„O passłordsach, emefejach i innych magicznych zaklęciach”

Czy wiemy jak ich używać?

.NET Group, Akademia Cybersecurity #1 @ZUT


PASSWORD PLEASE?

Porozmawiajmy o bezpieczeństwie

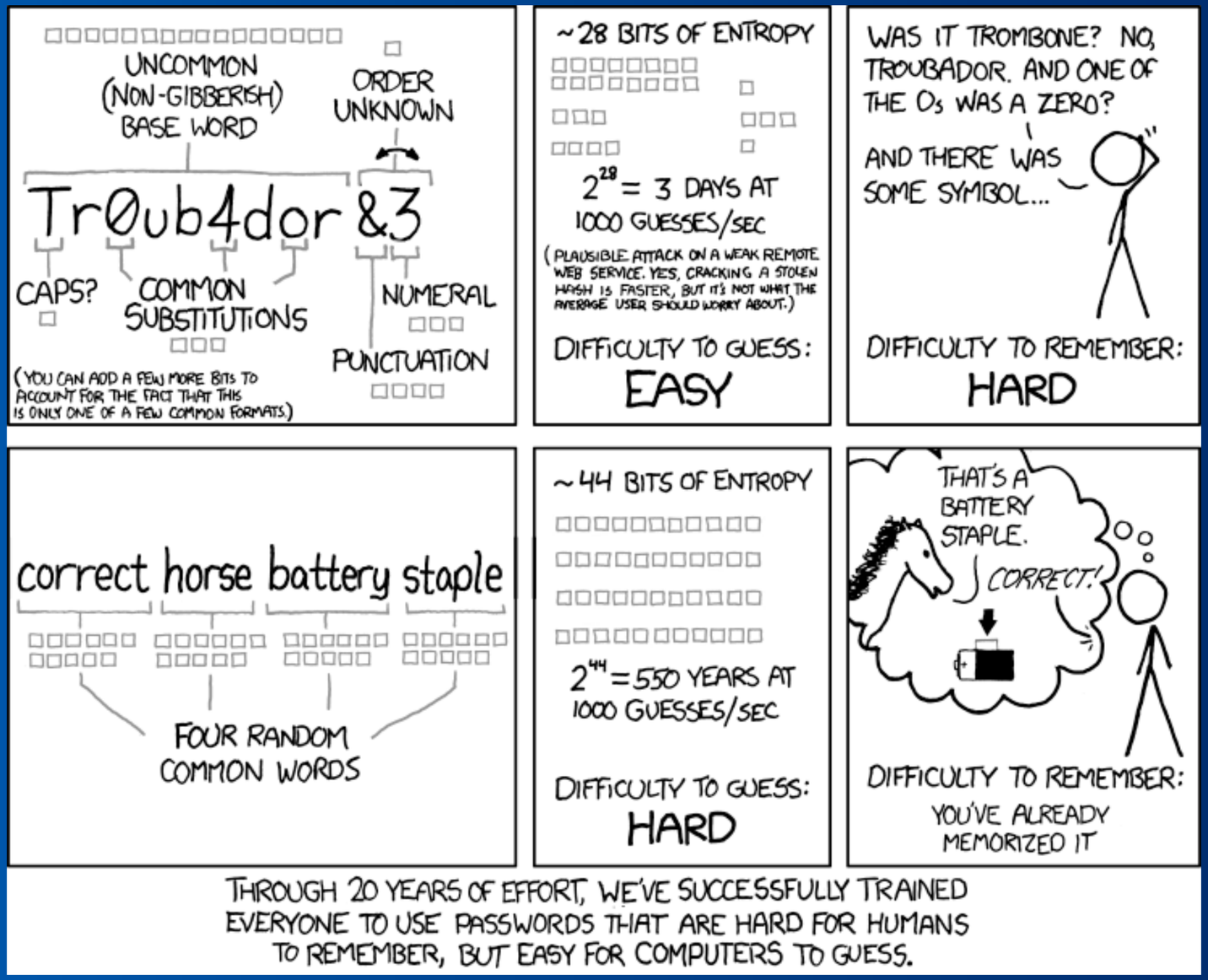
- Rodzaje haseł
- Które hasło jest bezpieczniejsze?
- Gdzie je trzymać?
- Jakie mamy alternatywy dla używania haseł?
- Czy są one całkowicie bezpieczne?

