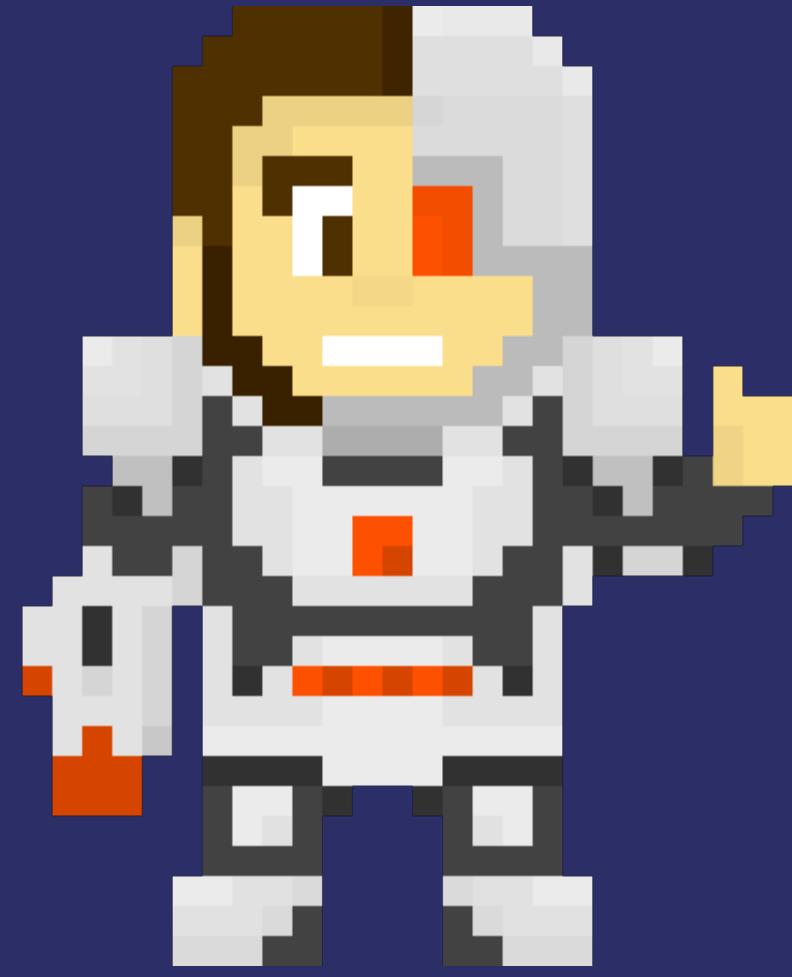


2FA, WTF?

I'm Dominik!



About me

Developer Evangelist at



Get in touch with me!

[@dkundel](https://twitter.com/dkundel)
dkundel@twilio.com
[github/dkundel](https://github.com/dkundel)



HACKERS!

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta



Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta



Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta



Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

2FA, WITF?

Two-Factor Authentication

Hacking in progress . . .



Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

Two-Factor Authentication

Two different forms of identification from the user

Typically:

- Something that you know
- Something that you have

Why?

**Passwords
Alone Are
Weak**



Story Time!

Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

Mark Zuckerberg

Users are bad with passwords!

Top 10 Passwords of 2015

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball

Source: <https://www.teamsid.com/worst-passwords-2015/>



**Other websites are bad
with passwords!**



LastPass...|

A portrait of Mat Honan, a man with light brown hair and a beard, wearing glasses and a dark turtleneck sweater. He is looking slightly to his left. The background is a solid teal color.

Mat Honan

Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

Hacking Timeline

- Hackers find his personal website and then his Gmail
- Detect alternative email through Gmail password recovery
 - Get Honan's address through whois on his domain
- Phone Amazon to add a new credit card to Honan's account
 - Call again to recover the Amazon account
- Hacker log into Amazon to retrieve last 4 digits of his actual card

Hacking Timeline

- **4:33pm** Call Apple to recover the iCloud access using the billing address and 4 digits of the credit card
- **4:50pm** Permanently reset iCloud password
 - **4:52pm** Reset Gmail password
- **5:00pm** Hacker delete his iPad and iPhone
 - **5:02pm** Reset Twitter password
 - **5:05pm** Wipe Macbook
- **5:12pm** Hacker tweet to tack credit



Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta



Social engineering works!

