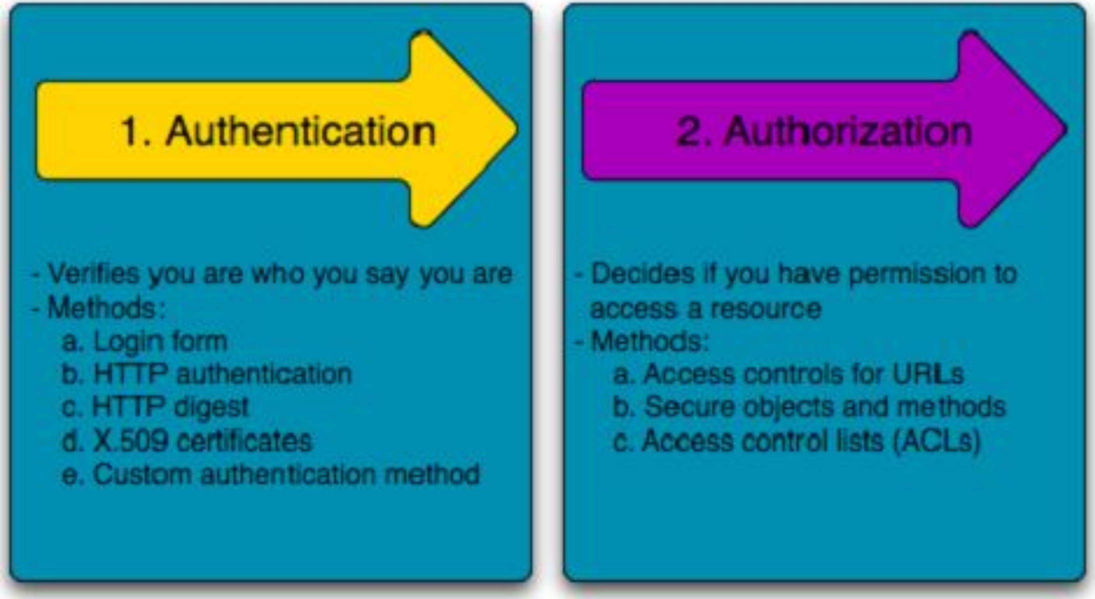
nimble

Let’s GO Passwordless

Trung

Growth Session #20 - XX - December 20-21 2018

Authentication & Authorization



1. Authentication

- Verifies you are who you say you are
- Methods:
  a. Login form
  b. HTTP authentication
  c. HTTP digest
  d. X.509 certificates
  e. Custom authentication method

2. Authorization

- Decides if you have permission to access a resource
- Methods:
  a. Access controls for URLs
  b. Secure objects and methods
  c. Access control lists (ACLs)

