## 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)



 Everyone agrees in advance on a well-known (large) prime p and a corresponding g: 1 < g < p-1</li>



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

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



 $A = g^a \mod p$ 

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

4. Alice sends  $A = g^a \mod p$  to Bob

5. Bob sends  $B = g^b \mod p$  to Alice



В

- g<sup>b</sup> mod p = B
- 6. Alice knows {a, A, B}, computes
  K = B<sup>a</sup> mod p = (g<sup>b</sup>)<sup>a</sup> = g<sup>ba</sup> mod p
- 7. Bob knows {b, A, B}, computes
  K = A<sup>b</sup> mod p = (g<sup>a</sup>)<sup>b</sup> = g<sup>ab</sup> mod p
- 8. K is now the shared secret key.



While Eve knows {p, g, g<sup>a</sup> mod p, g<sup>b</sup> mod p}, believed to be *computationally infeasible* for her to then deduce K = g<sup>ab</sup> mod p. She can easily construct A·B = g<sup>a</sup>·g<sup>b</sup> mod p = g<sup>a+b</sup> mod p. But computing g<sup>ab</sup> requires ability to take *discrete logarithms* mod p.



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



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



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

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



 $A = g^a \mod p$ 

4. Alice sends  $A = g^a \mod p$  to Bob

5. Mallory prevents Bob from receiving A



 $A = g^a \mod p$ 

6. Mallory generates her own a', b'

7. Mallory sends  $A' = g^{a'} \mod p$  to Bob



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

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



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

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



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*



## 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 ...

 $C \rightarrow S: GET http://mybank.com/$  $S \rightarrow C$ : page, including a login form  $C \rightarrow S$ : POST http://mybank.com/login? u=USER&p=PASSWD [server marks this session as authenticated]  $S \rightarrow C$ : Set-Cookie: sessionid=NONCE (Cookie is an "authenticator" for session)  $C \rightarrow S$ : 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
- 3<sup>rd</sup>-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



Ways to make them better?

### **IEEE Symposium on Security & Privacy**

The 2012 symposium will mark the 33<sup>rd</sup> 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 passwordcracking 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

[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)

				Us	sabili	ty		Dep	loyał	oility			Sec	urity						
	The Quest to Rep													2						
A Framework for C	The Quest to Replace Passwords: Framework for Comparative Evaluation of Web Authentication Schemes*													tion	s stron	ng	.Ventue			
Joseph Bonneau University of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk	-Effortess Users	arry	ffortless n	lse rugre	ry-from-Loss	ost-per-User	atible watible	arv	Physical-Observa	largeted-Imperson Throttled-Guessin,	Inthrottled-Guess Internal-Observat	.eaks-from-Other Phishing	Theft Third-Party	plicit-Consent						
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	df	escribed in	eference	temorywise calable-for-	othing-to-C	hysically-E asy-to-Lear	flicient-to-U	asy-Recove	ccessible egligible-C	erver-Comp rowser-Con	lature on-Propriet	esilient-to-l	esthent-to- esilient-to-	esultent-to-	esuient-to-l esilient-to-l	esilient-to-7 o-Trusted-7	equiring-E	nunkapte
		Category	Scheme	<u>A</u>	~	20	2	<u>e</u> E	E. 2		<u> </u>	S m	22	2	2 2 1	2 2	* *	~ ~	~	2
		(Incumbent)	Web passwords	ш	[13]		•	•	• •	•	•••	•••	•••		0			•••		2
		Password managers	Firefox LastPass	IV-A	[22]	0.	0	0.0		0		:		0	00	ŏ				
			URRSA	IV-B	[5]	•	T	•		2					0	0	۰	ŤŤ	• •	5
		Proxy	Impostor		[23]	0.	•	٠		•	•	• •	•		0	0	•	•		
			OpenID	IV-C	[27]	0.	•	0 0	• •	••	••	•	••	o	οö	Ö	•	• =	•	
			Microsoft Passport		[43]	0.	•	ō •	•	•	•	•	•	ø	οŏ	Ö	•	•	•	
		Federated	Facebook Connect		[44]	0.	•	• •	•	••	••	•	•	0	0 0	o	•	•		
			BrowserID		[45]	0.	•	•			•••	0	•	0	00	0		•	•	
			OTP over email	IVD	[46]	0.	-			-			-	0	00	0				
		Graphical	PCCP	IV-D	[7]		-		22		=:	= :								
		-	GrIDeure (original)	IV-F	[47]	-	÷		00		÷				-			•••		-
			Weinshall	IV-L	[30]		•	Ē			•			0	ē					
		Cognitive	Hopper Blum		[49]		•				••	•	•	0	•			• •		
			Word Association		[50]		٠	٠	• •	0 0	••	•	•					••	• • •	
			OTPW	IV-F	[33]			•		•	•	•	• •		• •	• •		• •	• • •	•
		Paper tokens	S/KEY		[32]			•	<b>_</b>	•	•	•	••		• •	• •	• •	•	•••	
			PIN+TAN		[51]			•	<u> </u>	0	0	•	••		••	••	••	• •	•••	
		Visual crypto	PassWindow		[52]	•	_	_			0	-	•	0	••	••	••	<u> </u>		
			RSA SecurID	IV-G	[34]		Ξ		00	2 🗐				н						
		TT-shows to be a	rubikey		[33]				20	5 🗐				н			- 2			
		Hardware tokens	CAP reader		[54]		1			5 🗐						• •	. 2			5
			Pico		[8]			•	0 0	5	ΞΞ			•						
			Phoolproof	IV-H	[36]		0	•	0 0	<b>&gt;</b>	0 0	0	•	•		• 0		• •		
			Cronto		[56]		0	٠	0 0	> 🔳	•	•	•	•	• •	• 0	• •	• •	• • •	
		Phone-based	MP-Auth		[6]	1	0	٠	0	0	0 0		•		0		٠	••	•••	
			OTP over SMS			••	0	٠	<b>_</b> c	0	0	•	••	۲	• •	• 0	• •	0	•	
			Google 2-Step		[57]		0	•	0 0	0 0	0	•	•	0	0	•	• •	••	•••	2
			Fingerprint	IV-I	[38]			•	0		0		0							
		Biometric	Iris		[39]				0		0.0		8							
			Personal Imenuladara		[40]	0	-	<u> </u>				-			v					
		Recovery	Preference-based		[50]	0			0	0	••				0					5
		Recovery	Social re-auth		[60]		•				••		0	0		• 0	• •	•	•	2
			ooona ro-aaan		[[00]		-	5		_				1						

•= 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.

						U:	sabilit	ty	D	eploya	ability		Security	r	
The	Quest to Replace	e Passwords:									_				
A Framework for Compa	rative Evaluatior	n of Web Authe	ntication Schem	es*				U	se	er (	do	esn	't h	ave	e to
Joseph Bonneau Co University of Cambridge Micro Cambridge, UK Redn	rmac Herley Paul osoft Research Carl	C. van Oorschot leton University wa. ON. Canada	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK			2		m	er	nc	oriz	ze a	any	thin	g
jcb82@cl.cam.ac.uk cormac	@microsoft.com paulv	@scs.carleton.ca fr	ank.stajano@cl.cam.ac.ul	section		Efforte: Users arry	fortless	(N	/e	ak	er	: ju	st 1	se	cret)
https://www.cl.cam.ac.u	uk/techreports/UCA	AM-CL-TR-817.p	odf	cribed in	srence	torywise- able-for-l hing-to-C	sically-Ef	zient-to-l 2quent-E	y-Recove essible	ligible-C er-Com	wser-Con ure - Proprie	lient-to- lient-to- lient-to-	lient-to- lient-to- lient-to-	lient-to- Trusted- uiring-E inkable	
		Category	Scheme	Des	Refe	Men Scal Noti	Phy. Easy	副	Eas) Aco	Serv Serv	Mat Non	Resi Resi Resi Par	Resi Resi Resi Resi	Resi No-' Req Unli	
		(Incumbent)	Web passwords	III	[13]	V •	•	• •	• •	•••	•••	0		••••	
		Password managers	Firefox LastPass	IV-A	[22] [42]	0 0 0	0.0	•	•	••	•••	0000		••••	
		Proxy	URRSA	IV-B	[5]		:	0		• •	•	• •	0.0		
			OpenID	IV-C	[27]	0	0 0			•		0000		• •	
			Microsoft Passport		[43]		0.	•	• •		• • =	0000	•	• •	
		Federated	Facebook Connect		[44]	0	0 •	• •	• •	•	• • =	0000	•	•	
		locitico	BrowserID		[45]	0	0 •	• •	• •	•	• •	0000	•	• •	
			OTP over email		[46]	0	•	•	• •	•	• = •	0000		• •	
		Graphical	PCCP	IV-D	[7]	•	•	0 0	•	•	• •	• •	• •	••••	
		Oraphical	PassGo		[47]	•	•	00	•	•	• • •	۰		••••	
			GrIDsure (original)	IV-E	[30]	•	•	00	•	•	•	•	-	••••	
		Cognitive	Weinshall		[48]			==		•		0.		••••	
		Coginate	Hopper Blum		[49]							••			
			Word Association	TUE	[50]	•	-	• •		-					<u>'</u>
			OIPW	IV-F	[33]	_		_							
		Paper tokens	5/KE I DINATAN		[32]										
		Visual ammto	PIN+IAN DeseWindow		[51]		-		-	0					
		visual crypto	Passwindow RSA SecurID	IVG	[34]	-	-	0 0	글을	-					
			Vubikey	14-0	[54]			00	•						
		Hardwara tokana	Ironkey		[54]		0 0	0 0	i i	•		• •			
		Haluwale tokens	CAP reader		[55]		•	0 0			• • =				
			Pico		[8]		•	0 0			•				
			Phoolproof	IV-H	[36]	0	٠	00	0	00	•				7
			Cronto		[56]	0	•	0 0		0	• • =				
		Phone-based	MP-Auth		[6]	0	•	0	0 0	0	•	0	•		
			OTP over SMS				•	0	00					0 = • •	
			Google 2-Step		[57]	0	•	0 0	0 0		••=	0000			
			Fingerprint	IV-I	[38]		0 •	0	0		0	• •		••	
		Biometric	Iris		[39]	• • •	• •	0	0		0	• •		• 0	
			Voice		[40]		• •	0	0	0	0 0	• •			
			Personal knowledge		[58]	•	•	• •	•••	•	•••				
		Recovery	Preference-based		[59]	•	•		•						
			Social re-auth.		[60]	•	•		•	• = •	• • • =				£

•= offers the benefit;  $\mathbf{o}$ = almost offers the benefit; no circle = does not offer the benefit.

	The Orest to Der	la an Danamandar					Usabilit	ty	De	eployal	bility	;	Security			
A Framework for C	omparative Evalua	ntion of Web Auther	ntication Schem	es*					С	OC	yni	tive	ly p	orac	ctica	
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 fro	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK unk.stajano@cl.cam.ac.uk	in section		e-Effortless r-Users	Carry Effortless am	-Use Errors	fc ad	or i CC	JS OU	er h nts	avi	ng	man	ıу
https://www.or.ca		Category	Scheme	Described	Reference	Memorywi Scalable-fo	Vothing-to Physically- Easy-to-Le	Efficient-to	Accessible	Negugibie- Server-Con Browser-Co	Mature Non-Propr	Kesilient-to Resilient-to Resilient-to Resilient-to	Resilient-to Resilient-to Resilient-to Resilient-to	No-Trusted Requiring- Unlinkable		
		(Incumbent)	Wah passwords	Ē	1(12)	FU						0				
		(incumbent)	Web passwords		[15]							<u> </u>				
		Password managers	Firefox LastPass	IV-A	[22]	0.	000					0000				
			URRSA	IV-B	[5]	•	•	0				0	0 0	••		
		Proxy	Impostor		[23]	0.	• •		• •	• •	•	• •				
			OpenID	IV-C	[27]	0.	00	•	• • •	• = •		0000				
			Microsoft Passport		[43]	0.	• • •	•	• • •	•	• =	0000	• •	•		
		Federated	Facebook Connect		[44]	0.	• • •	•	• • •	•	•	0000	• •			
			BrowserID		[45]	0.	• •	•	• • •	• •	• •	0000		•		
			OTP over email	TUD	[46]		••		•••		•	0000		•		
		Graphical	PCCP	IV-D	[7]			00								
			Passuo CelDaura (ariainal)	NE	[47]			00								
			Weinshall	IV-E	[30]											
		Cognitive	Hopper Blum		[40]				•							
			Word Association		150		• •	• 0			•					
			OTPW	IV-F	[33]		•		• = •							
		Paper tokens	S/KEY		[32]		•	0	• = •	• = •						
			PIN+TAN		[51]	il i	•	0	0 0	•						
		Visual crypto	PassWindow		[52]					•	•					
			RSA SecurID	IV-G	[34]	I I	•	00		•	•			•••		
			Yubikey		[53]		•	00	•	•						
		Hardware tokens	Ironkey		[54]	••	00	00	•	•••						
			CAP reader		[55]			00		•						
			Pico	IV II	[8]			00	0.0							
			Cronto	IV-H	[30]			00	Ŭ							
		Dhana hasad	MP-Auth		[50]	4	•	0	0 0 0	0	•	0				
		Phone-based	OTP over SMS				• •	0	00							
			Google 2-Step		[57]		•	0 0	0 0	•	• =					
			Fingerprint	IV-I	[38]	••	• 0 •	0	0		0	• •		••		
		Biometric	Iris		[39]	••	• •	0	0		0			• •		
			Voice		[40]	••	• •	0	0 0	0 0	0	• •		••		
			Personal knowledge		[58]	0	•	• •	• • •		••					
		Recovery	Preference-based		[59]	0			•							
			Social re-auth.		[[00]											

