1Password.com

What does “MFA” mean?

Jeffrey Goldberg

jeff@1Password.com

1Password.com

What does “MFA” mean?

It means multi-factor authentication.

In certain cases it is called “2FA” for two-factor authentication.

What does it mean …

1. For ordinary users?
2. For knowledgeable users?
3. In terms of the actual security properties it offers?

Jeffrey Goldberg
jeff@1Password.com

What do you believe?

What do you believe?

1. Does MFA mean that you need all factors to authenticate?

What do you believe?

1. Does MFA mean that you need all factors to authenticate?
2. Does MFA help protect you if your computer is compromised?

What do you believe?

1. Does MFA mean that you need all factors to authenticate?
2. Does MFA help protect you if your computer is compromised?
3. Does MFA protect you if the server is compromised?

What do you believe?

1. Does MFA mean that you need all factors to authenticate?
2. Does MFA help protect you if your computer is compromised?
3. Does MFA protect you if the server is compromised?
4. Does MFA make make it safe to reuse passwords?

What do you believe?

1. Does MFA mean that you need all factors to authenticate?
2. Does MFA help protect you if your computer is compromised?
3. Does MFA protect you if the server is compromised?
4. Does MFA make make it safe to reuse passwords?
5. Does having a second factor help you if you need to reset a forgotten password?

Mind the gaps

Claims

1. ∃ gaps twixt ordinary user understandings and actual security properties of MFA
2. ∃ gaps twixt expert user understandings and actual security properties of MFA
3. These gaps can lead to dangerous behavior

Evidence for claims

Evidence for claims

- Anecdotes

Evidence for claims

- Anecdotes
- Hearsay

Evidence for claims

- Anecdotes
- Hearsay
- Divine revelation?

Evidence for claims

- Anecdotes
- Hearsay
- Divine revelation?

“Anecdote” is the singular of “data”, right?

Who goes there?

Who goes there?
It is I, Penelope! 👋
Penelope

Authentication

Authentication is the process of proving that you are who you say you are.*

You provide your proof to a verifier, who either accepts it or rejects it. If *V* accepts it, they will grant you access to something.

*"Who you say you are" may mean the owner of some anonymous account. It doesn't have to be a legal identity.

What does "MFA" mean?