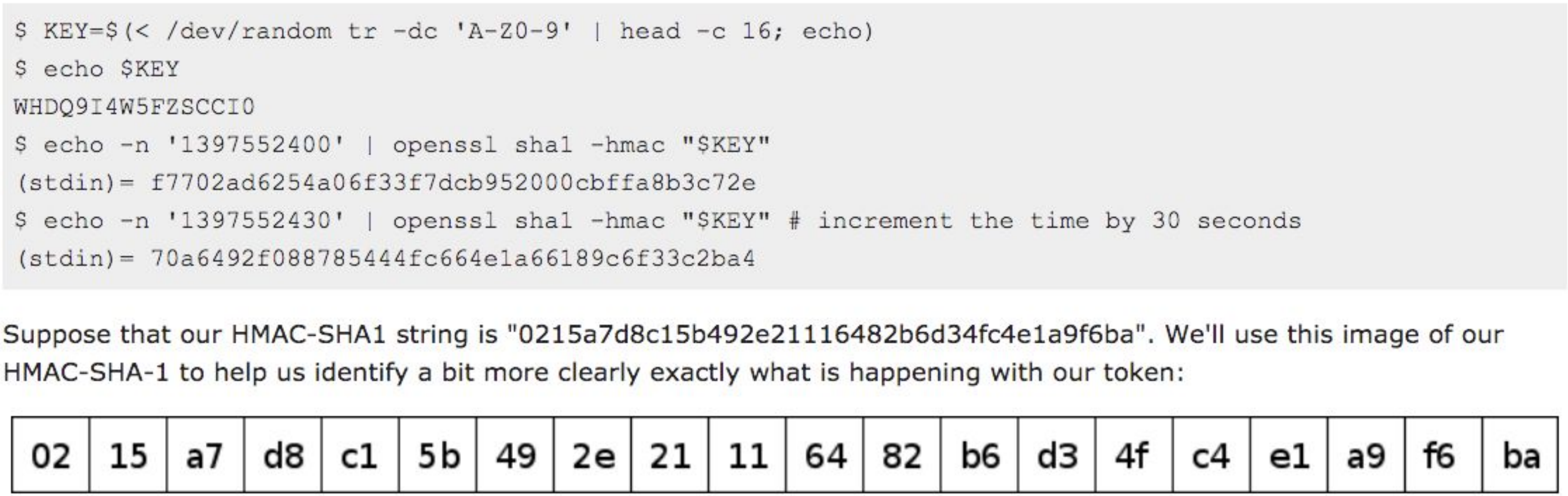
The Authentication story

- Single-factor authentication system such as username and password is not unbreakable.
- How many ways can we secure our authentication?
- The 2 Factor Authentication comes to rescue.
- And MFA?

The importance of Time

- Making the shared secret into a moving target.
- TOTP uses the UNIX epoch as its time scale, in seconds.
- There is no use of remember a same shared secret,
- Clients should be able to provide corresponding reply to the server side challenging request, just to prove your identity at the time request is made.

How to compute the TOPT



```
$ KEY=$(< /dev/random tr -dc 'A-Z0-9' | head -c 16; echo)
$ echo $KEY
WHDQ9I4W5FZSCCI0
$ echo -n '1397552400' | openssl sha1 -hmac "$KEY"
(stdin)= f7702ad6254a06f33f7dcb952000cbffa8b3c72e
$ echo -n '1397552430' | openssl sha1 -hmac "$KEY" # increment the time by 30 seconds
(stdin)= 70a6492f088785444fc664e1a66189c6f33c2ba4
```

Suppose that our HMAC-SHA1 string is "0215a7d8c15b492e21116482b6d34fc4e1a9f6ba". We'll use this image of our HMAC-SHA-1 to help us identify a bit more clearly exactly what is happening with our token:

02	15	a7	d8	c1	5b	49	2e	21	11	64	82	b6	d3	4f	c4	e1	a9	f6	ba

Dynamic truncation

- Take the last 4 bits:

02	15	a7	d8	c1	5b	49	2e	21	11	64	82	b6	d3	4f	c4	e1	a9	f6	ba

- ‘A’ in Hex = 10 in Dec

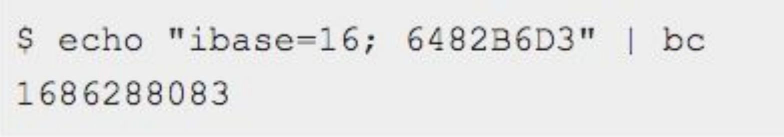
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
02	15	a7	d8	c1	5b	49	2e	21	11	64	82	b6	d3	4f	c4	e1	a9	f6	ba