Hasła

„Co do zasady stosuję 3 rodzaje haseł – pierwszy gatunek to trywialne (np. kluska997), drugi gatunek to trudne ale do zapamiętania (np. Makaron@Gotowany#Trzy$Minuty%678) oraz trzeci gatunek to bardzo trudne, nie do zapamiętania, generowane losowo (np. 1KvuSPm&i21F”EsW^R4H).”

~Adam Haertle, Z3S ([5EA])

Hasła słowne (phrase passwords / Mnemonic passwords)



Hasła słowne (phrase passwords / Mnemonic passwords)

Na ile to prawda?

[4E8]

Entropia

1 bit

1 0

Pojedyncze znaki
(Litery, cyfry, znaki)
~ 70

VS

170 000 słów ?

Hasła słowne (phrase passwords / Mnemonic passwords)

Dyskusja

So, that's not all that horrible. It's not exactly future proof, but not as horrible as this article would have us believe. I managed to find someone running 450 billion MD5 hashes per second on a p3.16xlarge on AWS at a cost of $24.48 per hour.

That means only just over 4 days to crack your password, but it also means someone just spent $2,417 to crack it. For a single password.

Sure, there probably are cheaper and more efficient ways, but for the general public a 4 word password isn't horrible. A 4 word password as a master password in a password manager would be pretty great for most.

1 ^ | v · Reply · Share ›

Dyskusja

howsecureismypassword.net

Jak przechowywane są hasła?

Funkcje skrótu, salt

F(1234) = FCAF52F9EE7CBFF

F() =

F( + ) = ?

Problem?

username	password
user1	71d00b760d017b2999eb54e32f41f592
user7	71d00b760d017b2999eb54e32f41f592
user13	71d00b760d017b2999eb54e32f41f592

VS

username	salt	password
user1	SALT	a66a96b36d78e452202c12d36b6d198c
user7	ASDF	8062279f0ba04fa6ee41d0a9e04f4c93
user13	ABCD	5743092bfb79214247c50c4102af0b99

[A1D]

Problem?

Hash function	Security claim	Best attack	Publish date	Comment
MD5	2^{64}	2^{18} time	2013-03-25	This attack takes seconds on a regular PC. Two-block collisions in 2^{18}, single-block collisions in 2^{41}.[1]
SHA-1	2^{80}	$2^{61.2}$	2020-01-08	Paper by Gaëtan Leurent and Thomas Peyrin[2]
SHA256	2^{128}	31 of 64 rounds ($2^{65.5}$)	2013-05-28	Two-block collision.[3]
SHA512	2^{256}	24 of 80 rounds ($2^{32.5}$)	2008-11-25	Paper.[4]
SHA-3	Up to 2^{512}	6 of 24 rounds (2^{50})	2017	Paper.[5]
BLAKE2s	2^{128}	2.5 of 10 rounds (2^{112})	2009-05-26	Paper.[6]
BLAKE2b	2^{256}	2.5 of 12 rounds (2^{224})	2009-05-26	Paper.[6]

Table color key [edit]

No attack successfully demonstrated — attack only breaks a reduced version of the hash or requires more work than the claimed security level of the hash

Attack demonstrated in theory — attack breaks all rounds and has lower complexity than security claim

Attack demonstrated in practice

Problem?

#> hydra -L usernames.txt
-P passwords.txt
192.168.2.62 http-post-form

#> hashcat -m 13400 -a 0 -w 1
CrackThis.hash cracklib-words

Alternatywy

Diceware

```
...
43136   mulct
43141   mule
43142   mull
43143   multi
43144   mum
43145   mummy
43146   munch
43151   mung
...
```