Classic Authentication

Classic Authentication

V asks P for her username

Jeffrey Goldberg
jeff@1Password.com

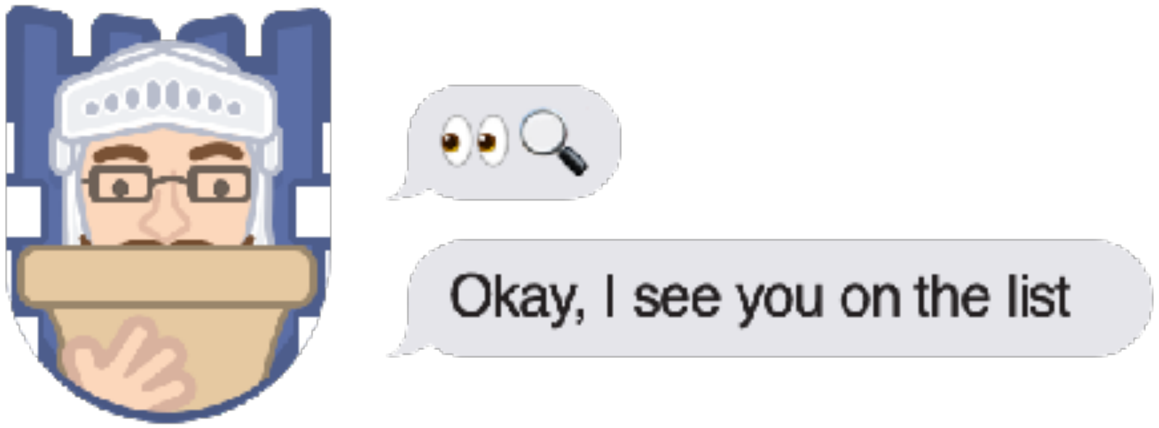
Classic Authentication

VINCENT
Who goes there?
It is I, Penelope! 👋
Penelope

V asks P for her username

P tells V her username

Classic Authentication



V asks P for her username

P tells V her username

V checks that there is such a username

Classic Authentication

V asks P for her username

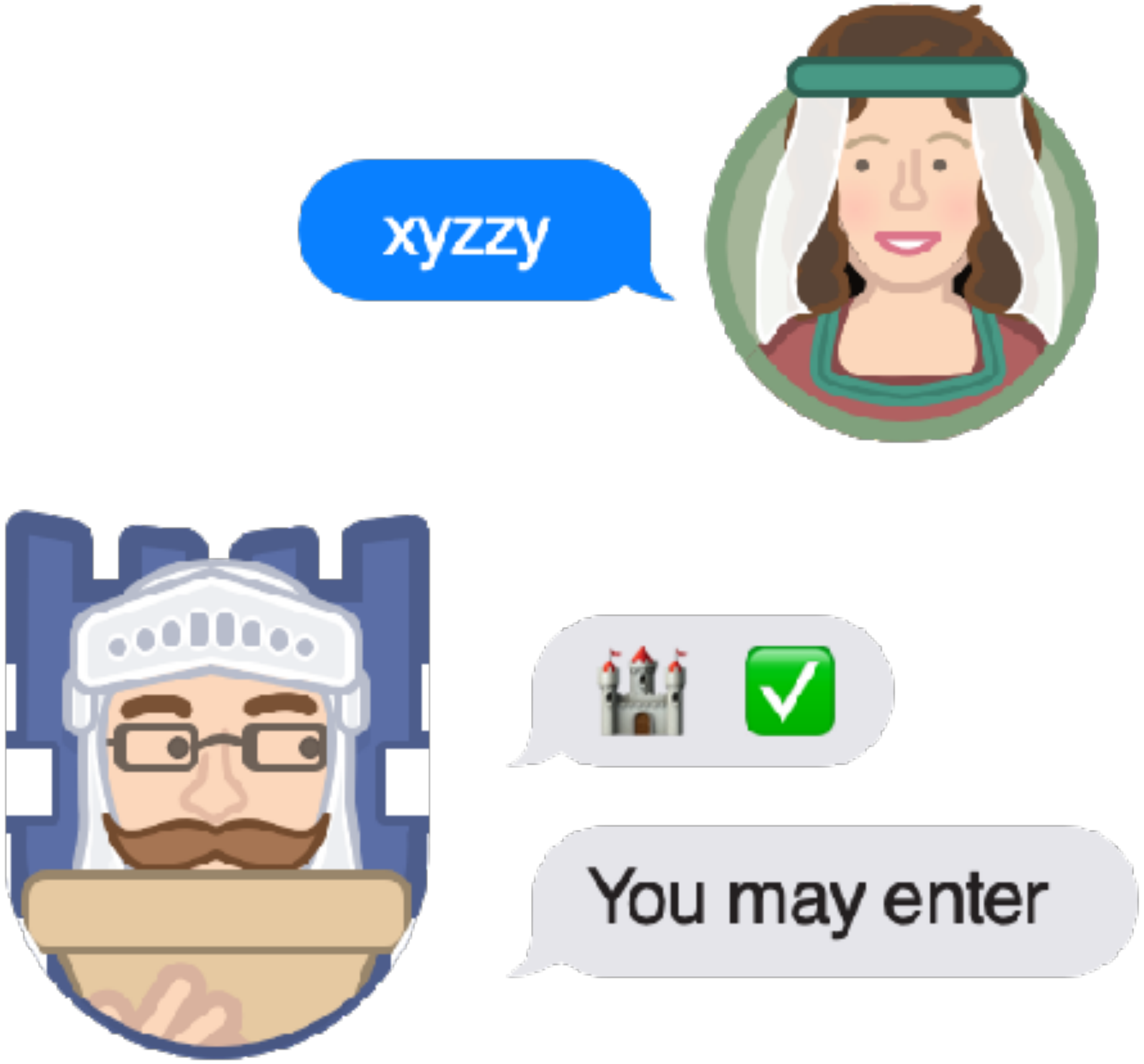
P tells V her username

V checks that there is such a username

V asks P for her password

Jeffrey Goldberg
jeff@1Password.com

Classic Authentication



V asks P for her username

P tells V her username

V checks that there is such a username

V asks P for her password

P tells V her password.

V checks that P provided

V verifies that the password is correct and grants her access if it is

Classic problems

- *V* learns *P*’s secret
- Eavesdroppers learn *P*’s secret
- *P*’s secret is guessable
- *P* never learns if *V* is really *V*
- *P*’s secret, if captured, can be used to enter this castle
- *P*’s secret, if captured, might be usable at other castles

Modern password problems

- What *V* stores may be used for cracking
- *P* is not informed when some tries to enter the castle using her name
- *P*’s password is the only thing required to gain entry

Security properties

Useful security properties

- *P* proves identity to *V*
- *V* proves identity to *P*
- No-one learns any secrets during authentication
- Big H: Long term secrets are unguessable
- Long term secrets are unique
- What *V* stores long term is not usable for guessing *P*'s long term secret.
- More than one kind of secret required

Useful properties (continued)

- *P* is made aware of any attempts to use her name
- If *P* loses or forgets one of her long term secrets, she can get it reset using the one that she maintains

Non-Authentication security properties

Some security properties have little to do with authentication.

Once more into the breach!

Penelope’s precious stuff, stored within the castle, is kept safe from

