Lecture Outline

- Review of Diffie-Hellman key exchange
- Looking at Authentication from a number of perspectives
  - Today: authenticating users, services

Agreeing on Secret Keys *Without Prior Arrangement*

Diffie-Hellman Key Exchange

- While we have powerful symmetric-key technology, it requires Alice & Bob to agree on a secret key *ahead of time*
- What if instead they can somehow generate such a key *when needed*?
- Seems impossible in the presence of Eve observing all of their communication …
  - How can they exchange a key without her learning it?
- But: actually is possible using public-key technology
  - Requires that Alice & Bob **know** that their messages will reach one another without any meddling
  - So works for Eve-the-eavesdropper, but not Mallory-the-MITM
  - Protocol: *Diffie-Hellman Key Exchange* (DHE)

Diffie-Hellman Key Exchange

p, g

Eve

p, g

Alice

p, g

Bob

1. Everyone agrees in advance on a well-known (large) prime **p** and a corresponding **g**: $1 < g < p-1$

Diffie-Hellman Key Exchange

p, g

a? b?

Eve

p, g

a

Alice

p, g

b

Bob

2. Alice picks random secret '**a**': 1 < a < p-1

3. Bob picks random secret '**b**': 1 < b < p-1

Diffie-Hellman Key Exchange

p, g

A

B

a? b?

Eve

p, g

a

Alice

p, g

b

Bob

$A = g^a \bmod p$

$g^b \bmod p = B$

4. Alice sends $A = g^a \bmod p$ to Bob
5. Bob sends $B = g^b \bmod p$ to Alice

Diffie-Hellman Key Exchange

p, g

A

B

a? b?

Eve

p, g

a

K

Alice

p, g

b

K

Bob

$A = g^a \bmod p$

B

A

$g^b \bmod p = B$

6. Alice knows {a, A, B}, computes
   $K = B^a \bmod p = (g^b)^a = g^{ba} \bmod p$
7. Bob knows {b, A, B}, computes
   $K = A^b \bmod p = (g^a)^b = g^{ab} \bmod p$
8. K is now the shared secret key.

Diffie-Hellman Key Exchange

p, g

A

B

a? b?

K?

Eve

p, g

a

K

Alice

p, g

b

K

Bob

$A = g^a \bmod p$

B

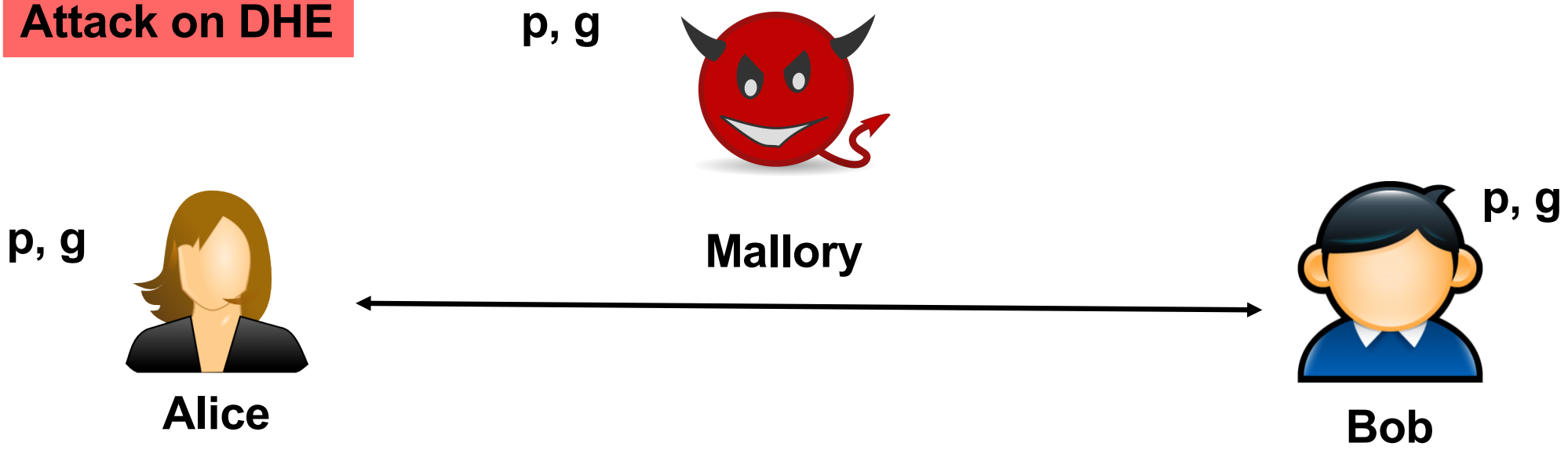
A

$g^b \bmod p = B$

While Eve knows {p, g, $g^a \bmod p$, $g^b \bmod p$}, believed to be ***computationally infeasible*** for her to then deduce K = $g^{ab} \bmod p$.

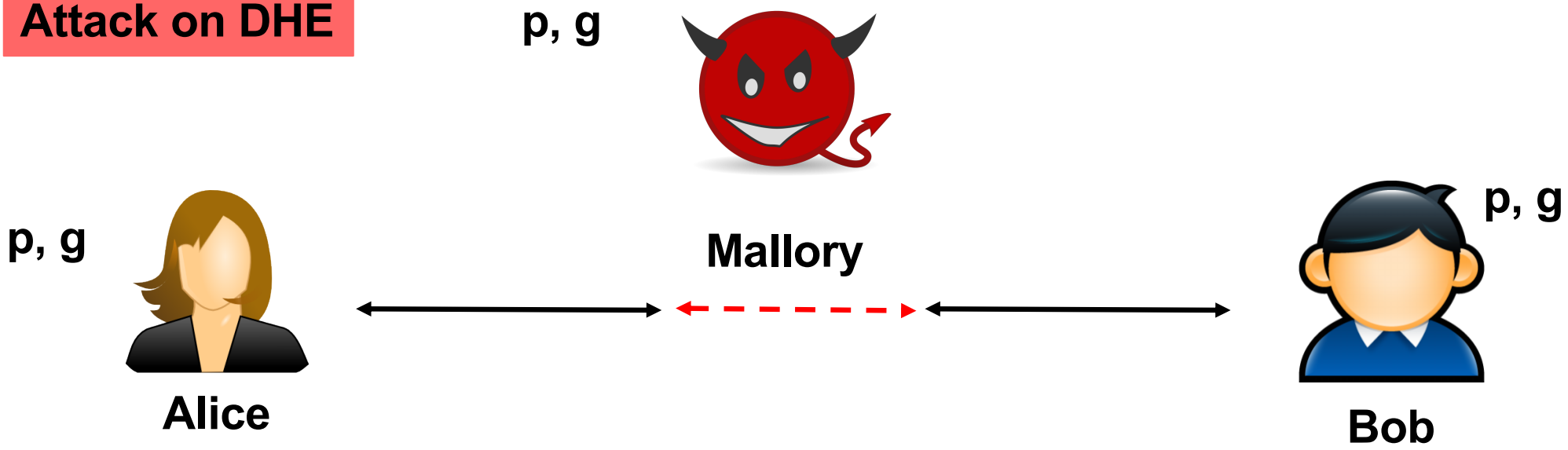
She can easily construct $A \cdot B = g^a \cdot g^b \bmod p = g^{a+b} \bmod p$.
But computing g^{ab} requires ability to take *discrete logarithms* mod p.

Attack on DHE



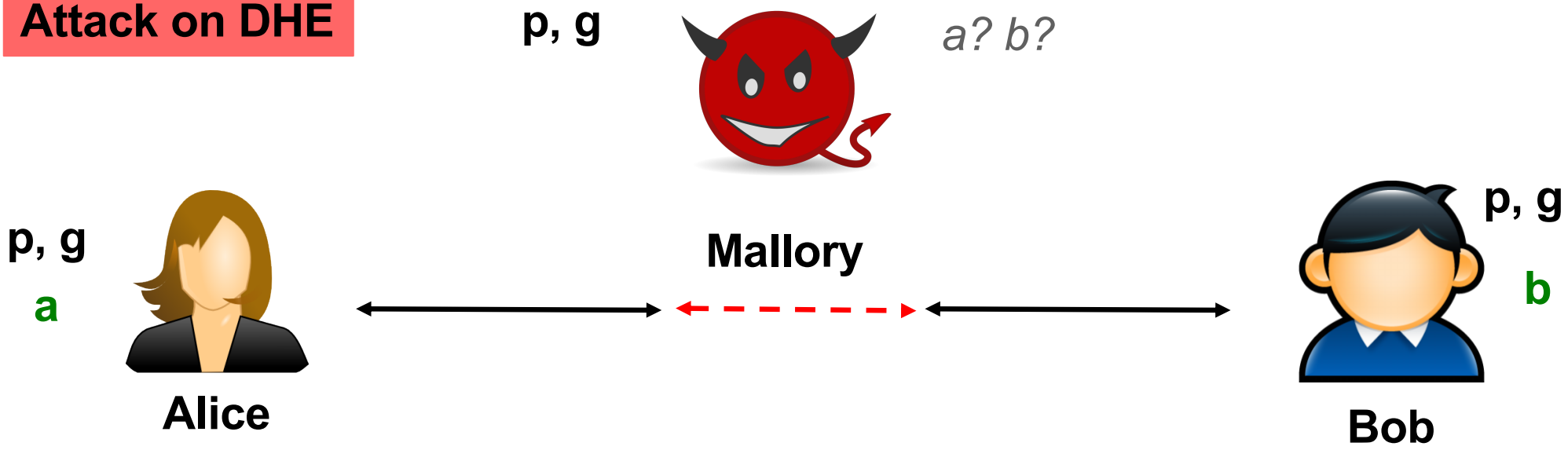
What happens if instead of Eve watching, Alice & Bob face the threat of a hidden Mallory (MITM)?

Attack on DHE



What happens if instead of Eve watching, Alice & Bob face the threat of a hidden Mallory (MITM)?