$7{,}776^{3}$

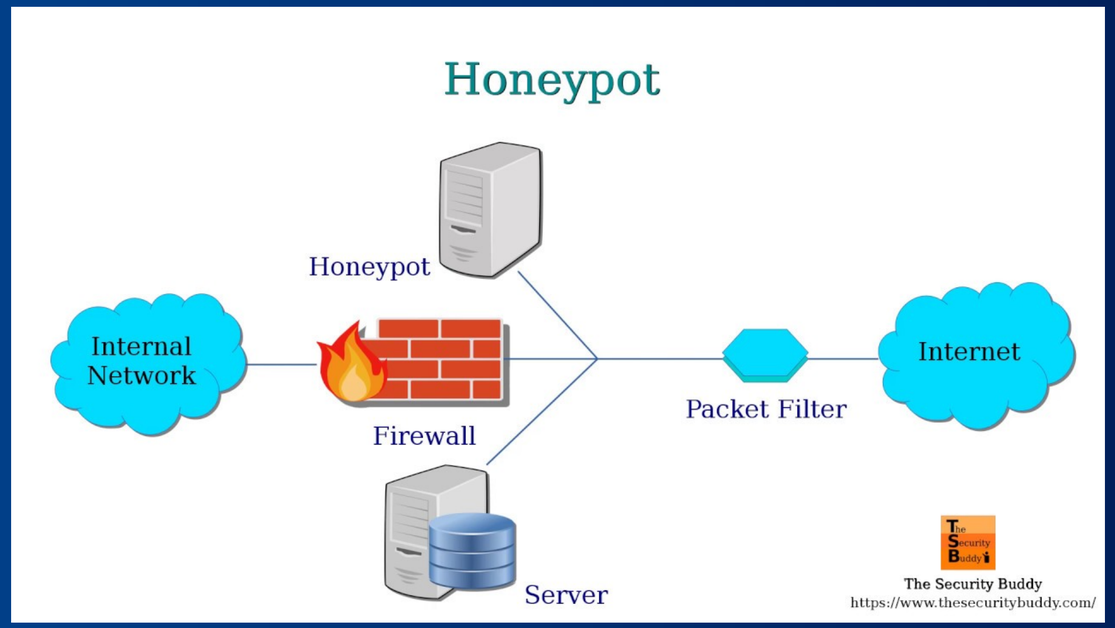
[DB2]

Hasła? A gdzie je trzymać?

Paranoja?

[8EA]

Honeywords - ciekawostki



Strengthening Password Security through Honeyword and HoneyEncryption Technique

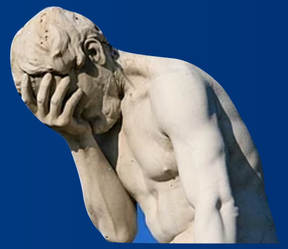
Mrs.Vasundhara R.Pagar
M.E Second Year
Department of Information Technology, PCCOE
Pune, India
vasu.pawar186@gmail.com

Mrs.Rohini G.Pise
Assistant Professor
Department of Information Technology, PCCOE
Pune, India
rohinipise@gmail.com

[CA8]

Ogólne rady, dyskusja

1. Regularnie zmieniaj hasła
2. Używaj unikalnych haseł
3. Używaj haseł złożonych ze słów, są łatwiejsze!
4. Używaj dodatkowych metod uwierzytelniania
5. Nigdy nie przechowuj haseł w niezaszyfrowanej formie

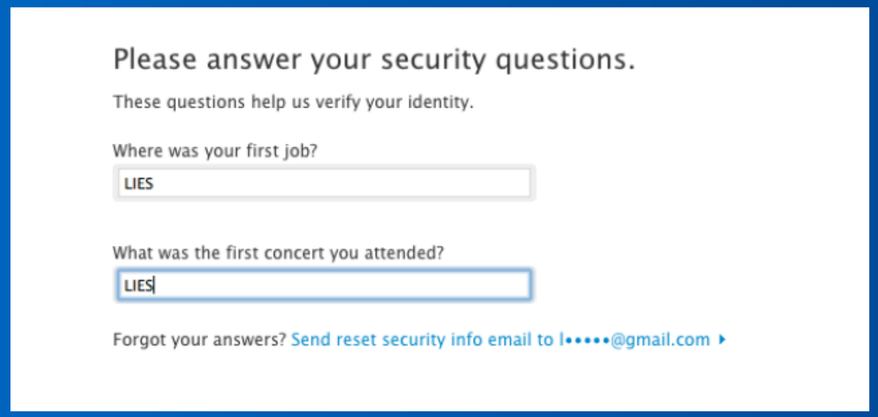


Źródło: [EAA]

Co poza hasłami?