- A breach in the walls
- Dragons flying over the wall
- Treachery from within the walls

Bewitched

Penelope's precious stuff, stored within the castle, is kept safe even if …

Penelope is bewitched so that she is under the control of an evil wizard after she enters the castle

Major misunderstanding

Forgetting the auth

With (proper) MFA the *authentication process* remains secure as long as at least one factor remains secure.

“A keylogger on my device”

“With the speed zero day malware are created these days and with the tools and the many advanced techniques they have available, […] users are at risk almost on a daily basis. […] I am not even sure I can trust that my own computer is truly secure despite the fact that it is behind an IDP/Firewall device.”

—Other forum user, January 2017

“A keylogger on my device”

> “If I happen to have a key logger on my computer or if I use a public computer to access my account, my entire account key could be copied by someone. [...] I have 2FA set up on my email account, so I have to authenticate using 2FA any time I'm not at home.”
>
> —Forum user, January 2017

Alternative Auth

If a service uses access to a single factor for recovery or reset it is making it easier for attackers

Weakening other factors

Using a second factor may give people confidence to use a weaker primary factor than they otherwise might.

Weakening is fine

Except for when it isn’t

If the factor that people chose to weaken is important for more than just authentication, they may do serious damage

Conclusions?

- The security properties on any give MFA system depend on many subtle things about the implementation, service, and threats
- Using MFA in some circumstances may add only tiny improvements to authentication security, but may encourage users to behave in ways that substantially weaken there security

Call for help

- Can we give customers what they demand without harming their security?
- Can my speculations about user behavior be studied and tested to see if my worries are justified?