•= 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 De	nlass Deservender					Usabilit	y	D	eployat	oility		Securit	у		
A Framework for C	omparative Evalu	ation of Web Authe	ntication Schem	es*					N	0	ph	iysi	cal	obj	ect	
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 fro	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK ank.stajano@cl.cam.ac.ul	section		-Effortless Users	fortless	lse rrors	(v a	ve ny	ak wa	ær: ay)	yo	u ca	arry	it
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	odf	escribed in	eference	temorywise calable-for	hysically-E asy-to-Lea	fficient-to-l tyrequent-E	asy-kecov ccessible	egugible- erver-Com 'rowser-Co	fature 'on-Propri	esilient-to esilient-to esilient-to esilient-to	esilient-to esilient-to esilient-to	esilient-to o-Trusted equiring-l	липкарів	
		Category	Scheme	<u> </u>	×	5.05	2 9, 12	E. Z 6	2 43	2 2 8	NN N	8 N N N	***	****	2	
		(Incumbent)	Web passwords	ш	[13]		• •	• • •	• •	•••	••	0				
		Deserved an end	Firefox	IV-A	[22]	0.00	00	• •	•	••	••	00			Þ	
		Password managers	LastPass		[42]	0.0	00	• •	•	• •	•	0000	0.	• = • •	▶	
		2	URRSA	IV-B	[5]	•	•	0		• •		0	0		Þ	
		Proxy	Impostor	1	[23]	0	• •		• •	• 0	•	• •	•			
			OpenID	IV-C	[27]	0.00	00		• • •	• = •	••	0000		• •		
			Microsoft Passport		[43]	0			• •	•	• =	0000				
		Fadaratad	Facebook Connect		[44]	0.					•	0000		•		
		rederated	BrowserID		[45]					. 0	0.	0000				
			OTP over email		[45]							0000				
			DCCP	IVD	[40]			0.0								
		Graphical	PeecCo	14-D	47											
		-	Passoo	TVE	[47]			00							-	
			GriDsure (original)	IV-E	[30]											
		Cognitive	Weinshall		[48]			==:								
			Hopper Blum		[49]											
			Word Association		[50]		•••	• • •		•					-	
			OTPW	IV-F	[33]		•		• = '	•	•••					
		Paper tokens	S/KEY		[32]		•	0	•	• = •	••		•••	$= \bullet \bullet \bullet$		
			PIN+TAN		[51]		•	0	0	• •	••			$0 \bullet \bullet \bullet$	<u>•</u>	
		Visual crypto	PassWindow		[52]				==!	• = •	• =				Þ	
			RSA SecurID	IV-G	[34]		•	00		•	•			• = • •		
			Yubikey		[53]		•	00	•	•	•			• = • •		
		Hardware tokens	Ironkey		[54]	0.	0 0	00	•	••	•	• •	•			
			CAP reader		[55]		•	0 0		•	•					
			Pico		[8]			00			•			$0 \bullet \bullet \bullet$		
			Phoolproof	IV-H	[36]		•	00	0	0 0	•		0		Þ	
			Cronto		[56]		•	00		• •	• =		0.0.0			
		Phone-based	MP-Auth		[6]		•	0 0	0 0	0	•	0				
			OTP over SMS				•	0	0 0	•	••			0 0 0		
			Google 2-Step		[57]	3	•	00	0 0	•	•	000				
			Fingerprint	IV-I	[38]		• • •	0	0		0	• •				
		Biometric	Iris		[39]		• • •	0	0		0	• •		• 0		
			Voice		[40]		• 0 •	0	0	0 0	0	• 0				
			Personal knowledge		[58]	0	• •	• • •	• •	• = •						
		Recovery	Preference-based		[59]	0	• •		•	• •		0				
		inconcery.	Social re-auth.		[60]		• •		•	•	0		00.	• = • •	2	
					[00]	C		1				C.				

•= 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.

#### Usability Deployability

Security

or: upor chooke)

No user action required

#### 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 University	Frank Stajano <sup>†</sup> University of Cambridge						()	VV	ec	an	e	•	u	5E	;1	5	JE	ans)
Cambridge, UK jcb82@cl.cam.ac.uk	Redmond, WA, USA cormac@microsoft.com	Ottawa, ON, Canada paulv@scs.carleton.ca fro	Cambridge, UK ank.stajano@cl.cam.ac.uk	ection		fortless	rry		e 213	-from-Lo	t-per-Us	atible	ý	ysical-O rgeted-In	rottled-C uthrottled	ternal-Ol aks-from	ishing oft	ind-Party	licit-Con	
https://www.cl.ca	m.ac.uk/techreports	s/UCAM-CL-TR-817.p	df	cribed in s	crence	norywise-E lable-for-U	hing-to-Ca	y-to-Learn	zient-to-Us equent-Ern	y-Recovery	ligible-Cos	vser-Compa	ure - Proprieta	ilient-to-Ph ilient-to-Ta	llient-to-Th llient-to-Uh	ilient-to-Im ilient-to-Le	llient-to-Ph	Trusted-Th	uiring-Exp inkable	
		Category	Scheme	Des	Ref	Men	Not	Eas	Ц.	Eas	Neg	Broi	Non	Resi Resi	Res	Resi	Res	No-	Vnl	
		(Incumbent)	Web passwords	III	[13]		•	•	• •	•				0			•		••	
		Password managers	Firefox	IV-A	[22]	0.	00	•	•				•	00				: <u> </u>	•••	
			LastPass	TUD	[42]			-		<u> </u>				00	~ ~	<u> </u>				
		Proxy	UKRSA Impostor	IV-B	[23]				Ŭ				•	• •		ö				
			OpenID	IV.C	[27]	0	• Ö	0		•		•		0 0	õ õ	- •			•	
			Microsoft Passport	IV-C	[43]	0	• 0	ē	•			•		ōŏ	0 0			i 🗐 🤇		
		Federated	Facebook Connect		[44]	0.	. 0	•		•		•	• =	0 0	0 0		•			
		rederated	BrowserID		[45]	0		•		•		0	• •	0 0	0 0		•		•	
			OTP over email		[46]	0	•	•	۰	•		•	•	0 0	0 0				•	
			PCCP	IV-D	[7]	-	•	•	0 0	•	•	•	•	•	0				••	
		Graphical	PassGo		[47]	ıl 👘	•	•	0 0	•	•	•	• •	•			•		••	
			GrIDsure (original)	IV-E	[30]	il –	•	•	0 0	•	٠	٠		۲			•	) • (	••	
			Weinshall		[48]	il	•				•	•	•	• •					••	
		Cognitive	Hopper Blum		[49]	il 👘	•		= =		•	•	•	• •					••	
			Word Association		[50]		•	•	• •	0		•	•	=			•		••	
			OTPW	IV-F	[33]		-	•	= =	•	٠	•		•					••	
		Paper tokens	S/KEY		[32]			•	0	•	•	•	• •				0	<b>•</b> • •	••	
		ruper tokens	PIN+TAN		[51]			•	0	0	0	•		•					• •	
		Visual crypto	PassWindow		[52]						0	•	• =					•	••	
		· isual cippio	RSA SecurID	IV-G	[34]		-	•	0 0			•	• =						••	
			Yubikey		[53]			•	0 0			•	•					) 🗐 (	••	
		Hardware tokens	Ironkey		[54]	0	o	0	0 0					. 0		0			••	
		Hardware tokens	CAP reader		[55]			•	0 0			•	•						••	
			Pico		[8]				0 0				•						••	
			PhooIproof	IV-H	[36]	1	0	•	0 0		000	<b>o</b>	•			0.			••	
			Cronto		[56]		0	•	0 0		0	•							••	
		Phone based	MP-Auth		[6]	4	0		0	0	0 0		•	0					• •	
		rnone-based	OTP over SMS		101		0	•	0	0	2	•								
			Google 2-Step		[57]		0	•	0 0	0	>	•	•	0 0					• •	
			Fingerprint	IV-I	[38]		• 0	•	0	-	2		0	•	•			•	•	
		Biometric	Iris		[39]			•	0	-	>		0	•	۲			•	0	
			Voice		[40]			•	•		0 0	0	0	•	0			•	•	
			Personal knowledge		[58]	0	•	•	• •	•		•		-			-		••	
		Recovery	Preference-based		[59]	0	•	•		0	• •	•		0					••	
		in the second se	Social re-auth.		[60]		•	•	٠		••	•	0	0		0 0			• •	
					- · · ·															

•= offers the benefit; •= almost offers the benefit; no circle = does not offer the benefit.

#### 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 University	Frank Stajano <sup>†</sup> University of Cambridge						i	n	-У	0	ur	<b>`_</b> ł	າຍ	a	d	S	ch	em	e)
Cambridge, UK	Redmond, WA, USA	Ottawa, ON, Canada	Cambridge, UK			less	5	20		"-Lo	- IIe	3	0	0-12	u-pa	1-0	mou ou	0	6 6 0 1		
JCD82@C1.Cam.ac.uk	cormac@microsoji.com	paurv@scs.carieion.ca jre	unk.siajano@ci.cam.ac.uk	ctio,		ton	121			rs from	1	ple	IQUI .	y sicc	gete	hro	ks-J chin	\$	cit-		
				so		E.	5.64	OL E	Use	e c	1 oct	Dati	pdu.	Phys	Tan,	Unt	Lea	L le	n la		
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	df	d ir	9	vise	2 2 2	Lea Lea	10-1	-II-I	e e	E.	Ş.	-to-	\$ \$	9 9	\$ \$	2	- E - E	16	
				ije	enc	12-3	-84	to-I	-Jura	Rec	disi	şŲ	rer a	ent	ent	ent	ent	ent	in in i	Kar	
				csci	efer	in a	oth.	-ASI	hci	is for	ces	e a	atu	-mo	lisa	sili sili	sili	Sil.	mba	100	
		Category	Scheme	Ă	Ř	N O	5 Z B	Σĕ	Ξ.	E' 🗳	Ϋ́×	5	S NX	žŽ	2 2	2 2	2 2	2	ž nž i	5	
		(Incumbent)	Web passwords	Ш	[13]		•		•	••	••	•	•••	•	0			•	•••		
		Password managers	Firefox	IV-A	[22]										0	0					
			LIBRSA	IV-B	[42]					0		0	•	~	0	0				1	
		Proxy	Impostor		[23]	0	•	•		•	•	•	0	•	0	0		•			
			OpenID	IV-C	[27]	0 0		0 0	•		• •			• 0	00	Ö	۲	•	٠	=	
			Microsoft Passport		[43]	0	•	• •	•	• •	•		••	o	00	0 0	۰	•	•	=	
		Federated	Facebook Connect		[44]	0		•	•		•		••	0	00	00		•		<u> </u>	
			BrowserID		[45]		1.1								00		Ξ.				
			PCCP	IV-D	[40]		-		0						• 0						
		Graphical	PassGo	11-2	[47]	d l	ě		0	•				•	•						
			GrIDsure (original)	IV-E	[30]		٠	•	0	• •	-		•		۲			•		•	
		Comitive	Weinshall		[48]	1	٠	=			•		•	• 0	۲		•	•	•••	•	
		Coginuve	Hopper Blum		[49]	l	•				••		•	• •	•		• •		•••		
			Word Association		[50]	4	•	•	•	00	••		• = •	•	_			•	•••	2	
		Down to have	OIPW	IV-F	[33]										H		H				
		Paper tokens	PIN+TAN		[52]				Ξ.	0 0		5									
		Visual crypto	PassWindow		[52]						-	>		0						5	
			RSA SecurID	IV-G	[34]			•	0	0				•			•	•	•	<b>N</b>	
			Yubikey		[53]			٠	0	0	•		••	۰	•			•	•	•	
		Hardware tokens	Ironkey		[54]	0		0 0	0	0	•	•	••	•	0	0		•	•••		
			CAP reader		[55]			•	0	0			••							2	
			Pico Dhaalaanaf	IN II	[8]		<u> </u>	-	0				_				H			4	
			Cronto	IV-H	[30]		õ		ŏ	0	č	š ~ .	• •		H		H				
		Phone-based	MP-Auth		[50]	4	0		0	0	0 0			•	0						
		r none-based	OTP over SMS		1.43		0	•		0 0	0			•				0	•	•	
			Google 2-Step		[57]		0	•	0	0 0	0		••	0	0			•	•••	•	
			Fingerprint	IV-I	[38]		•	• •	0		0		0	۲					••		
		Biometric	Iris		[39]			•	0		0		•						• •	-	
			Voice		[40]										- 9					-	
		Pacouany	Preference-based		[38]	0	-								0					5	
		Recovery	Social re-auth.		[60]		•		Ē		•		• •	0	Ě.		0	•	•	2	

Deployability

(E.g.: not a do-crypto-

Usability

•= offers the benefit; •= almost offers the benefit; no circle = does not offer the benefit.