Co poza hasłami?

Metody uwierzytelniania w XXI



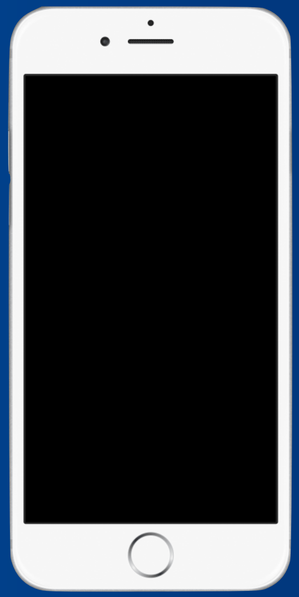
2FA (2-Factor Authentication)

MFA (Multi Factor Authentication)

(SYH, SYK, SYA)

Metody uwierzytelniania w XXI

Fingerprint



Metody uwierzytelniania w XXI

Fingerprint

Chińczycy: jesteśmy w stanie obejść *każdy* czytnik palca w telefonie. Wystarczy np. zdjęcie kieliszka z odciskiem

04 LISTOPADA 2019, 20:29 | W BIEGU | KOMENTARZE 4

TAGI: ANDROID, BIOMETRIA, IPHONE, OBEJŚCIE, TELEFONY

SEKURAK TV : oglądaj sekurakowe live-streamy o bezpieczeństwie IT.

[E4B]

Metody uwierzytelniania w XXI

Fingerprint

Chińczycy: jesteśmy w stanie obejść *każdy* czytnik palca w telefonie. Wystarczy np. zdjęcie kieliszka z odciskiem

04 LISTOPADA 2019, 20:29 | W BIEGU | KOMENTARZE 4

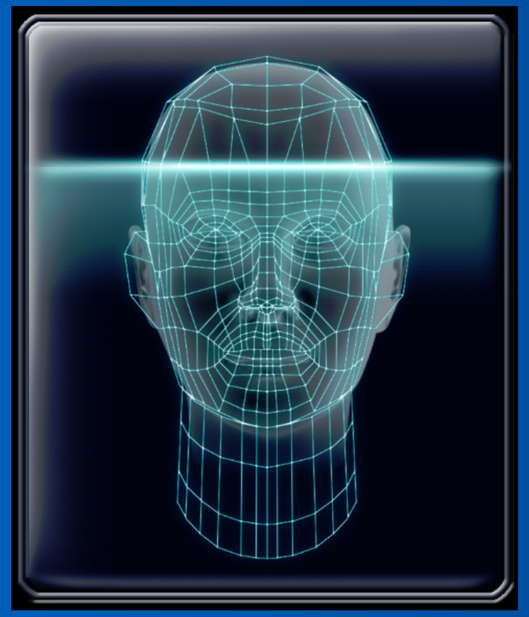
TAGI: ANDROID, BIOMETRIA, IPHONE, OBEJŚCIE, TELEFONY

SEKURAK TV : oglądaj sekurakowe live-streamy o bezpieczeństwie IT.

[E4B]