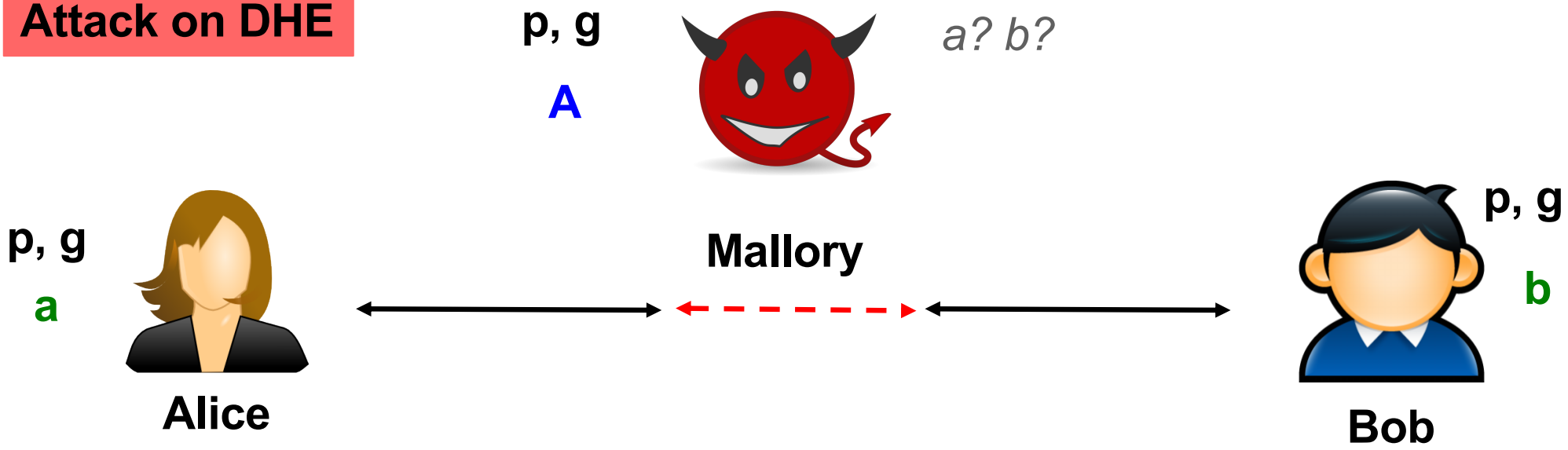
Attack on DHE



2. Alice picks random secret '**a**': 1 < a < p-1

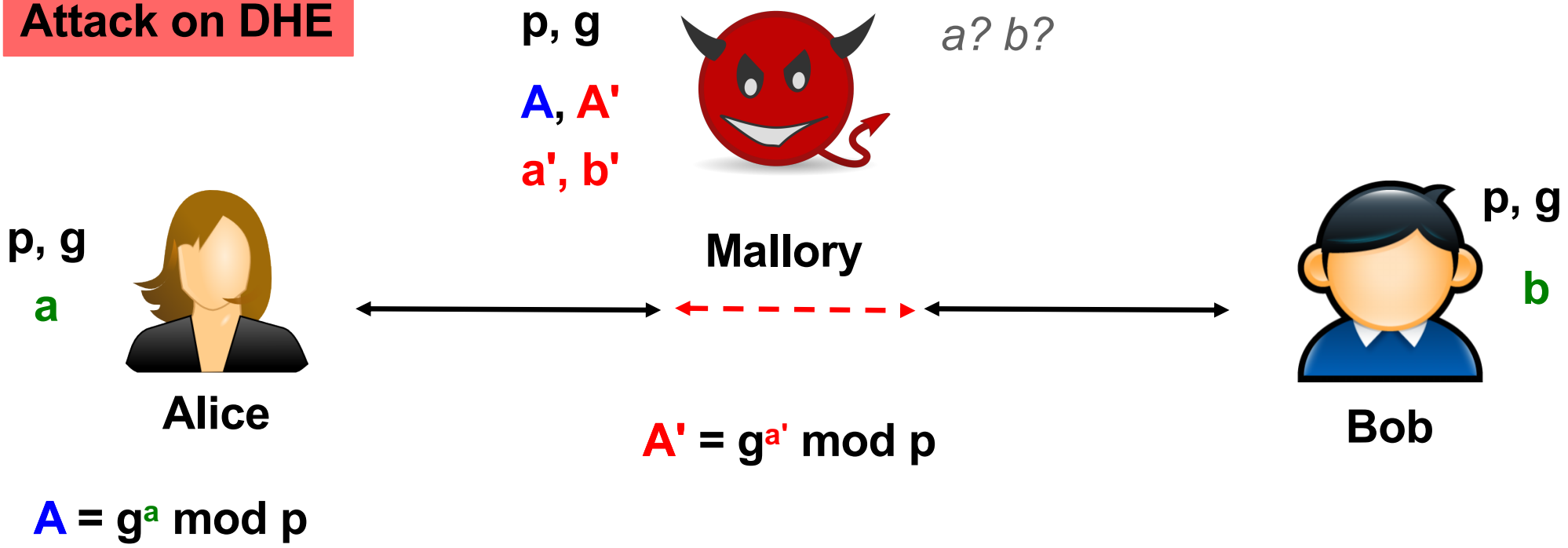
3. Bob picks random secret '**b**': 1 < b < p-1

Attack on DHE



4. Alice sends $A = g^a \bmod p$ to Bob
5. Mallory prevents Bob from receiving A

Attack on DHE



6. Mallory generates her own a', b'
7. Mallory sends $A' = g^{a'} \bmod p$ to Bob

Attack on DHE

p, g

A, A'

a', b'

a? b?

p, g

a

Alice

Mallory

p, g

b

Bob

$A' = g^{a'} \bmod p$

$A = g^{a} \bmod p$

A'

$g^{b} \bmod p = B$

8. The same happens for Bob and B/B'

Attack on DHE

p, g

A, B, A', B'

a', b'

a? b?

p, g

a

Alice

Mallory

p, g

b

Bob

$A = g^a \bmod p$

$A' = g^{a'} \bmod p$

$B' = g^{b'} \bmod p$

A'

$g^b \bmod p = B$

8. The same happens for Bob and B/B'

Attack on DHE

p, g

A, B, A', B'

a', b'

a? b?

p, g

a

Alice

Mallory

p, g

b

Bob

$A = g^a \bmod p$

B'

$A' = g^{a'} \bmod p$

$B' = g^{b'} \bmod p$

$K'_1 = A^{b'} \bmod p = g^{ab'} \bmod p$

$K'_2 = B^{a'} \bmod p = g^{ba'} \bmod p$

A'

$g^b \bmod p = B$

$K'_1 = (B')^a \bmod p$
$= (g^{b'})^a = g^{b'a} \bmod p$

$K'_2 = (A')^b \bmod p$
$= (g^{a'})^b = g^{a'b} \bmod p$

9. Alice and Bob now compute keys they share with … Mallory!
10. Mallory can relay encrypted traffic between the two …

    10'. Modifying it or making stuff up *however she wishes*

Questions?

Thinking about Authentication

- Fundamental issue for networking:
  - Parties only connected by untrustworthy medium
- Broad & evolving topic
- Goal: develop a sense for authentication paradigms & issues
  - Including *weaker* forms
- Will include some review
- Will skip some (much) state-of-the-art

Thinking about Authentication, con't

- Spectrum:
  - Which user (human) am I dealing with?
  - Which server (institution) am I dealing with?
  - What attributes does this party have?
    - Affiliation, human-or-program, country, …
  - Is this the same entity as before?

- A springboard for discussion: Let's start with very basic circa 1990s web authentication …

C → S: **`GET http://mybank.com/`**

S → C: page, including a login form

C → S: **`POST http://mybank.com/login?`**
`u=`*USER*`&p=`***PASSWD***

[*server marks this session as authenticated*]

S → C: **`Set-Cookie: sessionid=`***NONCE*

(Cookie is an "authenticator" for session)

C → S: **`GET http://mybank.com/moneyxfer.cgi`**
`Cookie: sessionid=`*NONCE*

Threats?

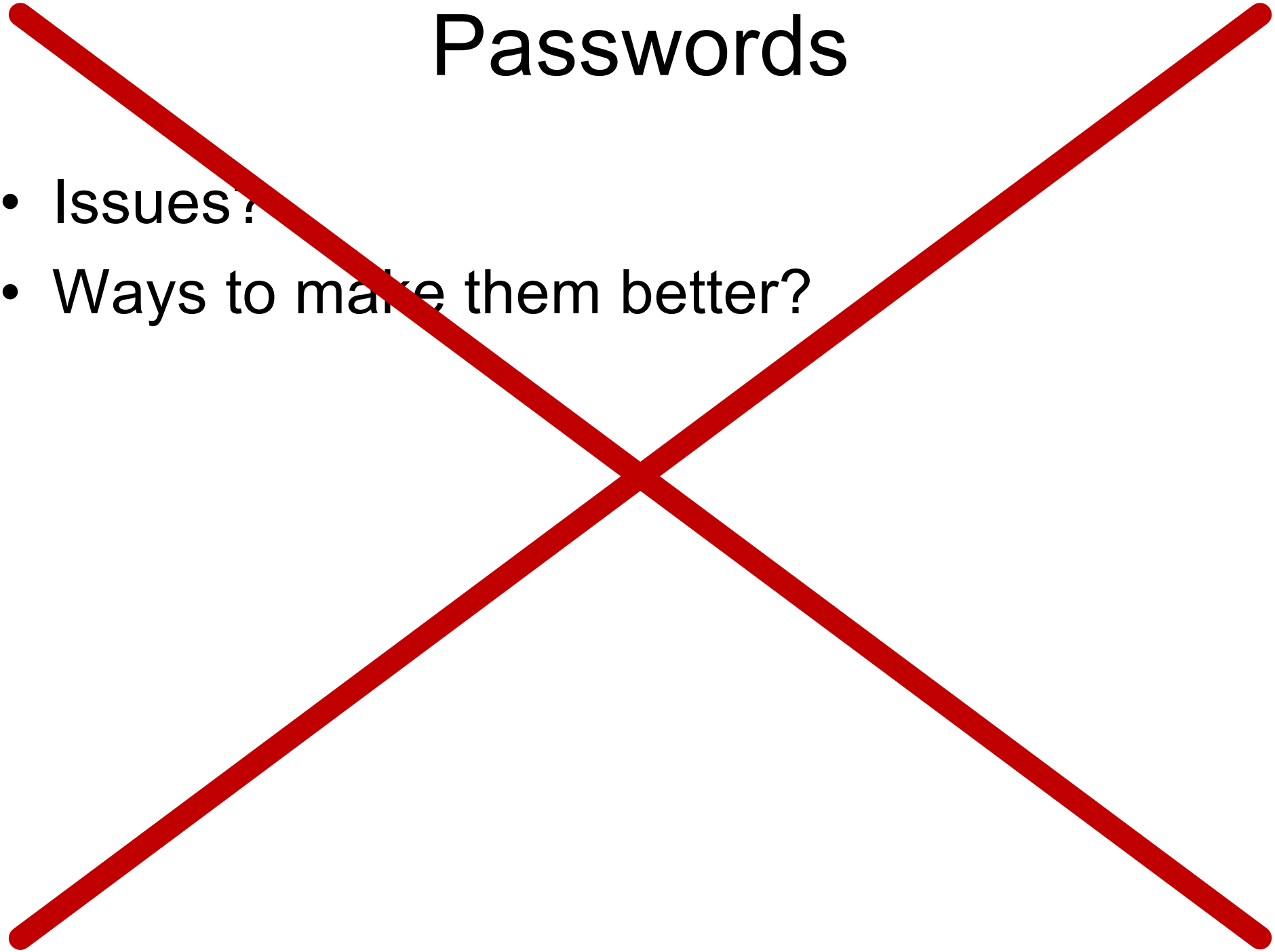
- No encryption: can know password, username, cookie
- MITM can manipulate cookies, migrate user associated with activity
- Weak passwords
- Reused passwords

Threats?

- Sniffing, MITM (network; app-level relay)
  ⇒ Theft of password and/or authenticator
- 3rd-party manipulation of automation
  - E.g. CSRF (browser fetching of images)
  - E.g. XSS (browser execution of JS replies)
- Password security
  - Blind guessing / bruteforcing
  - Reuse (breaches)
  - Phishing
- Compromised client: hijacking

Passwords

- Issues?
- Ways to make them better?



IEEE Symposium on Security & Privacy

The 2012 symposium will mark the 33rd annual meeting of this flagship conference. Since 1980, the IEEE Symposium on Security and Privacy has been the premier forum for presenting developments in computer security and electronic privacy, and for bringing together researchers and practitioners in the field. The symposium will be held in the San Francisco Bay Area, California.

10:30-11:45 Session 11: Passwords

Chair: William Enck

Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms

Patrick Gage Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Tim Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, and Julio Lopez (Carnegie Mellon University)

slides

SoK = *Systemization of Knowledge*

ized corpus of 70 million passwords

)

[SoK] The quest to replace passwords: A framework for comparative evaluation of web authentication schemes

Joseph Bonneau (University of Cambridge), Cormac Herley (Microsoft Research), Paul C. van Oorschot (Carleton U), and Frank Stajano (University of Cambridge)