- Read the 31 bits start from the offset of 10

02	15	a7	d8	c1	5b	49	2e	21	11	64	82	b6	d3	4f	c4	e1	a9	f6	ba

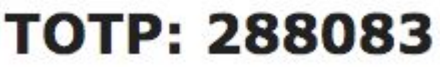
Last steps

- Convert to base16



```
$ echo "ibase=16; 6482B6D3" | bc
1686288083
```

- Finally modulo it for 1.000.000 you should get the OTP

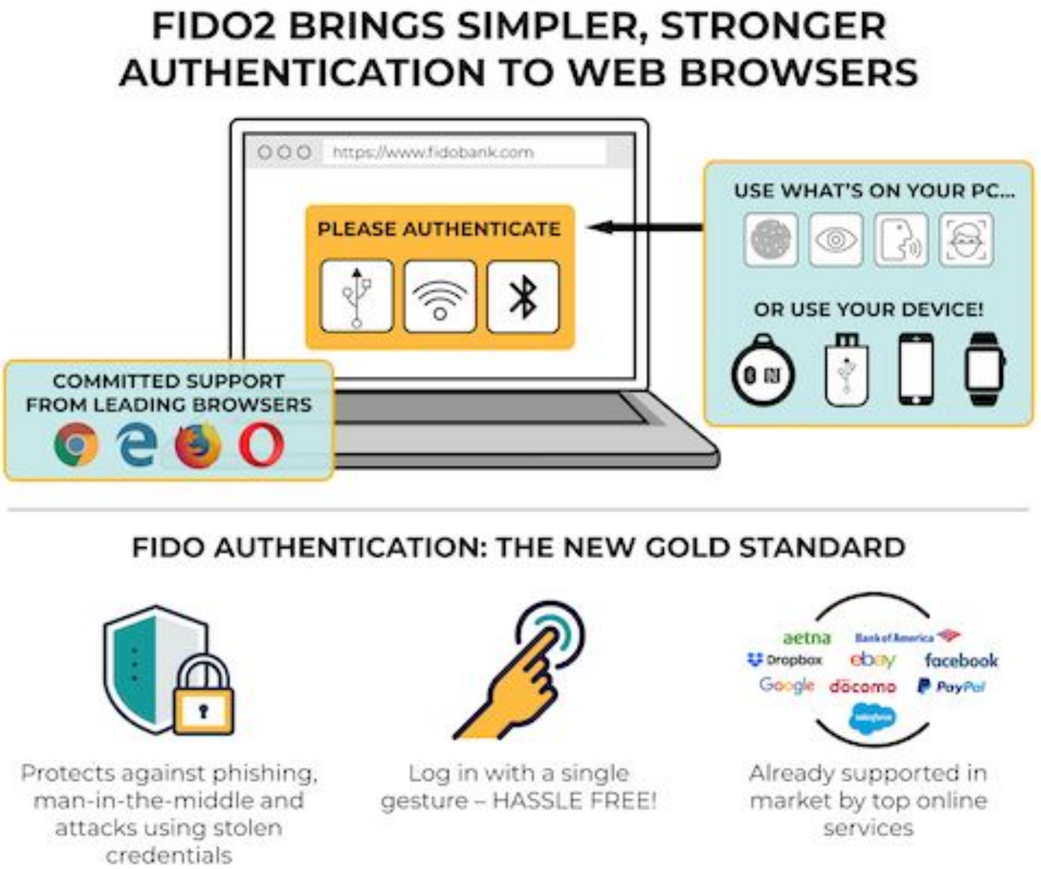


TOTP: 288083

What is WebAuthn

- An effort from Google, FIDO Alliance and W3C to develop a new way to reduce the reliance on passwords and the auth methods, but still keep the security hard.
- Under the hood, the WebAuthn spec uses public key cryptography to provide a way for browsers to sign a challenge using a private key stored by the operating system or on a physical hardware token