Metody uwierzytelniania w XXI

Face ID

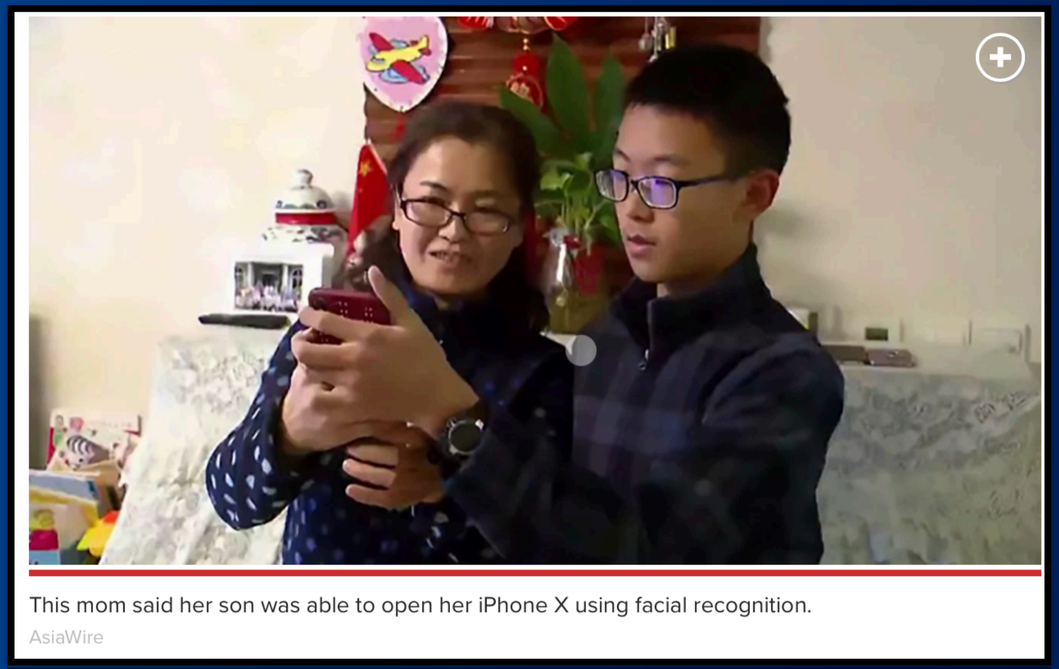


[EF4]

Metody uwierzytelniania w XXI

Face ID

„Cross-race Effect”



[AC4, 5DF]

Metody uwierzytelniania w XXI

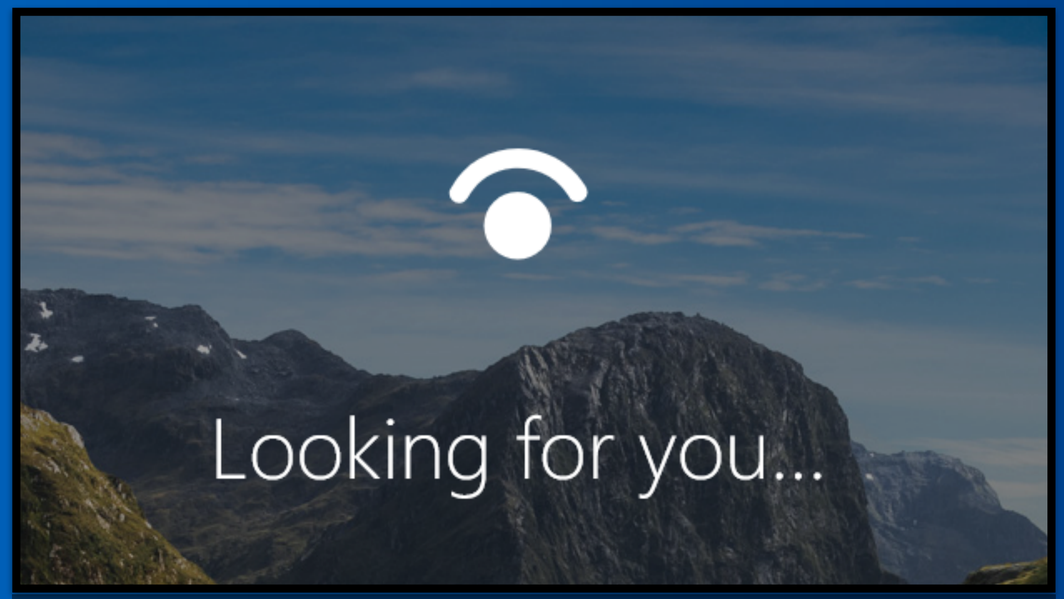
Face ID

„According to Apple, Face ID is more secure than Touch ID because there are slimmer chances of a mismatch. There's a 1 in 50,000 chance someone will be able to unlock your iPhone with their fingerprint, but a 1 in 1,000,000 chance someone else's face will fool Face ID. That doesn't count for twins, though -- if you have an identical twin, that error rate increases.”

