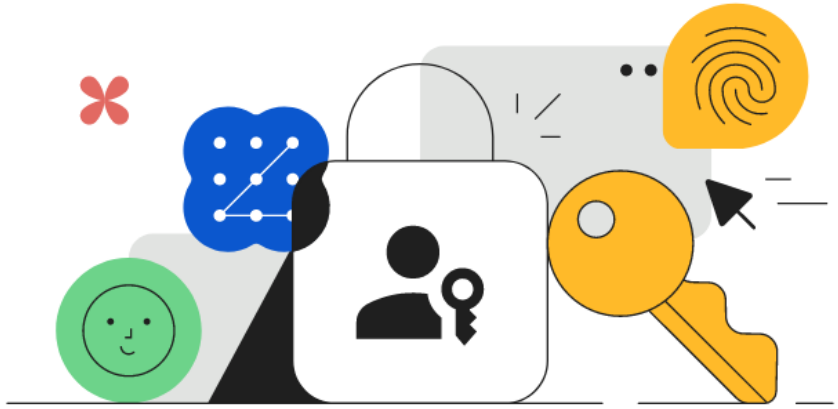
Google Identity

Authentication

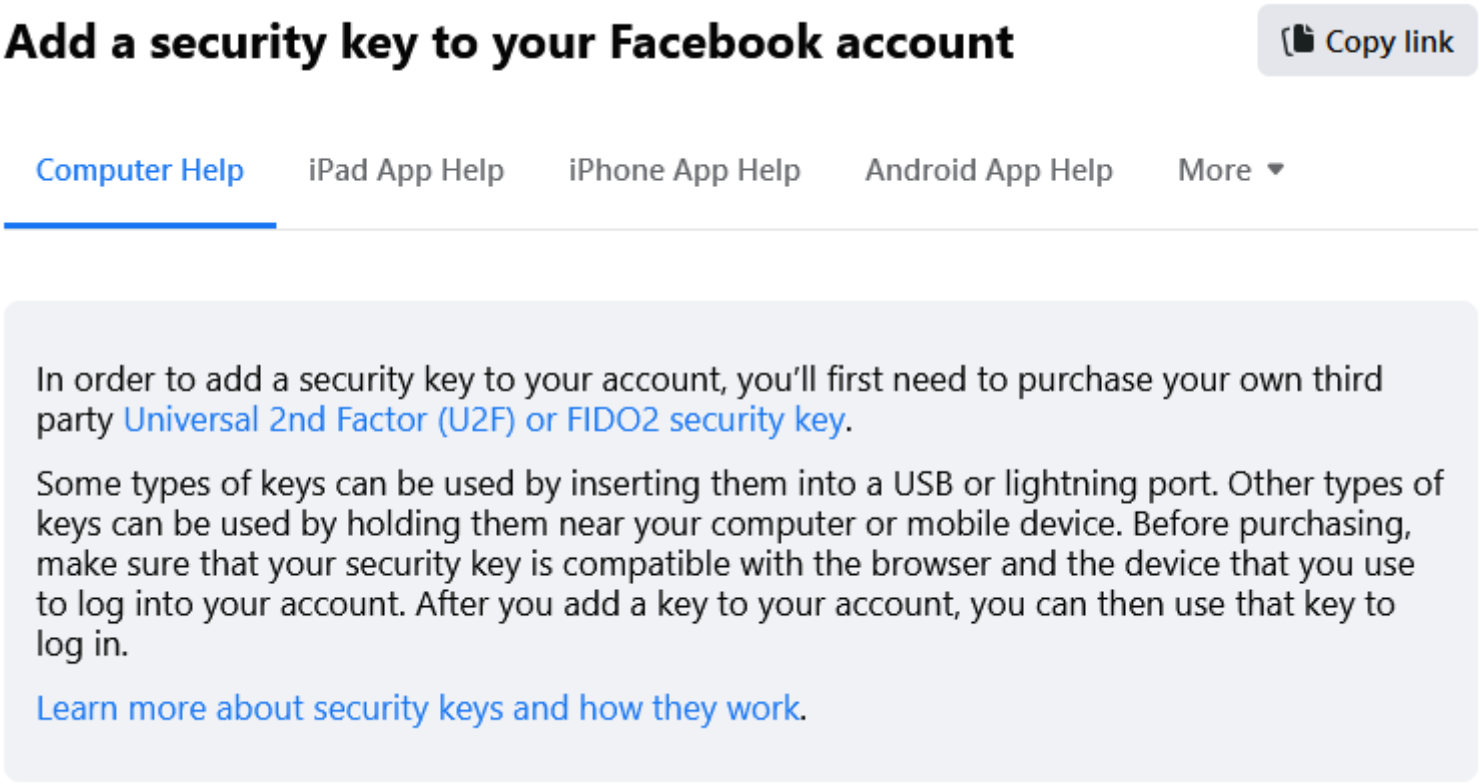
The simplest and most secure way to sign in to your Google Account