#### 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

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

Univers Cambridge, UK Ottawa, ON, Canada o-Trusted-Third-Part quiring-Explicit-Con emorywise-Effortles. section Physical Phishing frank.stajano@cl.cam.ac.uk paulv@scs.carleton.ca Nothing-to-Carry Physically-Effortless Compatible Scalable-for-Users egligible-Cost-pe Compatible Theft Sasy-Recovery-fro requent-Errors Proprietary flicient-to-Use ev-to-Learn .Е https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.pdf esilient-toģ esilient-tolinkable Described Reference Resilient-Resilientccessibl Resilient-Resilient Resilient DWSer ver ature 2 Category Scheme Ш Web passwords [13] 0 (Incumbent) 0 Firefox IV-A [22] 0 o Password managers LastPass [42] 0000 URRSA IV-B [5] 0 Proxy Impostor [23] OpenID IV-C [27 0 Microsoft Passport [43 Facebook Connect [44] Federated BrowserID [45] OTP over email [46] 0 IV-D [7] PCCP Graphical [47 PassGo GrIDsure (original) IV-E [30] Weinshall [48] Cognitive [49] Hopper Blum Word Association [50] IV-F [33] OTPW = [32] S/KEY Paper tokens 0 PIN+TAN [51] ο PassWindow [52] Visual crypto RSA SecurID IV-G [34] • **o** o Yubikey [53] o 0 [54] Ironkey 0 Hardware tokens CAP reader [55] Pico [8] Phoolproof IV-H [36] [56] Cronto MP-Auth Phone-based [6] 0 0 OTP over SMS Google 2-Step [57 Fingerprint IV-I [38] [39] Iris o Biometric Voice [40] 0 o o Personal knowledge [58] ο ο [59] 0 Preference-based Recovery Social re-auth. [60] o =

•= offers the benefit; •= almost offers the benefit; no circle = does not offer the benefit.

							Usabi	lity	De	ploya	ability	1		Secu	rity		
A Framework for C	The Quest to Re	place Passwords:	ntication Schem	oc*									u.	fiers			
A Flamework for C		ation of web Autre	inication Schem	63								5	ti u	8 z 9			
Joseph Bonneau University of Cambridge	Cormac Herley Microsoft Research	Paul C. van Oorschot Carleton University	Fran Wor	ı't	fr	ันร	str	ate		eg	git	u	se	ers		ty nsent	
jcb82@cl.cam.ac.uk	cormac@microsoft.com	paulv@scs.carleton.ca fr	ank.stajano@cl.cam.ac.uk	ction		fortles ers	ry rless	trom-1	l and	ble	alan	sical-	geted- ottled	rnal-C ks-fro	shing	d-Par cit-Co	
https://www.cl.ca	m.ac.uk/techreports	s/UCAM-CL-TR-817.p	odf	escribed in se	eference	emorywise-Eff alable-for-Us	othing-to-Carl tysically-Effor	hicient-to-Use frequent-Erro	cessible Cont	rver-Compati	owser-Compa ature 2n-Pronrietar	silient-to-Phy	silient-to-Ian silient-to-Thr	sauent-10- Uni ssilient-to-Inte ssilient-to-Lea	silient-to-Phi	o-Trusted-Thin quiring-Expli	nlinkable
		Category	Scheme	Ă	Ř	N S	N A A	2222	¥×	2 2 4	6 N 2	2	2 2 0	2 2 2	2 2	22	s
		(Incumbent)	Web passwords	Ш	[13]		• •	•••	• • •		•••		0		•		•
		Password managers	Firefox	IV-A	[22]	0.	000		•	••	•••	• •	0				•
		- ussingers	LastPass	RI D	[42]	0.	000		•		•	0	000	0 0			-
		Proxy	URRSA	IV-B	[5]								0	2			
			Impostor	WC	[23]		-							<u> </u>	-		-
			Microsoft Peseport	IV-C	[27]							ŏ	0 0				
		Enderstad	Facebook Connect		[45]							ŏ	0 0				
		Federated	BrowserID		[44]						00	0	00				
			OTP over email		[46]	0.	•		•			0	00				
		Graphical	PCCP PassGo	IV-D	[7] [47]		•				• • •	3	• •	٠			•
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49]		•		•			0	•		H		•
		Paper tokens	OTPW S/KEY	IV-F	[33] [32]	•		0							0	••	•
			PIN+TAN		[51]			• • • •		0	•••				• •		•
		Visual crypto	PassWindow	NV C	[52]	•	_					0					-
		Hardware tokens	Yubikey Ironkey CAP reader	14-0	[54] [53] [54] [55]	•	0		÷	•	••		0	0			•
			Pico		[8]			00				44					-
			Phoolproof	IV-H	[36]				0.0						н		
		Diana la sel	Cronto MD Auth		[20]	-	ă i		0				0		Η.		
		Phone-based	MP-Auth OTP over SMS		[0]		ě i		0	í .							
			Google 2-Step		[57]		0	000	0			0	0				•
			Fingerprint	IV-I	[38]			0	0		0					••	
		Biometric	Iris		[39]				0		0	•				• 0	
		L'Internet I to	Voice		[40]			• •	0 0		0 0	۲	0		- 8	••	
			Personal knowledge		[58]	0	• •		• • •						•		•
		Recovery	Preference-based		[59]	0	•		•		•		0				•
			Social re-auth.		[60]		•	• = • =	•		• •	0				) 🗏 🛛 !	0

•= 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 Rep	lace Passwords:					Usabili	ty	De	eployab	oility		Security	,		
A Framework for C	omparative Evalua	tion of Web Auther	ntication Schem	es*						R	ec	OVE	ery	is	q	uick,
Joseph Bonneau University of Cambridge Cambridge, UK icb82@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 fra	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK unk.stajano@cl.cam.ac.ul	. 5		tless	22	m-Loss		lo	W	-has	ssle	Э,	as	sured
https://www.cl.ca	m.ac.uk/techreports/l	UCAM-CL-TR-817.p	df	escribed in secti	eference	emorywise-Effor zalable-for-Users	othing-to-Carry hysically-Effortle asy-to-Learn	ficient-to-Use freauent-Ermrs asy-Recovery-fro	ccessible colinible Cont of	ezuguore-Cost-pr erver-Compatible rowser-Compatil	ature on-Proprietary	esilient- to- Physic esilient- to- Targei esilient- to- Thrott esilient- to- Unthr	esilient- to- Intern esilient- to- Leaks esilient- to- Phishi	esilient-to-Theft o-Trusted-Third-	equiring-Explicit nlinkable	
		Category	Scheme	Ã	R	NS	2 1 1	252	¥¥	B N S	ΝŇ	$R_{c}$	2 Z Z	22	2 2	
		(Incumbent)	Web passwords	III	[13]		• •	• • •	• •		••	0		••	••	
		Password managers	Firefox LastPass	IV-A	[22] [42]	0.	000	• •	•		•••	0 0 0 0 0 0 0 0		•	•••	
		Proxy	URRSA Impostor	IV-B	[5] [23]	•		•	•	• • •	•	0 • 0	0 • 0 •	•	••	
		Federated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]										•	
		Graphical	PCCP PassGo	IV-D	[7] [47]		: :	000		::	•	• •	• •	•••	••	
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]			• • •	•		•	• • •	::	•••	••• ••• •••	
		Paper tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]		:	00			::		•••	•••	•••	
		Visual crypto	PassWindow		[52]					•	•				••	
		Hardware tokens	RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55] [8]			0 0 0 0 0 0 0 0	•			• •	0		••• ••• ••• •••	
		Phone-based	Phoolproof Cronto MP-Auth OTP over SMS	IV-Н	[36] [56] [6]		0000		000	•	•	0	0.00	•••	•••	
		Biometric	Google 2-Step Fingerprint Iris Voice	IV-I	[57] [38] [39] [40]			000	0000	•	• • •		••	•••	0	
		Recovery	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0		• 0 • • • •	•		•••	0	o o •	•••	•••	

•= 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 Ponnesu	Cormoo Harlou	Paul C yan Oorachat	Eronk Staignat		١	V	Vo	rk	(S	f	0	^ ر	ISe	ers	5 V	//	pł	٦y	sical
University of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk	Microsoft Research Redmond, WA, USA cormac@microsoft.com	Carleton University Ottawa, ON, Canada paulv@scs.carleton.ca fr	University of Cambridge Cambridge, UK ank.stajano@cl.cam.ac.ul	k ini	(	d	isa	ak	bil	liti	ie	s/	CC	one	diti	or	າຣ	;	
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	odf	scribed in sec	ference	morywise-Eff	alable-for-Uše thing-to-Carr	ysically-Effor	icient-to-Use	requent-Error sy Recovery-fi	cessible	rver-Compatib	awser-Compan ature m-Proprietary	silient-to-Phys silient-to-Targ	silient-to-Thro silient-to-Unth silient-to-Inter	silient-to-Leak	silient-to-Thef	quiring-Explic linkable	
		Category	Scheme	Ď	Re	Me	No	Ph	99	E S	Ac	Sei	NON	Re	Re	Re	Re	2 2	
		(Incumbent)	Web passwords	Ш	[13]	]	٠	•	•	• •	$\mathbf{\vee}$	•••		0			• •		
		Password managers	Firefox LastPass	IV-A	[22] [42]	] 0 ] 0	• 0	0		• •	•		••	00	0 0	•	•	•••	
		Proxy	URRSA Impostor	IV-B	[5] [23]	) 0				•	•	•	•	• 0	0		•	••	
		Federated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]	00000		0 0 0						000000	000000	:	•	• • •	
		Graphical	PCCP PassGo	IV-D	[7] [47]	]	•		0	0 • 0 •					0	• •	•••		
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]	]	•		•	0 • 0 0				0.0		::	•••••••••••••••••••••••••••••••••••••••		
		Paper tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]	] ] ● ]				0 0 0 0						• •			
		Visual crypto	PassWindow		[52]	]					= <		••	• •					
		Hardware tokens	RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55]	] ] ]		0		0	•	•		• •					
		Phone-based	Phoolproof Cronto MP-Auth OTP over SMS	IV-Н	[36] [56] [6]		0000		0	0				•••	•••		• •		
			Google 2-Step Fingerprint	IV-I	[57] [38]		0	0	0	0 0	0		•	•	• •	• •	••		
		Biometric	Iris Voice		[39] [40]		••	0	0		0	, ,	00		•			•	
		Recovery	Personal knowledge Preference-based Social re-auth		[58] [59]	0	:		0	0 • • 0 • •	•••			0			•••		

Usability

Deployability

•= 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.