[4E3]

Metody uwierzytelniania w XXI

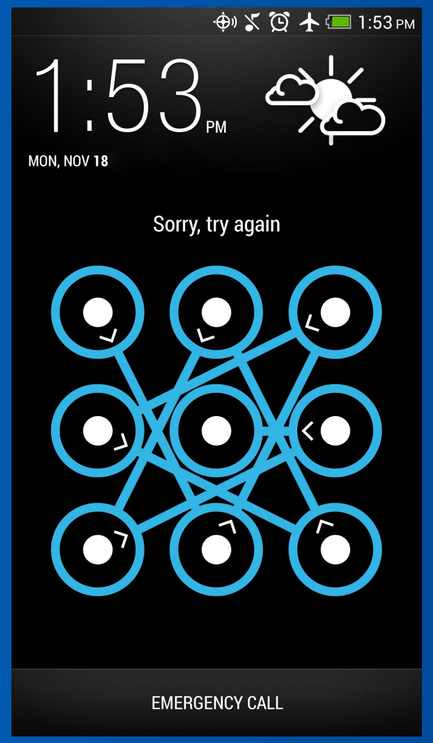
Windows Hello



[3BD]

Metody uwierzytelniania w XXI - inne

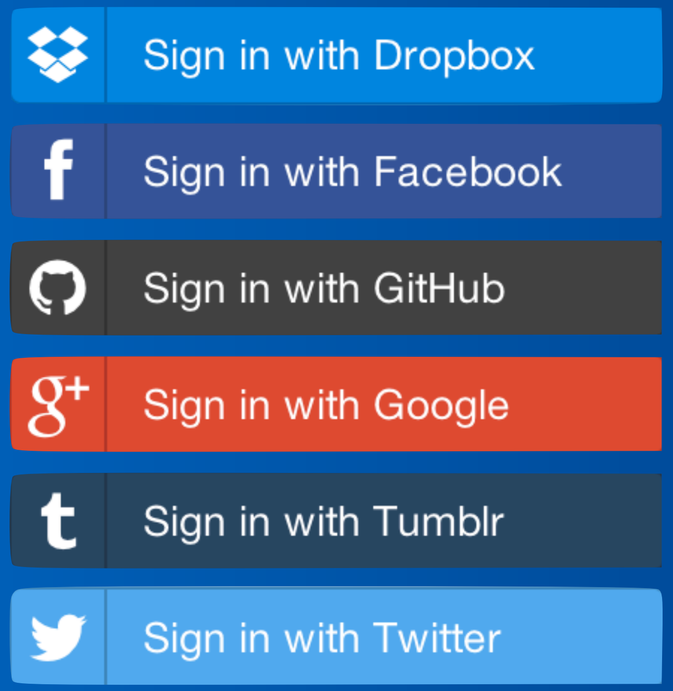
Lock screen pattern



Cracking Android Pattern Lock in Five Attempts

Guixin Ye[†], Zhanyong Tang[*,†], Dingyi Fang[†], Xiaojiang Chen[†], Kwang In Kim[‡], Ben Taylor[§], and Zheng Wang[*,§]
[†]School of Information Science and Technology, Northwest University, China
Email: gxye@stumail.nwu.edu.cn, {zytang, dyf, xjchen}@nwu.edu.cn
[‡]Department of Computer Science, University of Bath, UK
Email: k.kim@bath.ac.uk
[§]School of Computing and Communications, Lancaster University, UK
Email: {b.d.taylor, z.wang}@lancaster.ac.uk

Metody uwierzytelniania w XXI



SSO (Single Sign On)

[E1D]