Passkeys are an easier and more secure alternative to passwords.
They let you sign in with just your fingerprint, face scan or screen lock.

Get passkeys



Facebook Too



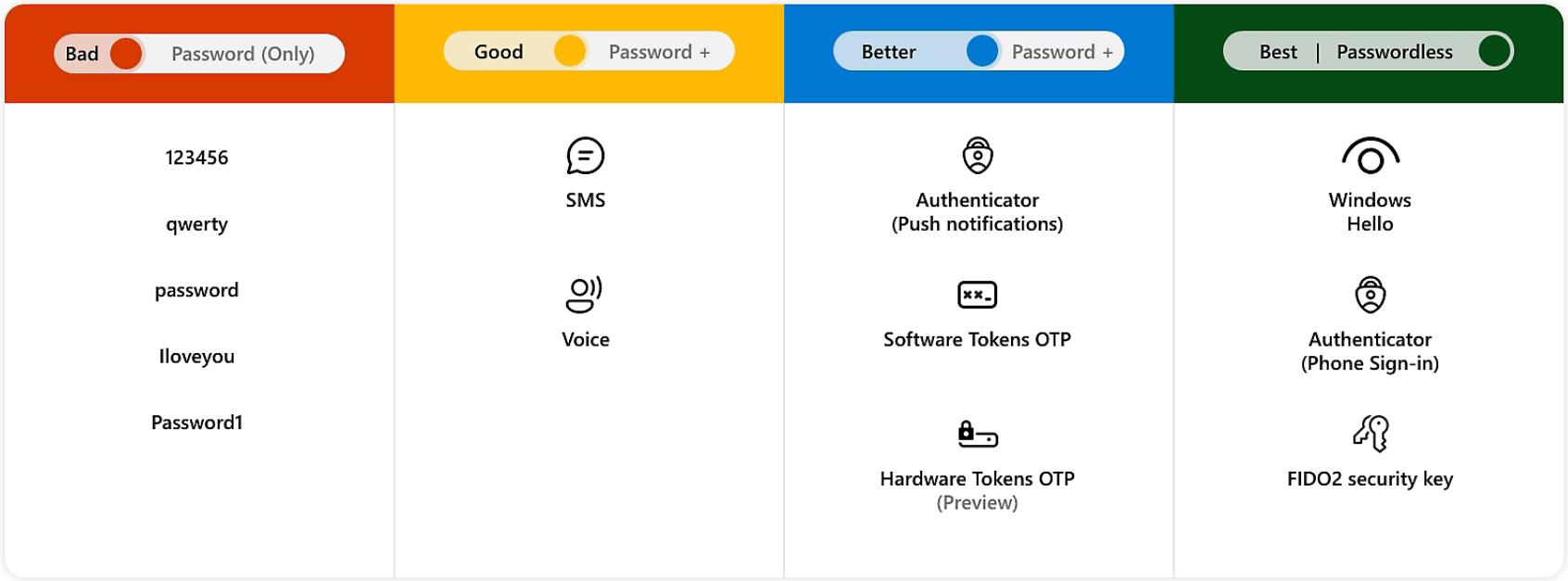
Microsoft Too

Passwordless authentication

Hackers don't break in—they sign in. Protect one of attackers' most common entry points by going passwordless.

