24. Hardware Security (Meltdown, Spectre, TEE) & Authentication Part 3

Blase Ur and David Cash
March 8th, 2021
CMSC 23200 / 33250

THE UNIVERSITY OF CHICAGO

Hardware Security: A Broad View

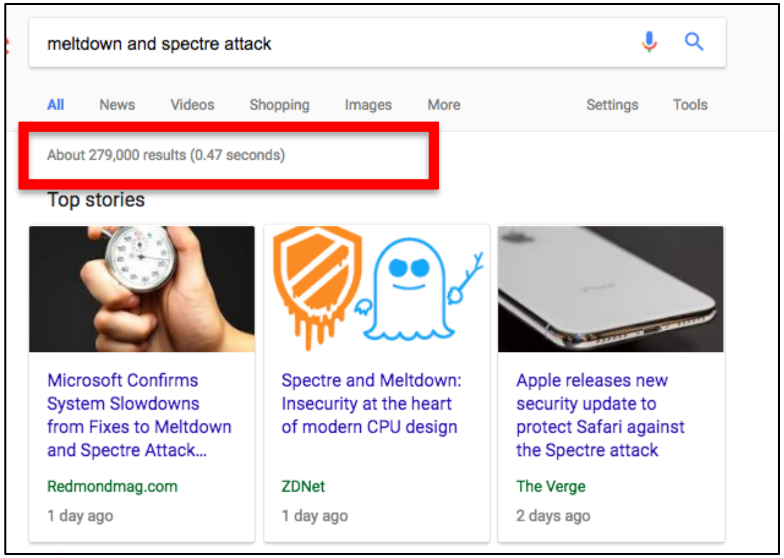
- What do we trust?
- How do we know we have the right code?
  - Recall software checksums, Subresource Integrity (SRI)
- What is our root of trust? Can we establish a smaller one?
- Can we minimize the Trusted Computing Base (TCB)?
- Can processor design lead to insecurity?
  - Yes! ☹

Attacks that exploit processor vulnerabilities

Can leak sensitive data

Relatively hard to mitigate

Lots of media attention



meltdown and spectre attack

About 279,000 results (0.47 seconds)

Top stories

Microsoft Confirms System Slowdowns from Fixes to Meltdown and Spectre Attack...
Redmondmag.com
1 day ago

Spectre and Meltdown: Insecurity at the heart of modern CPU design
ZDNet
1 day ago

Apple releases new security update to protect Safari against the Spectre attack
The Verge
2 days ago

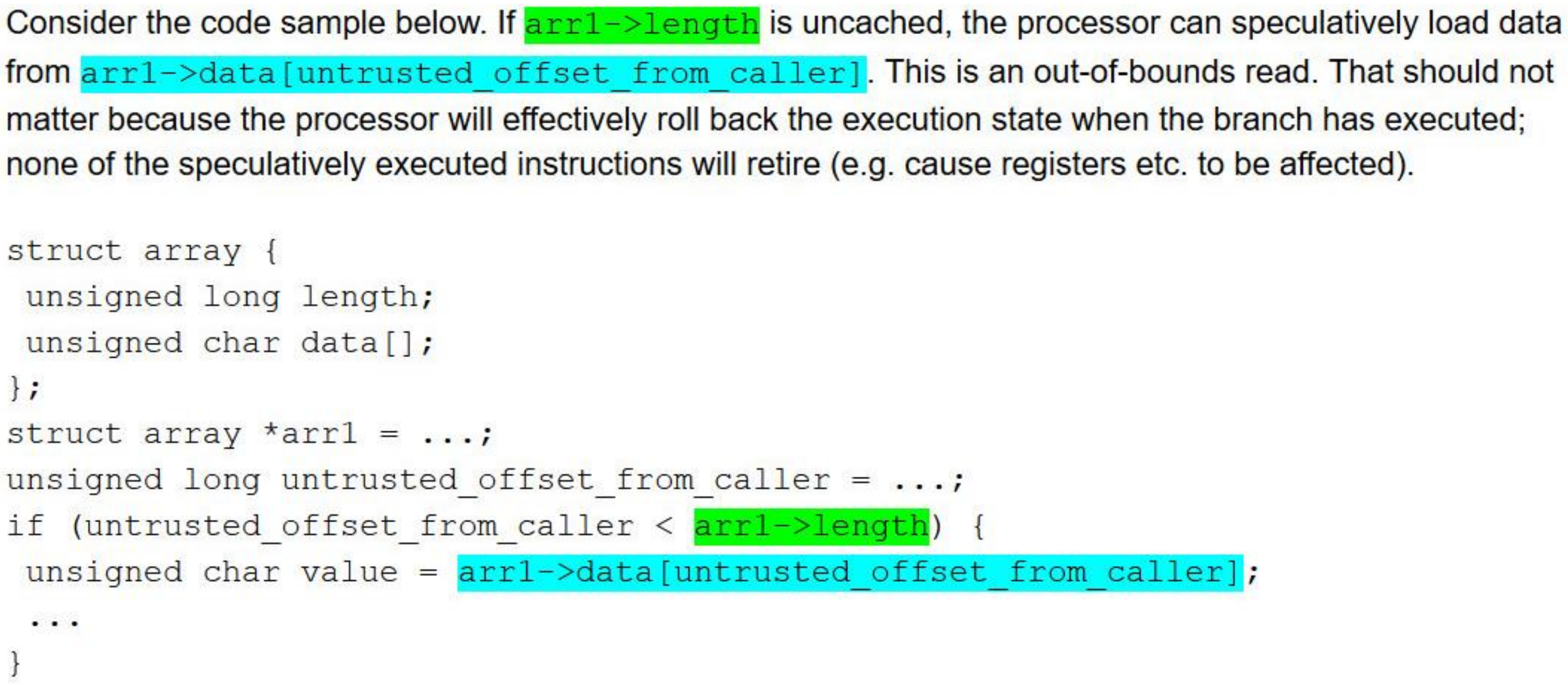
Relevant Ideas in CPUs

- **Memory isolation**: Processes should only be able to read their own memory
  - Virtual (paged) memory
  - Protected memory / Protection domains
- CPUs have a relatively small, and very fast, cache
  - Loading uncached data can take >100 CPU cycles
- **Out-of-order execution**: Order of processing in CPU can differ from the order in code
  - Instructions are much faster than memory access; you might be waiting for operands to be read from memory
  - Instructions **retire** (return to the system) in order even if they executed out of order

Relevant Ideas in CPUs

- There might be a conditional branch in the instructions
- **Speculative execution**: Rather than waiting to determine which branch of a conditional to take, go ahead anyway
  - **Predictive execution**: Guess which branch to take
  - **Eager execution**: Take both branches
- When the CPU realizes that the branch was mis-speculatively executed, it tries to eliminate the effects
- A core idea underlying Spectre/Meltdown: The results of the instruction(s) that were mis-speculatively executed will be cached in the CPU *[yikes!]*

Example (Not bad)

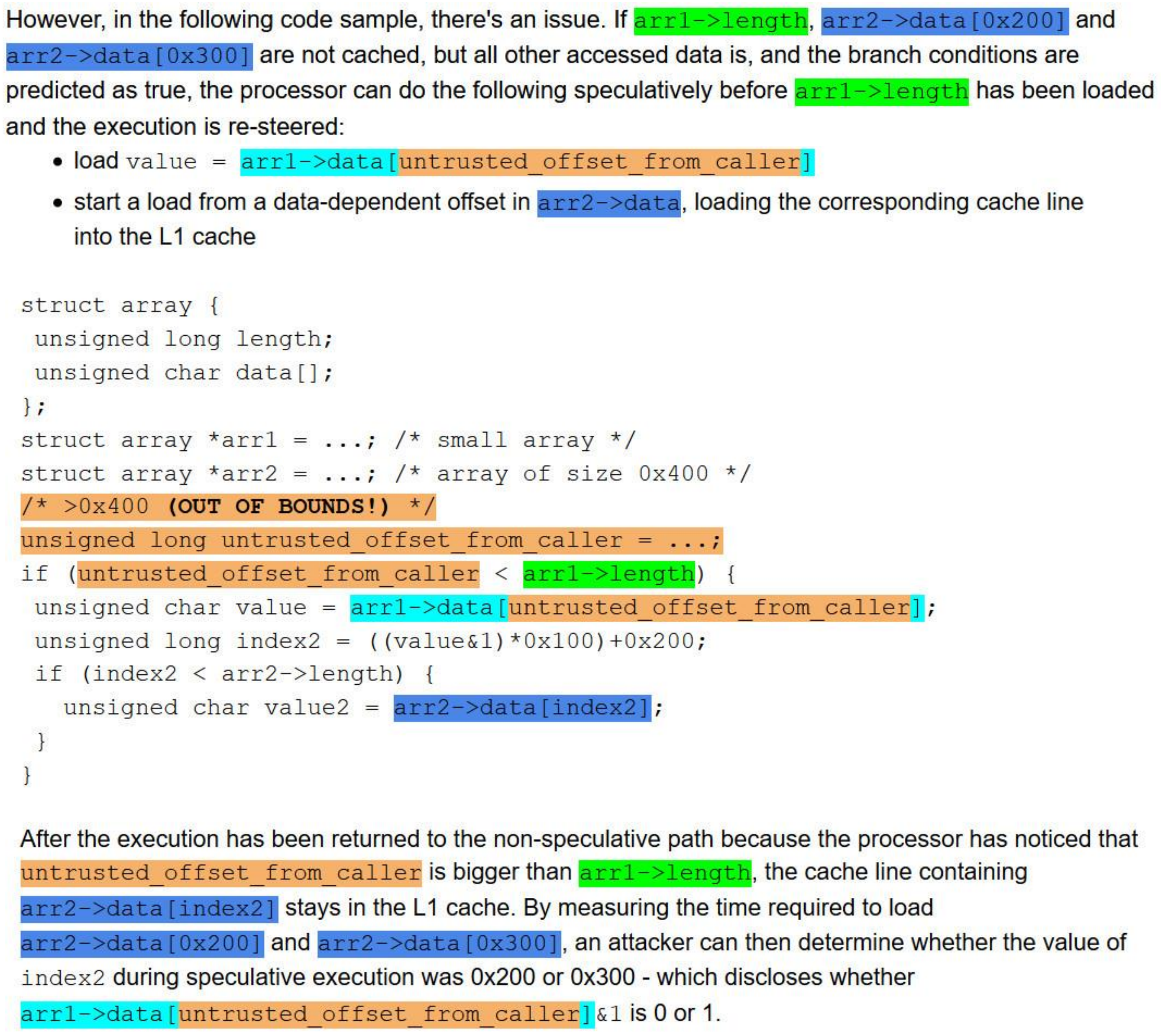


Consider the code sample below. If `arr1->length` is uncached, the processor can speculatively load data from `arr1->data[untrusted_offset_from_caller]`. This is an out-of-bounds read. That should not matter because the processor will effectively roll back the execution state when the branch has executed; none of the speculatively executed instructions will retire (e.g. cause registers etc. to be affected).

```
struct array {
 unsigned long length;
 unsigned char data[];
};
struct array *arr1 = ...;
unsigned long untrusted_offset_from_caller = ...;
if (untrusted_offset_from_caller < arr1->length) {
 unsigned char value = arr1->data[untrusted_offset_from_caller];
 ...
}
```

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

Example (Bad!!!)