Security

iers

The Quest to Poplace Person	ndar			U	sability		Deployat	bility		Security			
A Framework for Comparative Evaluation of Web	Authentication Schen	nes*						Ε	.g.:	pla	ausi	ble	for
Joseph BonneauCormac HerleyPaul C. van OorseUniversity of CambridgeMicrosoft ResearchCarleton UniversCambridge, UKRedmond, WA, USAOttawa, ON, Can	hot Frank Stajano <sup>†</sup> ity University of Cambridge ada Cambridge, UK			\$\$2		-Loss	User	S	tartı	Jps	to	use	
jcb82@cl.cam.ac.uk cormac@microsoft.com paulv@scs.carletor	n.ca frank.stajano@cl.cam.ac.u	w section		-Efford Users Zarry	ffortless m Ise	rrors ry-from	ost-per- xatible npatible	tary	Physica Targetei Throttle Unthrot	Interna Leaks-fi Phishin	Theft Third-P xplicit-C		
https://www.cl.cam.ac.uk/techreports/UCAM-CL-TI	R-817.pdf	escribed in	eference	emorywise alable-for othing-to-(	tysically-E tsy-to-Lea ficient-to-l	frequent-E tsy-Recove	cessible gligible-C rver-Com owser-Com	ature on-Proprie	salient-to- salient-to- salient-to- salient-to-	silient-to- silient-to- silient-to-	ssilient-to- o-Trusted- quiring-E		
Cate	gory Scheme	Ă	Ř	N S N	E E E	Ec	B Se NG	NN	Re Re	$R_e$	2 2 2 2	5	
(Incumber	<li>t) Web passwords</li>	Ш	[13]	•	••	0.			0				
Password	managers Firefox LastPass	IV-A	[22] [42]	000	0	• •	• • •	•	000	•	• • • •		
Proxy	URRSA Impostor	IV-B	[5] [23]	•	•	•	• •	•	• •	°.	•		
Federated	OpenID Microsoft Passport Facebook Connect BrowserID	IV-C	[27] [43] [44] [45]				• • •				• •		
Graphical	PCCP PassGo	IV-D	[7] [47]		• 0	0.	• •		• •	••	•••		
Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]	•	• •	00	• • • • • •		•	::	••••		
Paper toke	ns S/KEY PIN+TAN	IV-F	[33] [32] [51]		•	0 0 0 0	• • • •			•••			
Visual cry	pto PassWindow		[52]	•			• •	•					
Hardware	tokens CAP reader Pico	IV-G	[34] [53] [54] [55] [8]	••		00000	• • •		• •	0			
Phone-bas	Phoolproof Cronto MP-Auth OTP over SMS Google 2-Step	IV-H	[36] [56] [6]	000000000000000000000000000000000000000	• 0 • 0 • 0	000000	0000		0				
Biometric	Fingerprint Iris Voice	IV-I	[38] [39] [40]				0000	0	• •		• • • 0 • •		
Recovery	Personal knowledge Preference-based Social re-auth.	e	[58] [59] [60]	0	• •	••	••••••••••••••••••••••••••••••••••••••	0	0	• • •	• • •	2	

•= 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.

							Usa	bility		Dep	loyab	ility			Secu	rity			
	The Ouest to Rep	place Passwords:													2				
A Enomorrowly for C	ammonotive Evolu	ation of Web Author	ntiontion Cohom	*								_			fe)				
A Framework for C	omparative Evalua	ation of web Authe	nucation Schem	es									_		_		_		
													$\mathbf{C}$	ar	ע ר		hk l	likc	2
Joseph Bonneau	Cormac Herley	Paul C. van Oorschot	Frank Stajano <sup>†</sup>										U	a	1 1			IIII	ر
University of Cambridge	Microsoft Research	Carleton University	University of Cambridge						22	5								4.99	
Cambridge, UK	Redmond, WA, USA	Ottawa, ON, Canada	Cambridge, UK			3			2	C.St	$\wedge$		"н	nc	II	nr		nt"	
jcb82@cl.cam.ac.uk	cormac@microsoft.com	paulv@scs.carleton.ca fr	ank.stajano@cl.cam.ac.uk	5		2 s	222		÷	1	je .				u	IIK		I I C	
				SCI.		8 2	54		z f	<u></u>	ld i								
				s		95	88	ES	EÈ	8	a di		<b>†</b> ∩	2 (	ρr	`\ <i>\</i>	2rc		
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	odf	-=	•	fo is	9 H	ea.	Pre F	2			i C			V		•	
				ĕ	ъč	E.S	8-1 alb	1-	le n	191	Ϋ́		2		22	2 2	si in	a	
				Ċ,	ere	10 fg	hin	y-t cie	y-k	ess Field	le la	24	lie	ilie ilie	ilie	ilie ilie	T'n'	ž.	
		Catagon	Cahama	Se	čef	5 8	to A	35	15	2 S	5	1ai Von	Ses	s s s	ses a	les Res	eg .	E C	
		Category	Scheme Web accounted	<u> </u>	1121	< 2	~~		~~~			~~			~~~	~~~		-	
		(incumbent)	Web passwords		[15]		-				Y			<u></u>					
		Password managers	FIFEIOX	IV-A	[22]								õ.						
			Lastrass	TVD	[42]				0						<u> </u>				
		Proxy	Impostor	IV-D	[23]		•							5	ŏ				
		-	OpenID	WC	[23]								0	000				-	
			Microsoft Passport	IV-C	[47]					•			0						
		Endorstad	Facebook Connect		[45]		. 0						0	0 0 0		ē			
		Federated	BrowserID		[44]		. 0				0		0	0 0 0		ē	•		
			OTP over email		[46]	0.	•	•					0	0 0 0					
			PCCP	IV-D	[7]		•	• 0	0.					0				•	
		Graphical	PassGo		[47]		•	. 0	• •	•	•							•	
			GrIDsure (original)	IV-E	[30]		•	• 0	0.	•	•	==				•		•	
			Weinshall		[48]		•			•	•	•	0		۲			•	
		Cognitive	Hopper Blum		[49]		•			••	•	•	0		۰			•	
			Word Association		[50]	1	•	••	0 0	••	•	•				•		•	
			OTPW	IV-F	[33]			•		•	•	• •						•	
		Paper tokens	S/KEY		[32]			• 🔳	ο •	•	•	••				0	••	•	
			PIN+TAN		[51]			• 🔳	0 0	0	•	••					••	•	
		Visual crypto	PassWindow		[52]	•				0	•	•	0				•••	•	
			RSA SecurID	IV-G	[34]			• 0	0		•	•	•					•	
			Yubikey		[53]			• •	0	•	•	•	•			••	•	•	
		Hardware tokens	Ironkey		[54]	0.	0	00	0	•	••	•	• •	D C	0	••	•••	•	
			CAP reader		[55]			• •	0		•	•	•				•••	•	
			Pico		[8]	••		0	0			•				• •	•••	•	
			Phoolproof	IV-H	[36]		0	• •	0	00	•	•				••	•••	•	
			Cronto		[56]		•	• •	0	0	•	•			0.		•••		
		Phone-based	MP-Auth		[6]		0	• •	0	00							•••		
			OTP over SMS				0		00	0									
			Google 2-Step	11.1.7	[57]				00	0	=-	-	00					-	
			Fingerprint	11/-1	[38]					0		0							
		Biometric	ITIS		[39]					0.0		~							
			Voice		[40]				-					9					
		D	Personal knowledge		[58]	0								<b>`</b>					
		Recovery	Secial re outh		[39]	<b>~</b>						~	~ `						
			Social re-auth.		[00]		•	•=				-	N.				= • :		

•= 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.
						Usabil	ity	D	eploya	ability	/		Secur	ity		
The Quest to Replace Pas A Framework for Comparative Evaluation of V	sswords: Web Authen	tication Schem	es*						_		ation	nation ng	tion r-Verifiers			
Joseph Bonneau University of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk bttps://www.cl.cam.ac.uk/tec	quire r: ver	s HTM y comn	L5 nc	5/. on	JS p	; lug	gin	IS	con per cael	ompatible	etary - Physical-Observ	<ul> <li>Targeted-Imperso</li> <li>Throttled-Guessi</li> <li>Truth mutiled-Guessi</li> </ul>	-Internal-Observe -Leaks-from-Othe	- Phishing - Theft	-1 mra-rarry Explicit-Consent	
	Category	Scheme	Described	Reference	Memorywi Scalable-fo	Notning-to Physically- Easy-to-Le	Efficient-to Infrequent-	Easy-Recor Accessible	Negligible-	Browser-C	Resilient-to	Resilient-to Resilient-to	Resilient-to Resilient-to	Resilient-to Resilient-to	No-1 rustea Requiring- Unlinkable	
(Incu	mbent)	Web passwords	Ш	[13]		••	• •	• •	••	• • •	•	0		•		
Passy	word managers	Firefox	IV-A	[22]	0.0		• •	•	••	•	• 0	0	ŏ		•••	
Proxy	y	URRSA Impostor	IV-B	[ <del>4</del> 2] [5] [23]	•		0	•••	• •	•	•	0	0	•	••	
Feder	rated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]				• • • • • • • •	•					• • • •	•	
Grap	hical	PCCP PassGo	IV-D	[7] [47]		•••	00	•	:	• •	•	• •	۲	•	•••	
Cogn	iitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]			• 0	•	•	•	0	•	•		• • • • • • • • •	
Paper	r tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]	•	:	0	•	•		•				•••	
Visua	al crypto	PassWindow		[52]	•				0	••	0					
Hard	ware tokens	RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55] [8]	00			•		••		0	0			
Phon	e-based	Phoolproof Cronto MP-Auth OTP over SMS Google 2-Step	IV-H	[36] [56] [6] [57]	• •			00000	00	••	•	0	0			
Biom	netric	Fingerprint Iris Voice	IV-I	[38] [39] [40]			0 0 0	0	0	000	•	•			0	
Reco	very	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0		• •		•	•••	0	•	000		•••	
-																

							Usa	bility		Depl	oyability	/		Securi	ity		
	The Quest to Re	place Passwords:												22			
A Framework for C	omparative Evalu	ation of Web Auther	ntication Schem	es*									5	nifie			
	•											tion	sing	Ne Ve			
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 fro	Frank Stajano <sup>†</sup> University of Cambrid Cambridge, UK unk.stajano@cl.cam.d	No	ot St	ju of	IS1	t a	r /ta	es	ea	rc	h	ernal-Observa iks-from-Other	ishing sfi	rd-Party icit-Consent	
			. · · · · · · · · · · · · · · · · · · ·				- y F		/ ιι	Jy				Lec	L L		
https://www.cl.car	m.ac.uk/techreports	s/UCAM-CL-TR-817.p	df	cribed	crence	torywis lable-fo	hing-to-	y-to-Le	equent- y-Recov	essible ligible-	wser-Con wre-Con wre	lient-to	tient-to lient-to lient-to	lient-to- lient-to-	dient-to-	I rusted- uiring-E inkable	
		Category	Scheme	Des	Ref	Men Sca	Not Phy	Effi	Eas	Aco Neg	Mat Mat	Res	Res Res	Res	Res Res	Req Unl	5
		(Incumbent)	Web passwords	Ш	[13]		•	•••	0.	•••			<u> </u>		•	•••	4 –
		Password managers	Firefox LastPass	IV-A	[22]	0	00			• •		0		ö			
			URRSA	IV-B	[42]	•		•	0			-	5	0	•	••	4
		Proxy	Impostor		[23]		•	•	•	• = •	• •	• • •	5	0		•	4
			OpenID	IV-C	[27]	0.	• 0	0.	••	••	••	• 0 0	000	۲	•	•	1
			Microsoft Passport		[43]	0.	• 0	•••		•	•••	00	000		•	•	1
		Federated	Facebook Connect		[44]				21				000			•	
			OTP over email		[46]	0.	•	•		••	•		000			÷	
		Gradial	PCCP	IV-D	[7]		•	• •	0.	•	•	•	0	۰	••		1
		Graphical	PassGo		[47]		•	• •	• •	•	• •	•			•	•••	4
			GrIDsure (original)	IV-E	[30]		•	• •	••	•	•					•••	1
		Cognitive	Weinshall Hopper Blum		[48]					• •							
			Word Association		[50]		ě	••	0 0	••	•	•					
			OTPW	IV-F	[33]			•	•	•	••	•		• •	••		1
		Paper tokens	S/KEY		[32]			•	• •	•	••	•		• •	0	•••	1
		87 1 to	PIN+TAN		[51]		_	•	00	0	•••	•			• •	•••	4
		visual crypto	Passwindow RSA SecurID	IV-G	[34]		-	• •	0								4
			Yubikev	11-0	[53]			• •	õ	•	••	•				••	
		Hardware tokens	Ironkey		[54]	0.	0	00	o 📃	•		•	2	0	••	•••	4
			CAP reader		[55]			• •	0		••			••	••	•••	1
			Pico	IV H	[8]			0	0		-						4
			Cronto	1 ү-п	[50]	-	õ	• •	ŏ	õ						•••	
		Phone-based	MP-Auth		[6]		0	• •	•	00		• •	>				4
			OTP over SMS			• •	0	•	0 0	0	••	•		0 .	• •	••	1
			Google 2-Step	11/2 7	[57]		0	• •	00	0	••	0 0		۰	••	•••	4
		Diamatria	Fingerprint	11-1	[38]					0	0						
		Biometric	Voice		[40]		• 0	• 0		00	00	ē	ō			• •	í
			Personal knowledge		[58]	0	•	••	0.	••	••	•			•	•••	1
		Recovery	Preference-based		[59]	0	•	• •	• •	••	•		>		••	•••	1
			Social re-auth.		[60]		•	• =		••	• 0	0		00	••	• 0	1

