ECE458/ECE750T27: Computer Security

Authentication

Dr. Kami Vaniea
Electrical and Computer Engineering
kami.vaniea@uwaterloo.ca

First, the news...

- First 5 minutes we talk about something interesting and recent
- You will not be tested on the news part of lecture
- You may use news as an example on tests
- Why do this?
    1. Some students show up late for various good reasons
    2. Reward students who show up on time
    3. Important to see real world examples

News...

Add a file to a GitHub comment

It gets auto uploaded and given a URL within the GitHub project

Send link that looks like legit repo link, but actually is malicious

Schneier on Security

Blog | Newsletter | Books | Essays | News | Talks | Academic | About M

Home > Blog

Using Legitimate GitHub URLs for Malware

Interesting social-engineering attack vector:

> McAfee released a report on a new LUA malware loader distributed through what appeared to be a legitimate Microsoft GitHub repository for the "C++ Library Manager for Windows, Linux, and MacOS," known as vcpkg.

The attacker is exploiting a property of GitHub: comments to a particular repo can contain files, and those files will be associated with the project in the URL.

What this means is that someone can upload malware and "attach" it to a legitimate and trusted project.

> As the file's URL contains the name of the repository the comment was created in, and as almost every software company uses GitHub, this flaw can allow threat actors to develop extraordinarily crafty and trustworthy lures.
>
> For example, a threat actor could upload a malware executable in NVIDIA's driver installer repo that pretends to be a new driver fixing issues in a popular game. Or a threat actor could upload a file in a comment to the Google Chromium source code and pretend it's a new test version of the web browser.
>
> These URLs would also appear to belong to the company's repositories, making them far more trustworthy.

University of Waterloo Territorial Acknowledgement

The University of Waterloo acknowledges that much of our work takes place on the traditional territory of the Neutral, Anishinaabeg and Haudenosaunee peoples.

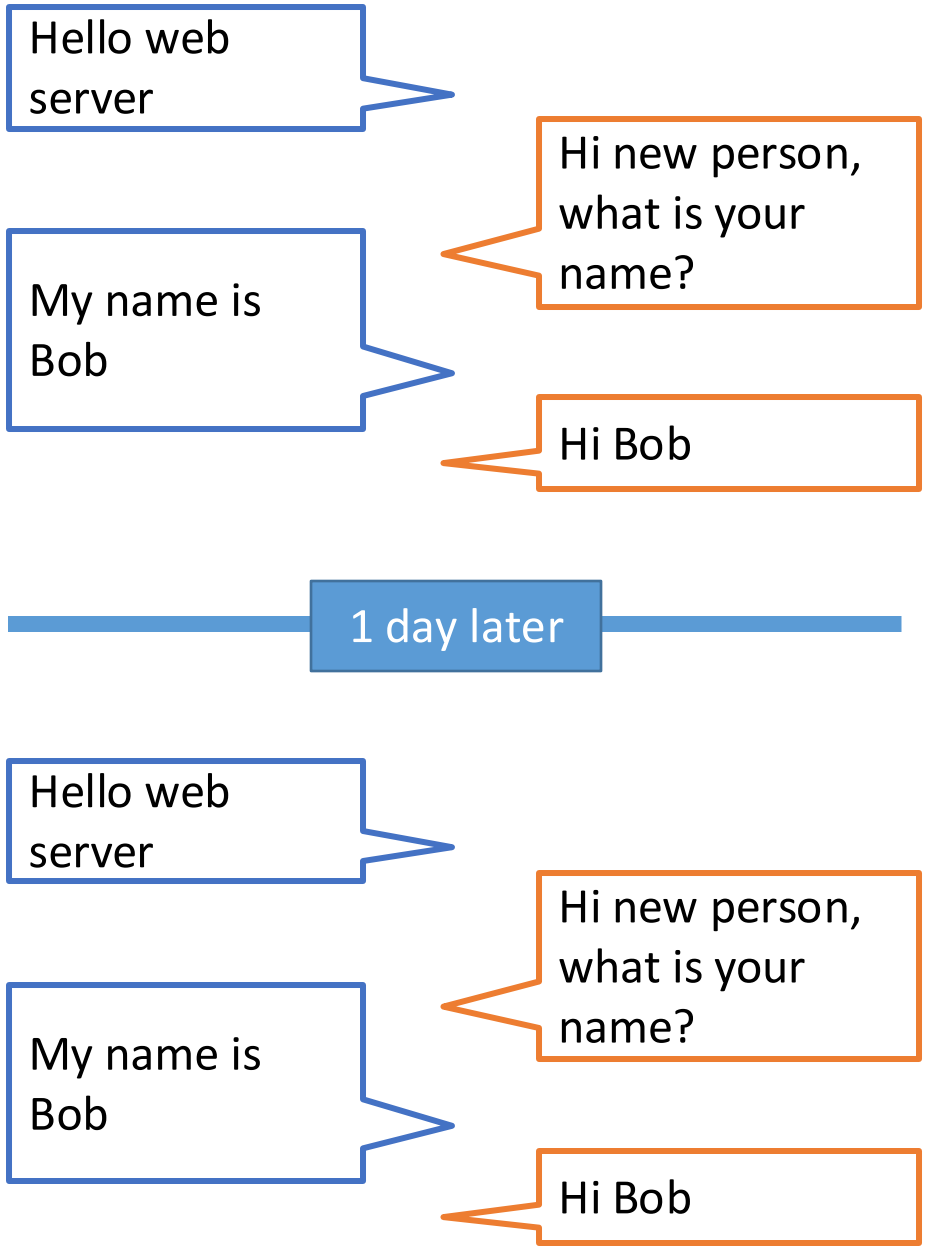
Our main campus is situated on the Haldimand Tract, the land granted to the Six Nations that includes six miles on each side of the Grand River.

Our active work toward reconciliation takes place across our campuses through research, learning, teaching, and community building, and is centralized within the Office of Indigenous Relations.

Map source:Adam Lewis, "Living on Stolen Land"
*Alternatives Journal*December 2015
uwaterloo.ca/engineering/about/territorial-acknowledgement

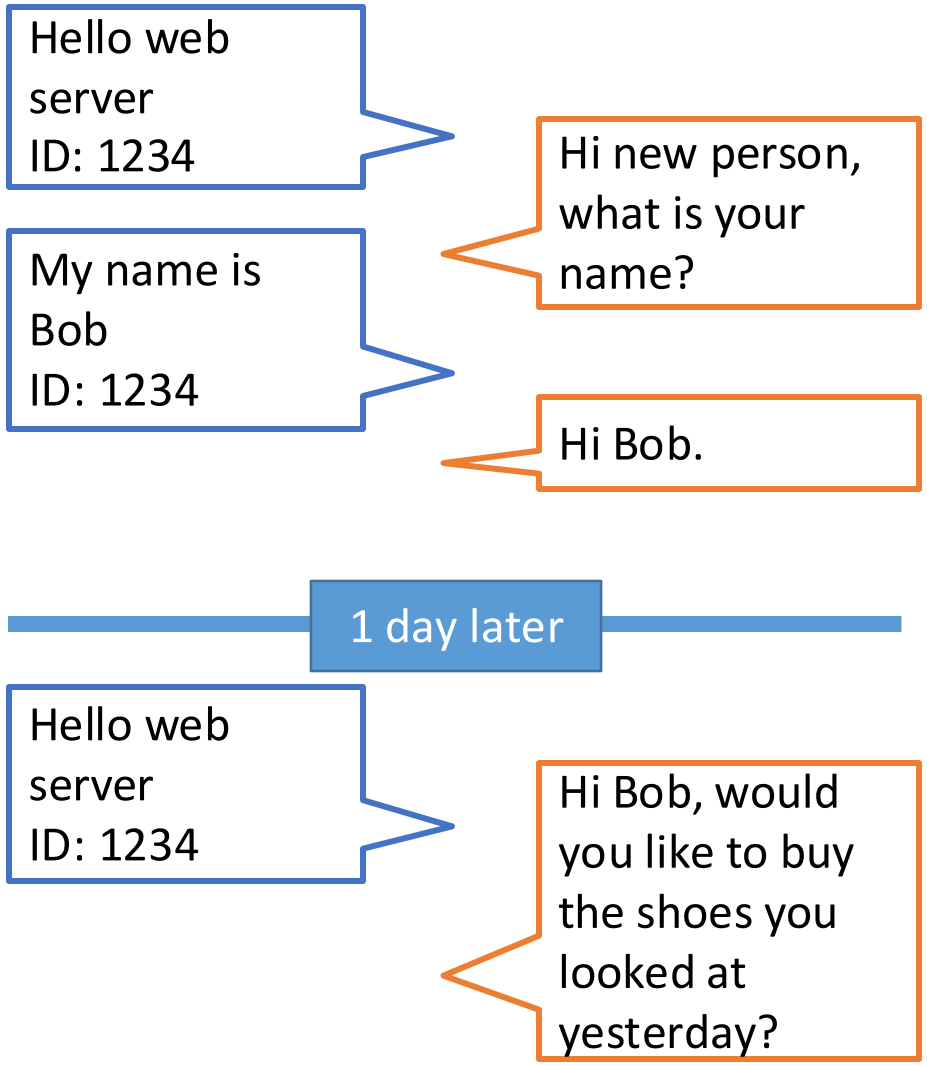
COOKIES

The year is 1994 and there is a problem… the internet has no ability to remember a person between page reloads.