However, in the following code sample, there's an issue. If `arr1->length`, `arr2->data[0x200]` and `arr2->data[0x300]` are not cached, but all other accessed data is, and the branch conditions are predicted as true, the processor can do the following speculatively before `arr1->length` has been loaded and the execution is re-steered:

- load `value = arr1->data[untrusted_offset_from_caller]`
- start a load from a data-dependent offset in `arr2->data`, loading the corresponding cache line into the L1 cache

```
struct array {
 unsigned long length;
 unsigned char data[];
};
struct array *arr1 = ...; /* small array */
struct array *arr2 = ...; /* array of size 0x400 */
/* >0x400 (OUT OF BOUNDS!) */
unsigned long untrusted_offset_from_caller = ...;
if (untrusted_offset_from_caller < arr1->length) {
 unsigned char value = arr1->data[untrusted_offset_from_caller];
 unsigned long index2 = ((value&1)*0x100)+0x200;
 if (index2 < arr2->length) {
   unsigned char value2 = arr2->data[index2];
 }
}
```

After the execution has been returned to the non-speculative path because the processor has noticed that `untrusted_offset_from_caller` is bigger than `arr1->length`, the cache line containing `arr2->data[index2]` stays in the L1 cache. By measuring the time required to load `arr2->data[0x200]` and `arr2->data[0x300]`, an attacker can then determine whether the value of `index2` during speculative execution was 0x200 or 0x300 - which discloses whether `arr1->data[untrusted_offset_from_caller]&1` is 0 or 1.

https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html

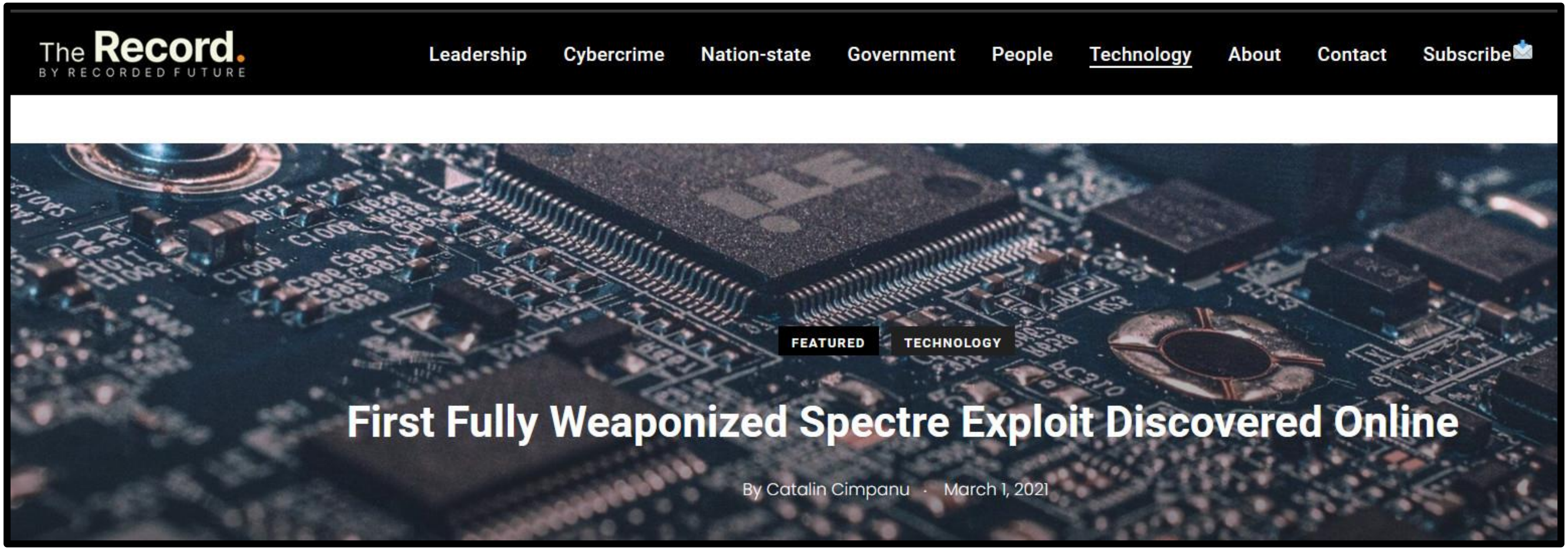
Spectre: Key Idea

- Use branch prediction as on the previous slide
- Conducting a timing side-channel attack on the cache
- Determine the value of interest based on the speed with which it returns
- Spectre allows you to read any memory from your process **for nearly every CPU**

Spectre: Exploitation Scenarios

- Leaking browser memory
- JavaScript (e.g., in an ad) can run Spectre
- Can leak browser cache, session key, other site data

Spectre: Exploitation Scenarios



The Record. BY RECORDED FUTURE

First Fully Weaponized Spectre Exploit Discovered Online

By Catalin Cimpanu · March 1, 2021

"But today, Voisin said he discovered new Spectre exploits—one for Windows and one for Linux—different from the ones before. In particular, Voisin said he found a Linux Spectre exploit capable of dumping the contents of ***/etc/shadow***, a Linux file that stores details on OS user accounts"

https://therecord.media/first-fully-weaponized-spectre-exploit-discovered-online/

Meltdown: Key Idea

1. Attempt instruction with memory operand (Base+A), where A is a value forbidden to the process
2. The CPU schedules a privilege check and the actual access
3. The privilege check fails, but due to speculative executive, the access has already run and the result has been cached
4. Conduct a timing attack reading memory at the address (Base+A) for all possible values of A. The one that ran will return faster

Meltdown allows you to read **any memory in the address space (<u>even from other processes</u>)** but only on some Intel/ARM CPUs

Meltdown Attack (Timing)

- Now the attacker read each page of probe array
- 255 of them will be slow
- The Xth page will be faster (it is cached!)
- We get the value of X using cache-timing side channel

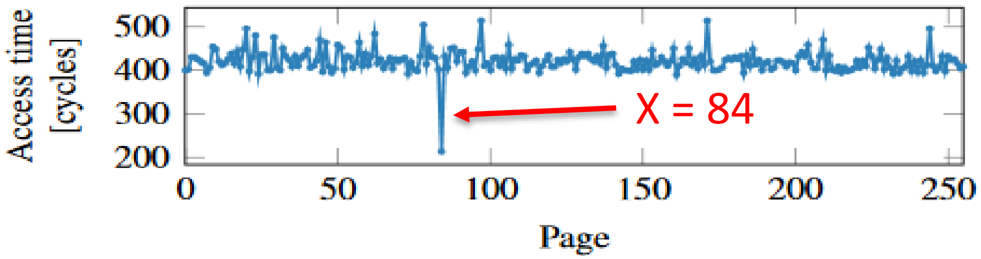


Figure 4: Even if a memory location is only accessed during out-of-order execution, it remains cached. Iterating over the 256 pages of probe_array shows one cache hit, exactly on the page that was accessed during the out-of-order execution.

Meltdown: Mitigation

- KAISER/KPTI (kernel page table isolation)
- Remove kernel memory mapping in user space processes
- Has non-negligible performance impact
- Some kernel memory still needs to be mapped

Trusted Computing

Trusted Platform Module (TPM)

- Standardization of cryptoprocessors, or microcontrollers dedicated to crypto functions w/ built-in keys
- Core functionality:

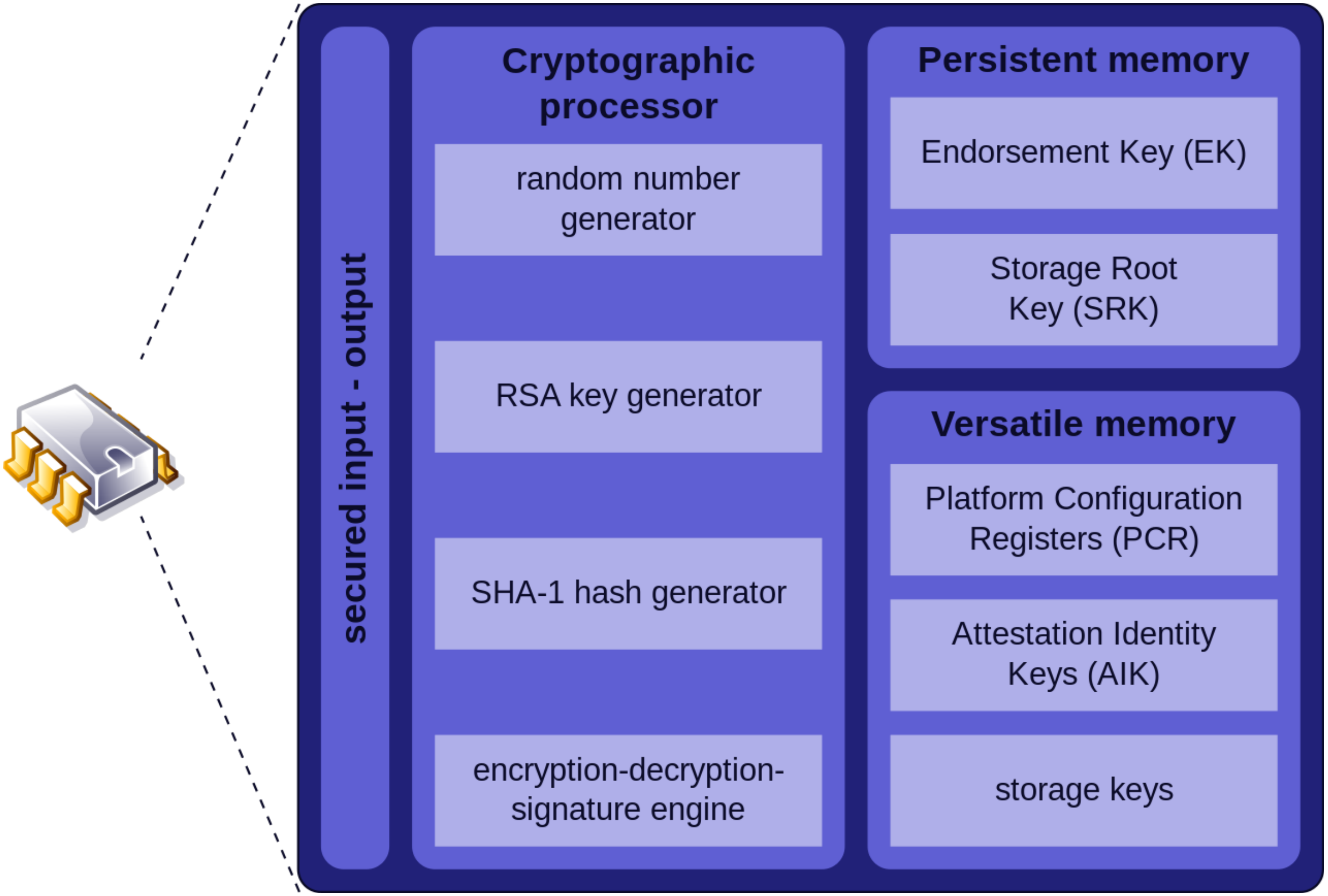
1) Random number generation, crypto key creation