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

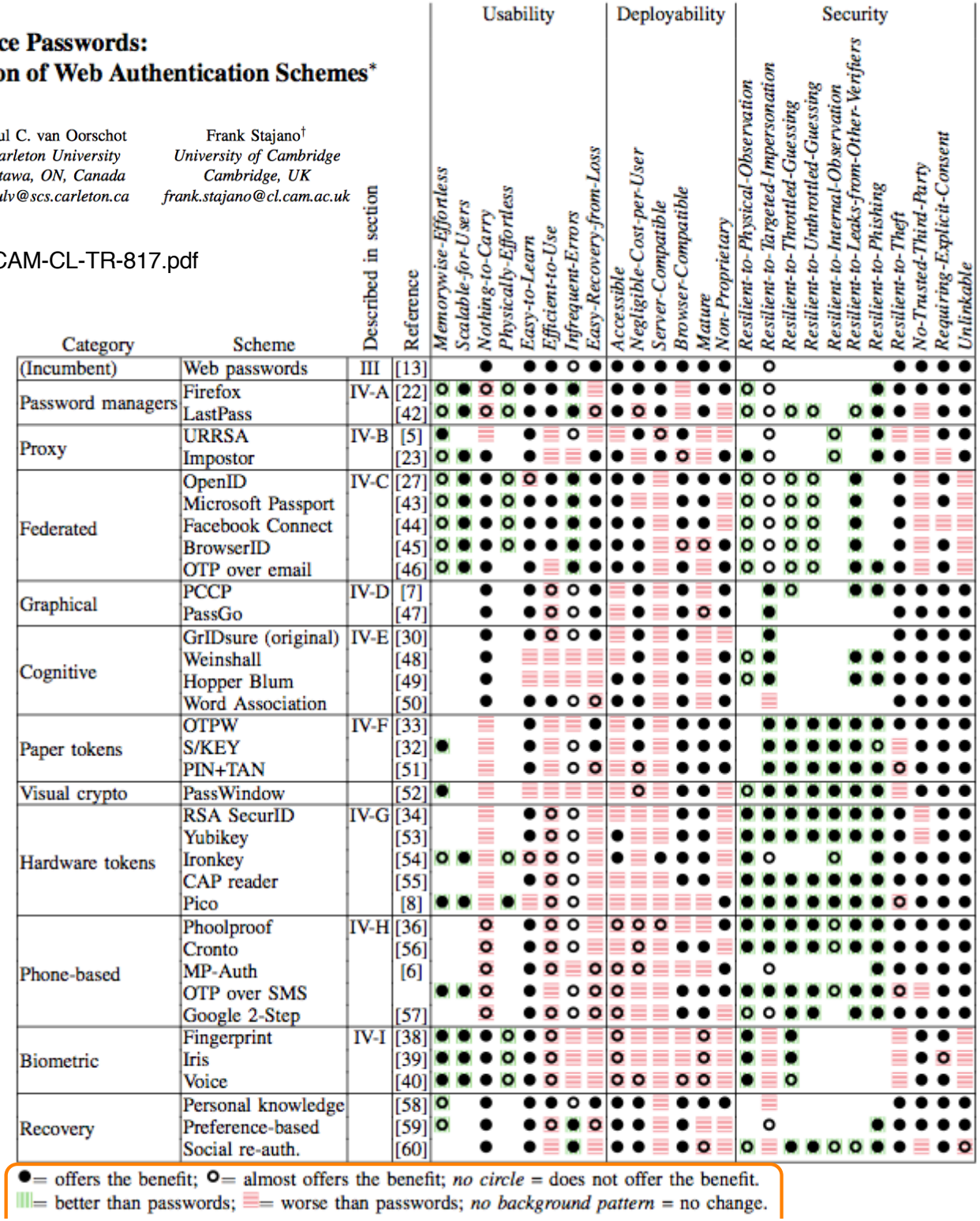
Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf



The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau, *University of Cambridge, Cambridge, UK, jcb82@cl.cam.ac.uk*

Cormac Herley, *Microsoft Research, Redmond, WA, USA, cormac@microsoft.com*

Paul C. van Oorschot, *Carleton University, Ottawa, ON, Canada, paulv@scs.carleton.ca*

Frank Stajano†, *University of Cambridge, Cambridge, UK, frank.stajano@cl.cam.ac.uk*

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

User doesn't have to memorize anything (weaker: just 1 secret)

				Usability								Deployability						Security										
Category	Scheme	Described in section	Reference	*Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Lea*	*Efficient-to-*	*Infrequent-E*	*Easy-Recove*	*Accessible*	*Negligible-C*	*Server-Com*	*Browser-Co*	*Mature*	*Non-Proprie*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*No-Trusted-*	*Requiring-E*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●		●	●	●		●		○	○				●	●	●		●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●		●		○	○	○	○		○	●	●		●
Proxy	URRSA	IV-B	[5]	●				●		○			●	○	●				○			○	●	●		●
	Impostor		[23]	○	●	●		●				●		●	○		●	●	○			○	●	●		●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●		●	●	●	○	○	○	○	●		●			
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●			●	●		○	○	○	○	●		●		●	
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○	●		●			
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●		○	○	●	○	○	○	○	●		●		●	
	OTP over email		[46]	○	●	●		●		●	●	●	●		●		●	○	○	○	○	●	●	●		●	
Graphical	PCCP	IV-D	[7]			●		●	○	○	●		●		●		●		●	○		●	●	●		●	●
	PassGo		[47]			●		●	○	○	●		●		●	○	●		●					●		●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●		●		●		●		●					●		●	●
	Weinshall		[48]			●							●		●		●	○	●			●	●	●		●	●
	Hopper Blum		[49]			●						●	●		●		●	○	●			●	●	●		●	●
	Word Association		[50]			●		●	●	○	○	●	●		●		●							●		●	●
Paper tokens	OTPW	IV-F	[33]					●			●		●		●	●	●		●	●	●	●	●	●		●	●
	S/KEY		[32]	●				●		○	●		●		●	●	●		●	●	●	●	○			●	●
	PIN+TAN		[51]					●		○	○		○		●	●	●		●	●	●	●	●	○		●	●
Visual crypto	PassWindow		[52]	●									○		●	●		○	●	●	●	●	●			●	●
Hardware tokens	RSA SecurID	IV-G	[34]					●	○	○					●	●			●	●	●	●	●	●		●	●
	Yubikey		[53]					●	○	○		●			●	●			●	●	●	●	●	●		●	●
	Ironkey		[54]	○	●		○	○	○	○		●		●	●	●			○			○		●		●	●
	CAP reader		[55]					●	○	○					●	●			●	●	●	●	●	●		●	●
	Pico		[8]	●	●		●		○	○						●			●	●	●	●	●	○		●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○		○	○	○			●		●	●	●	○	●	●		●	●
	Cronto		[56]			○		●	○	○			○		●	●			●	●	●	○	●	●		●	●
	MP-Auth		[6]			○		●	○		○	○	○				●		○					●		●	●
	OTP over SMS			●	●	○		●		○	○	○			●	●	●		●	●	●	○	●	○		●	●
	Google 2-Step		[57]			○		●	○	○	○	○			●	●			○	○	●		●	●		●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Cognitively practical for user having many accounts

				Usability								Deployability						Security									
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-Recov*	*Accessible*	*Negligible-C*	*Server-Com*	*Browser-Co*	*Mature*	*Non-Propri*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*No-Trusted*	*Requiring-I*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○				●	●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○		○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○		○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○	●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○	●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○	●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○	●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○	●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○		●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●					●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	●		●					●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒					●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○			●	●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

No physical object (weaker: you carry it anyway)

				Usability								Deployability					Security										
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-Recov*	*Accessible*	*Negligible-C*	*Server-Com*	*Browser-Co*	*Mature*	*Non-Propri*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*Resilient-to*	*No-Trusted*	*Requiring-I*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○				●	●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○			●	●	●	●	▒	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○		○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○		○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○	●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○	●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○	●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○	●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○	●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○		●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●					●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●					●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒					●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○			●	●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

No user action required (weaker: user speaks)

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-Lo	Accessible	Negligible-Cost-per-Us	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Resilient-to-Physical-O	Resilient-to-Targeted-In	Resilient-to-Throttled-C	Resilient-to-Unthrottled	Resilient-to-Internal-Ob	Resilient-to-Leaks-from	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Con	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

(E.g.: not a do-crypto-in-your-head scheme)

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-Lo	Accessible	Negligible-Cost-per-Us	Server-Compatible	Browser-Compatible	Mature	Non-Proprietary	Resilient-to-Physical-O	Resilient-to-Targeted-In	Resilient-to-Throttled-G	Resilient-to-Unthrottled	Resilient-to-Internal-Ob	Resilient-to-Leaks-from	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Con	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒		●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●		●	●	●	●	○	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords:
A Framework for Comparative Evaluation of Web Authentica

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Fr
Univers
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Doesn't require much user time; new associations aren't burdensome

				Usability								Deployability					Security										
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-Lo*	*Accessible*	*Negligible-Cost-per-Us*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-O*	*Resilient-to-Targeted-In*	*Resilient-to-Throttled-C*	*Resilient-to-Unthrottled*	*Resilient-to-Internal-On*	*Resilient-to-Leaks-from*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Con*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	●	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Fran
Universi
Cambridge, UK
frank.stajano@cl.cam.ac.uk

Won't frustrate legit users

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability							Deployability					Security											
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-L*	*Accessible*	*Negligible-Cost-per-U*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-*	*Resilient-to-Targeted-*	*Resilient-to-Throttled-*	*Resilient-to-Unthrottl*	*Resilient-to-Internal-C*	*Resilient-to-Leaks-fro*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	●	▒	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	●	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Recovery is quick, low-hassle, assured

				Usability								Deployability						Security														
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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	▒	●	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	▒	●	▒	●	●	▒	●	○		○		●	●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	●	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒	●	●	●	●	●	●	○	▒	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○				●	●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Works for users w/ physical disabilities/conditions

				Usability								Deployability					Security										
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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	≡	●	●	●	≡	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	≡	●	≡	○	○	○	○	○	●	●	≡	●	●
Proxy	URRSA	IV-B	[5]	●		≡		●	≡	○	≡	≡	●	○	●	≡	≡		○			○		●	≡	●	●
	Impostor		[23]	○	●	●		●	≡	≡	●	●	≡	●	○	≡	●	●	○			○		●	●	≡	●	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	≡	●	●	●	○	○	○	○		●		●	≡	●	≡
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	≡	≡	●	●	≡	○	○	○	○		●		●	≡	●	≡
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	≡	●	●	≡	○	○	○	○		●		●	≡	≡	≡
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	≡	○	○	●	○	○	○	○		●		●	≡	●	≡
	OTP over email		[46]	○	●	●		●	≡	●	●	●	●	≡	●	≡	●	○	○	○	○		●	●	●	≡	●	≡
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	≡	●	≡	●	≡	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	≡	●	≡	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	≡	●	≡	●	≡	≡		●						●	●	●	●
	Weinshall		[48]			●		≡	≡	≡	≡	≡	●	≡	●	≡	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		≡	≡	≡	≡	●	●	≡	●	≡	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	≡	●	≡	●		≡						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			≡		●	≡	≡	●	≡	●	≡	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		≡		●	≡	○	●	≡	●	≡	●	●	●		●	●	●	●	●	○	≡	●	●	●
	PIN+TAN		[51]			≡		●	≡	○	○	≡	○	≡	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		≡		≡	≡	≡	≡	≡	○	≡	●	●	≡	○	●	●	●	●	●	●	≡	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			≡		●	○	○	≡	≡	≡	≡	●	●	≡		●	●	●	●	●	●	●	≡	●	●
	Yubikey		[53]			≡		●	○	○	≡	●	≡	≡	●	●	≡		●	●	●	●	●	●	●	≡	●	●
	Ironkey		[54]	○	●	≡	○	○	○	○	≡	●	≡	●	●	●	≡		●	○		○		●	●	●	●	●
	CAP reader		[55]			≡		●	○	○	≡	≡	≡	≡	●	●	≡		●	●	●	●	●	●	●	≡	●	●
	Pico		[8]	●	●	≡	●	≡	○	○	≡	≡	≡	≡	≡	≡	●		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	≡	○	○	○	≡	≡	●		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	≡	≡	○	≡	●	●	≡		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	≡	○	○	○	≡	≡	≡	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	≡	○	○	○	≡	≡	●	●	●		●	●	●	●	○	●	○	≡	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	≡	≡	●	●	≡		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

E.g.: plausible for startups to use

				Usability							Deployability					Security									
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-Physica*	*Resilient-to-Targete*	*Resilient-to-Throttle*	*Resilient-to-Unthrot*	*Resilient-to-Interna*	*Resilient-to-Leaks-f*	*Resilient-to-Phishin*	*Resilient-to-Theft*	*No-Trusted-Third-P*	*Requiring-Explicit-C*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Can look like "incumbent" to servers

Category	Scheme	Described in section	Reference	Usability: *Memorywise-Effortless*	*Scalable-for-Users*	*Nothing-to-Carry*	*Physically-Effortless*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-from-Loss*	Deployability: *Accessible*	*Negligible-Cost-per-User*	*Server-Compatible*	*Browser-Compatible*	*Mature*	*Non-Pro*	Security: *Resilien*	*Resilien*	*Resilien*	*Resilien*	*Resilien*	*Resilien*	*Resilien*	*No-Trus*	*Requirin*	*Unlinka*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		▒	●	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●				●	●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●					●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●			●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒					●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒		●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	●		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○				●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●		●	●	●	○	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac H
Microsoft Re
Redmond, W
cormac@micr

Just requires HTML5/JS; weaker: very common plugins

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability									Deployability				Security														
Category	Scheme	Described	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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambri
Cambridge, UK
frank.stajano@cl.cam.