							Usat	bility		Dep	loyab	ility		S	ecurity	y	
	The Quest to Re	place Passwords:													8		
A Framework for C	omparative Evalu	ation of Web Authe	nticatio						10								
			NO		Ce	ens	SIr	າດ	1/2	<b>r</b>	ec	IU	ire	C			
Jaconh Donnoou	Corran Harlay	Paul C yer Oorschot	Fronk Staional					-3	• •								
University of Cambridge Cambridge, UK ich82@cl.cam.ac.uk	Microsoft Research Redmond, WA, USA	Carleton University Ottawa, ON, Canada	University of Cambridge Cambridge, UK	Ę		less	55		n-Loss	r-User	le	$\wedge$	al-Obse d-Imper ad-Cuor	tiled-G	trom-Other from-Other free	arty	Consen
Jeboz e encantación	connac e nacrosoja com	paur escolaricionica gr		sectic		-Effon Users	Jorde Jforde	nn Jse	rrors rry-froi	ost-pe	oatible npatib	tary	rhysic Targete Throtel	Unthro	Interno Leaks- Phishii	Theft Third-1	xplicit-
https://www.cl.ca	m.ac.uk/techreports	s/UCAM-CL-TR-817. <sub>f</sub>	odf	scribed ir	erence	morywise ilable-for	thing-to-(	ry-to-Lea	requent-E	zessible gligible-C	ver-Com	iare n-Proprie	silient-to- silient-to-	vilient-to-	sultent-to- silient-to- silient-to-	vilient-to- Trusted-	quiring-E linkable
		Category	Scheme	Ď	Ref	Me	P <sup>N</sup> O	Eg	East	Nes	Bro	2 S	Res	Res	Res Res	No.	Un.
		(Incumbent)	Web passwords	Ш	[13]		•	• •	0.	••	••	••	0	_		• •	••
		Paceword manager	Firefox	IV-A	[22]	0.	0 0	••	•	••	•	• •	00		۲	••	••
		Password manager	LastPass		[42]	0.	0 0	••	• •	• 0	•	•	000	> 0	0 .	•	••
		Proxy	URRSA	IV-B	[5]			•	°	•	••		0				••
			Impostor	RV C	[23]	0.				•							
			OpenID Microsoft Passport	IV-C	[27]								0 0 0	50			
		Federated	Facebook Connect		[43]	0.	• 0				÷	•	0 0 0	0 0		•	
		reuerateu	BrowserID		[45]	0.	• 0	••		••	0	•	000	0 0	۲	•	•
			OTP over email		[46]	0.	•	•		••	•	•	000	0 (		•	•
		Graphical	PCCP	IV-D	[7]		:	• 0	0.	•	:	•	•	2	• •		•••
			GrIDsure (original)	IV-E	[30]	-	•	• 0	0.	•	•					••	••
			Weinshall		[48]		•			•	•	•					••
		Cognitive	Hopper Blum		[49]	1	•			••	•	•	0.			••	••
			Word Association		[50]		•	••	0 0	••	•	•				••	••
			OTPW	IV-F	[33]			•	•	•	•	••	• •			••	••
		Paper tokens	S/KEY		[32]	•		•	•	•	•	•••				•	••
			PIN+TAN		[51]	_	_	•	00	0		•••	• •			0.	••
		Visual crypto	PassWindow	NV C	[52]	•			-	0		•					•••
			RSA SecuriD	IV-G	[34]	-			~		=:		HH	181			
		Hardwara takana	Ironkey		[55]		o	0 0	ŏ		••		• •	177			••
		Haldware tokens	CAP reader		[55]				0			•		a la i			••
			Pico		[8]	• •	۰	0	0			•				0.	••
			Phoolproof	IV-H	[36]		0	• 0	0	00	0	•				••	••
			Cronto		[56]	1	0	• 0	0	0	•	• 🔳				••	••
		Phone-based	MP-Auth		[6]		0	• •	•	00		•	0		۲	••	••
			OTP over SMS			••	0	•	00	0	•	••	•••			0	••
			Google 2-Step	1117	[57]		0	• •	00	0	<b>.</b>	•	000	<u></u>			••
		Discontrol	Fingerprint	11/-1	[38]					0		0					-
		Biometric	Voice		[39]					0.0	0			5			
			Personal knowledge		[58]	0	•		0.								••
		Recovery	Preference-based		[50]	0	•					Ĩ	o				
		Recovery	Social re-auth.		[60]		•	•	•	••	•	0	0			•	• •
			a serie re unun		11001												

#### 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)

								- <b>-</b>						S	9	- 24	- <b>1</b>	2.0	¥ 🥹	# . #	- 4	. 4	2,	·B '	2
Catalogue	Cabama	Jesc	tefe	1em	cal	Voth Physics	asv	ffic	nfre	asy	cce	e81	nov	fatt	jon-	esi		tesi 		lesi	lesil	tesil	I-0/	lequ	mm
Category	Scheme		P4	1	S,	<u>&lt; -</u>			-	-	1			<	<	4	~	~ ~			14	-	~	-	2
(Incumbent)	Web passwords	ш	[13]		-	•	_	-	0	-			_	-	•	~	0					-	-	-	-
Password managers	Firefox	IV-A	[22]	0		0		•			•			•	•	0	0			144		•	•	•	-
- usses or a managers	LastPass		[42]	0		0	2	•		0	•			•	=	o	0	0 0	2	0		•	=	<u>•</u>	-
Proxy	URRSA	IV-B	[5]		_		•		0					2			0		•	)			=	• •	•
TIONY	Impostor		[23]	0		•	•		=	•	•	-	0		•	۰	0			2	•	•			•
	OpenID	IV-C	[27]	0	•	•	0	•	۰	•	•	•	•	•	•	o	0	0 (	2			•	=	•	
	Microsoft Passport		[43]	0	•	•		•	٠	•	•		•	•	=	o	0	0 (	D			•	=	•	
Federated	Facebook Connect		[44]	0	۰	• 0		•	۰	•	•	•	•	•		o	0	0 (	0			٠			
	BrowserID		[45]	0	۰	•	•	•	۰	•	•	•	0	0	•	o	0	0 (	0			٠		•	
	OTP over email		[46]	0	۰	•	•		۰	•	• •	•	•		•	o	0	0 (	2			•		•	
Crarbinal	PCCP	IV-D	[7]			•	•	0	0	•		•	•		•		٠	0			•	٠	٠	• •	•
Graphical	PassGo		[47]			•	•	0	ο	•		•	•	0	•		٠					٠	٠	•	•
	GrIDsure (original)	IV-E	[30]			•	•	0	0	•		•	•				۰					٠	٠	•	D
0	Weinshall		[48]	1		•			=			•	•		•	o	۰					•	٠	•	D
Cognitive	Hopper Blum		[49]	1		•			=		•	•	•		•	o	۰					•	٠	•	D
	Word Association		[50]	1		•	•	•	ο	0	•	•	•		•							٠	٠	•	D
	OTPW	IV-F	[33]				•		Ξ	•		•	•	•	•		٠	• •	Т			٠	٠	•	Þ
Paper tokens	S/KEY		[32]				•		ο	•		•	•	•	•		٠	•	1		0	$\equiv$	٠	•	•
	PIN+TAN		[51]	1			•		ο	0		0	•	•	•		٠	•	1			0	٠	•	•
Visual crypto	PassWindow		[52]						Ξ			0	•	•		o	۰	• •	Т			Ξ	٠	•	D
	RSA SecurID	IV-G	[34]				•	0	0				•	•		۰	۰	• •	Т			٠	Ξ	• •	Þ
	Yubikey		[53]	1			•	0	ο		•		•	•		۰	٠	• •	1			•		•	D
Hardware tokens	Ironkey		[54]	0	•	•	0	0	ο		•	•	•	•		۰	ο		(	2	۰	•	٠	•	
	CAP reader		[55]				•	0	ο				•	•		۰	٠	•				•	٠	•	
	Pico		[8]		•			0	ο						•	۰	۰	•				0	٠	•	
	Phoolproof	IV-H	[36]			0	•	0	0		0	0 0	>		•	۰	۰	• •		) (		٠	٠	•	D
	Cronto		[56]	1		0	•	0	ο			0	•	•		۰	۰	• •		) •		•	٠	•	
Phone-based	MP-Auth		[6]	1		0		0	=	0	0	0			•		ο				۰	•	٠	•	
I none-oused	OTP over SMS				•	0			ο	0	0		•		•	۰	۰	•				0		•	
	Google 2-Step		[57]			0		0	ο	0	0		•	•		0	o					•	٠	•	
	Fingerprint	IV-I	[38]		۰	• 0		0			0			0		٠		•				Ξ	٠	•	
Biometric	Iris		[39]		۲	•		0			0			0		۲		٠					٠	0	
	Voice		[40]		۲	•		0			0	0	0	0		۰		o					٠	•	
	Personal knowledge		[58]	0		•		•	0	•	• •	•	•		•							•	٠	•	
Recovery	Preference-based		[59]	0		•		0	•	0	•	•	•				0					•	•	•	
in the start of th	Social re-auth.		[60]			•			•		•	•		0		0		•		0 0		•	=	• 1	0
	overal re uuun		1001			-	-			-	-	-		-	_	-				_			_	-	_

Usability

Deployability

ysical-Observatio

Security

sted-Third-Party ing-Explicit-Consent

able

heft

•= 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.



•= 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.

						1	Usability		Deple	oyabili	ty		Security	1	
A Framework for C	The Quest to Re omparative Evalu	place Passwords: ation of Web Auther	ntication Schem	es*								ation ing ssing	ation er-Verifiers		
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, Canada paulv@scs.carleton.c	takes a	a /o	ot	of	gu	les	SS	es		cal-Observ ed Impers led-Guessi ottled-Gue	al-Observi -from-Othe ing	Party	-Consent
https://www.cl.ca	m.ac.uk/techreports	:/UCAM-CL-TR-817.p	df	scribed in secti	ference	morywise-Effo tlable-for-User thine-to-Cerry	ysically-Efforth sy-to-Learn icient-to-Use	requent-Errors sy-Recovery-fro	cessible gligible-Cost-p	ver-compation wser-Compation ture	n-Proprietary	silient-to-Physi silient-to-Turge silient-to-Thrott silient-to-Unthr	silient-to-Intern silient-to-Leaks silient-to-Phish	silient-to-Theft -Trusted-Third-	quiring-explica linkable
		Category	Scheme	ñ	Re	No No	Eff Ea	Ea	Ne	Brd Mc	No a	Re Re K	Re. Re.	No	Un C
		(Incumbent)	Web passwords	Ш	[13]	•		• •	•••	•••	٠	٥V		••	••
		Password managers	Firefox LastPass	IV-A	[22] [42]			• •	•••			0 0 0 0 0 0 0 0		• = (	
		Proxy	URRSA Impostor	IV-B	[5] [23]	•		•	•	• •	•	0 • 0	0 • 0 •	•	••
		Federated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]				* * * * * * * *		•	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
		Graphical	PCCP PassGo	IV-D	[7] [47]		• • •	0 • 0 •	•	• •	•	• •		•••	••
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]			00	• • • • •	:	•	0	::		•• •• ••
		Paper tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]	•	:	0 • 0 0	•	•••	•••••••••••••••••••••••••••••••••••••••				••
		Visual crypto	PassWindow		[52]	•			0	••	Ξ				••
		Hardware tokens	RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55] [8]	••		00000	•			0	0		· · · · · ·
		Phone-based	Phoolproof Cronto MP-Auth OTP over SMS Google 2-Step	IV-H	[36] [56] [6]			00000	0000	•••	•	0			
		Biometric	Fingerprint Iris Voice	IV-I	[38] [39] [40]				0 0 0	000		• •			
		Recovery	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0		0 • • •	••• ••• ••	•••		0			•••
		• affers the hear	Gu O almost off	d 1			· · · · · · · · · · · · · · · · · · ·			dia t		C.			