2) **Remote attestation** (hash hardware and software config and send it to a verifier)

3) **Bind/seal** data: encrypted using a TPM key and, for sealing, also the required TPM state for decryption

- Uses: DRM, disk encryption (BitLocker), auth

Trusted Platform Module (TPM)



secured input - output

Cryptographic processor

random number generator

RSA key generator

SHA-1 hash generator

encryption-decryption-signature engine

Persistent memory

Endorsement Key (EK)

Storage Root Key (SRK)

Versatile memory

Platform Configuration Registers (PCR)

Attestation Identity Keys (AIK)

storage keys

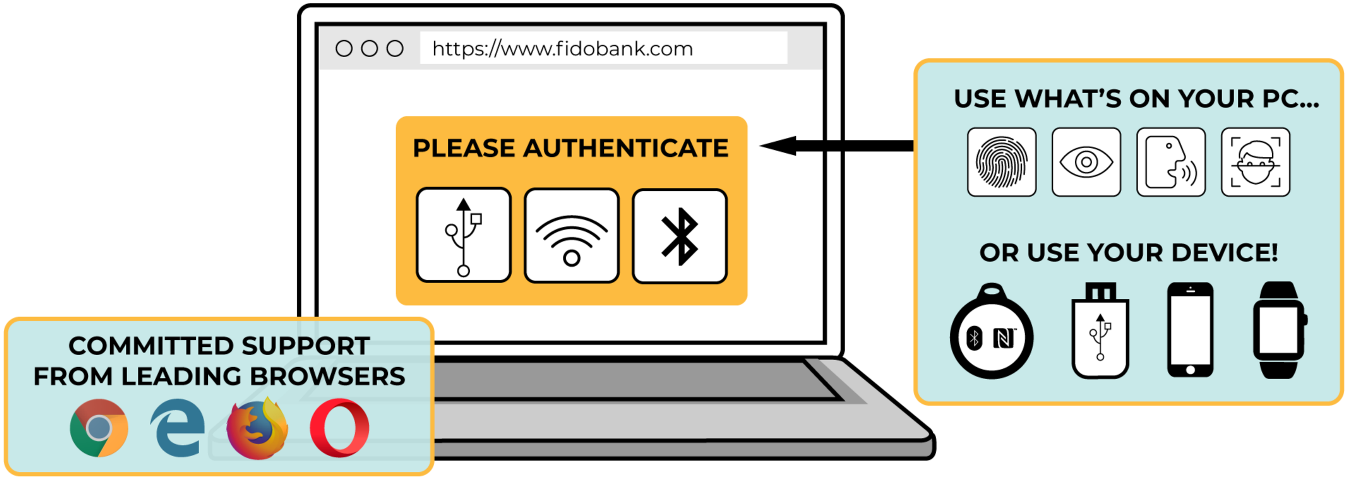
Trusted Execution Environment (TEE)

- TPMs are standalone companion chips, while TEEs are a secure area of a main processor
- Guarantees confidentiality and integrity for code in TEE
- Key example: Intel Software Guard Extensions (SGX)
- ***Enclaves* =** Private regions of memory that can’t be read by any process outside the enclave, even with root access
- Uses: DRM, mobile wallets, auth

Authentication in Practice: Moving Towards A Passwordless World?

Case Study: WebAuthn

FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS



https://www.fidobank.com

PLEASE AUTHENTICATE

USE WHAT'S ON YOUR PC...

OR USE YOUR DEVICE!

COMMITTED SUPPORT FROM LEADING BROWSERS

FIDO AUTHENTICATION: THE NEW GOLD STANDARD

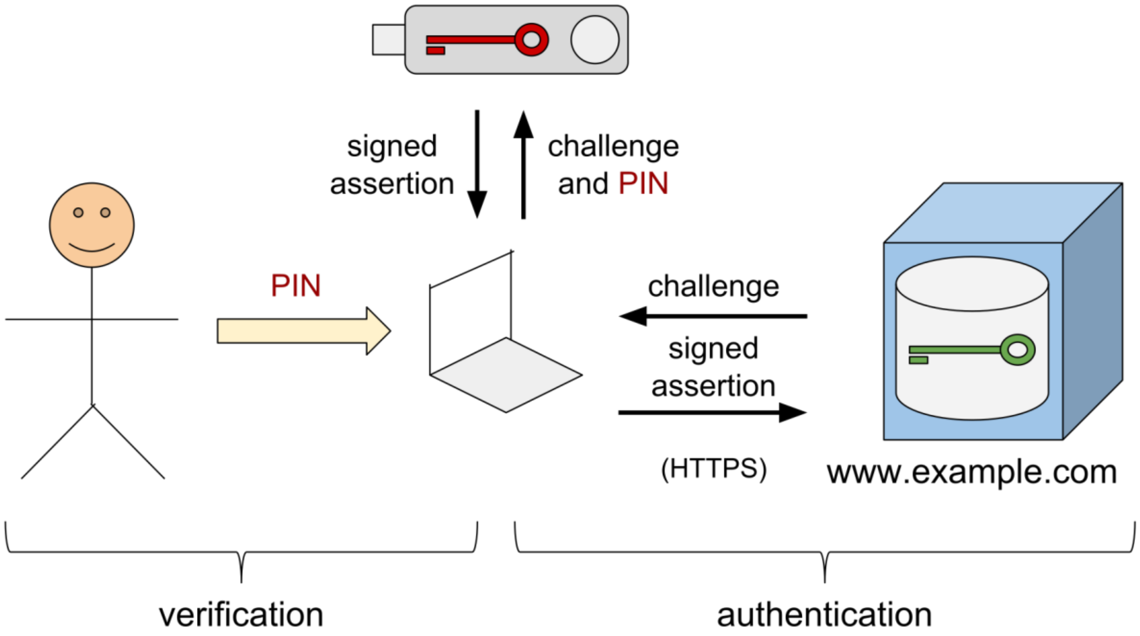
Protects against phishing, man-in-the-middle and attacks using stolen credentials

Log in with a single gesture – HASSLE FREE!

Already supported in market by top online services

Case Study: WebAuthn

- Created under the FIDO2 project, now a W3C standard
- Goal: Authenticate on web using public-key crypto
- Implemented in specialized hardware OR in software using a TPM/TEE



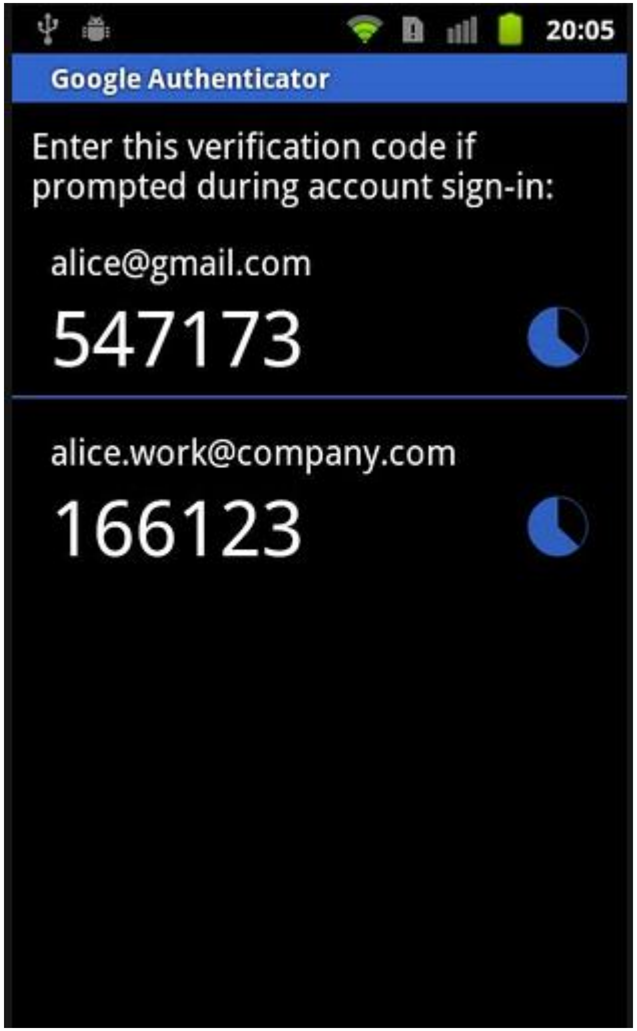
Case Study: WebAuthn

User interaction: Push a button on a key, type a PIN into the device, present biometric (fingerprint) to hardware reader

Authentication in Practice: Password Add-Ons / Alternatives

Single Sign-On

Two-Factor Auth



Enter this verification code if prompted during account sign-in:

alice@gmail.com

547173

alice.work@company.com

166123

Physical Tokens / Smart Cards

- Codes based on a cryptographic key
  - Token manufacturer also knows the key
- What if there is a breach?

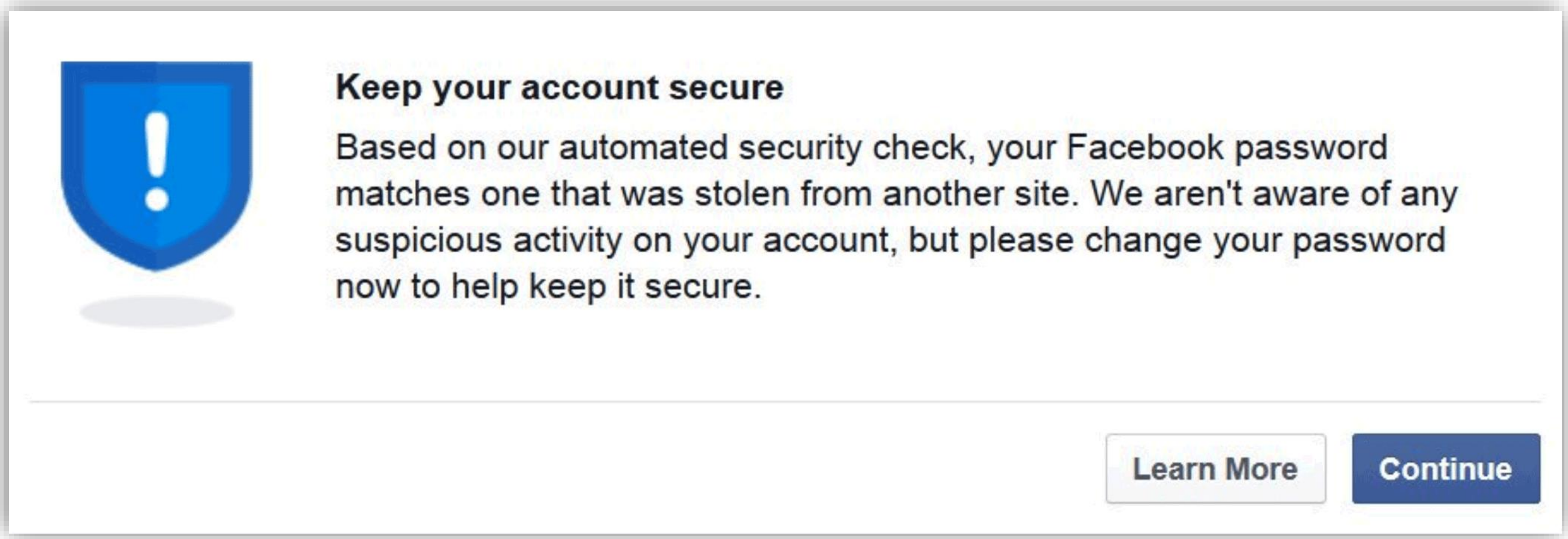
Authentication in Practice: I Forgot My Password

Resetting Accounts

- I forgot my password!
- Send an email?
- Security questions?
- In-person verification?
- Other steps?
- (No backup)

Authentication in Practice: Password Reuse ☹

Password Reuse-Based Attacks



Keep your account secure

Based on our automated security check, your Facebook password matches one that was stolen from another site. We aren't aware of any suspicious activity on your account, but please change your password now to help keep it secure.