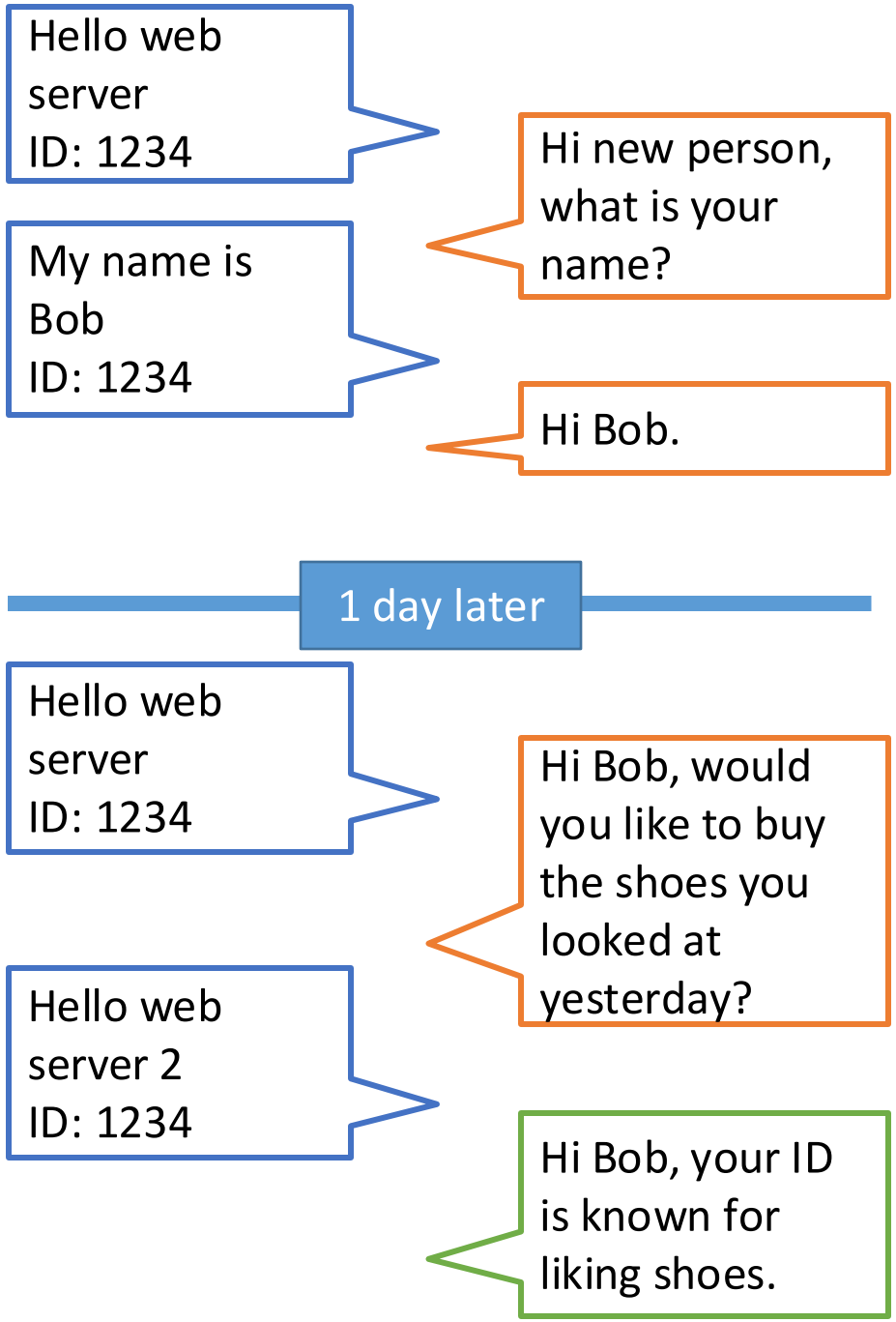


There is an obvious easy solution…

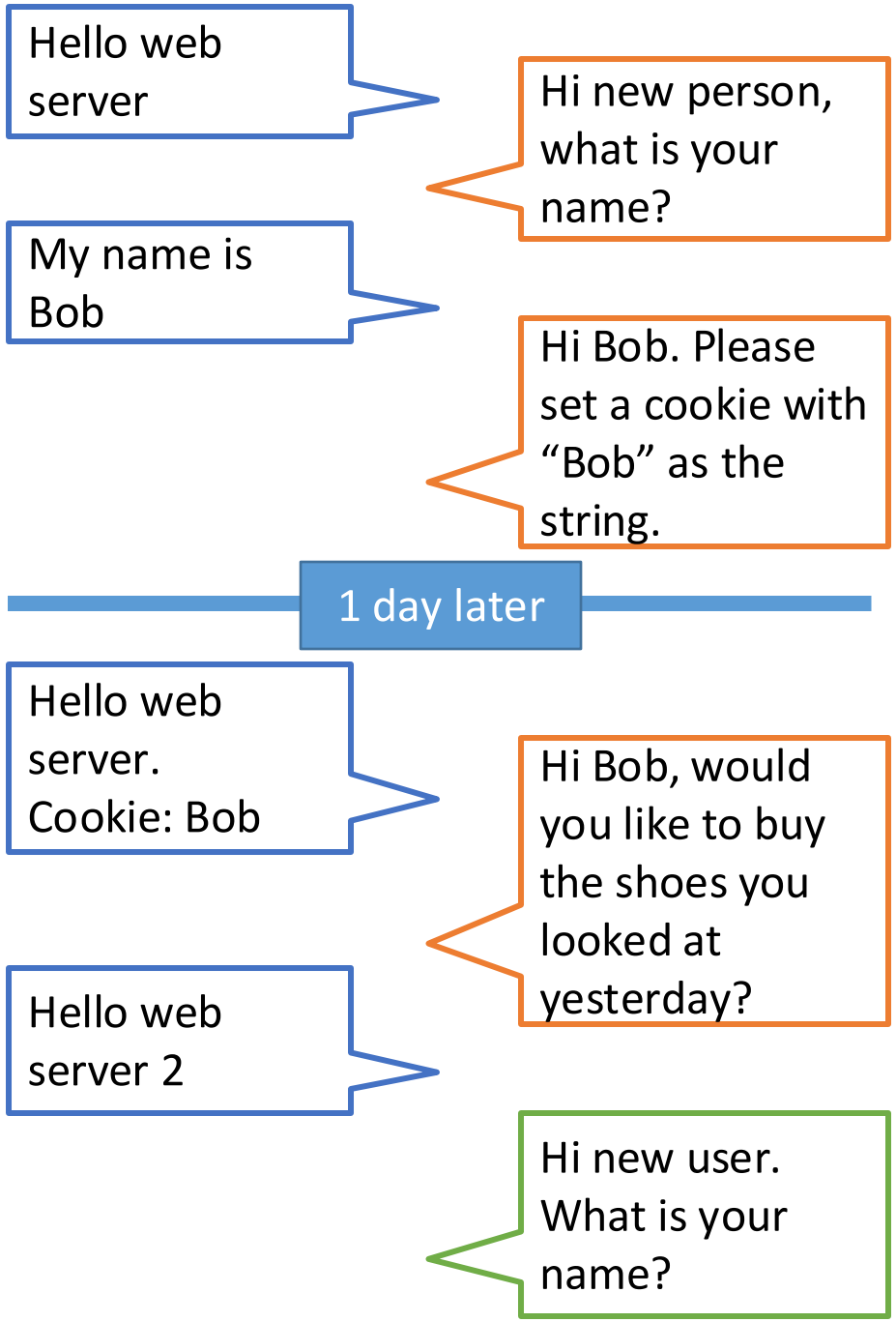
Give each browser a unique identifier that gets sent with every page request.