							Usabi	ility		Deplo	oyabili	ity		Se	curity			
	The Quest to Rep	place Passwords:													22			
A Framework for C	omparative Evalua	ation of Web Auther	ntication Schem	es*									ion	$\bigwedge$	nifie			
	-											- I-	nat	sing	- Ve			
Joseph Bonneau	Cormac Herley	Paul C. van Oorscho											DA L	ues	the		12	
University of Cambridge	Microsoft Research	Carleton University	c info a	cil	51	$\frown$ 1							a du	9 <u>1</u>	õ	2	rse1	
Cambridge, UK	Redmond, WA, USA	Ottawa, ON, Canado	5 IIIICa		אכ			gu		33	>		242	193	8	E.	Co	
jcb82@cl.cam.ac.uk	cormac@microsoft.com	paulv@scs.carleton.c					06				<b>、</b>		ete	101	hin	1-P	-ii-	
		(e	e.a. real		<b>^</b>	S	20	4 1	ri	es		- È,	arg arg	inter a	eak his	hin	plic	
https://www.cl.ca	m.ac.uk/techreports/	/UCAM-CL-TR-	.9.104		Ŭ						/		0 0	5 6 6	1-0	L-0	EX 。	
	1			bed	nce	yw Lej	g-t dlb	1+1 1-1	ec.	ig d	ζΫ́.	ob	1-12	i i i	1-12	nt-t ste	ing	
				cij	cre	la p	hin	y-re cie	y-R	ess ligi	WSé	4	the the	ilie ilie	ilie ilie	Tru	uir ink	
		Category	Scheme	Se	Ref	Men Sca	Vot	3	ar sa	Veg V	202 M	No.	Kes Res	Res	Res	Vo-	Req	
		(Incumbent)	Web passwords	Π	[13]	~ ~,			0.0				0	$\nabla$	~~		~~	
		(incumbent)	Firefox	IV-A	[22]	0.	00		•			•	0 0		۲		••	1
		Password managers	LastPass		[42]	0.	00	• •	• •	• • •	•		000	0 0	0.	•	••	
		Drown	URRSA	IV-B	[5]			• =	0 🔳	•	•		0	0	۰		••	1
		rioxy	Impostor		[23]	0.	•	•	•	•	• •	•	• •	0	•	•	•	
			OpenID	IV-C	[27]	0.	• 0	•		••	•••		000	00			•	
		P. I	Microsoft Passport		[43]										Ξ.		-	
		Federated	BrowserID		[44]	0.				••	0 0		0 0 0	ŏŏ	•		•	
			OTP over email		[46]		•	•		••	•	•	000	0 0		•	•	
		Construction of the second sec	PCCP	IV-D	[7]		•	• •	• •	•	٠	٠	• (	)		••	••	1
		Graphical	PassGo	1	[47]		•	• •	• •	•	• 0	•	۲			••	••	
			GrIDsure (original)	IV-E	[30]		•	• •	• •	•	•		۲			••	••	]
		Cognitive	Weinshall		[48]		•			••	•	•	••			•••	•••	
			Hopper Blum		[49]								•••					
			OTPW	IV-F	[33]	-	Ť	•	•	•	••					••	••	
		Paper tokens	S/KEY	111	[32]	•		•	• •	ė	••	•			. 0			
		i uper tonens	PIN+TAN		[51]			•	o <u>o</u>	0	••	•	•			•	••	
		Visual crypto	PassWindow		[52]					0	••				• •	•	••	1
			RSA SecurID	IV-G	[34]			• •	0		••		• • •		••	•	••	
			Yubikey		[53]			• •	0	•					• •	•	•••	
		Hardware tokens	CAP reader		[54]				0						- 5			
			Pico		[33]			ō	ŏ			•					••	
			Phoolproof	IV-H	[36]		0		0	000	<b>&gt;</b>	٠					••	1
			Cronto		[56]		0	• •	o 📃	0	••					••	••	
		Phone-based	MP-Auth		[6]		0	• •	0	0 0		•	0		•	••	••	
			OTP over SMS				0	•	0 0	•	••	•	•••		••	•	••	
			Google 2-Step	TVI	[57]				00	0	••					<u> </u>		
		Biometric	Iris	11-1	[30]					ŏ		5						
		Diometric	Voice		[40]		. 0			00	0 0	5		>		•	•	
			Personal knowledge		[58]	0	•		• •	••	••	•				••	••	1
		Recovery	Preference-based		[59]	0	•	• •	• •	••	•		0		۰	••	••	
			Social re-auth.		[60]		•	•		••	• •	2	•		• •	• =	• •	
		- offers the here	St. 0_ almost offer	thal	anal	G+	airala	- da		t offer	the h	anal	G.					-

#### 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 Pa Microsoft Research CC Redmond, WA, USA Ot cormac@microsoft.com pat

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

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

Usability

Deployability

Security

usted-Third-Party ring-Explicit-Consent

ıkable

nt-to-Phishing

ent-to-Theft

cronation

ent-to-Throttled-Guessing

ni-to-Unthrottlea

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

Category	Scheme	Des	Ref	Me	Sca	Noi	East	Effi	μĥ	Eas	Acc	Ser.	Bro	Ma	Do.	Res	Resi	Read	Resi	Kesi	Resi	Resi	1-0N	Kequ Unli
(Incumbent)	Web passwords	III	[13]			•	•	•	0	•	• •			•	•	C	)		J		_	• •	• •	••
<b>D</b>	Firefox	IV-A	[22]	o	•	0 0		•	۲		• •			•	• 6	0 0	)				۲	• (	• •	••
Password managers	LastPass		[42]	0	•	0 0	•	•	۰	0	• 3			•	k	0	0	Ö		0	۲	•	- (	••
D	URRSA	IV-B	[5]				•		0			0	•			C	)		0		•			••
Proxy	Impostor		[23]	0	•	•	•			•	•	•	0			• 0	)		0		٠	•		•
	OpenID	IV-C	[27]	0	۲	• (	0	٠	۲	•	• •		•	•	• K	0	Ö	Ö		۲		•	- (	•
	Microsoft Passport		[43]	o	۰	• (	•	•	۰	•	•		•	•	¢	0	Ö	Ö		۲		•	-	• =
Federated	Facebook Connect		[44]	0	۰	• (		•	۰	•	• •		•	•	K		0	o		۰		•		
	BrowserID		[45]	0	۰	• (		•	۰	•	• •		0	0	• •	0 0	0	o		۰		•	-	•
	OTP over email		[46]	0	۰	•	•		۰	•	• •		٠		• •	0 0	0	Ø		۲	۰	•		•
Graphical	PCCP	IV-D	[7]			•	•	0	0	•			•		•	•	0			٠	٠	•	• •	••
Orapinear	PassGo		[47]			•	•	0	0	•			•	0	•							•	• •	••
	GrIDsure (original)	IV-E	[30]			•	•	0	0	•			•			•	•					•	• •	••
Comitive	Weinshall		[48]			•	. =		=				•	=		•				٠	٠	• •	• •	••
Coginuve	Hopper Blum		[49]			•	-				• •		•							۰	•	• •	• •	••
	Word Association		[50]			•	•	•	0	0	• •		•	=		_						• •	• •	••
	OTPW	IV-F	[33]				•			•			•	•	•		•	٠	•	٠	٠	• •	• •	••
Paper tokens	S/KEY		[32]				•		0	•	-		•	•			•	•	•	۰	o	<u> </u>	• •	••
	PIN+TAN		[51]				•		0	0	•	>	٠	•	•	•		٠	•	۰	•	0	• •	••
Visual crypto	PassWindow		[52]		_		_				•	>	٠	•	¢				۰	۲	•		• •	••
	RSA SecurID	IV-G	[34]				•	0	0				•	•			•	•	•	٠	٠	•	•	••
	Yubikey		[53]				•	0	0		•		•	•			•	•	•	٠	٠	•		••
Hardware tokens	Ironkey		[54]	0	•		0	0	0		•	•	•	•		0	)		0		•	• •	• •	••
	CAP reader		[55]			=	•	0	0				•	•			•	•	•	•	•	• •	• •	••
	Pico		[8]		•			0	0									•	•	۰	•	0	• •	••
	Phoolproof	IV-H	[36]			0	•	0	0		0 0		)	=			•	•	0	•	•	• •	• •	••
	Cronto		[56]	Į.		•	•	0	0		5	2	•	•				•	0	۰	•	• •	• •	••
Phone-based	MP-Auth		[6]			•	•	0		0	0 0	2				C	)				•	•	• •	••
	OTP over SMS				•	•	•		0	0	•		•	•					0	•	•	0		••
	Google 2-Step		[57]		1	0	•	0	0	0	0		٠	•	•	00					•	• •	•	••
	Fingerprint	IV-I	[38]		•	•		0			0			0			•	1				= •	• :	•
Biometric	Iris		[39]		•	•		0			•			0			•	1				= •	•	•
	Voice		[40]			• 0		0			0 0	2	0	0			0					<u>_</u>	-	•
	Personal knowledge		[58]	0		•		•	0	•	•		•	•	•							• •	• •	
Recovery	Preference-based		[59]	0		•		0	•	0	•		•			0	•					• •	• •	
	Social re-auth.		[60]			•	•		•		• •		•	0					0	0		•		• •

•= 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.

							Usabi	ility		Deploy	ability		Se	curity	,		
	The Quest to Rep	place Passwords:												2			
A Framework for C	omnarative Evalue	ation of Web Authe	ntication Schem	ee*								u	<b>/</b>	file			
A Flamework for C	Unparative Evalua	ation of web Addie	inication Schem	60								on	gu	Ven			
												12 6	SSI 10	5			
Joseph Bonneau	Cormac Herley	Paul C. van C	coblom	of			$\sim$	ait.					- Suc	14		11	
University of Cambridge	Microsoft Research	Carleton Uni A U	UDIEIII	a	LC	ווכ	ヒ、	510	e				-pa	1	2	nse	
cambriage, UK ich82@cl.cam.ac.uk	Keamona, WA, USA	Ottawa, ON,		_					_				the control of the co	je s	- La	ပိ	
JCD02@Ci.Cum.uC.uk	cormat @microsoji.com		en't on	da	n		2r	∩t	h	r م	cit		hro	54	-1-p	cit-	
		uue		uc		iya		υ	110	יוכ	SIU	53	Inte	ea.	hin	plù	
https://www.cl.ca	m.ac.uk/techreports/	/UCAM-CL-1H-817.p	ai			0, 2,	67	262		. X 5		199	0 0 0		[-0]	е <sub>-</sub>	
·	•	•		ba	lce	1 A	212	7 7 8	20	Coppe	<b>Y</b>	불불불	1-12	1	ste	abl	
				-it	- Iei	ap 10	nin sice	v-tc ien	-8	ligi er-	WSe Pr	lie lie	lie lie	ie i	Tru	uin	
		0	0.1	ese	efe	g g	hy lot	5 <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	5	6 6 6	fat of	esi	esi	esi	es.	eq.	
		Category	Scheme		<u> 24</u>	<u> </u>				$< < \infty$	8 4 4		* * *	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	~ ~	2	
		(incumbent)	Web passwords	III IV A	[13]	0 -	0 0							<u> </u>			
		Password managers	L actPass	IV-A	[22]	0	0 0					0.0	0.0				
			Lastrass	IV-P	142		-					0					
		Proxy	Impostor	TA-D	[23]		•	•					0		•		
			OpenID	IV-C	[27]	0.		0				00	00		•	•	1
			Microsoft Passport	11-0	[43]		. 0		•			00	0 0		•	•	
		Federated	Facebook Connect		[44]	0.	• 0			• • =	••	00	0 0	۲	• =		
		rederated	BrowserID	1	[45]	0.	• 0	• • 🕷		• • =	00	00	00	۲	•	•	
			OTP over email	1	[46]	0.	•	• 📃 🕷		• • 🔳	• = •	00	00		•	•	
		Graphical	PCCP	IV-D	[7]		•	• • •	•	•	• = •		0	• •	••	••	1
		Graphical	PassGo		[47]		•	• • •	•	•	• • •				••	••	
			GrIDsure (original)	IV-E	[30]		•	• • •	• •	•	•	۲			••	••	
		Cognitive	Weinshall		[48]	l.	•			•	•	0.			••	•••	
		Coginate	Hopper Blum		[49]	L											
			Word Association	NUE	[50]	<u> </u>	-										
		Down to have	OIPW S/VEV	IV-F	[33]		=					1 8					
		Paper tokens	DINTTAN	-	[52]			•	0			1 8					
		Visual crypto	PaseWindow	-	[52]					0		0.					1
		visual crypto	RSA SecurID	IV-G	[34]			• • •	>						• =		
			Yubikey		[53]					•					•	• •	
		Hardware tokens	Ironkey		[54]	0.	0	0 0 0	> =	•	••	• •	0	•	••	••	
			CAP reader	1	[55]	1		• • •	> =		••				••	••	
			Pico		[8]		۰	0 0	> =						0.	••	
			Phoolproof	IV-H	[36]		0	• • •		000					••	••	
			Cronto		[56]	l.	0	• • •		•	••		• • 0		••	••	
		Phone-based	MP-Auth		[6]		0		0								
			OTP over SMS		1670		0										
			Google 2-Step	TV I	[37]		• •			-					<u> </u>		
		Diamatria	Irie	14-1	[30]								-				
		Biometric	Voice		[40]		• 0	• •		0 0	0 0		ō			ě	
			Personal knowledge		[58]	0	•								••		
		Recovery	Preference-based		[59]	0	•		0	••	•	0			••	••	
		in the second se	Social re-auth.		[60]	1	•	• = •		• •	• •	0			• =	• •	
					1.001	C+		1				<b>C</b> 1					1