Maximilian Golla, Miranda Wei, Juliette Hainline, Lydia Filipe, Markus Dürmuth, Elissa Redmiles, Blase Ur. “What was that site doing with my Facebook Password?” Designing Password-Reuse Notifications. In *Proc. CCS*, 2018.

People Reuse Passwords

Booking.com
reddit
淘宝网
Taobao.com
American Airlines
facebook
Adobe
ebay
Baidu 百度
airbnb
YouTube
SONY
slack
Microsoft
PayPal
WELLS FARGO
1&1
Dropbox
twitter
Spotify
Google

R0cky!14

R0cky!17

R0ckyBox

R0cky!17

R0cky!17

123456

R0ckyStar

R0cky!17

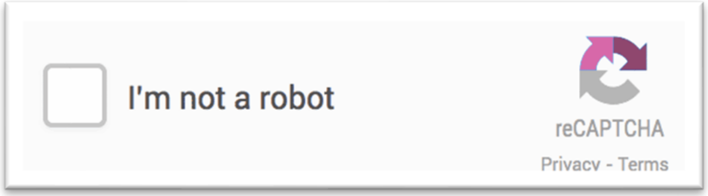
Rocky!16

AcmeCo

Memory-Hard Hash Function ✓

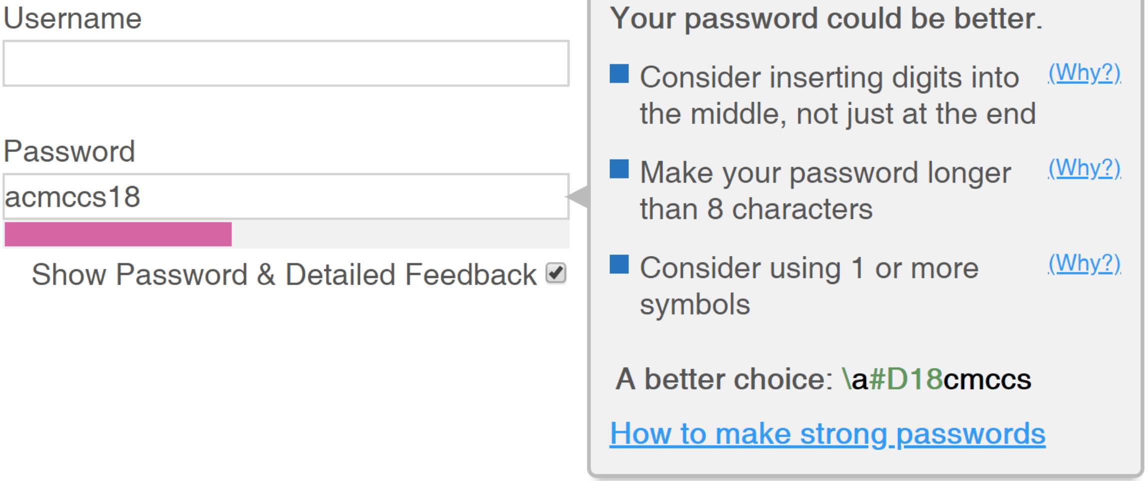
Email	Argon2i Hash of Password
…	…
jim@mail.com	$argon2i$v=19$m=4096,…
…	…

Rate-Limiting Guessing ✓



□ I'm not a robot

Password Strength Meter ✓



Username

Password

acmccs18

Show Password & Detailed Feedback ☑

Your password could be better.

- Consider inserting digits into the middle, not just at the end (Why?)
- Make your password longer than 8 characters (Why?)
- Consider using 1 or more symbols (Why?)

A better choice: \a#D18cmccs

How to make strong passwords

AcmeCo

Email
…
jim@mail.com
…

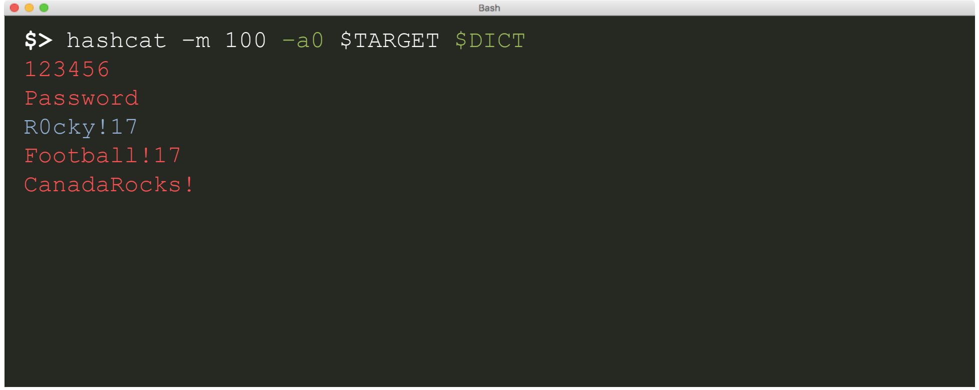
LinkedIn

Email
jane@aol.com
jessey@gmx.net
jenny@gmail.com
jim@mail.com
john@hotmail.com
…

LinkedIn

Email	SHA-1 Hash of Password
jane@aol.com	7c4a8d09ca3762af61e595209
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	7c222fb2927d828af22f59213
jim@mail.com	ba93664a90285b9ff18a7a081
john@hotmail.com	b1b3773a05c0ed0176787a4f1
...	...

Crack All The Things!



```
$> hashcat -m 100 -a0 $TARGET $DICT
123456
Password
R0cky!17
Football!17
CanadaRocks!
```

Linked in

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

Dead On Arrival

AcmeCo

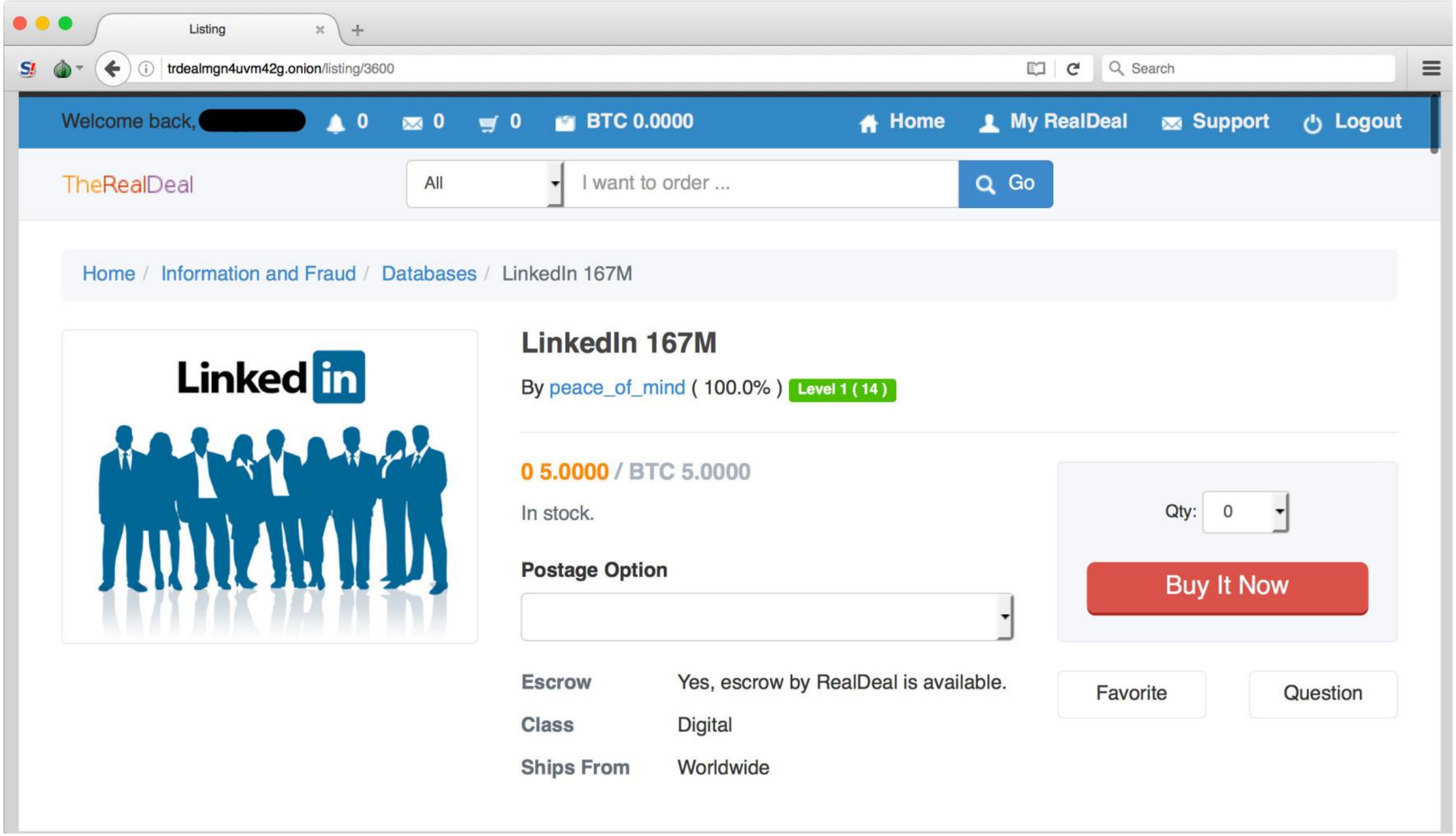
Email	Cracked
…	…
jim@mail.com	R0cky!17
…	…

LinkedIn

Email	Cracked SHA-1 Hashes
jane@aol.com	123456
jessey@gmx.net	5baa61e4c9b93f3f0682250b6
jenny@gmail.com	Canada4ever
jim@mail.com	R0cky!17
john@hotmail.com	HikingGuy89
…	…

1 guess is enough!