The problem with the obvious solution is privacy. Tracking would be possible with no visibility or control.



Instead Netscape implemented cookies. Small text strings the server could ask the browser to remember and give back to it later.



Phone apps work this way

Hello web server
ID: 1234

Hi new person, what is your name?

My name is Bob
ID: 1234

Hi Bob.

1 day later

Hello web server
ID: 1234

Hi Bob, would you like to buy the shoes you looked at yesterday?

Hello web server 2
ID: 1234

Hi Bob, your ID is known for liking shoes.

Browsers work this way

Hello web server

Hi new person, what is your name?

My name is Bob

Hi Bob. Please set a cookie with "Bob" as the string.

1 day later

Hello web server.
Cookie: Bob

Hi Bob, would you like to buy the shoes you looked at yesterday?

Hello web server 2

Hi new user. What is your name?

3rd party cookie reasoning

“Any company that had the ability to track users across a large section of the web would need to be a large publicly visible company.

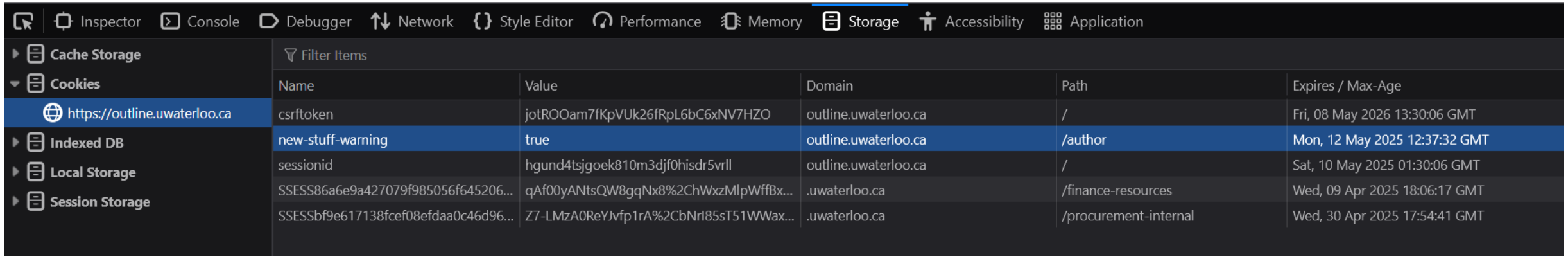
Cookies could be seen by users so a tracking company can't hide from the public.

In this way the public has a natural feedback mechanism to constrain those that would seek to track them.”

-- Lou Montulli

Cookies

- Small text strings associated with a variable name
- Allow web developers to store data on the user's computer
- Session cookies
  - Cookies with a short, or no, expiration date
  - In theory, used to track you only while you are interacting with the page

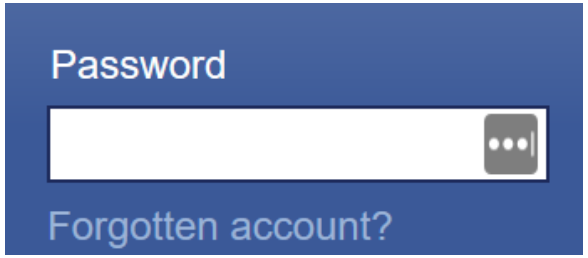


AUTHENTICATION

Security properties to ensure

Confidentiality	No improper information gathering
Integrity	Data has not been (maliciously) altered
Availability	Data/services can be accessed as desired
Accountability	Actions are traceable to those responsible
Authentication	User or data origin accurately identifiable

Authentication factors (for humans)



- Something you **know**
  - Password, mother's maiden name, your address
- Something you **have**
  - Student ID card, credit card chip, RSA key fob, Yubikey
- Something you **are**
  - Fingerprints, voice tones, iris, typing patterns

Where do various operating systems store password hashes

Windows	Password hashes are stored in the SAM file and locked by the operating system on boot. Attackers would need to read memory to find the hashes. Challenging to copy all hashes.
Linux	Password hashes are stored in /etc/shadow and only accessible by root or by using sudo. An attacker with sudo-level access can copy the whole file
Mac	Used to be /etc/shadow, but moved into a plist at /var/db/dslocal/nodes/Default/users/<username>.plist (according to Stack Exchange)
Android	/data/system/password.key for the hash and a SQLite database for the salt

All of the above operating systems hash the password, though with varying levels of hash function. They also all require root-level access to view the hashes.

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

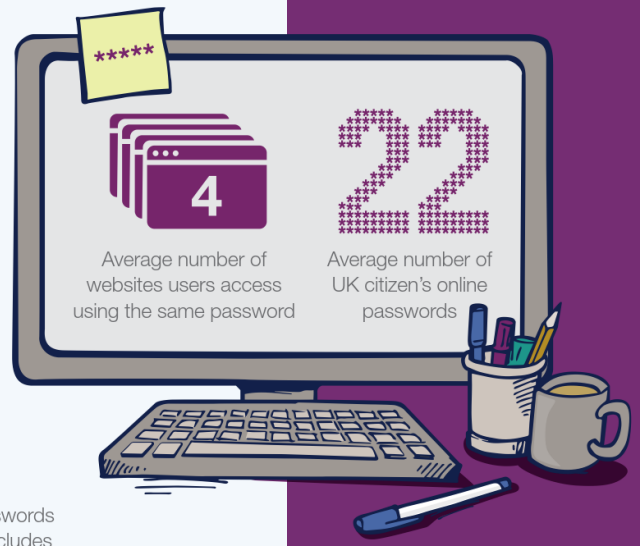
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

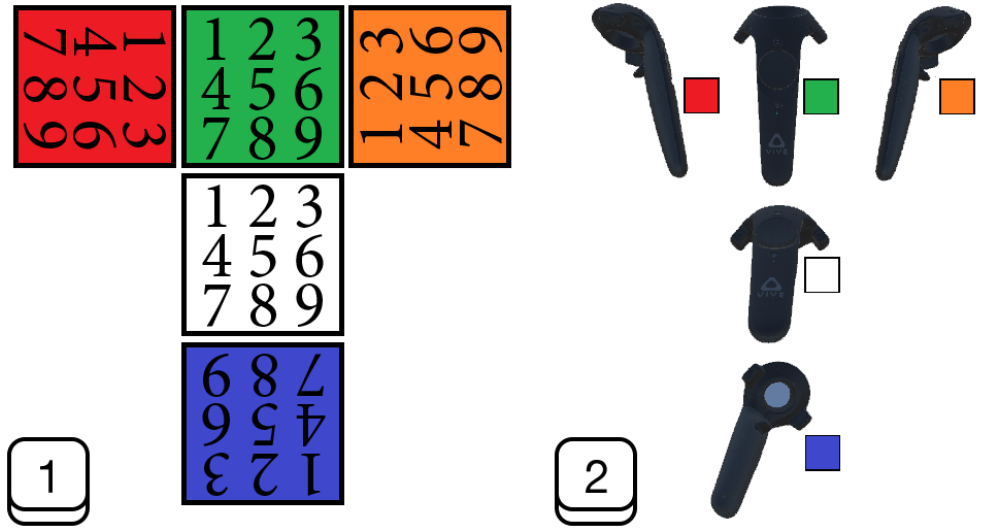
For more information go to www.ncsc.gov.uk @ncsc