OAuth 2.0

Metody uwierzytelniania w XXI

FIDO2

Smart Cards

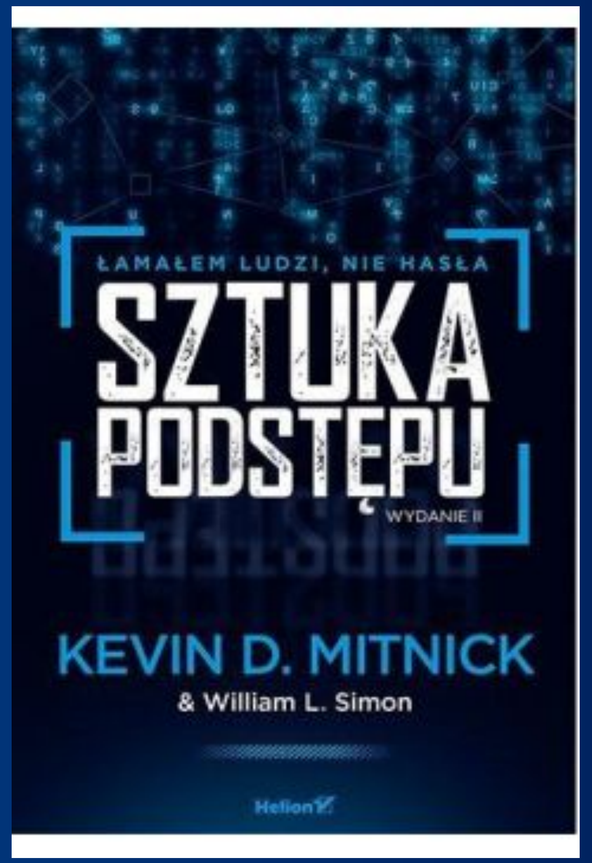
FIDO

W3C

[DCE]

Zagrożenia

- Wycieki danych
- Social Engineering
- Używanie prostych haseł



Najpopularniejsze hasła & wycieki

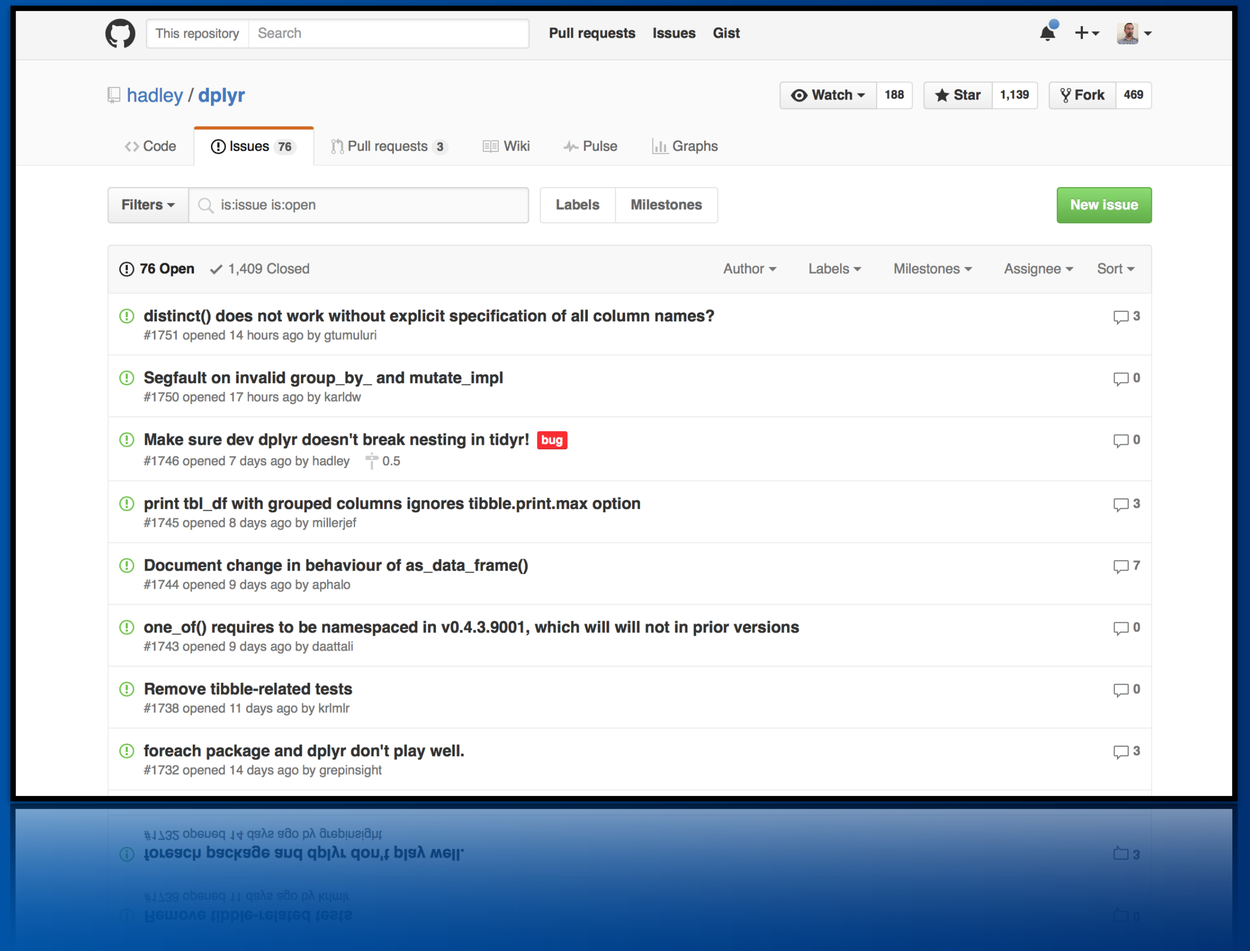
[E96]