Not just a research prototype/toy

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability								Deployability					Security												
Category	Scheme	Described	Reference	Memorywise-	Scalable-for-	Nothing-to-	Physically-	Easy-to-Le	Efficient-to-	Infrequent-	Easy-Recov	Accessible	Negligible-	Server-Cor	Browser-C	Mature	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	○	○	○	○	○	●	●	●	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒	○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●		●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●		●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●		●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords:
A Framework for Comparative Evaluation of Web Authenticatio

No licensing/$ required

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability								Deployability					Security										
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*	*Non-Proprietary*	*Resilient-to-Physical-Observ*	*Resilient-to-Targeted-Imper*	*Resilient-to-Throttled-Guess*	*Resilient-to-Unthrottled-Gu*	*Resilient-to-Internal-Observ*	*Resilient-to-Leaks-from-Oth*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	○	○	○	○		○	●	●	▒	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒		○			○		●	▒	▒	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	▒		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	▒		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	▒		●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	▒		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	▒		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●		●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	▒		○	○	●			●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

https://www.cl.can

Requires a bunch (> 10-20) of sessions for local attacker to subvert (even using sneaky techniques)

				Usability							Deployability					Security											
Category	Scheme	Desc	Refs	*Mem*	*Scal*	*Noth*	*Phys*	*Easy*	*Effic*	*Infre*	*Easy*	*Acce*	*Negl*	*Serv*	*Brow*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	▒	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	▒	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒		●	○			○		●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒		●	●	●	●	○	●	●	▒	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●		●	●	●	●	○	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords:
A Framework for Comparativ

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac He
Microsoft Re
Redmond, WA
cormac@micro

https://www.cl.cam.ac.uk/tec

Possessing personal knowledge doesn't help attacker; weaker: user must exercise discipline in choices

				Usability										Deployability					Security												
Category	Scheme	De	Re	*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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●	
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○		○		●	●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○		○		●	●	▒	▒	●	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	▒	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●				●		●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	●	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○				●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorscho
Carleton University
Ottawa, ON, Canad
paulv@scs.carleton.c

It takes a *lot* of guesses

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability								Deployability					Security											
Category	Scheme	Described in sect.	Reference	*Memorywise-Effo*	*Scalable-for-User*	*Nothing-to-Carry*	*Physically-Effortl*	*Easy-to-Learn*	*Efficient-to-Use*	*Infrequent-Errors*	*Easy-Recovery-fr*	*Accessible*	*Negligible-Cost-p*	*Server-Compatibl*	*Browser-Compati*	*Mature*	*Non-Proprietary*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○		○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○		○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○		○		●	●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorscho
Carleton University
Ottawa, ON, Canad
paulv@scs.carleton.c

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-

It's *infeasible* to guess (e.g. requires 2^{64} tries)

				Usability										Deployability					Security												
Category	Scheme	Described	Reference	*Memorywo*	*Scalable-*	*Nothing-t*	*Physically*	*Easy-to-L*	*Efficient-t*	*Infrequen*	*Easy-Rec*	*Accessible*	*Negligible*	*Server-Co*	*Browser-C*	*Mature*	*Non-Prop*	*Resilient-to-Physical-Observation*	*Resilient-to-Targeted-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●	
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	▒	○	○					●	●	▒	●	●	
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●	
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●	
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●	
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒	
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒	
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒	
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒	
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒	
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●	
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●	
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●	
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●	
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●	
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●	
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●	
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●	
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●	
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●	
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●	
	Yubikey		[53]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●	
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	▒	●	●	
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●	
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒	●	●	●	●	●	●	●	○	●	●	●	
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●	
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●	
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●	
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●	
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●	
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

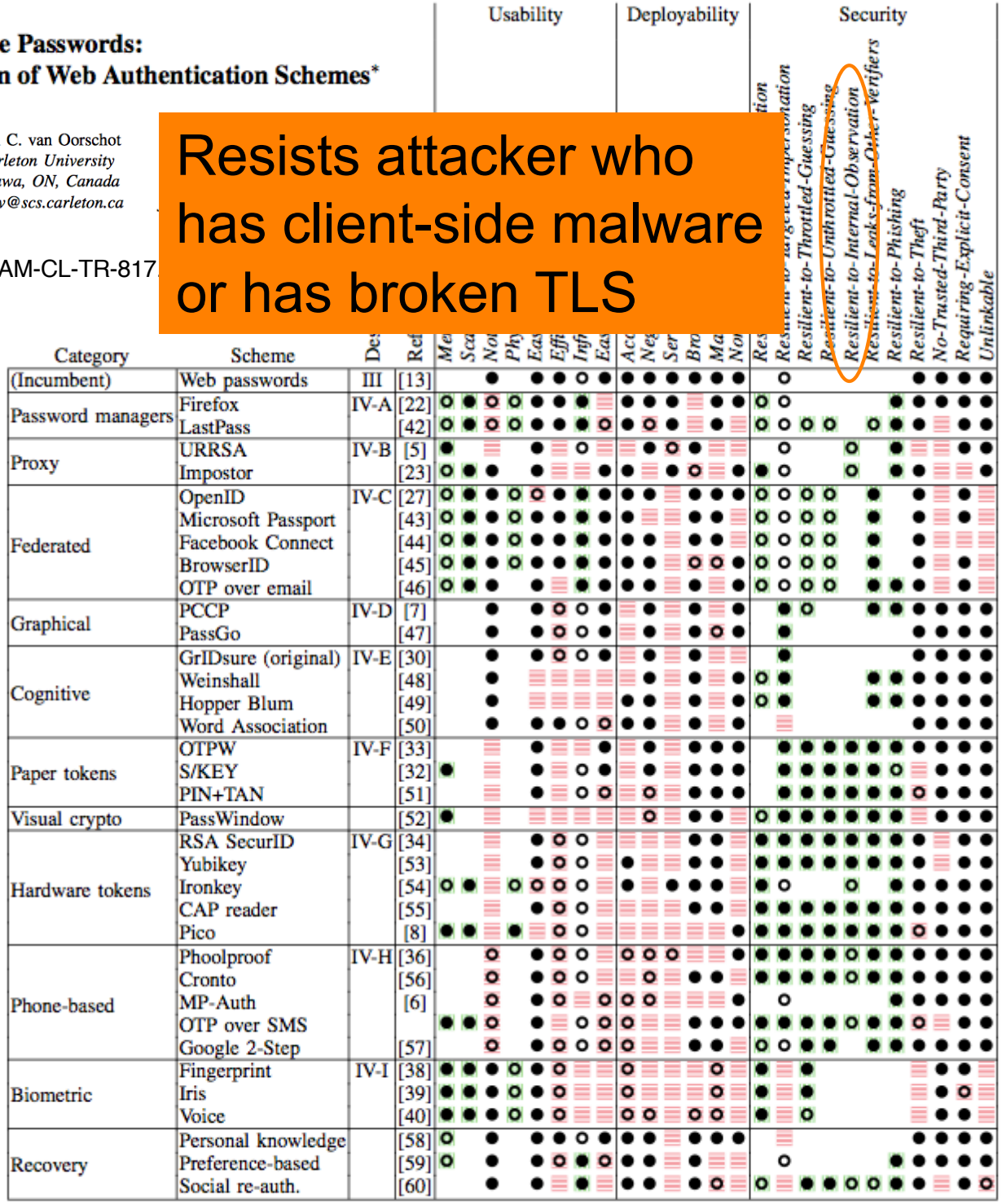
Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817

Resists attacker who has client-side malware or has broken TLS



Category	Scheme	Des.	Ref.	Usability										Deployability								Security											
				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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*						
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●					
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●		●	●	●		●	●	○	○					●	●								
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●		●		○	○	○	○		○	●	●								
Proxy	URRSA	IV-B	[5]	●				●		○			●	○	●				○			○		●			●	●					
	Impostor		[23]	○	●	●		●			●	●		●	○			●	○			○		●	●			●					
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●		●	●	●	○	○	○	○		●		●		●						
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●			●	●		○	○	○	○		●		●		●						
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●		●	●		○	○	○	○		●		●		●						
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●		○	○		○	○	○	○		●		●		●						
	OTP over email		[46]	○	●	●		●		●	●	●	●		●			○	○	○	○		●	●	●		●						
Graphical	PCCP	IV-D	[7]			●		●	○	○	●		●		●		●		●	○			●	●	●	●	●						
	PassGo		[47]			●		●	○	○	●		●		●	○	●		●						●	●	●						
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●		●		●		●		●						●	●	●						
	Weinshall		[48]			●					●		●		●		●	○	●				●	●	●	●	●						
	Hopper Blum		[49]			●					●		●		●		●	○	●				●	●	●	●	●						
	Word Association		[50]			●		●	●	○	○		●		●		●								●	●	●						
Paper tokens	OTPW	IV-F	[33]					●			●		●		●		●		●	●	●	●	●	●	●	●	●						
	S/KEY		[32]	●				●		○	●		●		●		●		●	●	●	●	○	●	●	●	●						
	PIN+TAN		[51]					●		○	○		○		●		●		●	●	●	●	●	○	●	●	●						
Visual crypto	PassWindow		[52]	●									○		●		●	○	●	●	●	●	●	●	●	●	●						
Hardware tokens	RSA SecurID	IV-G	[34]					●	○	○					●		●		●	●	●	●	●	●	●	●	●						
	Yubikey		[53]					●	○	○			●		●		●		●	●	●	●	●	●	●	●	●						
	Ironkey		[54]	○	●		○	○	○	○			●		●		●		●	○		○		●	●	●	●						
	CAP reader		[55]					●	○	○					●		●		●	●	●	●	●	●	●	●	●						
	Pico		[8]	●	●		●		○	○					●		●		●	●	●	●	●	●	○	●	●						
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○		○	○	○			●		●	●	●	○	●	●	●	●	●						
	Cronto		[56]			○		●	○	○			○		●		●		●	●	●	○	●	●	●	●	●						
	MP-Auth		[6]			○		●	○		○	○	○				●		○					●	●	●	●						
	OTP over SMS			●	●	○		●		○	○	○			●		●		●	●	●	○	●	●	○	●	●						
	Google 2-Step		[57]			○		●	○	○	○	○			●		●		○	○	●	●	●	●	●	●	●						
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van C
Carleton Uni
Ottawa, ON,
paulv@scs.car

A problem at one site doesn't endanger other sites

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability									Deployability					Security												
Category	Scheme	Described in	Reference	*Memorywise-*	*Scalable-for-*	*Nothing-to-*	*Physically-*	*Easy-to-Le-*	*Efficient-to-*	*Infrequent-*	*Easy-Recov-*	*Accessible*	*Negligible-C-*	*Server-Com-*	*Browser-Co-*	*Mature*	*Non-Propri-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*			
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●			
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	▒	●	●			
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●			
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●			
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●			
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒			
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒			
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒			
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒			
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒			
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●			
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●			
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●			
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●			
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●			
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●			
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●			
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●			
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●			
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●			
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●			
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●			
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	▒	●	●			
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●			
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	●	○	●	●	●			
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●			
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●			
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●			
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	▒	●	●	●	●	●	●	○	●	○	●	●	●	●			
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	●	○	○	●		●	●	●	●	●	●			
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

Resists off-line phishing

				Usability							Deployability						Security										
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-Obse*	*Resilient-to-Targeted-Impe*	*Resilient-to-Throttled-Gue*	*Resilient-to-Unthrottled-G*	*Resilient-to-Internal-Obse*	*Resilient-to-Leaks from-Ot*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consen*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords:
A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Pau
Ca
Otta
pau

https://www.cl.cam.ac.uk/techreports/UC

Attacker can't benefit by stealing physical object;
weaker: it's protected (e.g., PIN)

				Usability								Deployability					Security											
Category	Scheme	Des	Ref	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-Impersonation	Resilient-to-Throttled-Guessing	Resilient-to-Unthrottled-Guessing	Resilient-to-Internal-Observation	Resilient-to-Leaks-from-Other-Verifiers	Resilient-to-Phishing	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○							●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	▒	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	▒	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	▒	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	▒	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	▒	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒	●	●	●	●	●	●	●	○	▒	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords:
A Framework for Comparative Evaluation of Web Authentication Sch