Shoulder Surfing

Shoulder surfing: watching someone log in and memorizing the password

RubikAuth: Virtual Reality Authentication

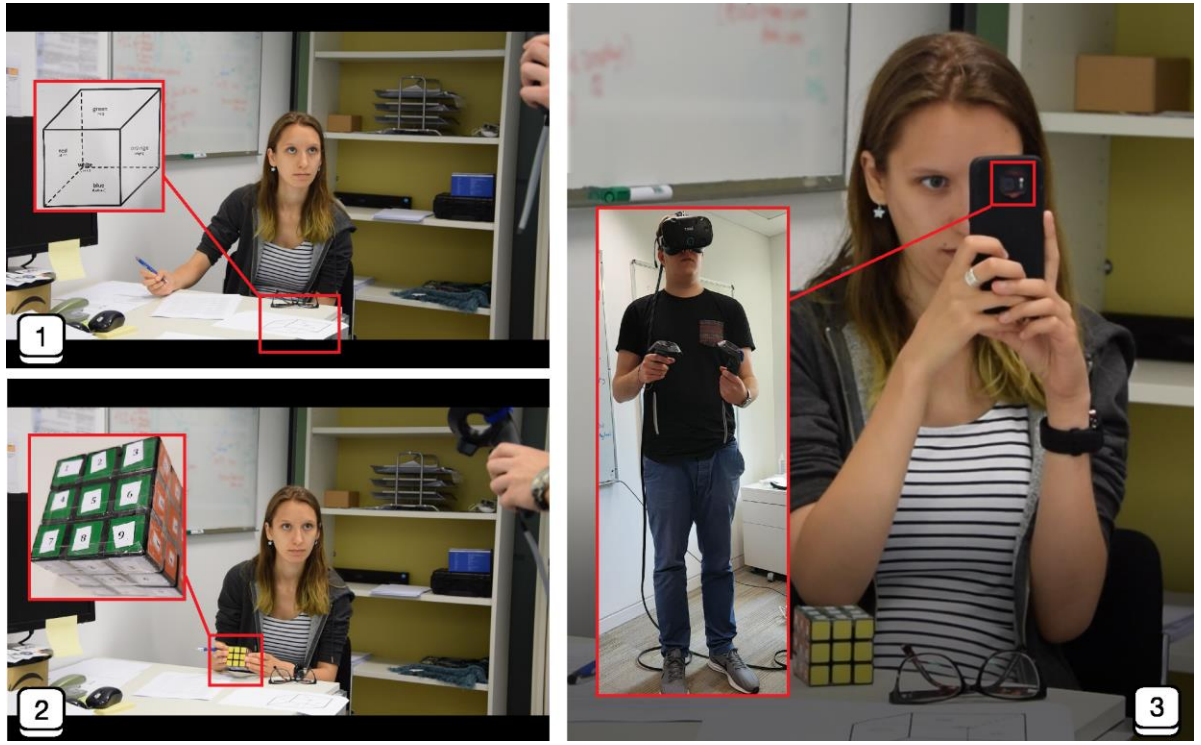
- User while in VR can enter their password by indicating a sequence of number/side combinations
  - 1G, 5R, 2Y, 2G
- VR users are particularly vulnerable to shoulder surfing because they cannot see surroundings



Florian Mathis, John H. Williamson, Kami Vaniea, Mohamed Khamis (2020). RubikAuth: Fast and Secure Authentication in Virtual Reality. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

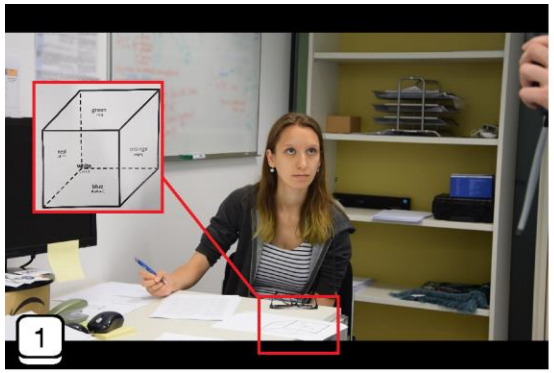
RubikAuth: Virtual Reality Authentication

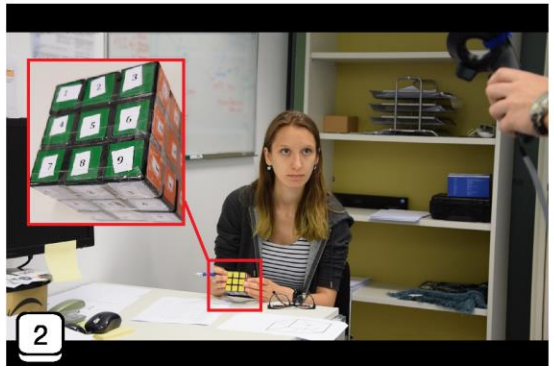
- "Attacker" could:
  1. Take notes on paper
  2. Take notes on a physical cube
  3. Video the entry

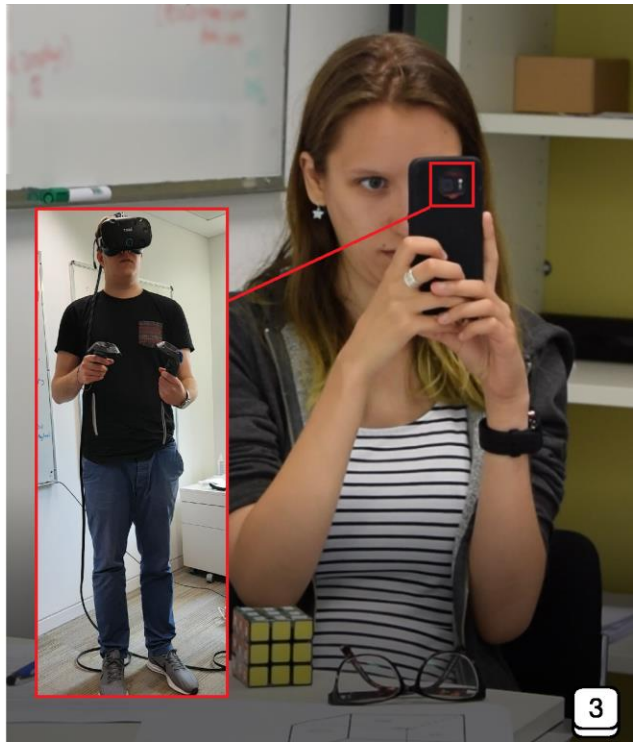


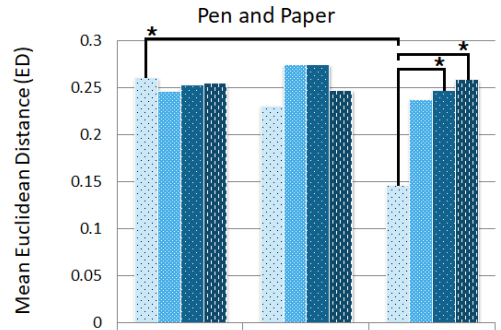
Florian Mathis, John H. Williamson, Kami Vaniea, Mohamed Khamis (2020). RubikAuth: Fast and Secure Authentication in Virtual Reality. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

RubikAuth: Virtual Reality Authentication

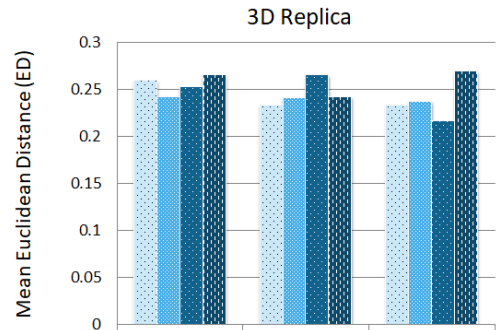






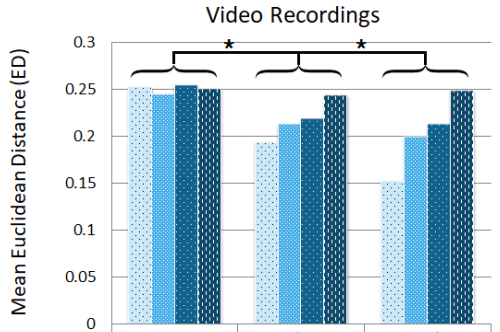


	Eye Gaze	Head Pose	Tapping
0-switches	0.261	0.231	0.147
1-switch	0.247	0.275	0.238
2-switches	0.253	0.275	0.248
3-switches	0.255	0.248	0.259



	Eye Gaze	Head Pose	Tapping
0-switches	0.259	0.233	0.233
1-switch	0.242	0.241	0.237
2-switches	0.252	0.265	0.216
3-switches	0.265	0.242	0.269