Monitoring the Black Market



trdealmgn4uvm42g.onion/listing/3600

Welcome back, [redacted] 0 0 0 BTC 0.0000

TheRealDeal

Home / Information and Fraud / Databases / LinkedIn 167M

LinkedIn 167M

By peace_of_mind (100.0%) Level 1 (14)

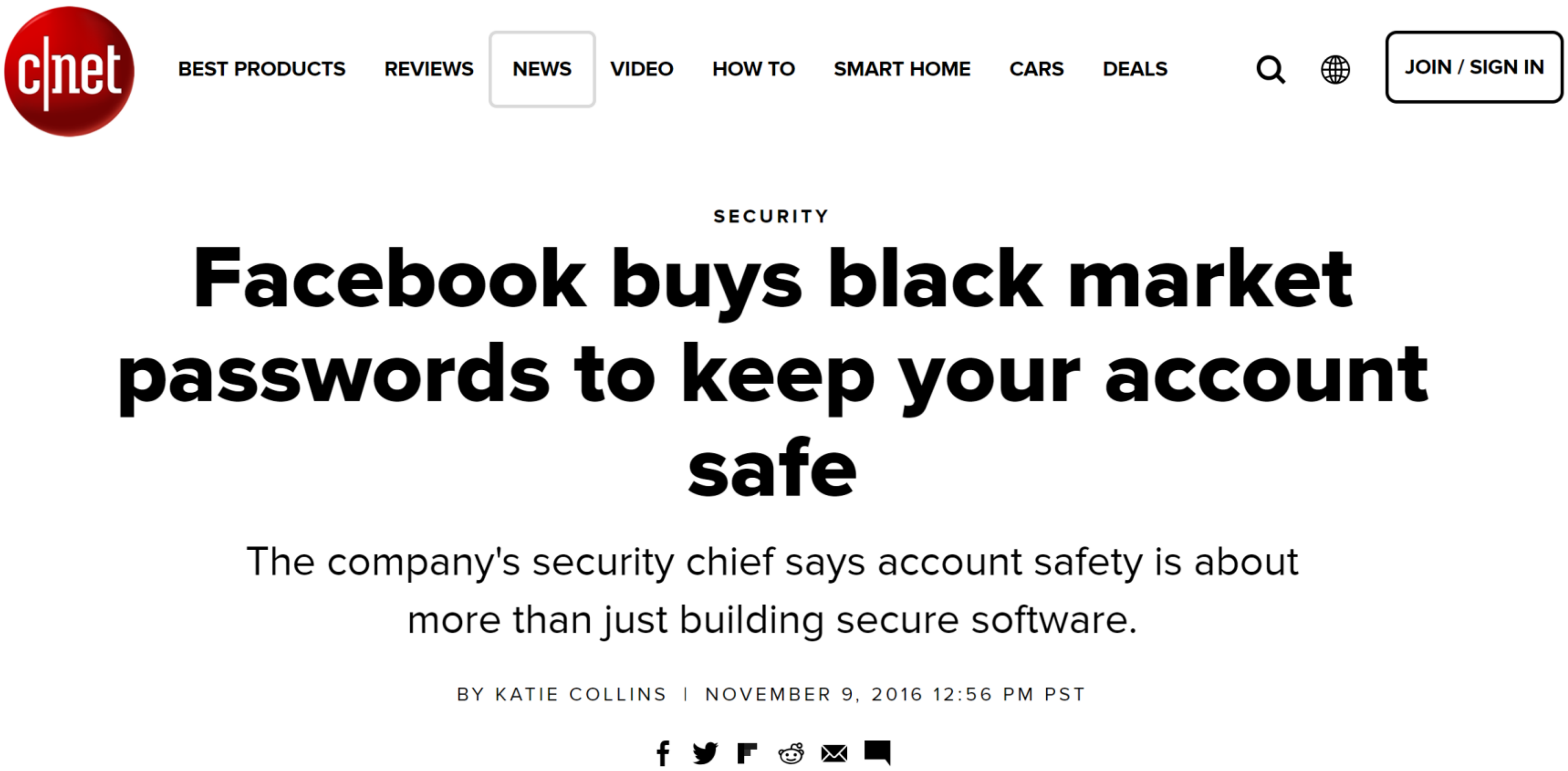
0 5.0000 / BTC 5.0000

In stock.

Qty: 0

Postage Option

Escrow	Yes, escrow by RealDeal is available.
Class	Digital
Ships From	Worldwide



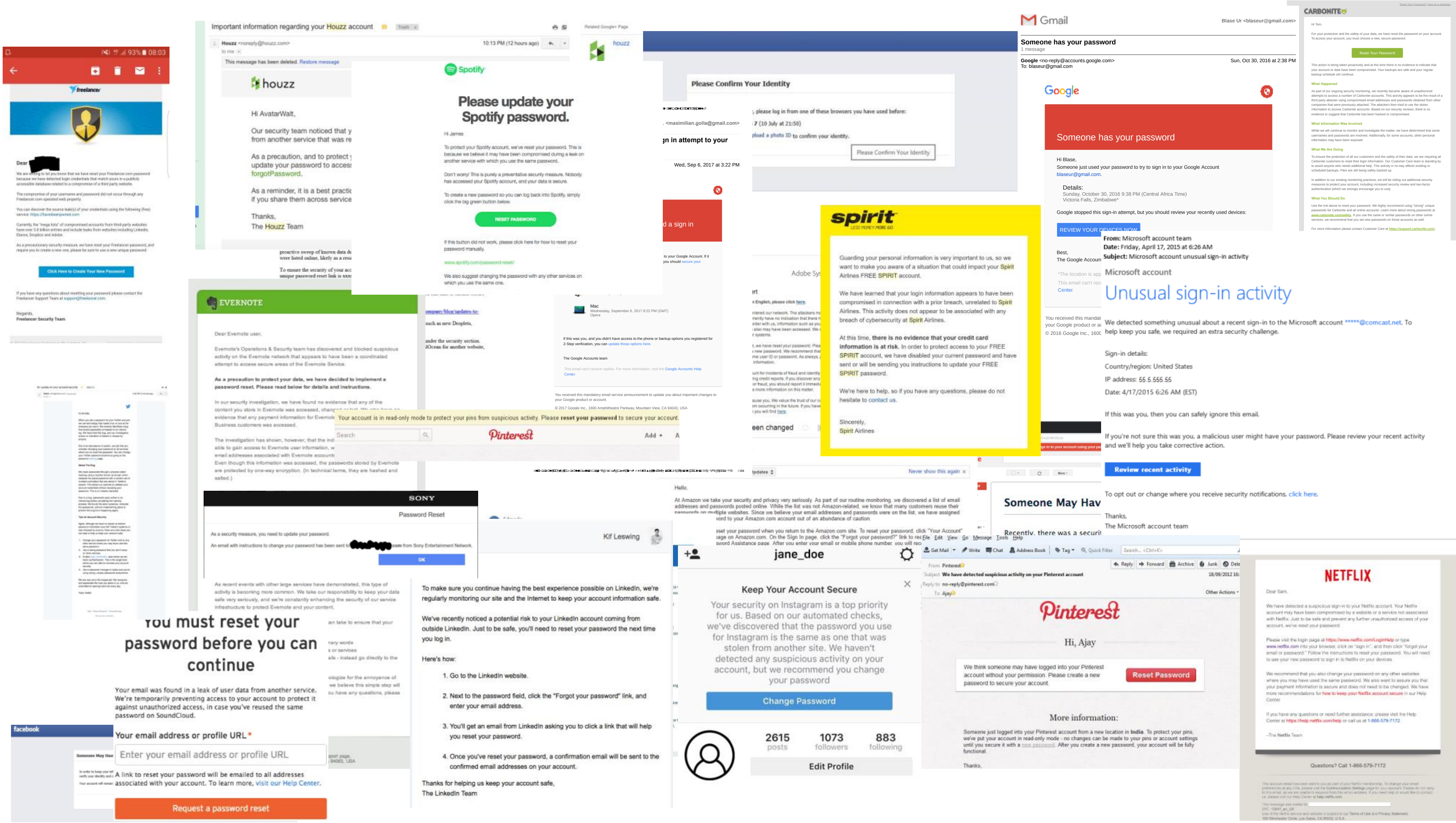
SECURITY

Facebook buys black market passwords to keep your account safe

The company's security chief says account safety is about more than just building secure software.

BY KATIE COLLINS | NOVEMBER 9, 2016 12:56 PM PST

Password-Reuse Notifications



freelancer

Dear [redacted]

We are writing to let you know that we have reset your Freelancer.com password because we have detected login credentials that match yours in a publicly accessible database related to a compromise of a third party website.

The compromise of your username and password did not occur through any Freelancer.com operated web property.

You can discover the source leak(s) of your credentials using the following (free) service: https://haveibeenpwned.com

Currently, the "mega lists" of compromised accounts from third-party websites have over 3.8 billion entries and include leaks from websites including LinkedIn, Elance, Dropbox and Adobe.

As a precautionary security measure, we have reset your Freelancer password, and require you to create a new one, please be sure to use a new unique password.

Click Here to Create Your New Password

If you have any questions about resetting your password please contact the Freelancer Support Team at support@freelancer.com

Regards,
Freelancer Security Team

Important information regarding your Houzz account

Houzz <noreply@houzz.com>
to me
10:13 PM (12 hours ago)

This message has been deleted. Restore message

houzz

Hi AvatarWalt,

Our security team noticed that y
from another service that was re

As a precaution, and to protect y
update your password to access
forgotPassword.

As a reminder, it is a best practic
if you share them across service

Thanks,
The Houzz Team

Spotify

Please update your Spotify password.

Hi James

To protect your Spotify account, we've reset your password. This is because we believe it may have been compromised during a leak on another service with which you use the same password.

Don't worry! This is purely a preventative security measure. Nobody has accessed your Spotify account, and your data is secure.

To create a new password so you can log back into Spotify, simply click the big green button below.

RESET PASSWORD

If this button did not work, please click here for how to reset your password manually.

www.spotify.com/password-reset/

We also suggest changing the password with any other services on which you use the same one.

Please Confirm Your Identity

Please Confirm Your Identity

EVERNOTE

Dear Evernote user,

Evernote's Operations & Security team has discovered and blocked suspicious activity on the Evernote network that appears to have been a coordinated attempt to access secure areas of the Evernote Service.

As a precaution to protect your data, we have decided to implement a password reset. Please read below for details and instructions.

In our security investigation, we have found no evidence that any of the content you store in Evernote was accessed, chang
evidence that any payment information for Evernote
Business customers was accessed.

The investigation has shown, however, that the ind
able to gain access to Evernote user information, w
email addresses associated with Evernote accounts
Even though this information was accessed, the passwords stored by Evernote are protected by one-way encryption. (In technical terms, they are hashed and salted.)

As recent events with other large services have demonstrated, this type of activity is becoming more common. We take our responsibility to keep your data safe very seriously, and we're constantly enhancing the security of our service infrastructure to protect Evernote and your content.

Your account is in read-only mode to protect your pins from suspicious activity. Please **reset your password** to secure your account.

SONY

Password Reset

As a security measure, you need to update your password.

An email with instructions to change your password has been sent to [redacted].com from Sony Entertainment Network.

OK

You must reset your password before you can continue

Your email was found in a leak of user data from another service. We're temporarily preventing access to your account to protect it against unauthorized access, in case you've reused the same password on SoundCloud.

Your email address or profile URL *

Enter your email address or profile URL

A link to reset your password will be emailed to all addresses associated with your account. To learn more, visit our Help Center.