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

#### **Resists off-line phishing**

Joseph Bonneau	Cormac Herley	Paul C. van Oorschot	Frank Stajano <sup>†</sup>											100	ຍ່ຄັບ	5.5.			5 1	Ĺ
University of Cambridge	Microsoft Research	Carleton University	University of Cambridge							082				sqc	ŧ.	2 2		8	rse	
Cambridge, UK	Redmond, WA, USA	Ottawa, ON, Canada	Cambridge, UK			les		50		7-		5	2	12		12 E	2 go	Lp	S	
JCD82@C1.Cam.ac.uk	cormac@microsoji.com	paulv@scs.carielon.ca jra	ink.siajano@ci.cam.ac.uk	ii.		HO I	6 2	fes		s un		1 2	10 H	sice	a la	on D	Sil.	17	4	
				Sec		8	212	lor.	se a	2-7		at i		Se .	24	n in	e iz ;	rin a	plic	
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	df	.Е		ė,	ξq	Ξų.	ΞP.	Vel Vel	L Ç	5 fr.	i o	1-0	22	5 5	22	1	ų 🕺	
		····		ed	ICe	WW S	51	1	Ϊž	ent	ble	10	2 B	4-1		4-12	4 4	ster	284	
				官	Ier	0.4	i, io	ic.	ien -	np.	22	0 5	a ad	lie.	ie.	lie.	lie:	Int.	nka	
				csc	efe	5	oth	NA.	3 E	ц, S	00	8		est	esi	esi	esi esi	5	eqi 'nli	
		Category	Scheme	<u>A</u>	2	20	2	<b>d</b> , <b>b</b>	व म्य	2 11	A X	5	<u>a 22</u>			~~	~~~	<u>&lt; 2</u>	2 2	
		(Incumbent)	Web passwords	Ш	[13]	~					•								•••	
		Password managers	Firefox	IV-A	[22]										- MI		~ ~			
			Lastrass	IV.P	[42]					0					0	<u> </u>				
		Proxy	Impostor	IY-D	[23]	0.			5 🗐		•				5	ō			i i	
			OpenID	IV-C	[27]	0		0			•			00	0 0	0		• =	•	
			Microsoft Passport		[43]	0		0	• •		•			0 0	o o	Ö		• 🔳	•	
		Federated	Facebook Connect		[44]	0	•	0	• •		•		• •	0 0	0 0	Ö I		• 🔳		
			BrowserID		[45]	0	•	0	• •		••		00	0	0 0	0		• 📃	•	
			OTP over email		[46]	0	•	•			• •			00	0 0	0		• 📃	•	
		Graphical	PCCP	IV-D	[7]		•		• •	••					• •			••	••	
		Orapinear	PassGo		[47]		-		0	0.			00		<u> </u>			••	••	
			GrIDsure (original)	IV-E	[30]				• •	••										
		Cognitive	Weinshall		[48]					==										
			Word Association		[49]					0 0										
			OTPW	IV-F	[30]	-	-												••	
		Paper tokens	S/KEY	11-1	[32]	•				0.										
		r uper tokens	PIN+TAN		[51]				•	0 0		>						• •	••	
		Visual crypto	PassWindow		[52]	۰						>		0				•	••	
			RSA SecurID	IV-G	[34]			•	0	0				•				• 🔳	••	
			Yubikey		[53]			•	• •	0	•		••	•				• 🔳	••	
		Hardware tokens	Ironkey		[54]	0		0	0 0	0	•	•	••	• •	2	0		••	••	
			CAP reader		[55]				• •	0			••						•••	
			Pico	***	[8]			-	0	0	~			-						
			PhooIproof	1 ү-н	[30]					~				++						
		Dhone haved	MP-Auth		[50]		ŏ			Ĭ	0	5					- E .			
		Phone-based	OTP over SMS		[0]					0 0	0					. 0		0	••	
			Google 2-Step		[57]		0			0 0	0			0 0				••	••	
			Fingerprint	IV-I	[38]		• •	0	0		0		0	۰	٠		1	•	•	
		Biometric	Iris		[39]		•	0	0		0		0	۲	۲		F	•	0	
			Voice		[40]		•	0	0		0 0		0 0	۲	Ö			•	•	
			Personal knowledge		[58]	0	•		• •	• •	• •		•••					••	••	
		Recovery	Preference-based		[59]	0	•		0	• •	•	!!!			2			•••	•••	
			Social re-auth.		[60]		•				•••			0	=		N N	• =	• •	

•= 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.



•= 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

University

#### Trust localized to user/service

Joseph Bonneau Iniversity of Cambridge Cambridge, UK jcb82@cl.cam.ac.uk https://www.cl.ca	Cormac Herley Microsoft Research Redmond, WA, USA cormac@microsoft.com	Paul C. van Oorschot Carleton University U Ottawa, ON, Canada paulv@scs.carleton.ca fro s/UCAM-CL-TR-817.p	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK ank.stajano@cl.cam.ac.uk odf	Described in section	keference	demorywise-Effortless	scalable-for-Users	votung-to-Carry Physically-Effortless	Casy-to-Learn	fficient-to-Use	ngrequent-triors Casy-Recovery-from-Loss	Accessible Veolioible-Cast-per-User	erver-Compatible	3rowser-Compatible	Aature Von-Proprietary	Cesilient-to-Physical-Observ	&esilient-to-Targeted-Impers &esilient-to-Throttled-Guess	Cesilient-to-Unthrottled-Gue	cesilient-to-Internal-Ubserv Resilient-to-Leaks-from-Oth	Resilient-to-Phishing 2003/10-11-17/10-12	Vo-Trusted-Third-Party	Inlinkable	
		(Incumbent)	Web passwords	m	1131	<u> </u>				•						-	0					Ĩ	
		Password managers	Firefox LastPass	IV-A	[22]	0		00		•		•••			•••	0	0 0	ō	0				
		Proxy	URRSA	IV-B	[5]	•			•	(	•		0	•			0		D				
		Federated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]	000000			•					•	•••	00000		000000		•			
		Graphical	PCCP PassGo	IV-D	[7] [47]			•	•	00	0 • 0 •			•	•		• •		٠	•••			
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]			• • •	•	• •	•			•	•	0	•		:				
		Paper tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]				:	0	•	•		•	::		::			• • • •			
		Visual crypto	PassWindow		[52]		_	_				0	<b>)</b>	•	•	0	• •			•	• •	••	
		Hardware tokens	RSA SecurID Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55] [8]	•	•	•	•			•	•		•	•	0						
		Phone-based	Phoolproof Cronto MP-Auth OTP over SMS Google 2-Sten	IV-H	[36] [56] [6]			0 0 0 0	•••••	000000	0000	0 0 0 0	00	•	•	•							
		Biometric	Fingerprint Iris Voice	IV-I	[38] [39] [40]			• 0 • 0	•	0		0	,	0	0	•	•				•••		
		Recovery	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0		•	:	•		•••		•	••	0	•		0 0			•	

•= 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.

A Framework for C	The Quest to Rep omparative Evalua	blace Passwords: ation of Web Auther	ntication Schem	es*			Usabil	lity		Depl	oyabil	ity	tton nation	g sing S	- Verifiers	ty	
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	er has to outhenti	0 C2	(k ati	nc lor	งพ า c	in DC	igl cl	y) Irr	) C in	oı g	ทร	er	nt	Theft	xplicit-Consent
https://www.cl.ca	m.ac.uk/techreports/	UCAM-CL-TH-OT7.p	Scheme	Described	Reference	Memorywis Scalable-fo	Nothing-to Physically- Facv-to-Le	Efficient-to	Ingrequent- Easy-Recov	Accessible Negligible-	Browser-Con	Non-Propr	Kesilient-to Resilient-to	Resilient-to Resilient-to	Resilient-to	Resilient-to- No.T	Requiring-E Uniinkable
		(Incumbent)	Web passwords	III	[13]		• •	•••	• •	•••		••	0			• •	, 🗸 💿
		Paseword managem	Firefox	IV-A	[22]	0.0	00			•••			00		l I	. • •	
		rassword managers	LastPass		[42]	0.	00		0	• •			00	00	0 (	. •	
		Proxy	URRSA	IV-B	[5]				0	•	•		0	C			••
		11049	Impostor		[23]	0.	•		•		• •		• •	0	<u>x 1</u>		•
		Federated	OpenID Microsoft Passport Facebook Connect BrowserID OTP over email	IV-C	[27] [43] [44] [45] [46]											•	•
		Graphical	PCCP PassGo	IV-D	[7] [47]		•	00	0 • 0 •	:	•	•	:	0	• •	•••	) • • ) • •
		Cognitive	GrIDsure (original) Weinshall Hopper Blum Word Association	IV-E	[30] [48] [49] [50]				0 0	••••	•	•	•				
		Paper tokens	OTPW S/KEY PIN+TAN	IV-F	[33] [32] [51]	•			•	••••	•					0	
		Visual crypto	PassWindow		[52]					0	•		••				,
		Hardware tokens	RSA SecuriD Yubikey Ironkey CAP reader Pico	IV-G	[34] [53] [54] [55] [8]	••	0			•			0				
		Phone-based	Phoolproof Cronto MP-Auth OTP over SMS Google 2-Step	IV-H	[36] [56] [6]						• •						
		Biometric	Fingerprint Iris Voice	IV-I	[38] [39] [40]	•••	• • •	0		000	0			•			0
		Recovery	Personal knowledge Preference-based Social re-auth.		[58] [59] [60]	0				•••	•		•				•••
		<ul> <li>e offers the benef</li> <li>better than pass</li> </ul>	fit; $\mathbf{o} =$ almost offers swords; $\equiv =$ worse the	s the b nan pa	benef asswo	it; <i>no o</i> ords; <i>n</i>	circle o back	= do kgrou	es no nd po	t offe uttern	the = no	benef chan	iit. ige.				