Take sign-in security from better to best

Minimize the threat of password theft for good with the strongest authentication method available in the marketplace.



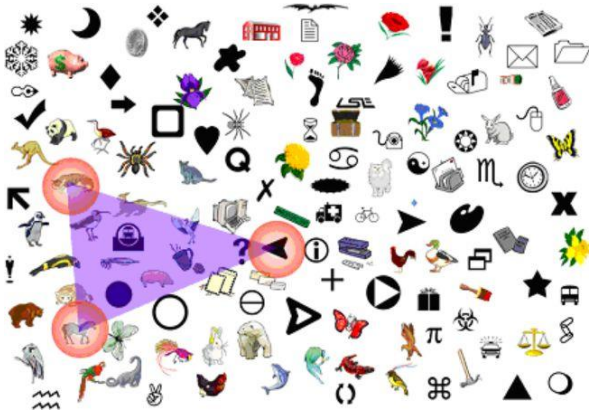
So Far

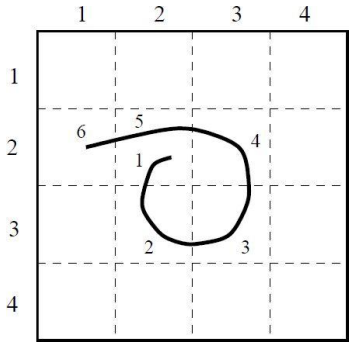
- Password storage
- Password alternatives

Password Alternatives

Graphical Passwords

Photo courtesy of Philip Greenspoon





Biometrics

- Finger/Hand print
- Iris
- Cadence (typing, walking)
- Voice print
- Face

- Challenges:
  - Collection/Enrollment
  - Theft
  - Ambiguity/Uniqueness
  - Accuracy of reader

Biometrics: Fingerprints

- Relatively cheap ($10 for a simple)
- Can match quickly (2s)
- Data is small (<1KB), so database is small
- Less affected by vandalism/dirt
- Can detect fakes/late

Issues:

- Caucasians have best defined prints
- Women have finer prints
- Manual workers, elderly have less defined prints
- Building trusted path to reader

Technique	Size	Cost	Ease of Use	Dirt Affected	Wear Affected	Easily Duped
Optical	Small	Low	Easy	Yes	Yes	Easy
Capacitance	Small	V. Low	Easy	Yes	Yes	Easy
RF	Small	V. Low	Easy	No	No	Difficult
Ultrasound	V. Large	V. High	Easy	No	Yes	Medium
Thermal	V.Small	Low	Difficult	Yes	Yes	Medium
Pressure	Small	V. Low	Easy	Yes	Yes	Medium

Reference: Coventry “Fingerprint Authentication”. (2004)

Other Biometrics

Voice print: Speak a fixed statement prerecorded

- Issues:
  - High quality recordings of voice
  - Problems with voice – cold, cough, etc.

Retinal scans: Picture of back of eye

- Very high quality
- Issues:
  - Physical proximity
  - Relatively long scan time (15s)