Request a password reset

Kif Leswing

To make sure you continue having the best experience possible on LinkedIn, we're regularly monitoring our site and the Internet to keep your account information safe.

We've recently noticed a potential risk to your LinkedIn account coming from outside LinkedIn. Just to be safe, you'll need to reset your password the next time you log in.

Here's how:

1. Go to the LinkedIn website.
2. Next to the password field, click the "Forgot your password" link, and enter your email address.
3. You'll get an email from LinkedIn asking you to click a link that will help you reset your password.
4. Once you've reset your password, a confirmation email will be sent to the confirmed email addresses on your account.

Thanks for helping us keep your account safe,
The LinkedIn Team

spirit
LESS MONEY. MORE GO.

Guarding your personal information is very important to us, so we want to make you aware of a situation that could impact your Spirit Airlines FREE SPIRIT account.

We have learned that your login information appears to have been compromised in connection with a prior breach, unrelated to Spirit Airlines. This activity does not appear to be associated with any breach of cybersecurity at Spirit Airlines.

At this time, **there is no evidence that your credit card information is at risk.** In order to protect access to your FREE SPIRIT account, we have disabled your current password and have sent or will be sending you instructions to update your FREE SPIRIT password.

We're here to help, so if you have any questions, please do not hesitate to contact us.

Sincerely,
Spirit Airlines

Hello,

At Amazon we take your security and privacy very seriously. As part of our routine monitoring, we discovered a list of email addresses and passwords posted online. While the list was not Amazon-related, we know that many customers reuse their passwords on multiple websites. Since we believe your email addresses and passwords were on the list, we have assigned a temporary password to your Amazon.com account out of an abundance of caution.

jane_doe

Keep Your Account Secure

Your security on Instagram is a top priority for us. Based on our automated checks, we've discovered that the password you use for Instagram is the same as one that was stolen from another site. We haven't detected any suspicious activity on your account, but we recommend you change your password

Change Password

2615 posts 1073 followers 883 following

Edit Profile

Gmail

Blase Ur <blaseur@gmail.com>

Someone has your password
1 message

Google <no-reply@accounts.google.com> Sun, Oct 30, 2016 at 2:38 PM
To: blaseur@gmail.com

Google

Someone has your password

Hi Blase,
Someone just used your password to try to sign in to your Google Account blaseur@gmail.com.

Details:
Sunday, October 30, 2016 9:38 PM (Central Africa Time)
Victoria Falls, Zimbabwe*

Google stopped this sign-in attempt, but you should review your recently used devices:

REVIEW YOUR DEVICES NOW

Best,
The Google Account

CARBONITE

Hi Tom,

For your protection and the safety of your data, we have reset the password on your account. To access your account, you must choose a new, secure password.

Reset Your Password

This action is being taken proactively and at this time there is no evidence to indicate that your account or data have been compromised. Your backups are safe and your regular backup schedule will continue.

What Happened

As part of our ongoing security monitoring, we recently became aware of unauthorized attempts to access a number of Carbonite accounts. This activity appears to be the result of a third party attacker using compromised email addresses and passwords obtained from other companies that were previously attacked. The attackers then tried to use the stolen information to access Carbonite accounts. Based on our security reviews, there is no evidence to suggest that Carbonite has been hacked or compromised.

What Information Was Involved

While we will continue to monitor and investigate the matter, we have determined that some usernames and passwords are involved. Additionally, for some accounts, other personal information may have been exposed.

What We Are Doing

To ensure the protection of all our customers and the safety of their data, we are requiring all Carbonite customers to reset their login information. Our Customer Care team is standing by to assist anyone who needs additional help. This activity in no way affects existing or scheduled backups. Files are still being safely backed up.

In addition to our existing monitoring practices, we will be rolling out additional security measures to protect your account, including increased security review and two-factor authentication [which we strongly encourage you to use].

What You Should Do

Use the link above to reset your password. We highly recommend using "strong" unique passwords for Carbonite and all online accounts. Learn more about strong passwords at www.carbonite.com/safety. If you use the same or similar passwords on other online services, we recommend that you set new passwords on those accounts as well.

For more information please contact Customer Care at https://support.carbonite.com/.

From: Microsoft account team
Date: Friday, April 17, 2015 at 6:26 AM
Subject: Microsoft account unusual sign-in activity

Microsoft account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the Microsoft account *****@comcast.net. To help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: United States

IP address: 55.5.555.55

Date: 4/17/2015 6:26 AM (EST)

If this was you, then you can safely ignore this email.

If you're not sure this was you, a malicious user might have your password. Please review your recent activity and we'll help you take corrective action.

Review recent activity

To opt out or change where you receive security notifications, click here.

Thanks,
The Microsoft account team

Someone May Hav

Recently, there was a securit

From: Pinterest
Subject: **We have detected suspicious activity on your Pinterest account** 18/09/2012 16:
Reply to: no-reply@pinterest.com
To: Ajay

Pinterest

Hi, Ajay

We think someone may have logged into your Pinterest account without your permission. Please create a new password to secure your account.

Reset Password

More information:

Someone just logged into your Pinterest account from a new location in **India**. To protect your pins, we've put your account in read-only mode - no changes can be made to your pins or account settings until you secure it with a new password. After you create a new password, your account will be fully functional.

Thanks,

NETFLIX

Dear Sam,

We have detected a suspicious sign-in to your Netflix account. Your Netflix account may have been compromised by a website or a service not associated with Netflix. Just to be safe and prevent any further unauthorized access of your account, we've reset your password.

Please visit the login page at https://www.netflix.com/LoginHelp or type www.netflix.com into your browser, click on "sign in", and then click "forgot your email or password." Follow the instructions to reset your password. You will need to use your new password to sign in to Netflix on your devices.

We recommend that you also change your password on any other websites where you may have used the same password. We also want to assure you that your payment information is secure and does not need to be changed. We have more recommendations for how to keep your Netflix account secure in our Help Center.

If you have any questions or need further assistance, please visit the Help Center at https://help.netflix.com/help or call us at 1-866-579-7172.

–The Netflix Team

Questions? Call 1-866-579-7172

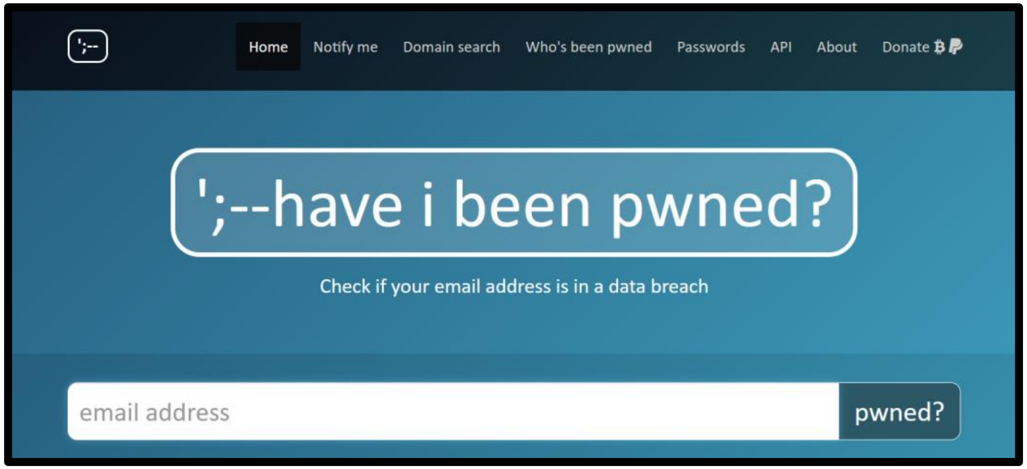
Authentication in Practice: Password Managers

Password Managers

- Trust all passwords to a single master password
  - Also trust software
  - Centralized vs. decentralized architectures

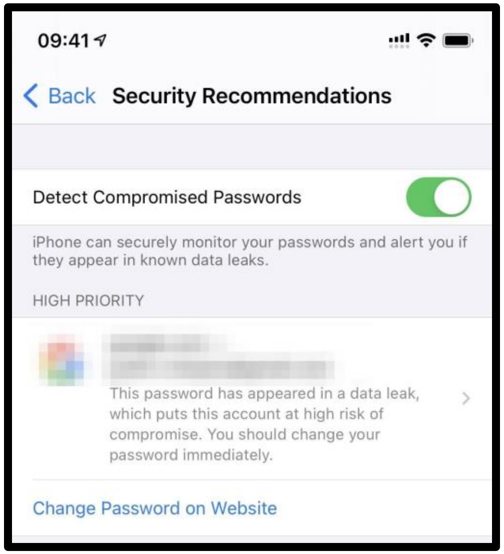
Authentication in Practice: Checking for Compromised Credentials

Checking for Compromised Credentials



';--have i been pwned?

Check if your email address is in a data breach



Security Recommendations

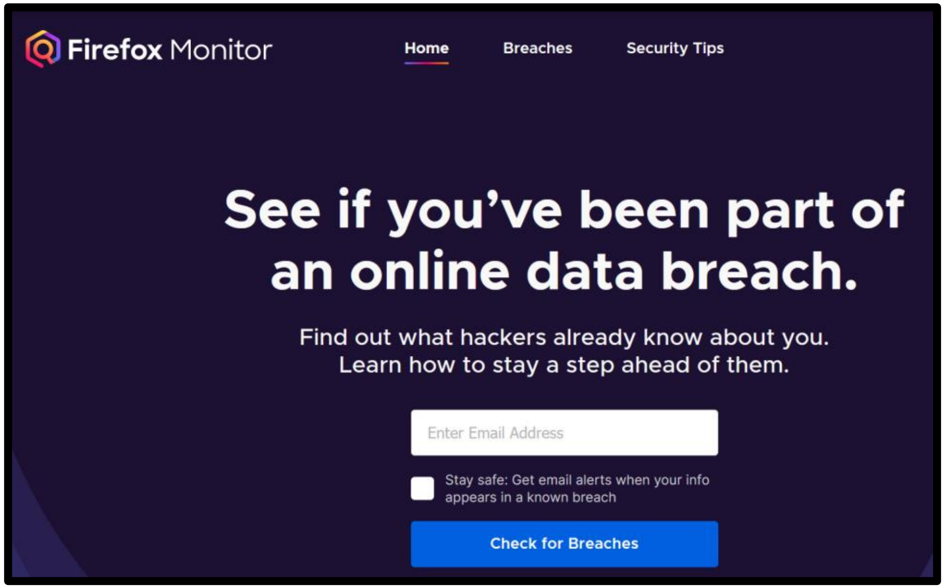
Detect Compromised Passwords

iPhone can securely monitor your passwords and alert you if they appear in known data leaks.