Trust localized to user/service

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability							Deployability						Security										
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-Observ*	*Resilient-to-Targeted-Impers*	*Resilient-to-Throttled-Guess*	*Resilient-to-Unthrottled-Gue*	*Resilient-to-Internal-Observ*	*Resilient-to-Leaks-from-Oth*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requires-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○						●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van O
Carleton Uni
Ottawa, ON,
paulv@scs.car

User has to (knowingly) consent to authentication occurring

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability								Deployability						Security													
Category	Scheme	Described	Reference	Memorywise-	Scalable-for-	Nothing-to-	Physically-	Easy-to-Le	Efficient-to-	Infrequent-	Easy-Recov	Accessible	Negligible-	Server-Cor	Browser-C	Mature	Non-Propri	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-	Resilient-to-Theft	No-Trusted-Third-Party	Requiring-Explicit-Consent	Unlinkable
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	●	●	▒	●	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○		○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○		○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	●		●						●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●			●	●		●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●			●	●		●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○		○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○				●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords
A Framework for Comparative Evaluation of Web Au

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Two verifiers who collude can't link user across them based on authenticaticator alone

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability									Deployability					Security										
Category	Scheme	Described in	Reference	*Memorywise*	*Scalable-for*	*Nothing-to-C*	*Physically-E*	*Easy-to-Lea*	*Efficient-to-*	*Infrequent-E*	*Easy-Recove*	*Accessible*	*Negligible-C*	*Server-Comp*	*Browser-Co*	*Mature*	*Non-Proprie*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*Resilient-to-*	*No-Trusted-*	*Requires-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●			●	●		●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●			●	●		●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒		●	○		○		●	●	▒	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒		●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	●	▒		●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●		●	●	●	●	○	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒		●	●	●	●	○	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●		●	●	●	●	○	●	○	▒	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒		○	○	●	●		●	●	●	●	●
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.

The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability							Deployability					Security									
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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○				●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○	○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	▒	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

Issues w/ Biometrics?

- Theft of artifact
  - High-res cameras + gummi bears
- Theft of digitization (replay)
  - Need challenge/response protocol
- Impairment
  - (Face recognition based on skull geometry)
- Irrevocable
  - More like a username than a password

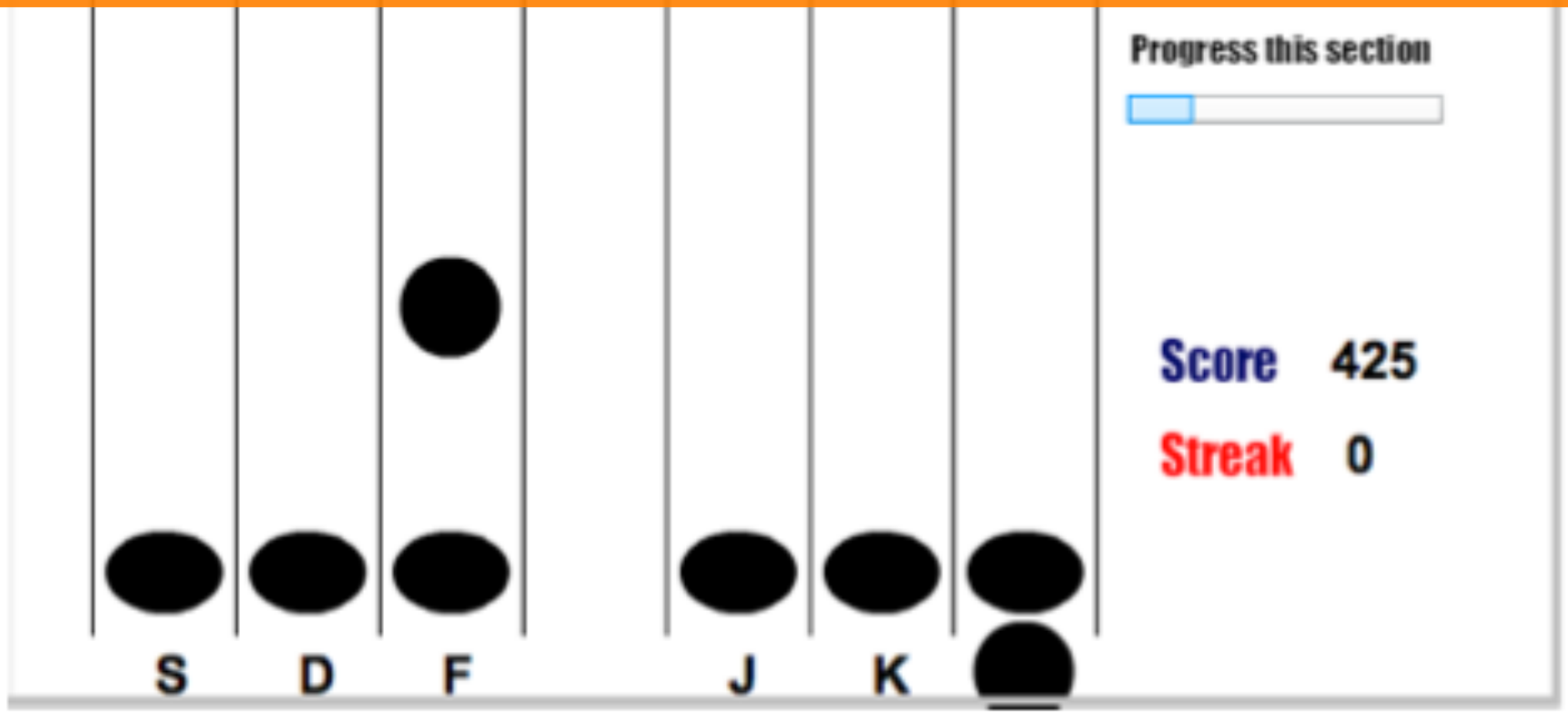
Issues w/ Biometrics?

- Theft of artifact
  - High-res cameras + gummi bears
- Theft of digitization (replay)
  - Need challenge/response protocol
- Impairment
  - (Face recognition based on skull geometry)
- Irrevocable?
  - What if sites could *implant* a biometric?

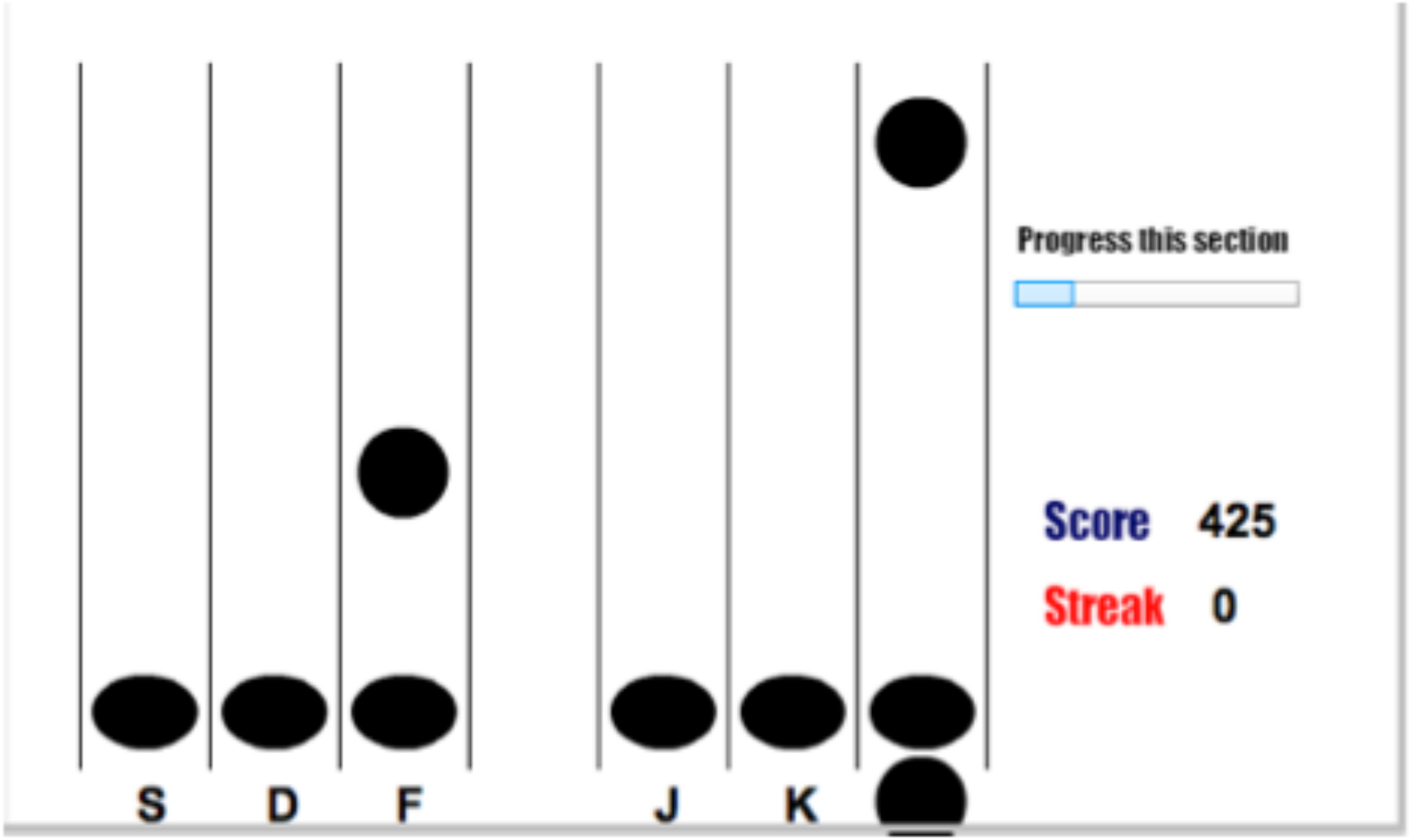
Implantable Biometrics

- Threat model: "*rubber hose cryptography*"
  - Any defenses?
- Consider scenario where authentication highly important
  - Can afford **lengthy** setup, validation sequences
- Abstract idea:
  - In setup phase, implant biometric password in *muscle memory*
  - Validation: probe muscle-memory response
- If user threatened, *they don't consciously know their password* ⇒ can't reveal it