**Passwords
Alone Are
Weak**

Physical protection layer for a digital world



Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

How?

Typical User Registration Flow

1. User visits registration page
2. Enters username and password
3. User is logged in

Typical User Log-in Flow

1. User visits log-in page
2. Enters username and password
3. System verifies details
4. User is logged in

Phone 2FA

SMS / Voice

SMS-based User Registration Flow

1. User visits registration page
2. Enters username, password and phone number
3. Verifies phone number
4. User is logged in

SMS-based User Log-in Flow

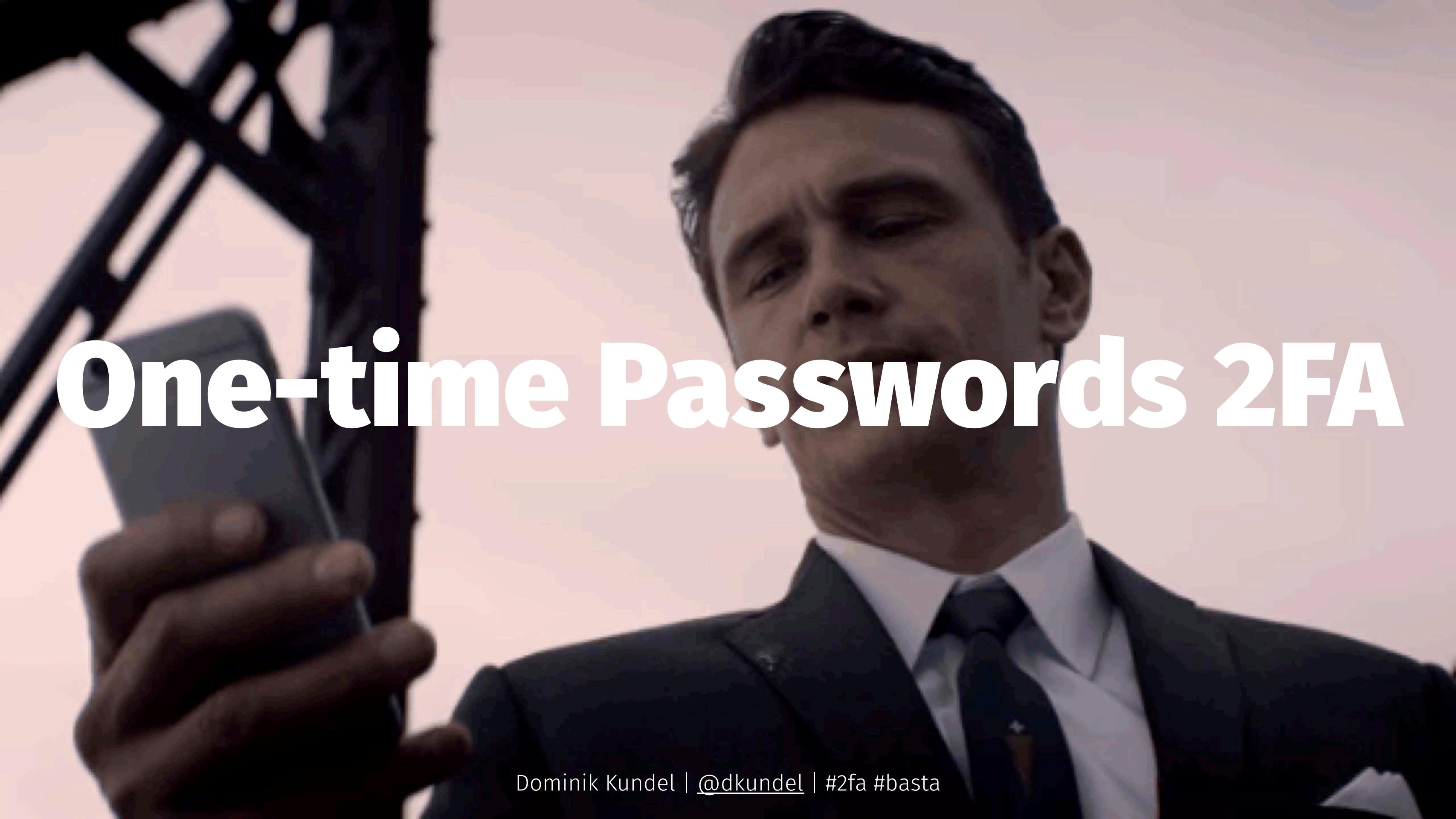
1. User visits log-in page
2. Enters username and password
3. System verifies details
4. System sends verification code to user by SMS
5. User enters verification code
6. System verifies code
7. User is logged in



Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

DeRay Mckesson

Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

A professional-looking man in a dark suit and tie is holding a smartphone in his right hand, looking down at the screen with a focused expression. The background is a plain, light-colored wall.

One-time Passwords 2FA

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

OTP-based User Registration Flow

1. User visits registration page
2. Enters username and password
3. Generate secret for the user
4. Share secret with the user
5. User is logged in

OTP-based User Log-in Flow

1. User visits log-in page
2. Enters username and password
3. System verifies details
4. User opens auth app
5. Enters app verification code on site
6. System verifies code
7. User is logged in

Secret based Codes

HOTP/TOTP

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

HOTP Formula

$\text{HOTP}(K, C) = \text{Truncate}(\text{HMAC}(K, C)) \ \& \ 0x7FFFFFFF$

HOTP-Value = $\text{HOTP}(K, C) \bmod 10^d$



This repository

Search

Pull requests Issues Gist



guyht / notp

Watch ▾

18

Star

295

Fork

Code

Issues 6

Pull requests 2

Pulse

Graphs

Node One Time Password library, supports HOTP, TOTP and works with Google Authenticator <https://github.com/guyht/notp>

67 commits

1 branch

3 releases

14 contributors

https://github.com/guyht/notp

guyht Merge pull request #32 from coolaj86/patch-4 ...

Latest commit bbdff82a on Oct 8, 2015

examples	Updated example to work with new API. Fixes issue #4	4 years ago
test	tests for not passing opt	2 years ago
.gitignore	update .gitignore	4 years ago
.travis.yml	remove node v0.4.x support	2 years ago
LICENSE	cleanup README	4 years ago
Readme.md	fix readme.md markdown so it renders properly on npmjs.com	11 months ago
index.js	Merge pull request #32 from coolaj86/patch-4	8 months ago
package.json	Dominik Kundel @dkundel #2fa #basta add thirty-two to dev-dependencies	2 years ago

DEMO

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

Sharing Secrets

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

QR Codes

otpauth://TYPE/LABEL?PARAMETERS

otpauth://totp/Example:dkundel@twilio.com?secret=MySecret&issuer=Example





Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

**Friends don't let friends write their own
authentication frameworks!**

**Friends don't let friends write their own
two-factor authentication frameworks!**



Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta

Authy-based User Registration Flow

1. User visits registration page
2. Enters username, password and phone number
3. System registers user with Authy
4. User is logged in

Authy-based User Log-in Flow

1. User visits log-in page
2. Enters username and password
3. System verifies details
4. Authy prompts user
5. User enters app verification code on site
6. System verifies success with Authy
7. User is logged in

A photograph of a man with dark hair and a beard, wearing a red long-sleeved shirt. He is sitting at a desk, looking intently at a laptop screen. In the background, there is a computer monitor on a desk with two windows open, and a person is visible in a room with a patterned wall.