- Cube rotations matter
- "Enter" method matters
- Recording method matters some



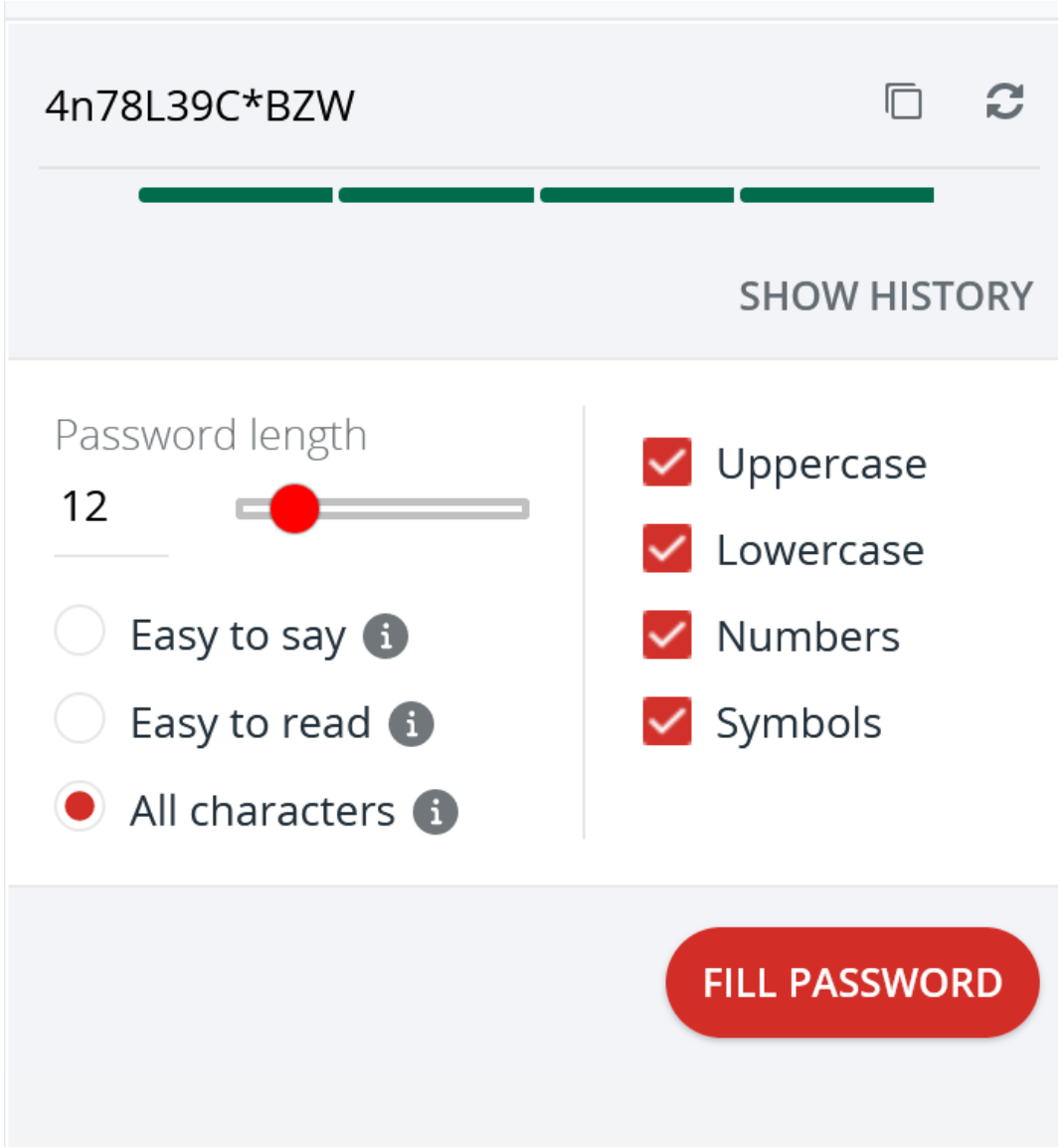
	Eye Gaze	Head Pose	Tapping
0-switches	0.252	0.194	0.153
1-switch	0.245	0.213	0.2
2-switches	0.254	0.219	0.213
3-switches	0.251	0.244	0.249

Florian Mathis, John H. Williamson, Kami Vaniea, Mohamed Khamis (2020). RubikAuth: Fast and Secure Authentication in Virtual Reality. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.

Password Managers

What does a password manager do?

- Generate passwords for you that are truly random (high entropy)
- Remember those passwords for you (no forgetting)
- Automatically insert the password into the website it goes to (computers are not fooled by sneaky-looking URLs)
- Store the passwords somewhere outside your computer (safe from coffee spillage)
- Give anyone with the master password access to all your passwords (um…. Bad?)
- Allow you to have a unique password for every website (why is this important?)



Password Meters

- Graphical indicators of password strength
- Intended to help people pick good passwords with high entropy
- What type of meter works the best?

How Does Your Password Measure Up?
The Effect of Strength Meters on Password Creation

Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass,
Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas,
Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor
Carnegie Mellon University
{*bur, pgage, sarangak, jlee, mmaass, mmazurek, tpassaro,*
rshay, tvidas, lbauer, nicolasc, lorrie}*@cmu.edu*

Abstract

To help users create stronger text-based passwords, many web sites have deployed password meters that provide visual feedback on password strength. Although these meters are in wide use, their effects on the security and usability of passwords have not been well studied.

We present a 2,931-subject study of password creation in the presence of 14 password meters. We found that meters with a variety of visual appearances led users to create longer passwords. However, significant increases in resistance to a password-cracking algorithm were only achieved using meters that scored passwords stringently.

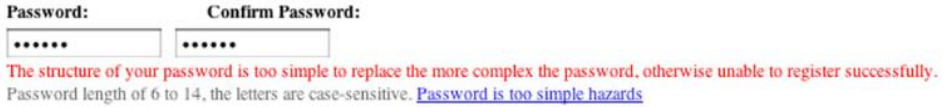
or write them down [28]. Password-composition policies, sets of requirements that every password on a system must meet, can also make passwords more difficult to guess [6, 38]. However, strict policies can lead to user frustration [29], and users may fulfill requirements in ways that are simple and predictable [6].

Another measure for encouraging users to create stronger passwords is the use of password meters. A password meter is a visual representation of password strength, often presented as a colored bar on screen. Password meters employ suggestions to assist users in creating stronger passwords. Many popular websites, from Google to Twitter, employ password meters.