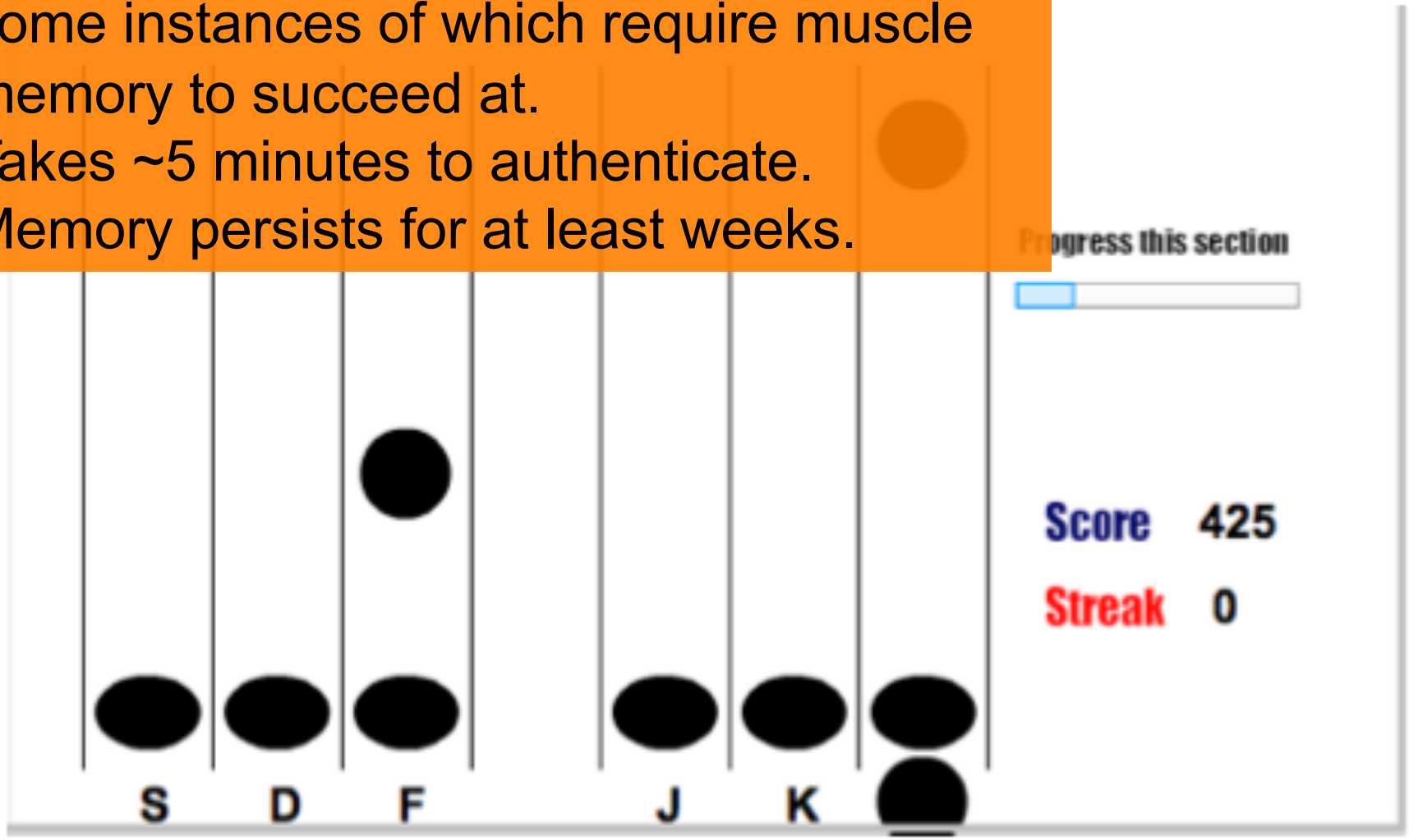
Authentication based on a game similar to *Guitar Hero*.
User presses a key corresponding to falling circles.
Game rachets up speed until user has a ~30% failure rate.
Embeds password in 80% of game instances.



30-45 minutes training: ~38 bits of entropy



Authentication: make user play game, some instances of which require muscle memory to succeed at.
Takes ~5 minutes to authenticate.
Memory persists for at least weeks.



The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes*

Joseph Bonneau
University of Cambridge
Cambridge, UK
jcb82@cl.cam.ac.uk

Cormac Herley
Microsoft Research
Redmond, WA, USA
cormac@microsoft.com

Paul C. van Oorschot
Carleton University
Ottawa, ON, Canada
paulv@scs.carleton.ca

Frank Stajano†
University of Cambridge
Cambridge, UK
frank.stajano@cl.cam.ac.uk

https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf

				Usability							Deployability					Security									
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-Impersonation*	*Resilient-to-Throttled-Guessing*	*Resilient-to-Unthrottled-Guessing*	*Resilient-to-Internal-Observation*	*Resilient-to-Leaks-from-Other-Verifiers*	*Resilient-to-Phishing*	*Resilient-to-Theft*	*No-Trusted-Third-Party*	*Requiring-Explicit-Consent*	*Unlinkable*
(Incumbent)	Web passwords	III	[13]			●		●	●	○	●	●	●	●	●	●	●		○					●	●	●	●
Password managers	Firefox	IV-A	[22]	○	●	○	○	●	●	●	▒	●	●	●	▒	●	●	○	○					●	●	●	●	●
	LastPass		[42]	○	●	○	○	●	●	●	○	●	○	●	▒	●	▒	○	○	○	○		○	●	●	▒	●	●
Proxy	URRSA	IV-B	[5]	●		▒		●	▒	○	▒	▒	●	○	●	▒	▒		○			○		●	▒	▒	●	●
	Impostor		[23]	○	●	●		●	▒	▒	●	●	▒	●	○	▒	●	●	○			○		●	●	▒	▒	●
Federated	OpenID	IV-C	[27]	○	●	●	○	○	●	●	●	●	●	▒	●	●	●	○	○	○	○		●		●	▒	●	▒
	Microsoft Passport		[43]	○	●	●	○	●	●	●	●	●	▒	▒	●	●	▒	○	○	○	○		●		●	▒	●	▒
	Facebook Connect		[44]	○	●	●	○	●	●	●	●	●	●	▒	●	●	▒	○	○	○	○		●		●	▒	▒	▒
	BrowserID		[45]	○	●	●	○	●	●	●	●	●	●	▒	○	○	●	○	○	○	○		●		●	▒	●	▒
	OTP over email		[46]	○	●	●		●	▒	●	●	●	●	▒	●	▒	●	○	○	○	○		●	●	●	▒	●	▒
Graphical	PCCP	IV-D	[7]			●		●	○	○	●	▒	●	▒	●	▒	●		●	○			●	●	●	●	●	●
	PassGo		[47]			●		●	○	○	●	▒	●	▒	●	○	●		●						●	●	●	●
Cognitive	GrIDsure (original)	IV-E	[30]			●		●	○	○	●	▒	●	▒	●	▒	▒		●						●	●	●	●
	Weinshall		[48]			●		▒	▒	▒	▒	▒	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Hopper Blum		[49]			●		▒	▒	▒	▒	●	●	▒	●	▒	●	○	●				●	●	●	●	●	●
	Word Association		[50]			●		●	●	○	○	●	●	▒	●	▒	●		▒						●	●	●	●
Paper tokens	OTPW	IV-F	[33]			▒		●	▒	▒	●	▒	●	▒	●	●	●		●	●	●	●	●	●	●	●	●	●
	S/KEY		[32]	●		▒		●	▒	○	●	▒	●	▒	●	●	●		●	●	●	●	●	○	●	●	●	●
	PIN+TAN		[51]			▒		●	▒	○	○	▒	○	▒	●	●	●		●	●	●	●	●	●	○	●	●	●
Visual crypto	PassWindow		[52]	●		▒		▒	▒	▒	▒	▒	○	▒	●	●	▒	○	●	●	●	●	●	●	▒	●	●	●
Hardware tokens	RSA SecurID	IV-G	[34]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Yubikey		[53]			▒		●	○	○	▒	●	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Ironkey		[54]	○	●	▒	○	○	○	○	▒	●	▒	●	●	●	▒	●	○			○		●	●	●	●	●
	CAP reader		[55]			▒		●	○	○	▒	▒	▒	▒	●	●	▒	●	●	●	●	●	●	●	●	▒	●	●
	Pico		[8]	●	●	▒	●	▒	○	○	▒	▒	▒	▒	▒	▒	●	●	●	●	●	●	●	○	●	●	●	●
Phone-based	Phoolproof	IV-H	[36]			○		●	○	○	▒	○	○	○	▒	▒	●	●	●	●	●	○	●	●	●	●	●	●
	Cronto		[56]			○		●	○	○	▒	▒	○	▒	●	●	▒	●	●	●	●	○	●	●	●	●	●	●
	MP-Auth		[6]			○		●	○	▒	○	○	○	▒	▒	▒	●		○					●	●	●	●	●
	OTP over SMS			●	●	○		●	▒	○	○	○	▒	▒	●	●	●	●	●	●	●	○	●	●	○	●	●	●
	Google 2-Step		[57]			○		●	○	○	○	○	▒	▒	●	●	▒	○	○	●	●		●	●	●	●	●	●
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.

Issues w/ Recovery?

- Knowledge-based recovery is vulnerable to targeting attacker
- Opens up phishing opportunities
- May compound mental burden
- Overall security = min(orig. sec., rec. sec.)

Issues w/ Recovery?

- Can reduce security to that of *simpler mode*
  - E.g. iOS fingerprint/faceprint reduced to PIN
- Gets especially iffy when recovery relies on *email* and uses varying, non-robust second factors
  - Real-life example from 2012 …

(1) Get victim's email & home (billing) address
(2) Call Amazon, say you're the victim & want to
add a credit card #
(2') Add bogus card
(3) Call Amazon: "I've lost access to my email account"
Provide name, billing addr, new credit card #
(3') Add new email account
(4) Go to Amazon web site, send password reset to new acct
(5) This provides access to last four digits of account CCs
(6) Go to Apple. Provide billing addr. & last 4 digits ...
(6') ... receive temporary iCloud password
(7) Go to *N* services: password resets emailed to iCloud acct.
(8) Brick victim's devices & PROFIT

Thinking about Authentication, con't

- Spectrum:
  - Which user (human) am I dealing with?
  - Which server (institution) am I dealing with?
  - What attributes does this party have?
    - Affiliation, human-or-program, country, …
  - Is this the same entity as before?

Phishing

- Involves two key fake-outs:
  - Fool user into thinking attacker is really desired site
  - Fool site into thinking attacker is really desired user
- Can we rely on user to judge whether a site is genuine?

Bank of the West – Home

https://bankofthewest.com

Search

Security | Locations ▾ | Customer Service ▾

BANK OF THE WEST

Personal | Small Business | Commercial | Wealth Management

Checking & Savings | Credit & Loans | Investments & Insurance | Online & Mobile Banking

Online Banking

Username: Enter Username

Password: Enter Password

Forgot Password

Sign In | Enroll ›

Sign in to other services ›

Open an Account

It's fast, secure and easy.

Choose an account | Go

Mobile Banking

Powerful banking tools you can take anywhere.

Locations

Find a branch or ATM.

Enter ZIP or City and State | Find

Bank of the West Premier

Explore a more rewarding relationship with a higher level of benefits.

Learn more ›

Security

Get the latest information to help you keep safe online.

Learn more ›

Quick Links

Select One | Go

Mortgage Help

Are financial hardships making your mortgage payments difficult to afford?

A Commitment to Community

We have committed $75 billion in loans, investments and charitable contributions to the neighborhoods we serve.

COMMITMENT

[+] Feedback

Bank of the West – Home

https://www.bankofthewest.com

Search

Security | Locations ▾ | Customer Service ▾

BANK OF THE WEST

Personal | Small Business | Commercial | Wealth Management

Checking & Savings | Credit & Loans | Investments & Insurance | Online & Mobile Banking

Online Banking

Username: Enter Username

Password: Enter Password

Forgot Password

Sign In | Enroll ›

Sign in to other services ›

Open an Account

It's fast, secure and easy.

Choose an account | Go

Mobile Banking

Powerful banking tools you can take anywhere.

Locations

Find a branch or ATM.

Enter ZIP or City and State | Find

Bank of the West Premier

Explore a more rewarding relationship with a higher level of benefits.

Learn more ›

Security

Get the latest information to help you keep safe online.