UX or 2FA

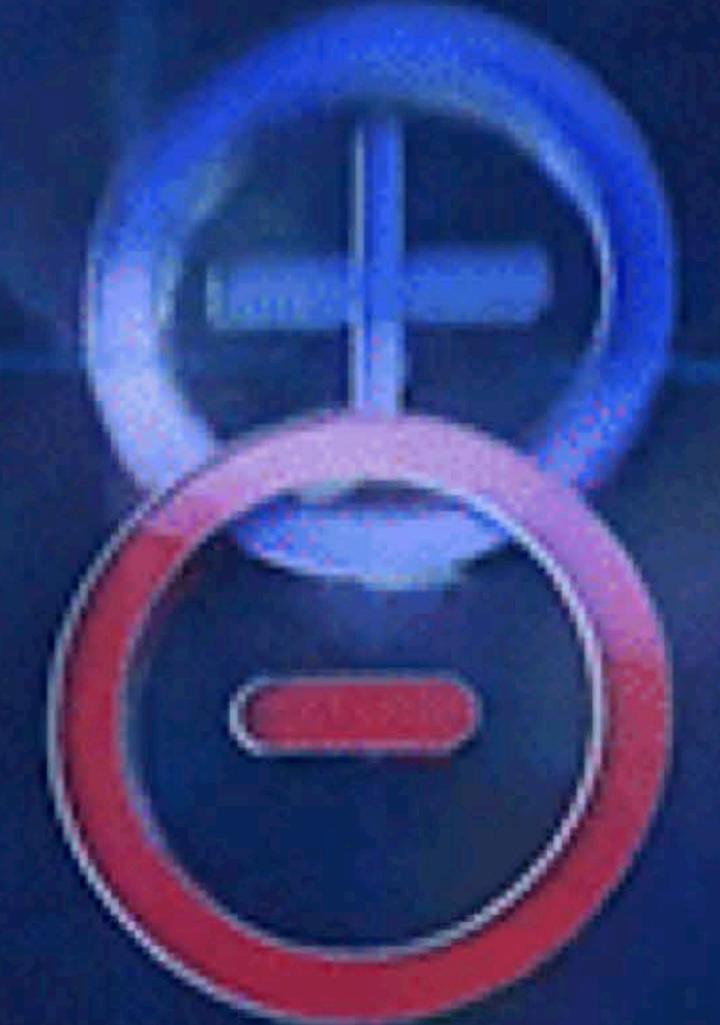
Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

Push notifications (OneTouch)

A photograph of a group of people, mostly young adults, looking towards the right side of the frame. They appear to be in a meeting or presentation setting. The background is slightly blurred.

demo

Dominik Kundel | [@dkundel](https://twitter.com/dkundel) | #2fa #basta



Dominik Kundel | [@dkundel](https://twitter.com/@dkundel) | #2fa #basta

Summary

Users are bad with passwords!

**Other websites are bad
with passwords!**

Social engineering works!

**2FA can be push, tokens
or SMS**

2FA is for your users!

PASSWORD

Thank You!

@dkundel
dkundel@twilio.com
github/dkundel



Credits:

<http://www.hackercg.com/wp-content/uploads/2015/12/Hacker.jpg>

<http://www.v3.co.uk/IMG/494/302494/hacker-hacking-dark-hoodie.jpg>

<http://qruniversity.hipscan.net/sites/default/files/article-images/computer-hacker.jpg>

<http://www.wpdroids.com/wp-content/uploads/2014/12/How-to-scan-QR-code-in-your-Smartphone.jpg>

https://img1.etsystatic.com/036/0/9343025/il_fullxfull.654477583_8ktu.jpg

<http://cdn1.tnwcdn.com/wp-content/blogs.dir/1/files/2015/01/mark-zuckerberg-qa-colombia.png>

<https://lastpass.com/press-room/>

http://66.media.tumblr.com/d19d0b84160d51e696aeaa939b84f4de/tumblr_ns7wyq9uVl1qhub34o10r1_500.gif