Just colored words

Facebook

Baidu



Green bars / Checkmark-x

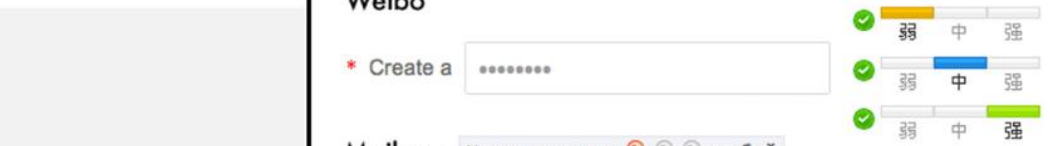
Twitter

Checklists

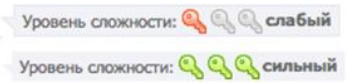
Apple

Segmented bars

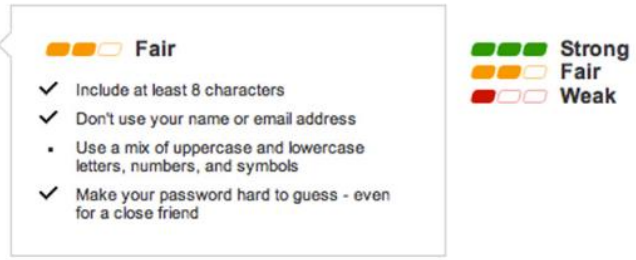
Weibo



Mail.ru

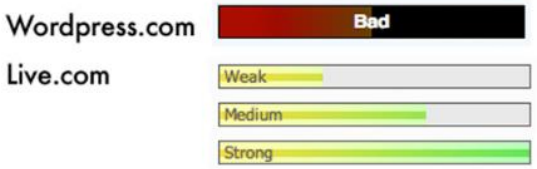


Paypal



Yahoo.jp and Yahoo

Gradient bars

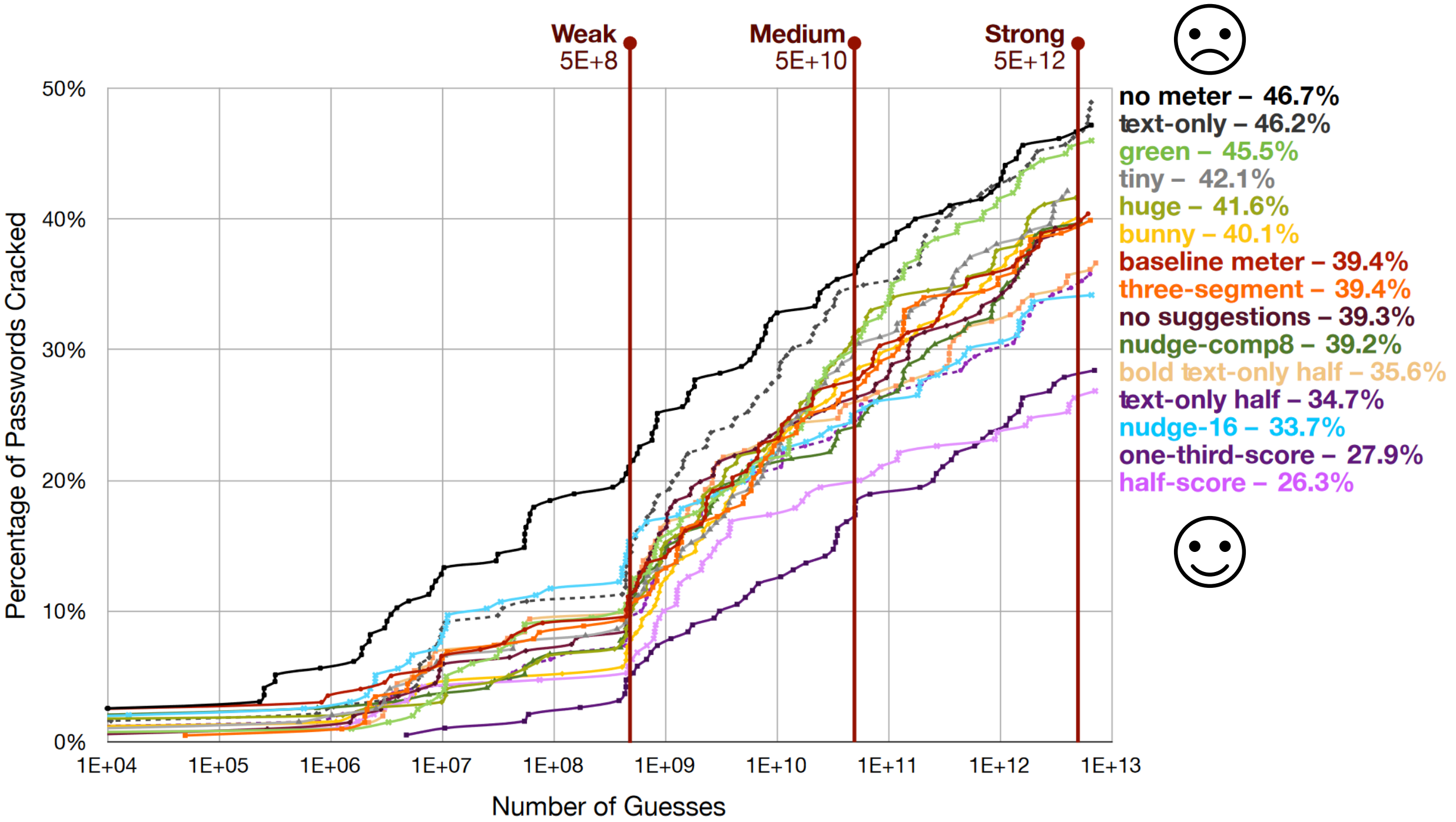


Color changing bars

Mediafire

Blogger

Google


Weak
5E+8
Medium
5E+10
Strong
5E+12
50%
40%
30%
20%
10%
0%
Percentage of Passwords Cracked
1E+04
1E+05
1E+06
1E+07
1E+08
1E+09
1E+10
1E+11
1E+12
1E+13
Number of Guesses
no meter – 46.7%
text-only – 46.2%
green – 45.5%
tiny – 42.1%
huge – 41.6%
bunny – 40.1%
baseline meter – 39.4%
three-segment – 39.4%
no suggestions – 39.3%
nudge-comp8 – 39.2%
bold text-only half – 35.6%
text-only half – 34.7%
nudge-16 – 33.7%
one-third-score – 27.9%
half-score – 26.3%

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How passwords are cracked...

Interception

Passwords can be intercepted as they are transmitted over a network.

Brute Force

Automated guessing of billions of passwords until the correct one is found.

Searching

IT infrastructure can be searched for electronically stored password information.

Stealing Passwords

Insecurely stored passwords can be stolen – this includes handwritten passwords hidden close to a device.

Manual Guessing

Personal information, such as name and date of birth can be used to guess common passwords.

Shoulder Surfing

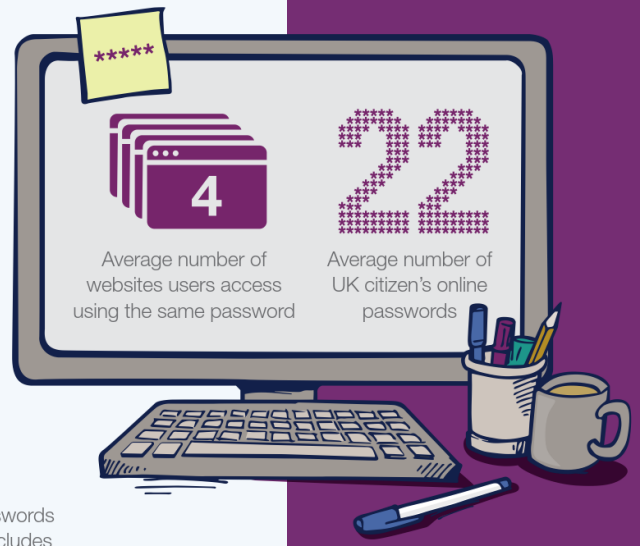
Observing someone typing their password.

Social Engineering

Attackers use social engineering techniques to trick people into revealing passwords.

Key Logging

An installed keylogger intercepts passwords as they are typed.



...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

For more information go to www.ncsc.gov.uk @ncsc

National Cyber Security Centre

Password security

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

How pas

Interception

Passwords can be intercepted as they a transmitted over a ne

Searching

IT infrastructure can b searched for electron stored password info

Manual Gues

Personal information, as name and date of can be used to guess common passwords.

Social Engineering

Attackers use social engineering techniqu trick people into revea passwords.

Help users cope with ‘password overload’

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

Attackers use a variety of techniques to discover passwords, including using powerful tools freely available on the internet. The following advice makes password security easier for your users – improving your system security as a result.

...and how to improve your system security

Help users cope with 'password overload'

- Only use passwords where they are really needed.
- Use technical solutions to reduce the burden on users.
- Allow users to securely record and store their passwords.
- Only ask users to change their passwords on indication of suspicion of compromise.
- Allow users to reset password easily, quickly and cheaply.

Help users generate appropriate passwords

- Put technical defences in place so that simpler passwords can be used.
- Steer users away from predictable passwords – and ban the most common.
- Encourage users to never re-use passwords between work and home.
- Train staff to help them avoid creating passwords that are easy to guess.
- Be aware of the limitations of password strength meters.

Blacklist the most common password choices

Monitor failed login attempts… train users to report suspicious activity

Prioritise administrator and remote user accounts

Don't store passwords in plain text format.

**** UPDATE

Change all default vendor supplied passwords before devices or software are deployed

Use account lockout, throttling or monitoring to help prevent brute force attacks

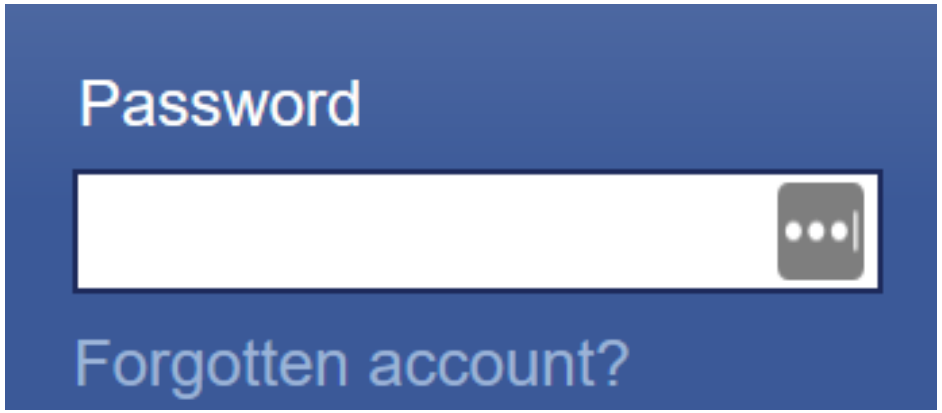
For more information go to **www.ncsc.gov.uk** **@ncsc**