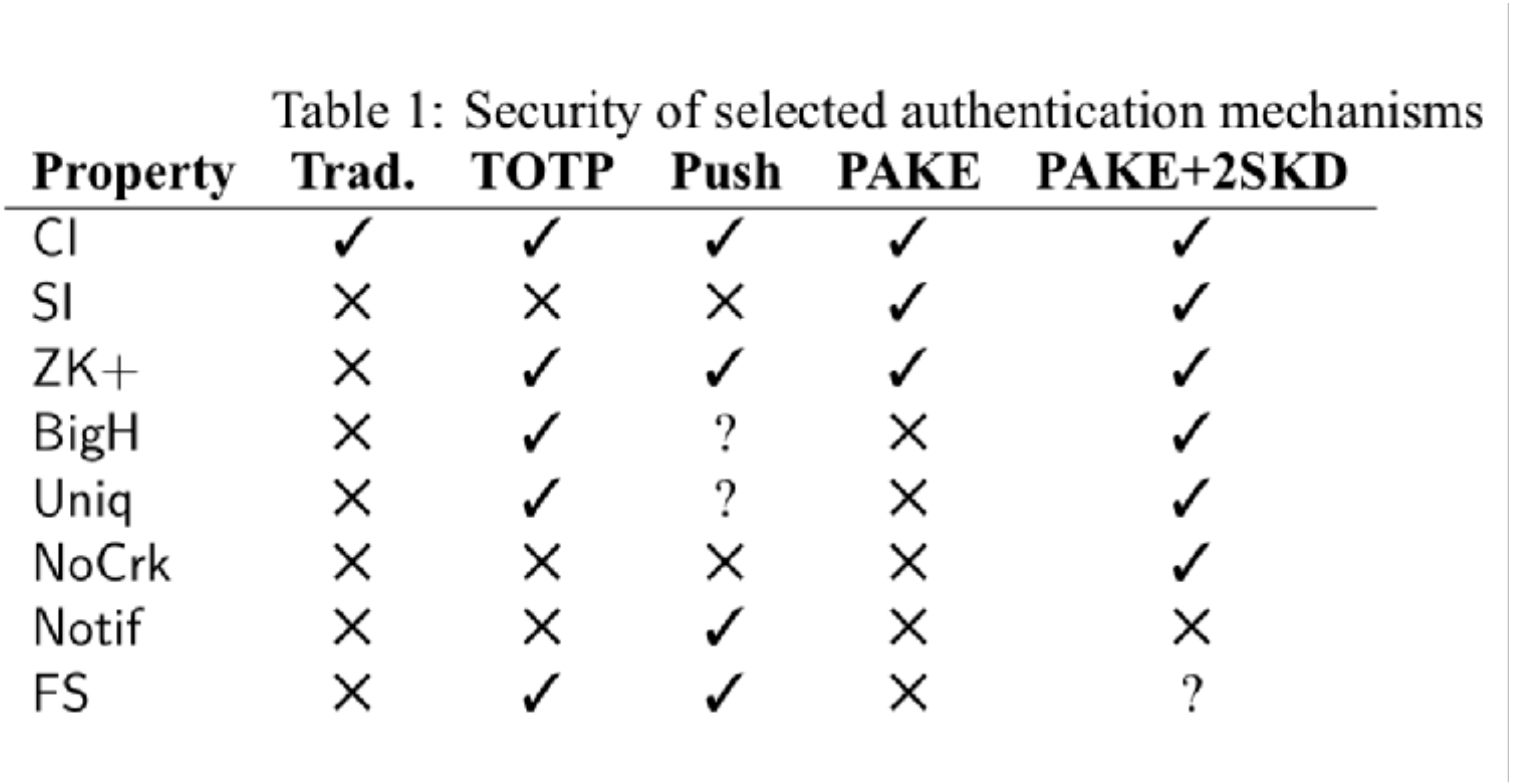


Table 1: Security of selected authentication mechanisms

Property	Trad.	TOTP	Push	PAKE	PAKE+2SKD
CI	✓	✓	✓	✓	✓
SI	×	×	×	✓	✓
ZK+	×	✓	✓	✓	✓
BigH	×	✓	?	×	✓
Uniq	×	✓	?	×	✓
NoCrk	×	×	×	×	✓
Notif	×	×	✓	×	×
FS	×	✓	✓	×	?

Table 1

Security Properties of different authentication schemes