HIGH PRIORITY

[redacted]

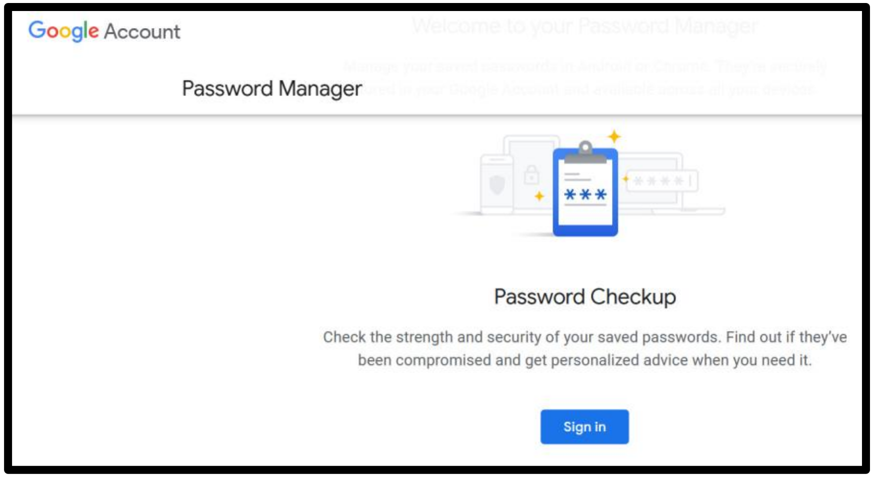
This password has appeared in a data leak, which puts this account at high risk of compromise. You should change your password immediately.



See if you've been part of an online data breach.

Find out what hackers already know about you.
Learn how to stay a step ahead of them.

□ Stay safe: Get email alerts when your info appears in a known breach



Password Checkup

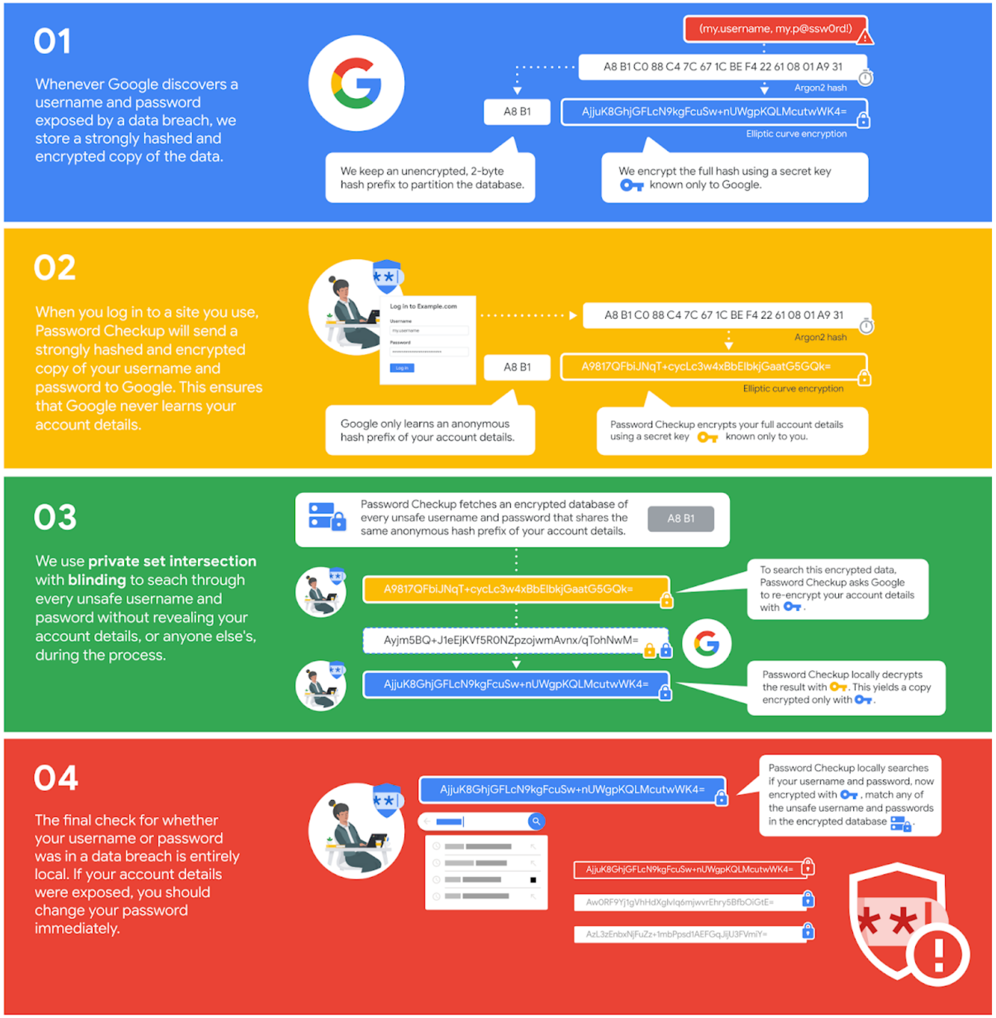
Check the strength and security of your saved passwords. Find out if they've been compromised and get personalized advice when you need it.

https://www.zdnet.com/article/google-launches-password-checkup-feature-will-add-it-to-chrome-later-this-year/
https://ios.gadgethacks.com/how-to/ios-14-monitors-your-passwords-protect-you-against-data-breaches-heres-works-0341281/

Checking for Compromised Credentials

Under the hood:

How Password Checkup helps keep your accounts safe



01

Whenever Google discovers a username and password exposed by a data breach, we store a strongly hashed and encrypted copy of the data.

We keep an unencrypted, 2-byte hash prefix to partition the database.

We encrypt the full hash using a secret key 🔑 known only to Google.

02

When you log in to a site you use, Password Checkup will send a strongly hashed and encrypted copy of your username and password to Google. This ensures that Google never learns your account details.

Google only learns an anonymous hash prefix of your account details.

Password Checkup encrypts your full account details using a secret key 🔑 known only to you.

03

We use **private set intersection** with **blinding** to seach through every unsafe username and pasword without revealing your account details, or anyone else's, during the process.

Password Checkup fetches an encrypted database of every unsafe username and password that shares the same anonymous hash prefix of your account details.

To search this encrypted data, Password Checkup asks Google to re-encrypt your account details with 🔑.

Password Checkup locally decrypts the result with 🔑. This yields a copy encrypted only with 🔑.

04

The final check for whether your username or password was in a data breach is entirely local. If your account details were exposed, you should change your password immediately.

Password Checkup locally searches if your username and password, now encrypted with 🔑, match any of the unsafe username and passwords in the encrypted database.

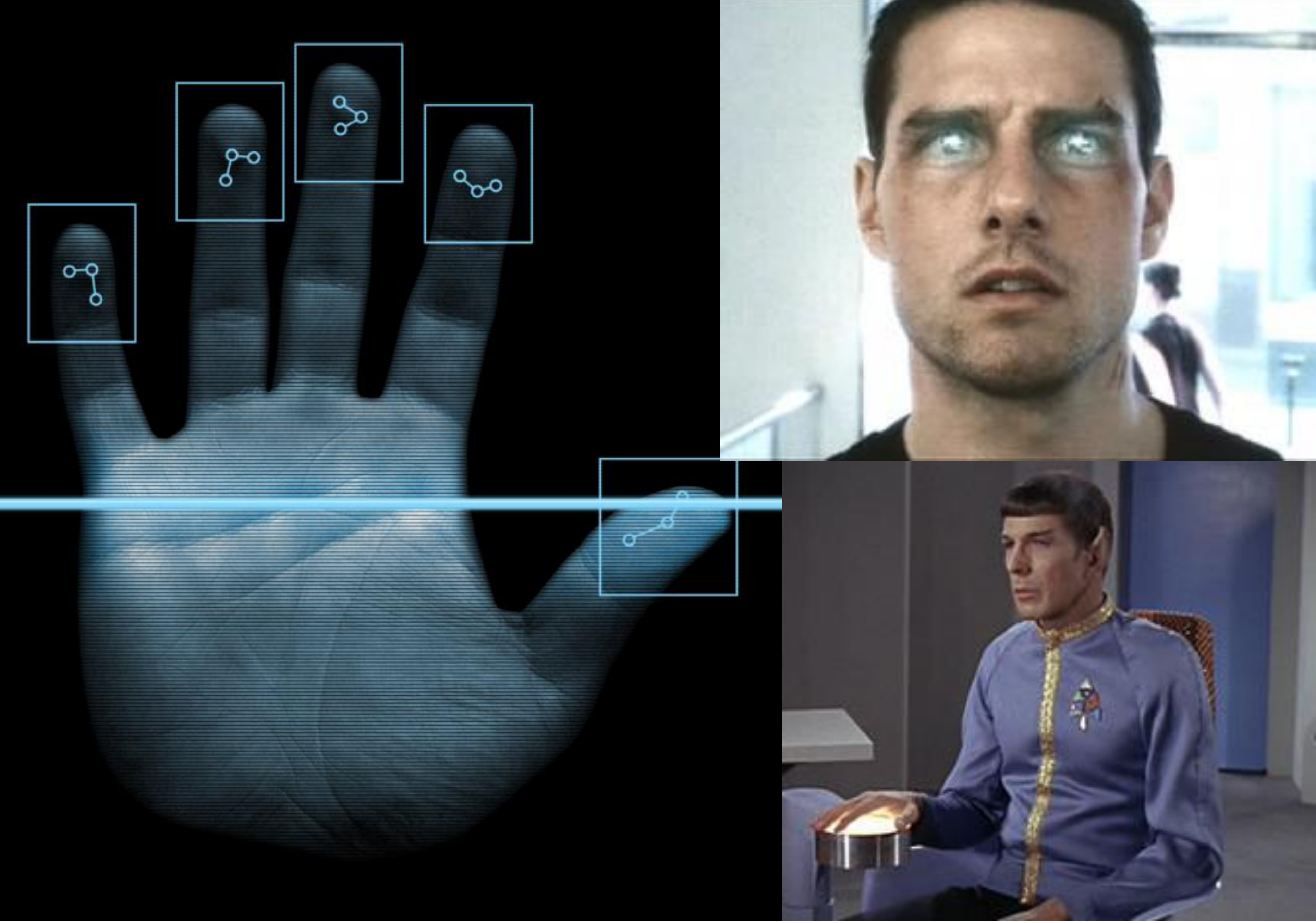
(my.username, my.p@ssw0rd!)
A8 B1 C0 88 C4 7C 67 1C BE F4 22 61 08 01 A9 31
Argon2 hash
A8 B1
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
Elliptic curve encryption
Log in to Example.com
Username
my.username
Password
Log in
A8 B1 C0 88 C4 7C 67 1C BE F4 22 61 08 01 A9 31
Argon2 hash
A8 B1
A9817QFbiJNqT+cycLc3w4xBbElbkjGaatG5GQk=
Elliptic curve encryption
A8 B1
A9817QFbiJNqT+cycLc3w4xBbElbkjGaatG5GQk=
Ayjm5BQ+J1eEjKVf5R0NZpzojwmAvnx/qTohNwM=
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
AjjuK8GhjGFLcN9kgFcuSw+nUWgpKQLMcutwWK4=
Aw0RF9Yj1gVhHdXglvlq6mjwvrEhry5BfbOiGtE=
AzL3zEnbxNjFuZz+1mbPpsd1AEFGqJijU3FVmiY=