Graphical Passwords

Recognition vs Recall

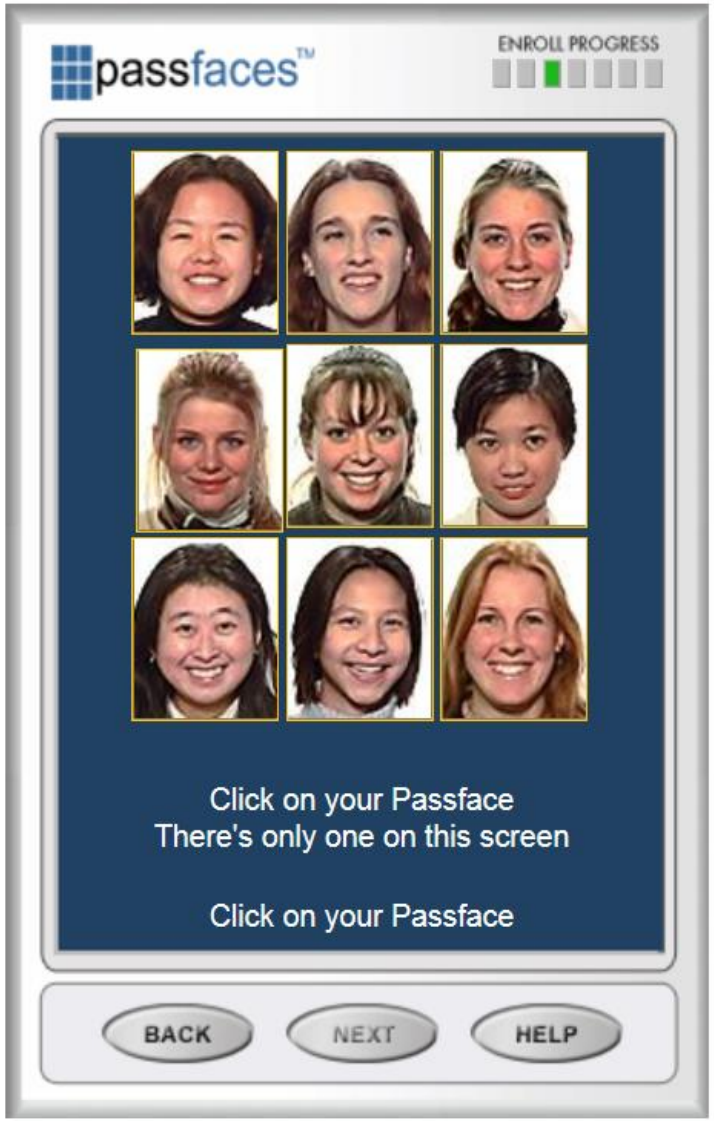
- Recognition – You are shown a set of things and asked to recognize the correct thing

- Recall – You must state the correct thing from memory



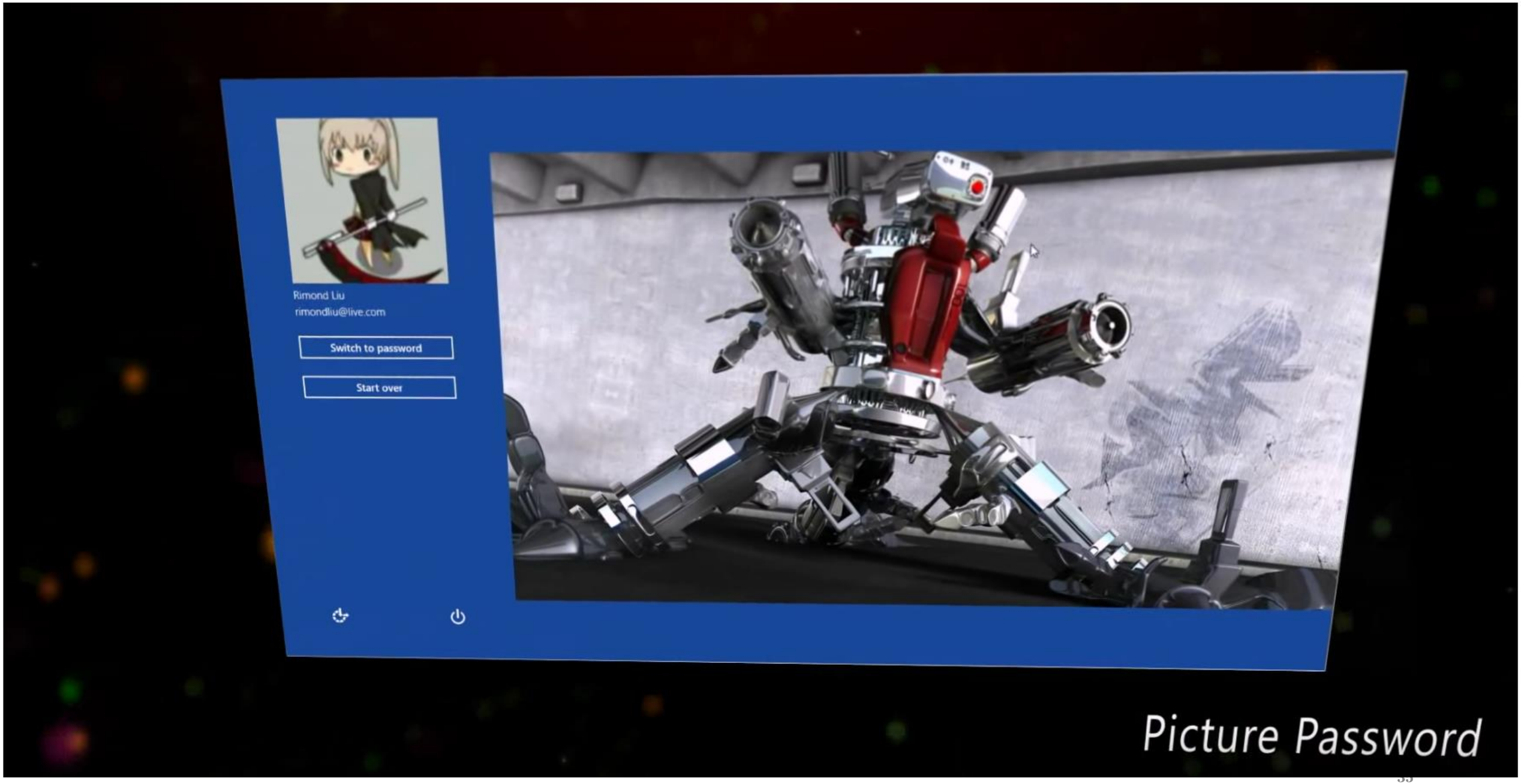
PassFaces

- Humans are better at recognizing things than they are at recalling information.
- High feature information, like faces, are easier to recognize
- Idea: Use high feature information as the pin, so humans can recognize their password
- Problem: People select faces that mean something to them. If you know basic characteristics about someone you can easily guess their PassFace.



PassFaces

- Password length = 4
- Each password selected from a set of 9 faces like what is shown on the right
- Theoretical password space = 6561
- What is the best way to break someone's password?
  - If the person is a white male, you can guess the correct password in about two guesses by selecting all the pretty white females.


Rimond Liu
rimondliu@live.com
Switch to password
Start over
Picture Password

Graphical passwords

Pros

- Easier to recall
- Theoretically a large password space
- Work well with touch screens