Learn more ›

Quick Links

Select One | Go

Mortgage Help

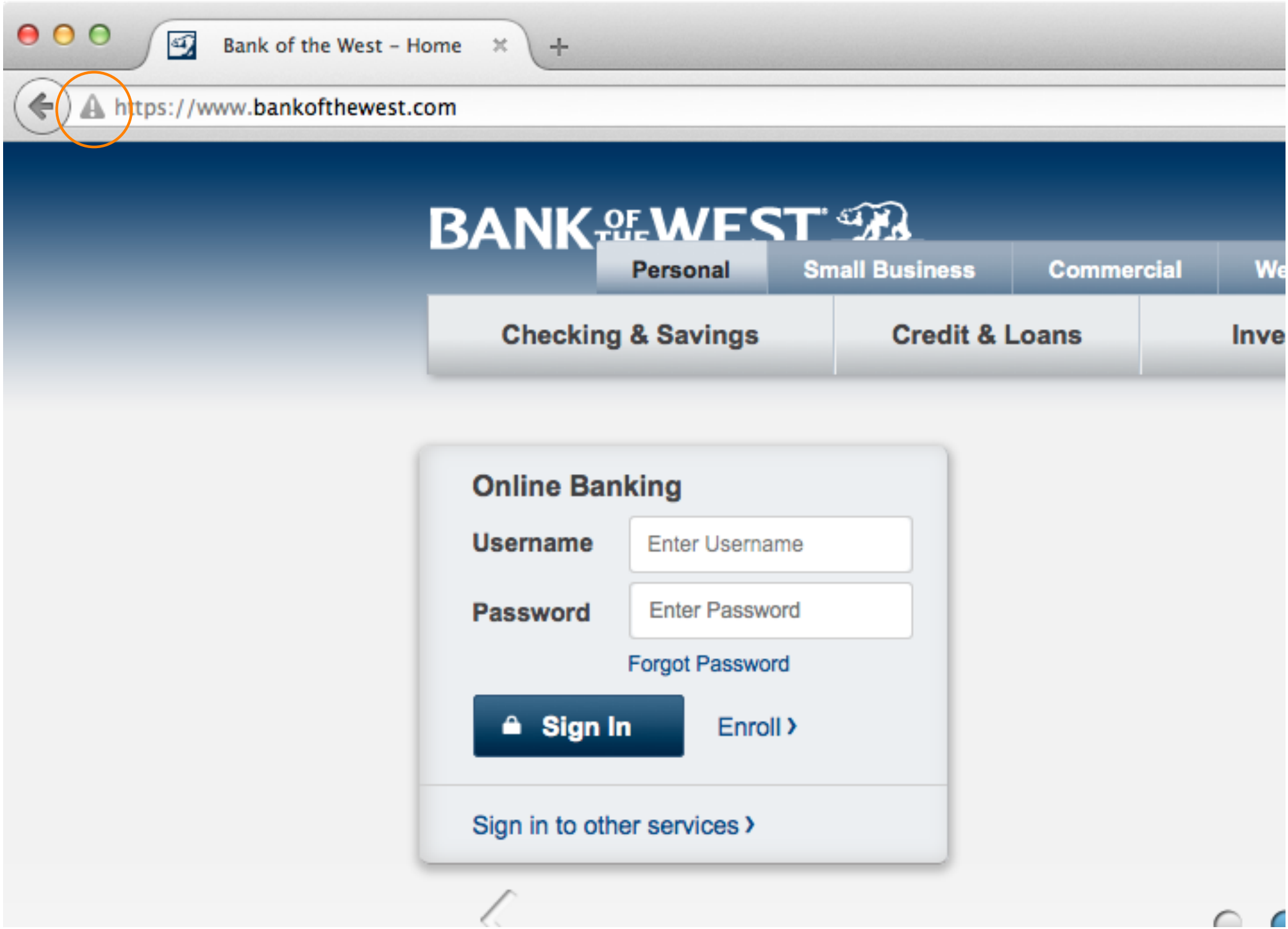
Are financial hardships making your mortgage payments difficult to afford?

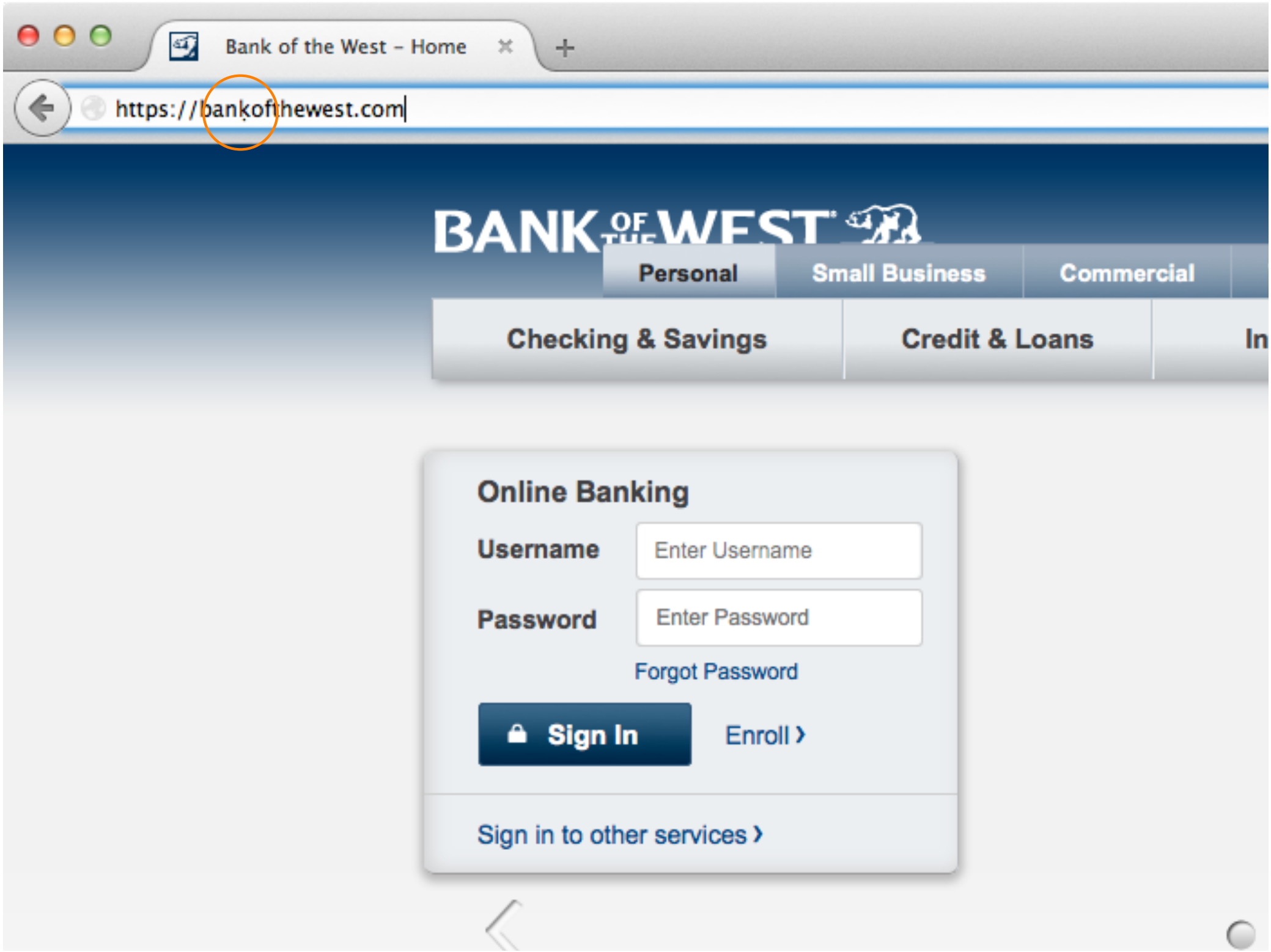
A Commitment to Community

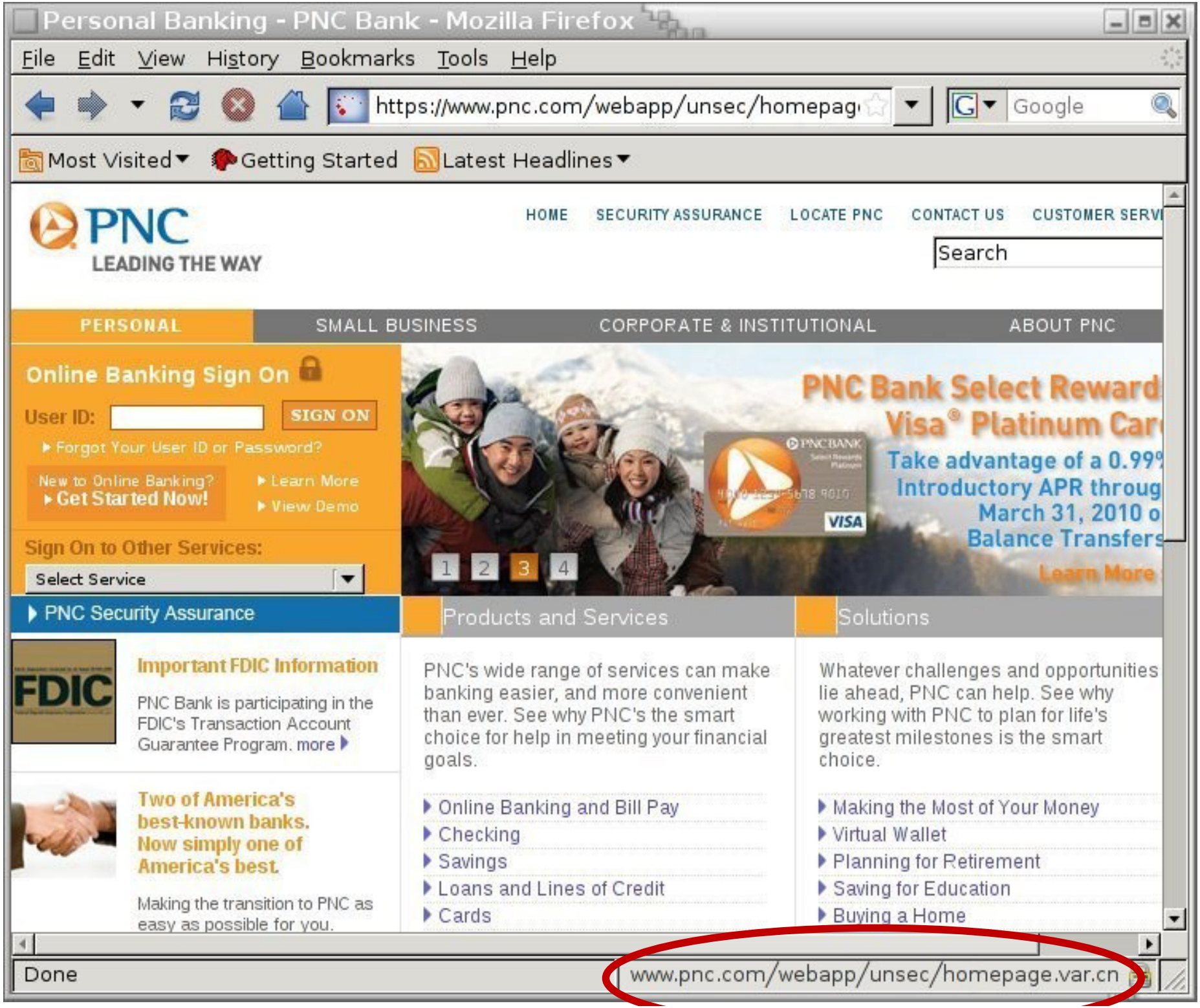
We have committed $75 billion in loans, investments and charitable contributions to the neighborhoods we serve.

COMMITMENT

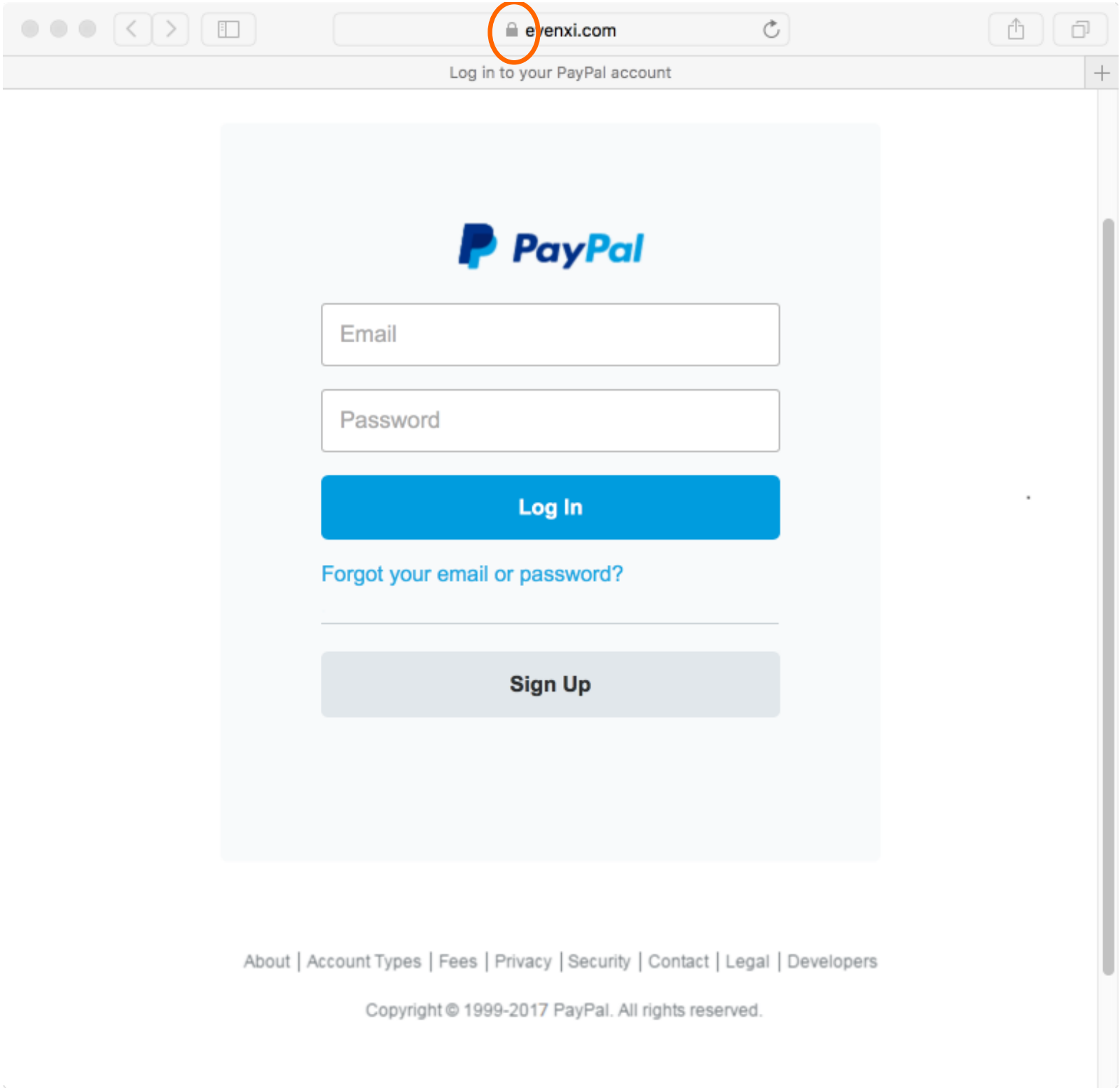
[–] Feedback


Bank of the West - Home
https://www.bankofthewest.com
BANK OF THE WEST
Personal
Small Business
Commercial
Checking & Savings
Credit & Loans
Online Banking
Username
Enter Username
Password
Enter Password
Forgot Password
Sign In
Enroll ›
Sign in to other services ›