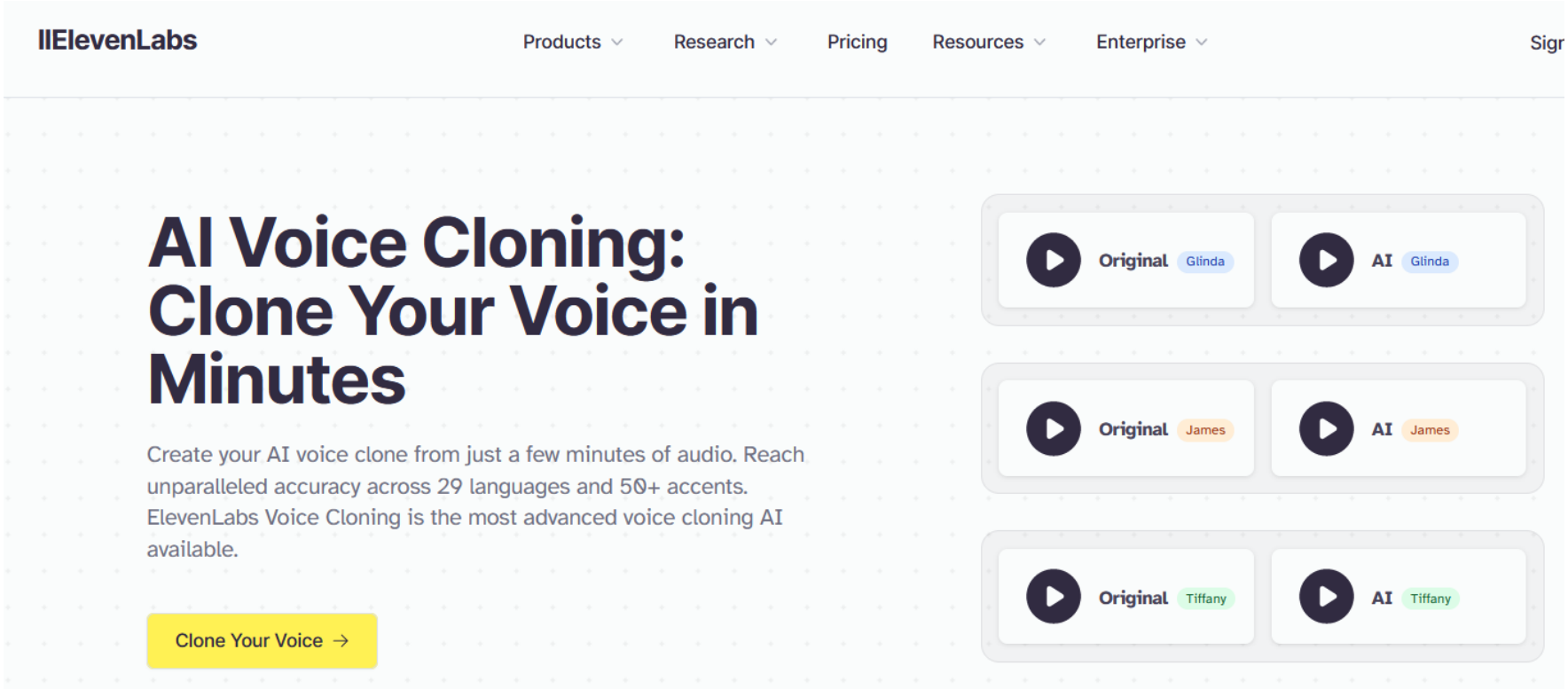
Iris scans: Scans iris pattern into a barcode

- Similar to retinal scan, but not as accurate

Facial recognition: Measure facial geometry

- Medium quality authentication
- Issues:
  - Masks, hats, bandages on face, facial hair
  - Reference: Alexander and Smith. “Engineering Privacy in Public: Confounding Face Recognition”. 2003

AI complicates voice



AI complicates facial recognition

IEEE Spectrum / Hackers Compete to Confound Facial Recognition

Type to search

NEWS | ARTIFICIAL INTELLIGENCE

Hackers Compete to Confound Facial Recognition

› Def Con challenge organizers hope to spur better security in the industry

BY EDD GENT | 29 AUG 2022 | 3 MIN READ

https://spectrum.ieee.org/facial-recognition

The real Brad Pitt (L) versus an AI Brad Pitt (R). LEFT: MATT SAYLES/AP; RIGHT: DEFCON

Conclusion

- Password storage
- Password alternatives