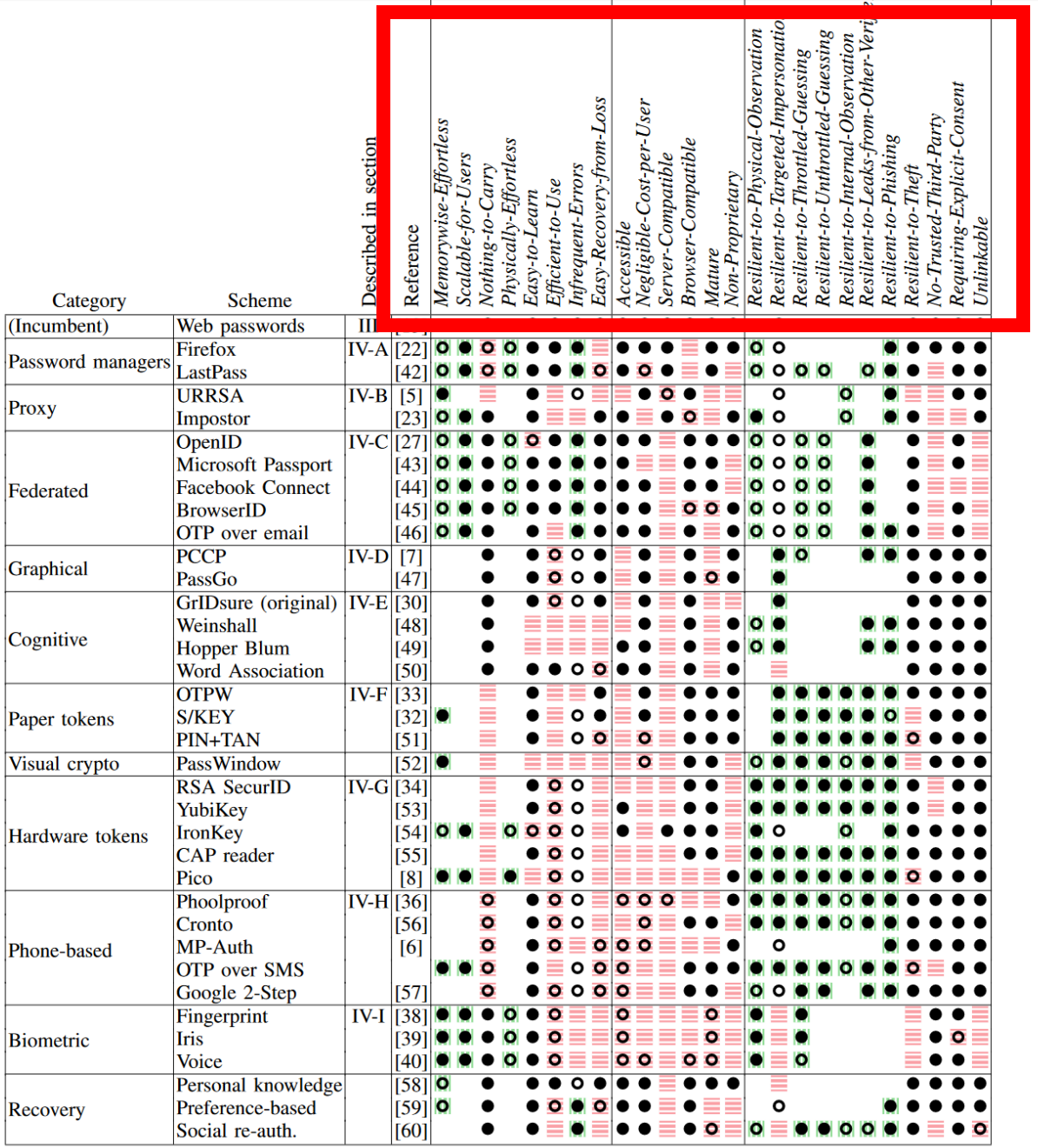
Cons

- Easier to guess
- Practically much smaller password space than theoretical
- Accessibility issues

Why do we still use passwords?

Bonneau et al.

Many ways exist to authenticate a person over just the web.



Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	*Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonatio*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Veri*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	II	[22]	○	●	○	○	●	●	●	▤	●	●	●	▤	●	●	○	○					●	●	●	●	●
Password managers	Firefox	IV-A	[42]	○	●	○	○	●	●	●	○	●	○	●	▤	●	▤	○	○	○	○		○	●	●	▤	●	●
Proxy	LastPass		[5]	●	▤	▤		●	▤	○	▤	▤	●	○	●	▤	▤		○			○		●	▤	▤	▤	●
	URRSA	IV-B	[23]	○	●	●		●	▤	▤	●	●	▤	●	○	▤	▤	●	○			○		●	●	▤	▤	●
Federated	Impostor		[27]	○	●	●	○	○	●	●	●	●	●	▤	●	●	▤	○	○	○	○		●		●	▤	●	▤
	OpenID	IV-C	[43]	○	●	●	○	●	●	●	●	●	▤	▤	●	●	▤	○	○	○	○		●		●	▤	●	▤
	Microsoft Passport		[44]	○	●	●	○	●	●	●	●	●	●	▤	●	●	▤	○	○	○	○		●		●	▤	▤	▤
	Facebook Connect		[45]	○	●	●	○	●	●	●	●	●	●	▤	○	○	●	○	○	○	○		●		●	▤	●	▤
	BrowserID		[46]	○	●	●		●	▤	●	●	●	●	▤	●	▤	●	○	○	○	○		●	●	●	▤	●	▤
Graphical	OTP over email		[7]			●		●	○	○	●	▤	●	▤	●	▤	●		●	○			●	●	●	●	●	●
	PCCP	IV-D	[47]			●		●	○	○	●	▤	●	▤	○	●	●		●						●	●	●	●
Cognitive	PassGo		[30]			●		●	○	○	●	▤	●	▤	●	▤	▤		●						●	●	●	●
	GrIDsure (original)	IV-E	[48]			●		▤	▤	▤	▤	▤	●	▤	●	▤	●	○	●			●	●	●	●	●	●	●
	Weinshall		[49]			●		▤	▤	▤	▤	●	●	▤	●	▤	●	○	●			●	●	●	●	●	●	●
	Hopper Blum		[50]			●		●	●	○	○	●	●	▤	●	▤	●		▤						●	●	●	●
Paper tokens	Word Association		[33]			▤		●	▤	▤	●	▤	●	▤	●	●	●		●	●	●	●	●	●	●	●	●	●
	OTPW	IV-F	[32]	●		▤		●	▤	○	●	▤	●	▤	●	●	●		●	●	●	●	●	○	▤	●	●	●
	S/KEY		[51]			▤		●	▤	○	○	▤	○	▤	●	●	●		●	●	●	●	●	●	○	▤	●	●	●
Visual crypto	PIN+TAN		[52]	●		▤		▤	▤	▤	▤	▤	○	▤	●	●	▤	○	●	●	●	○	●	●	▤	▤	●	●	●
Hardware tokens	PassWindow		[34]			▤		●	○	○	▤	▤	▤	▤	●	●	▤	●	●	●	●	●	●	●	●	▤	●	●
	RSA SecurID	IV-G	[53]			▤		●	○	○	▤	●	▤	▤	●	●	▤	●	●	●	●	●	●	●	●	▤	●	●
	YubiKey		[54]	○	●	▤	○	○	○	○	▤	●	▤	●	●	●	▤	●	○		○		●	●	●	●	●	●
	IronKey		[55]			▤		●	○	○	▤	▤	▤	▤	●	●	▤	●	●	●	●	●	●	●	●	●	●	●
	CAP reader		[8]	●	●	▤	●	▤	○	○	▤	▤	▤	▤	▤	▤	●	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Pico		[36]			○		●	○	○	▤	○	○	○	▤	▤	●	●	●	●	●	○	●	●	●	●	●	●
	Phoolproof	IV-H	[56]			○		●	○	○	▤	▤	○	▤	●	●	▤	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[6]			○		●	○	▤	○	○	○	▤	▤	▤	●		○					●	●	●	●	●
	MP-Auth			●	●	○		●	▤	○	○	○	▤	▤	●	●	●	●	●	●	●	○	●	●	○	▤	●	●
	OTP over SMS		[57]			○		●	○	○	○	○	▤	▤	●	●	▤	○	○	●	●		●	●	●	●	●	●
	Google 2-Step																											
Biometric	Fingerprint	IV-I	[38]	●	●	●	○	●	○	▤	▤	○	▤	▤	▤	○	▤	●	▤	●				▤	●	●	▤	
	Iris		[39]	●	●	●	○	●	○	▤	▤	○	▤	▤	▤	○	▤	●	▤	●				▤	●	○	▤	
	Voice		[40]	●	●	●	○	●	○	▤	▤	○	○	▤	▤	○	▤	●	▤	○				▤	●	●	▤	
Recovery	Personal knowledge		[58]	○		●		●	●	○	●	●	●	▤	●	●	●		▤						●	●	●	●
	Preference-based		[59]	○		●		●	○	●	○	●	●	▤	●	▤	▤		○					●	●	●	●	●
	Social re-auth.		[60]			●		●	▤	●	▤	●	●	▤	●	○	▤	○	▤	●	●	○	○	●	●	▤	●	○

●= offers the benefit; ○= almost offers the benefit; *no circle* = does not offer the benefit.
▥= better than passwords; ▤= worse than passwords; *no background pattern* = no change.
We group related schemes into categories. For space reasons, in the present paper we describe at most one representative scheme per category; the companion technical report [1] discusses all schemes listed.

Bonneau, Joseph, et al. "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes." *2012 IEEE Symposium on Security and Privacy*. IEEE, 2012.

A good authentication method:

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Passwords

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Graphical Passwords

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

One time password over SMS

User friendly

- Memory effortless
- Scalable for users
- Nothing to carry
- Physically effortless
- Easy to learn
- Efficient to use
- Infrequent errors
- Easy to recover from loss

Reasonable to implement

- Accessible
- Negligible cost per user
- Server compatible
- Browser compatible
- Mature
- Non-proprietary

Protects against attacks

- Resilient to:
  - Physical observation
  - Targeted impersonation
  - Throttled guessing
  - Unthrottled guessing
  - Internal observation
  - Leaks from other verifiers
  - Phishing
  - Theft
- No trusted third party
- Requiring explicit consent
- Unlinkable

Questions about Authentication?