https://security.googleblog.com/2019/02/protect-your-accounts-from-data.html

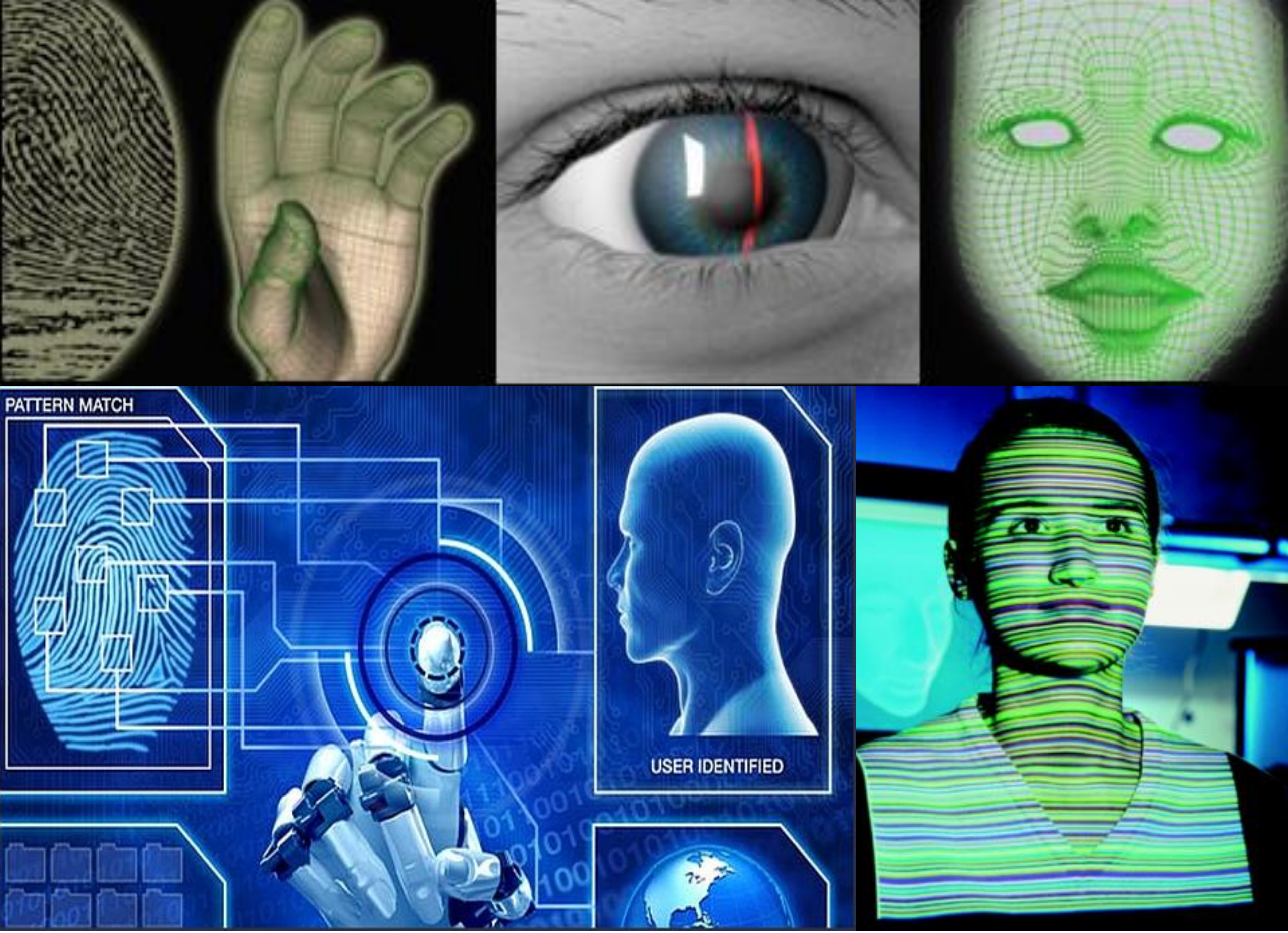
What about Biometrics?

nages on previous slide fair use from androidcentral.com and businessinsider.com. Photo above fair use from abcnews.com

nages fair use from wordpress.com and kaspersky.com, as well as Creative Commons from matsuyuki on Flickr



mages fair use from ccmcinc.com, filmjunk.com, and discovermagazine.com



Images fair use from fbi.gov, ifsecglobal.com, and siemens.com

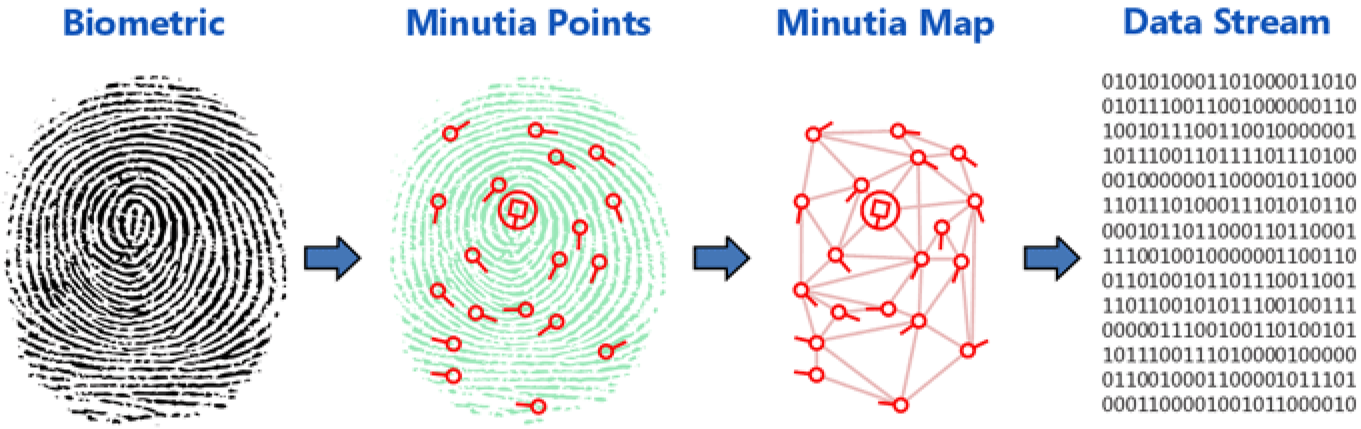
Biometrics

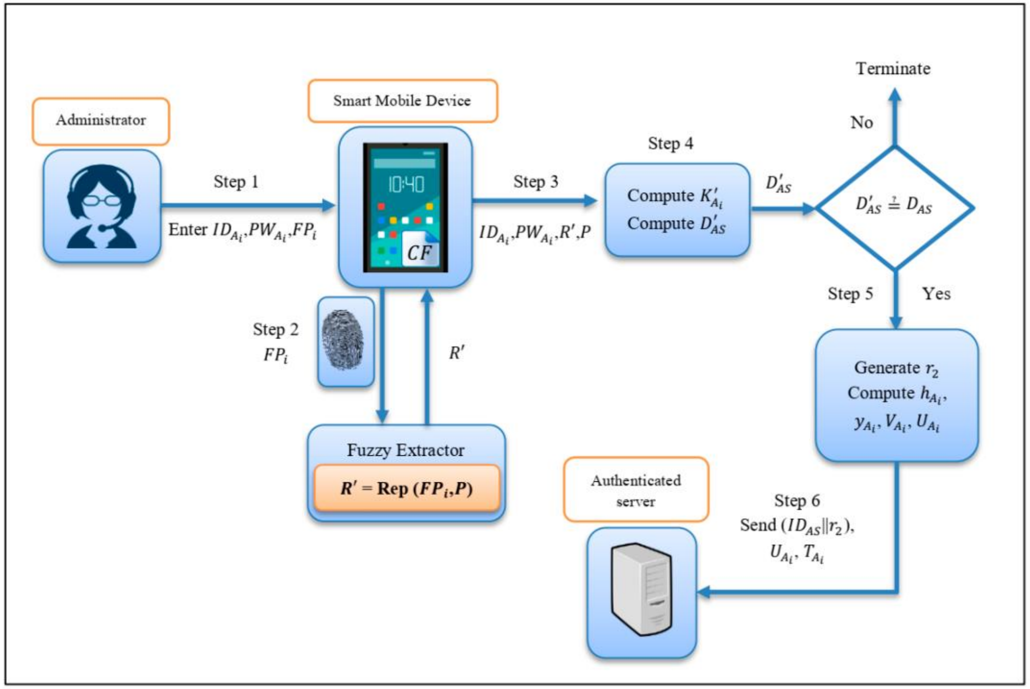
- Fingerprint
- Iris scans or retina scans
- Face recognition
- Finger/hand geometry
- Voice or speech recognition
- The way you type
- (Many others)

Practical Challenges for Biometrics

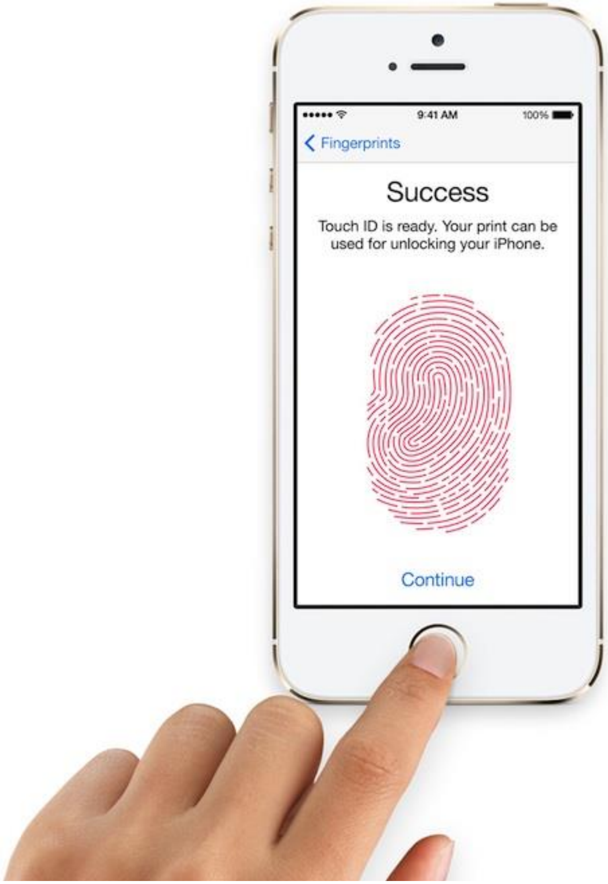
- Immutable (can’t be changed)
- Potentially sensitive data
- High equipment costs
- Sensitive to changes in the environment
- Biometrics can change over time

Storing Biometrics: Templates





iPhone
Touch ID



Success

Touch ID is ready. Your print can be used for unlocking your iPhone.

Android
Face Unlock

•Images fair use from androidcentral.com, creativebits.org, and businessinsider.com.

Smartphone Biometrics

- Purpose is to reduce the number of times a user must enter their password
- Falls back to the password
- Face recognition can be tricked by a photo
- Fingerprint recognition can be tricked by a gummy mold
- Users find fingerprint unlock convenient, but do not particularly like face unlock

Conclusions

- Authentication is really hard!
  - Hard for system administrators
  - Hard for users
- Unfortunately, authentication is necessary