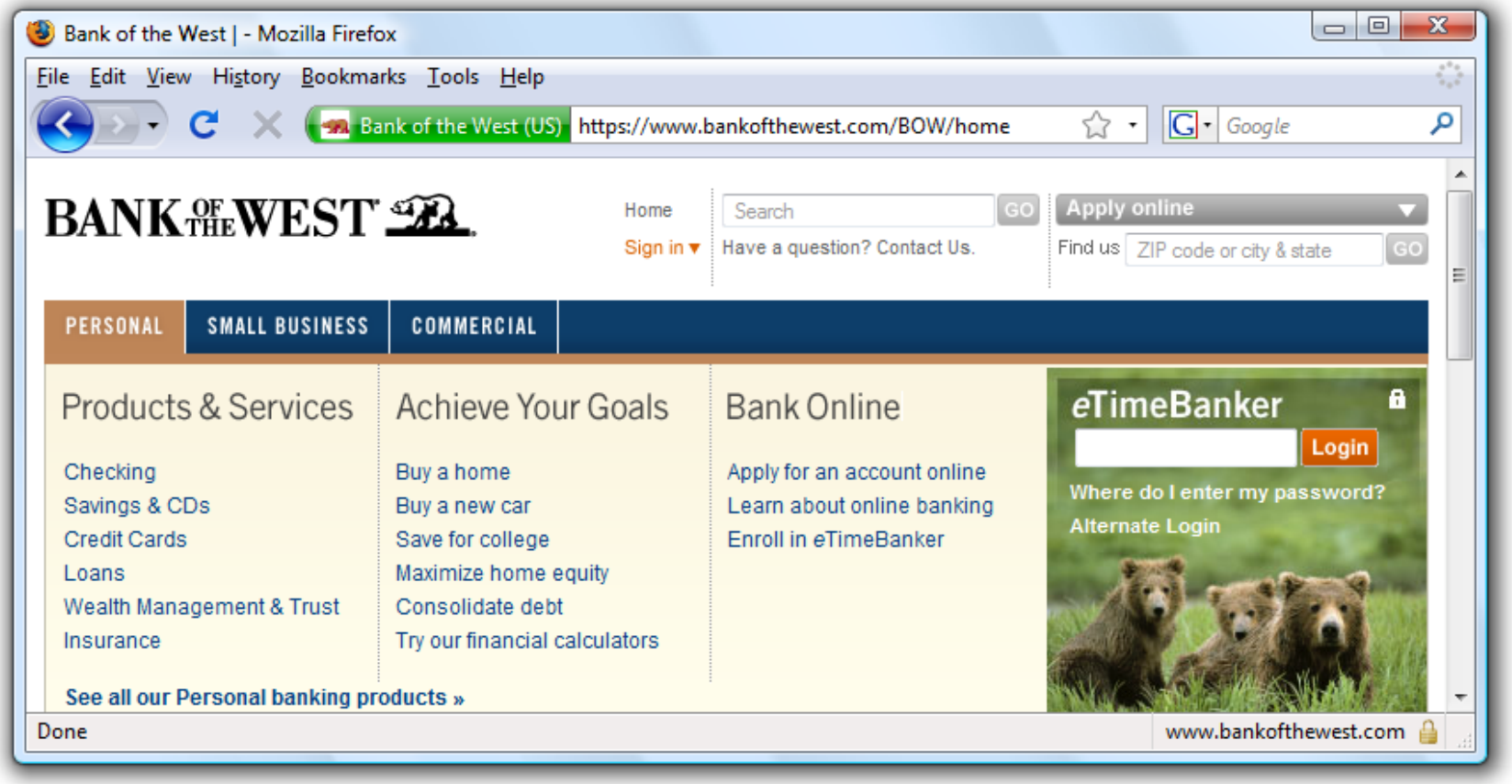

Bank of the West - Home
https://bankofthewest.com
BANK OF THE WEST
Personal
Small Business
Commercial
Checking & Savings
Credit & Loans
In
Online Banking
Username
Enter Username
Password
Enter Password
Forgot Password
Sign In
Enroll ›
Sign in to other services ›


Personal Banking - PNC Bank - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://www.pnc.com/webapp/unsec/homepag
Google
Most Visited
Getting Started
Latest Headlines
PNC
LEADING THE WAY
HOME
SECURITY ASSURANCE
LOCATE PNC
CONTACT US
CUSTOMER SERVI
Search
PERSONAL
SMALL BUSINESS
CORPORATE & INSTITUTIONAL
ABOUT PNC
Online Banking Sign On
User ID:
SIGN ON
Forgot Your User ID or Password?
New to Online Banking?
Get Started Now!
Learn More
View Demo
Sign On to Other Services:
Select Service
PNC Bank Select Reward
Visa® Platinum Car
Take advantage of a 0.99%
Introductory APR throug
March 31, 2010 o
Balance Transfers
Learn More
1 2 3 4
PNC Security Assurance
Products and Services
Solutions
FDIC
Important FDIC Information
PNC Bank is participating in the FDIC's Transaction Account Guarantee Program. more
Two of America's best-known banks. Now simply one of America's best.
Making the transition to PNC as easy as possible for you.
PNC's wide range of services can make banking easier, and more convenient than ever. See why PNC's the smart choice for help in meeting your financial goals.
Online Banking and Bill Pay
Checking
Savings
Loans and Lines of Credit
Cards
Whatever challenges and opportunities lie ahead, PNC can help. See why working with PNC to plan for life's greatest milestones is the smart choice.
Making the Most of Your Money
Virtual Wallet
Planning for Retirement
Saving for Education
Buying a Home
Done
www.pnc.com/webapp/unsec/homepage.var.cn

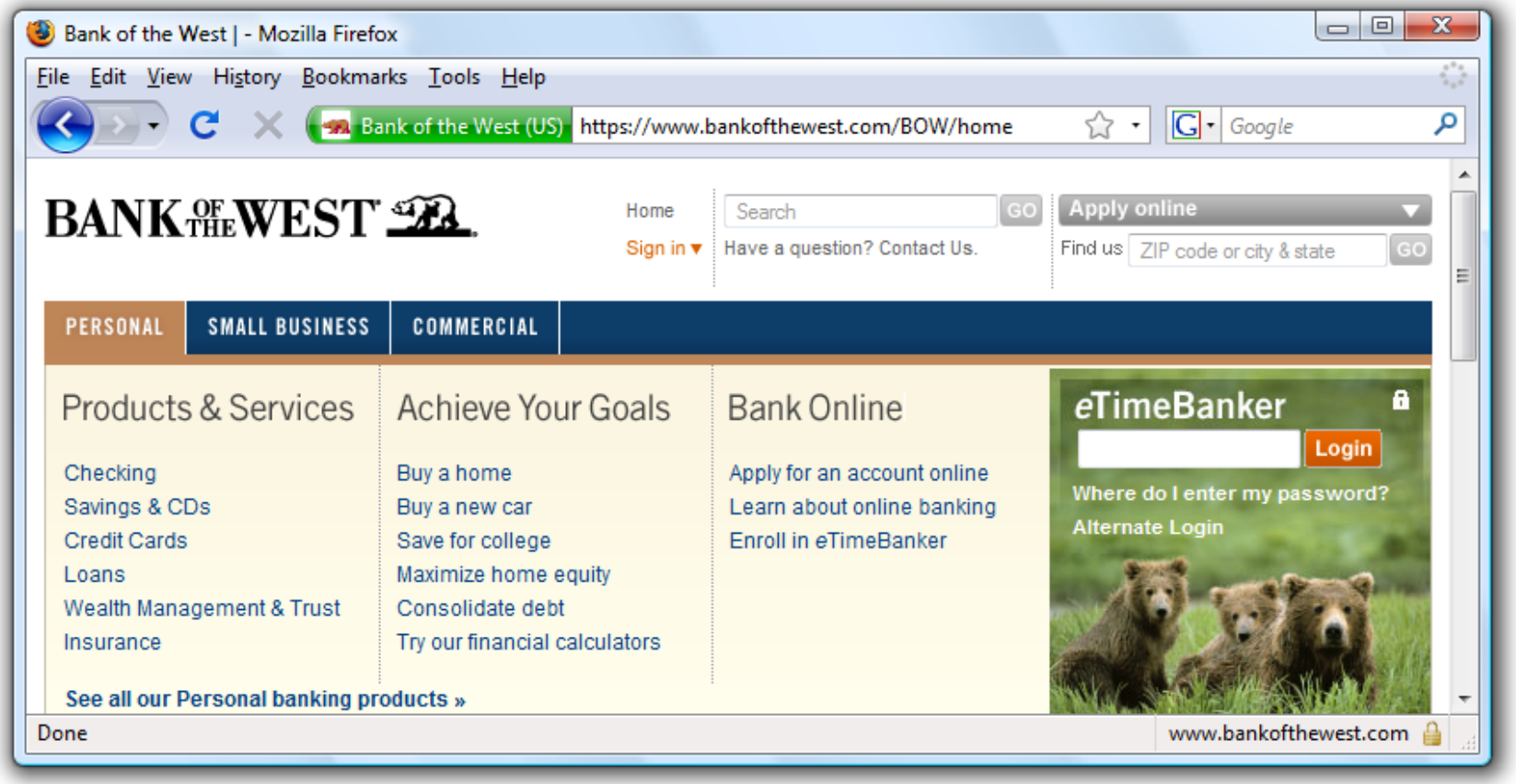

Wachovia - Personal Finance and Business Financial Services - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.wachovia.com/
WACHOVIA
LOGIN
User ID:
Remember my User ID
Password:
(case sensitive)
Service:
Choose a service...
Login
Forgot User ID or Password?
Retirement Plan Participants: Login
Education Loan Customers: Login
PERSONAL FINANCE
Online Services
Online Banking with BillPay
Mobile Banking
Online Brokerage
More...
Retirement Planning
Tools & information for
Lifetime Retirement Planning
Investing
Accounts & Services
IRAs
More...
Banking
Checking
Savings & CDs
Credit Cards
Check Cards
More...
Lending
Mortgage
Home Equity New!
Education Loans
Vehicle Loans
Rates
Mortgage Rates


evenxi.com
Log in to your PayPal account
PayPal
Email
Password
Log In
Forgot your email or password?
Sign Up
About | Account Types | Fees | Privacy | Security | Contact | Legal | Developers
Copyright © 1999-2017 PayPal. All rights reserved.

Check for “green glow” in address bar?



Check for Everything?



“Browser in Browser”