WebAuthn Use Case



FIDO2 BRINGS SIMPLER, STRONGER AUTHENTICATION TO WEB BROWSERS

FIDO AUTHENTICATION: THE NEW GOLD STANDARD

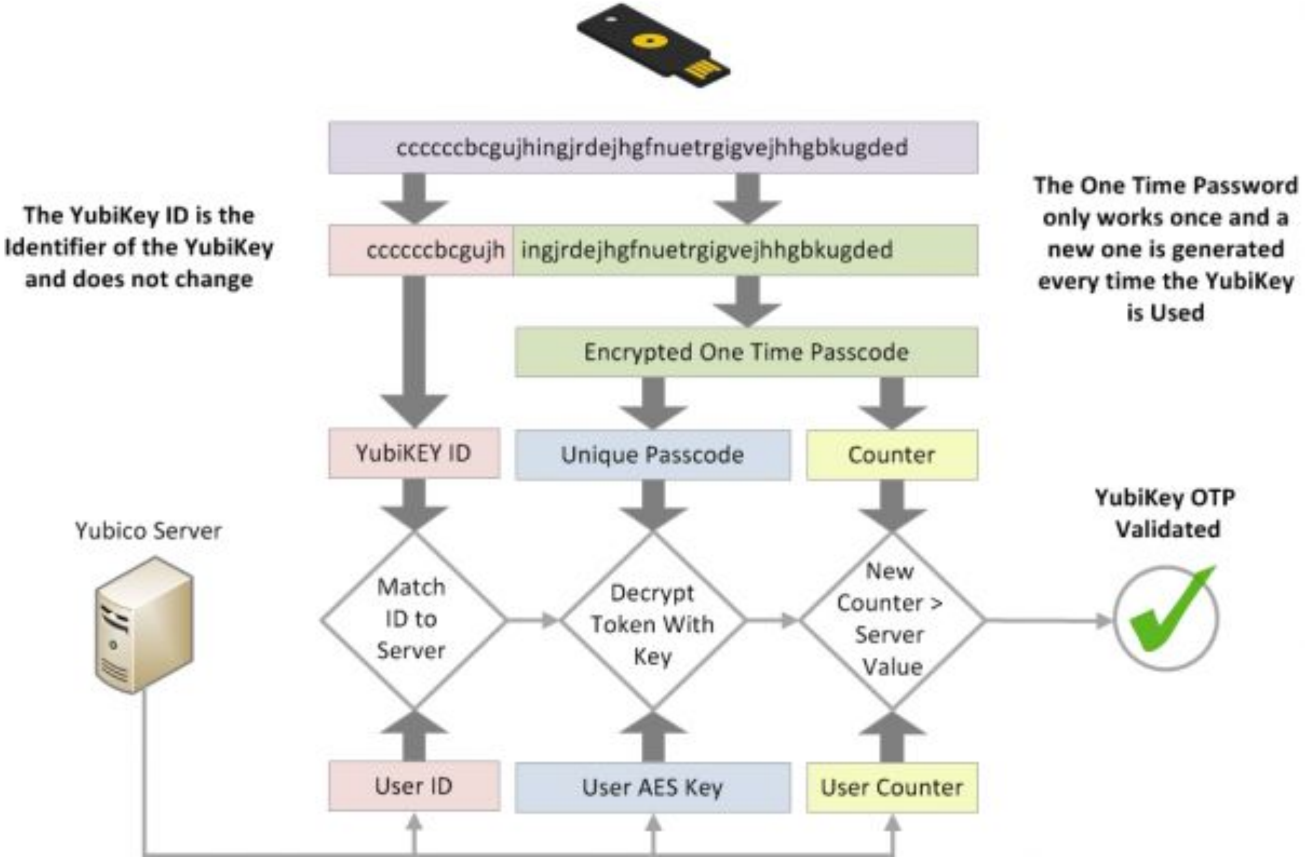
Protects against phishing, man-in-the-middle and attacks using stolen credentials

Log in with a single gesture – HASSLE FREE!

Already supported in market by top online services

The implementation

- The WebAuthn spec defines two new JavaScript APIs available to web applications: `navigator.credentials.create` and `navigator.credentials.get`.
- Yubikey in a nutshell:
  - A USB-key that simplifies the process of logging in with strong two factor authentication
  - With a simple touch on the device, it generates a One-Time Password (OTP) on any computer and platform without any client software needed
  - By touching the integrated button, the YubiKey sends a time-variant, secure login code as if it was typed in from a keyboard



The YubiKey ID is the Identifier of the YubiKey and does not change

The One Time Password only works once and a new one is generated every time the YubiKey is Used

cccccbcgujhingjrdejhgfnuetrgigvejhhgbkugded

cccccbcgujh

ingjrdejhgfnuetrgigvejhhgbkugded

Encrypted One Time Passcode

YubiKEY ID

Unique Passcode

Counter

Yubico Server

Match ID to Server

Decrypt Token With Key

New Counter > Server Value

YubiKey OTP Validated

User ID

User AES Key

User Counter

Progress and achievement

- Get to understand TOTP mechanism
- Implementation in a Go project
- Demo application

Next Steps

- DB connection
- OAuth, combination of MFA.

Disclaimer: WebAuthn is still under developing and not ready for Production yet!

Thanks!

Contact Nimble

nimblehq.co
hello@nimblehq.co

Bangkok

399 Interchange 21 Sukhumvit Road, Unit
#2402-03, Klong Toei, Wattana, Bangkok
10110, Thailand

Singapore

28C Stanley St, Singapore 068737

Hong Kong

20th Floor, Central Tower
28 Queen's Road, Central, Hong Kong

nimble