#### The Quest to Replace Passwords

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

Cormac Herley Paul C. van Oorschot Carleton University Microsoft Research Ottawa, ON, Canada Redmond, WA, USA cormac@microsoft.com paulv@scs.carleton.ca

#### A Framework for Comparative Evaluation of Web Au Two verifiers who collude can't link user across them based caticator alone on authenticaticator alone .=

Usability

Deployability

Security

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

		escribed	eference	emorywi	calable-f	hysically	asy-to-Le	ficient-to	ifrequent	asy-keco	egligible	erver-Co	rowser-C	ature on-Propi	esilient-t	esilient-t	esilient-h	eSutent-n	esutent-a esilient-b	esilient-t	esilient-t	o-Truster	Sur ung	<b>FLEFTINGENE</b>
Category	Scheme	<u> </u>	2	2.	23	2 94	E	<u>ы</u>		4	< 2	S	2	22	8	2	2 0	2 0	2 22	2	2	2		2
(Incumbent)	Web passwords	Ш	[13]					-	0	-		-	-			0					-	-		4
Password managers	Firefox	IV-A	[22]	0		00	•	•					Ξ		0	0		-				•		2
	LastPass		[42]	0	•	0	•	-				•	-	•	0	0	0	2	0		-			2
Proxy	URRSA	IV-B	[5]		_			3	•		•	•	•			0		5	2			Ξ.		2
	Impostor		[23]				-	-				-	-	_		÷		<u> </u>	-	-	-	=		4
	OpenID	IV-C	[27]	0			0	-				=			0	0	0	2		1		Ξ'		
	Microsoft Passport		[43]	0				-							0	0	0	2		1		Ξ.	•	
Federated	Facebook Connect		[44]	0				-				Ξ	•	-	0	0	0	2		1		=		
	BrowserID		[45]	0				-				Ξ	0	•	0	0	0	2		1		Ξ'		
	OTP over email		[46]	0			•	-				=	•	-	0	0	0 0	2	-		•		•	
Graphical	PCCP	IV-D	[7]			2	•	•	0		•		•	-			0		•		•	•		2
orupineur	PassGo		[47]		_		•	0	0	•	•	Ξ	•	••	1						•	•	•••	2
	GrIDsure (original)	IV-E	[30]				•	0	0		•	Ξ	•			•					•	•	•••	2
Comitive	Weinshall		[48]				Ξ	=	=		•	Ξ	•	•	0	•				•	•	•	• •	
Cognitive	Hopper Blum		[49]		•		=	=	=	•	••	=	•	-	0	۰			•	•	•	•	• •	
	Word Association		[50]		_		•	•	0		••		•	-		=		_			•	•	••	•
	OTPW	IV-F	[33]				٠			•	•		٠	••		۰	•			٠	٠	•	• •	
Paper tokens	S/KEY		[32]				٠	=	0	•	•		٠	••		٠	•			0		•	• •	•
-	PIN+TAN		[51]				٠	=	0	0	0		٠	••		۰	•			۰	0	•	• •	
Visual crypto	PassWindow		[52]								0		•	•	o	۰	•			۰	Ξ	•	• •	)
	RSA SecurID	IV-G	[34]				٠	0	0				٠	•	۰	۰	•			٠	٠		• •	7
	Yubikey		[53]				٠	0	0				٠	•	۲	۰	•			۰	٠		• •	
Hardware tokens	Ironkey		[54]	0	•	0	0	0	0			٠	٠	•	۲	ο		¢	2	۰	٠	•	• •	
	CAP reader		[55]				٠	0	0				٠	•	۲	۰	•			۰	٠	•	• •	
	Pico		[8]		•	٠		0	0					•	۲	۰	•			۰	0	•	• •	
	Phoolproof	IV-H	[36]		4	0	٠	0	0	•	0 0	0		•	۲	۰	•		) •	۰	٠	•	• •	5
	Cronto		[56]	1	4	0	٠	0	0		0		٠	•	۲	۰	•		) •	۲	٠	•	• •	
Phone-based	MP-Auth		[6]	1	4	0	٠	0		0	0 0			-		ο				۲	٠	•	• •	
	OTP over SMS				• <	0	٠	=	0	0	0		٠	••	۲	۰	•		) •	۲	0		• •	
	Google 2-Step		[57]	1	4	0	٠	0	0	0	0		٠	•	0	ο	•		٠	۲	٠	•	• •	
	Fingerprint	IV-I	[38]		• •	0	٠	0		•	0			0	۲	Ξ	٠	_			Ξ	•	•	
Biometric	Iris		[39]		•	0	•	0		4	0			0	۲		٠					• [	0	
	Voice		[40]			0	•	0		4	0 0		0	0	۲		o					•	•	
	Personal knowledge		[58]	0	•	•	٠	٠	0	•	•		٠	• •		Ξ					٠	•	• •	5
Recovery	Preference-based		[59]	0			٠	0	•	•	• •		•			0				۰	٠	•	• •	
,	Social re-auth.		[60]		•		٠		•		• •		•	0	0		•		0 0	۰	٠		• •	2
			-							_								_		_				_

•= 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.

				Usability			Dep	oloyal	bility	Security								
	The Quest to Rep	place Passwords:													1	2		
A Framework for Comparative Evaluation of Web Authentication Schemes*												ation	nanon 18	tsing tion - Vorifie	africa -			
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	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK ank.stajano@cl.cam.ac.uk	section		Effortess Users	arry Fortless	-	se rors y-from-Loss	st-per-User	atible matible	ary	hysical-Observ	hrottled-Guessi	nternal-Observa nternal-Observa	hishing	neji hird-Party	plicit-Consent
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	odf	escribed in	eference	lemorywise calable-for-	othing-to-C hysically-E	asy-to-Lear	green-w-v grequent-Ei asy-Recover	ccessible egligible-Co	erver-Comp mwser-Com	lature on-Propriet	esilient-to-l	esulent-w-1 esilient-to-7	esutent-to-t esilient-to-l	esilient-to-l	esuen-w-	equiring-Ex nlinkable
		Category	Scheme		<u>2</u>	20	2 9		1.12.10	22	S R	22	8 9		< ~ ~		< 2 -	
		(Incumbent)	Web passwords	Ш	[13]													
		Password managers	Firefox	IV-A	[22]		00						0 0	, No la la		. 27		
			LIRRSA	IV-B	[42]			•	0		0.			2	0			••
		Proxy	Impostor	11-1	[23]	0.	•	•	•	•			•	5	o			•
			OpenID	IV-C	[27]	0.	• 0	0			-		0 0	0 0	0			•
			Microsoft Passport		[43]	0.	• 0	• •		•	-	•	0 0	0 0 0	0	. (		•
	Fed		Facebook Connect		[44]	0.	• 0	• •		••	-	•	0 0	00	D C	8 (		
		1 Cuchated	BrowserID		[45]	0.	• 0	• •		••	0	• •	0 0	00	0	8 (	•	•
			OTP over email		[46]	0.	•	•		••	-	• = •	0 0	0 0	D I			•
		Graphical	PCCP	IV-D	[7]		•	•	00	•	•	•		• •			••	••
		Graphical	PassGo		[47]		•	• •	00	•		• •					••	••
			GrIDsure (original)	IV-E	[30]		•	• •	00	•	-							••
Comitiv		Cognitive	Weinshall		[48]		•	=		•			0					•••
			Hopper Blum		[49]													
			WORD Association	NE	[20]		-	-			=	_				100		
		Bapar tokana	S/KEV	IV-F	[33]		Ξ.		•								<b>.</b>	
		Paper tokens	PIN+TAN		[52]	-			00	ō			, i					• •
		Visual crypto	PassWindow		[52]	•	-			0		•	0				•	••
		· ioun cippio	RSA SecurID	IV-G	[34]		-	• •	0 0		-	•						••
			Yubikey		[53]			• •	0	•	•	•	•					••
		Hardware tokens	Ironkey		[54]	0.	0	0 0	0	•	••	•	• •	2	0	•	••	••
			CAP reader		[55]	1		• (	0		•	•						••
			Pico		[8]		•	= (	0			•					•	••
			Phoolproof	IV-H	[36]		0	• •	0 0	00	0	•	•				•••	••
			Cronto		[56]		•	•	0	0	•	•						•••
		Phone-based	MP-Auth		[6]		0	•		00		•		2				•••
			OTP over SMS		(cen		2			0							2 -	
			Google 2-Step	TVT	[20]		-			0						1 101		
		Diometria	Irie	17-1	[30]					0		õ						0
		Biometric	Voice		[40]				5	0 0		0		ō		- 7		•
		4	Personal knowledge		[58]	0	•	•										••
Perover		Recovery	Preference-based		[59]	0	•	•		••			0	2				••
Recovery		Social re-auth.		[60]		•	•	۰	••	-	0	0					• •	
										-								

## 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





				Usability				Dep	oloya	bility		Security								
	The Quest to Rep	place Passwords:															22			
A Framework for Comparative Evaluation of Web Authentication Schemes*													ation	nation	sing	uion r-Verifie	,			
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 fro	Frank Stajano <sup>†</sup> University of Cambridge Cambridge, UK ank.stajano@cl.cam.ac.uk	section		-Effortless Users	arry	fortless n	lse	rors ry-from-Loss	ost-per-User	atible	hanne	ary Physical-Observ	largeted-Imperso Throttled-Guessi	Inthrottled-Gues	nternal-Observa .eaks-from-Othe	hishing	hind-Party	plicit-Consent
https://www.cl.ca	m.ac.uk/techreports	/UCAM-CL-TR-817.p	Grberer	Described in	teference	Aemorywise calable-for-	Iothing-to-C	hysically-E lasy-to-Lear	fficient-to-U	njrequent-Er lasy-Recove	lccessible legligible-C	erver-Comp	dature	correction to l	lesilient-to-1	esilient-to-l	tesilient-to-1 esilient-to-1	lesilient-to-l	lo-Trusted-1	tequiring-Ex Inlinkable
		(Incumbent)	Web personale	<u> </u>	PA [[12]	<u> </u>	-					<b>S</b>			<u><u>v</u><u>v</u></u>	N.	2 2	2 2	$\leq$	
		(incumbent)	Firefox		[13]	0	0		-						ŏ				<u>.</u>	
		Password managers	LastPass	1 V-A	[42]	0	0	ō •						0	ŏĸ	0 0	Ö		S 📄	
			LIBRSA	IV-B	[42]	•		•		0	=•	0			0		<u> </u>		÷	••
		Proxy	Impostor		[23]	0.	•			•	•	• 3	5		õ	- i	0			
			OpenID	IV-C	[27]	0.	•	0 0	•		• •			0	00	0 0		(		•
			Microsoft Passport		[43]	0.	•	• •	•		•		•	o	00	0				•
		Federated	Facebook Connect		[44]	0.	•	ō •	•		• •		•	0	00	0	۰	•		
		redefated	BrowserID		[45]	0.	•	• •	•		••	-	00	0	00	0 0	۰	•		•
			OTP over email		[46]	0.	•	•			••			0	00	0	۰			•
		Combined	PCCP	IV-D	[7]		٠	•	0	• •	=•				• 0	,	٠	•	• •	••
		Graphical	PassGo		[47]	1	٠	٠	0	• •	•		0		٠				• •	••
			GrIDsure (original)	IV-E	[30]		٠	•	0	• •	•				۲			•	•	••
	Constitue		Weinshall		[48]		٠				•			0	٠		•		••	••
		Cognuve	Hopper Blum		[49]		٠				••			0	٠		•		••	••
			Word Association		[50]		•	•	• •	0 0	••	_			<u> </u>				••	••
			OTPW	IV-F	[33]			•	=	•	=•		•••				••		••	••
		Paper tokens	S/KEY		[32]					•								0		••
			PIN+TAN		[51]		_	-	-	00	0			•						•••
		Visual crypto	PassWindow	wo	[52]	•	-	_	-	_	•			0						
			KSA SecuriD	IV-G	[34]				2						22				1	
		TT- days to be a	Tubikey		[33]										5			Ξ.		
		Hardware tokens	CAP reader		[54]	-	1								Ň.	a mai				
			Pico		[33] [8]			•	0	0	==				22					
			PhooIproof	IV-H	[36]		0		0	0	0 0	0								••
			Cronto	1 4-11	[56]	1	0		0	0	0									
		Phone-based	MP-Auth		[6]		0		0	0	00				0					••
		r none-based	OTP over SMS		101		0			0 0	0						•	•	2	••
			Google 2-Step		[57]		0	•	0	0 0	0		•	0	0			•	• •	••
			Fingerprint	IV-I	[38]		•	• •	0		0		0	۲				Ē	•	•
		Biometric	Iris		[39]		•	• •	0		0		0	۲				F	•	0
			Voice		[40]	• •	•	•	0		0 0		0 0	۲	ď	8		Ē	•	•
			Personal knowledge		[58]	0	٠	•	• •	• •	••		•••	•				•	• •	••
		Recovery	Preference-based		[59]	0	٠	٠	0	• •	••				0			•	• •	••
			Social re-auth.		[60]		•	•			••		• •	0			0 0			• •

# 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?







Online Banking Username Enter Username					
Password Enter Password					
	Forgot Password				
Sign In Enroll >					
Sign in to oth	er services >				



Online Banking									
Username	Username Enter Username								
Password	Password Enter Password								
Forgot Password									
Sign In Enroll >									
Sign in to other services >									





$\bullet \bullet \checkmark \square$	l l evenxi.com ♂	1 D
	Log in to your PayPal account	+
	PayPal	I
	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"

Bank of the West   - Mozilla Fin	efox		
Eile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookr	marks <u>T</u> ools <u>H</u> elp Bank of the West (US) https://www.k	oankofthewest.com/BOW/home	☆ • Google 🔎
BANK offewes	Home Sign in ▼	Search GO Have a question? Contact Us.	Apply online Image: Constraint of the state   Find us ZIP code or city & state GO
PERSONAL SMALL BUSINES	s com Apparent b	prowser is just	
Products & Services Checking Savings & CDs Credit Cards	Achi Buyat Buyat Savef	eractive image by Javascript real browser!	eTimeBanker Login Where do I enter my password? Alternate Login
Loans Wealth Management & Trust Insurance See all our Personal banking	Maximize home equity Consolidate debt Try our financial calculators products »		mark hashefthewart can