Najpopularniejsze hasła & wycieki

(...)

[D7C]

Zagrożenia - klucze API



Zagrożenia - backdoory

```
1  def uwierzytelnianie(user_id, haslo):
2    # ....
3    haslo_hash = md5(haslo)
4
5    if haslo_hash == get_user_hash_from_database(user_id):
6      return True
7
8    if haslo == 'tajne_haslo_ktorego_nikt_nie_zgadnie':
9      return True
10
11   return False
12 #
```

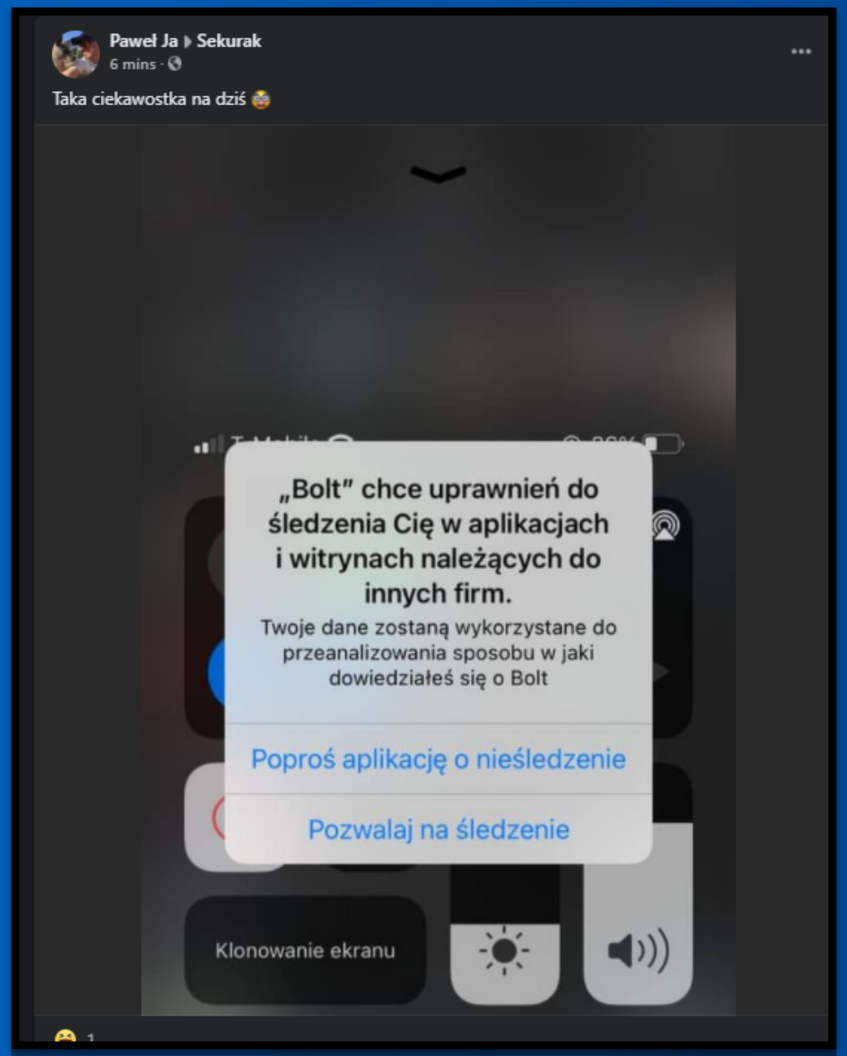
Zagrożenia, nieco inna perspektywa

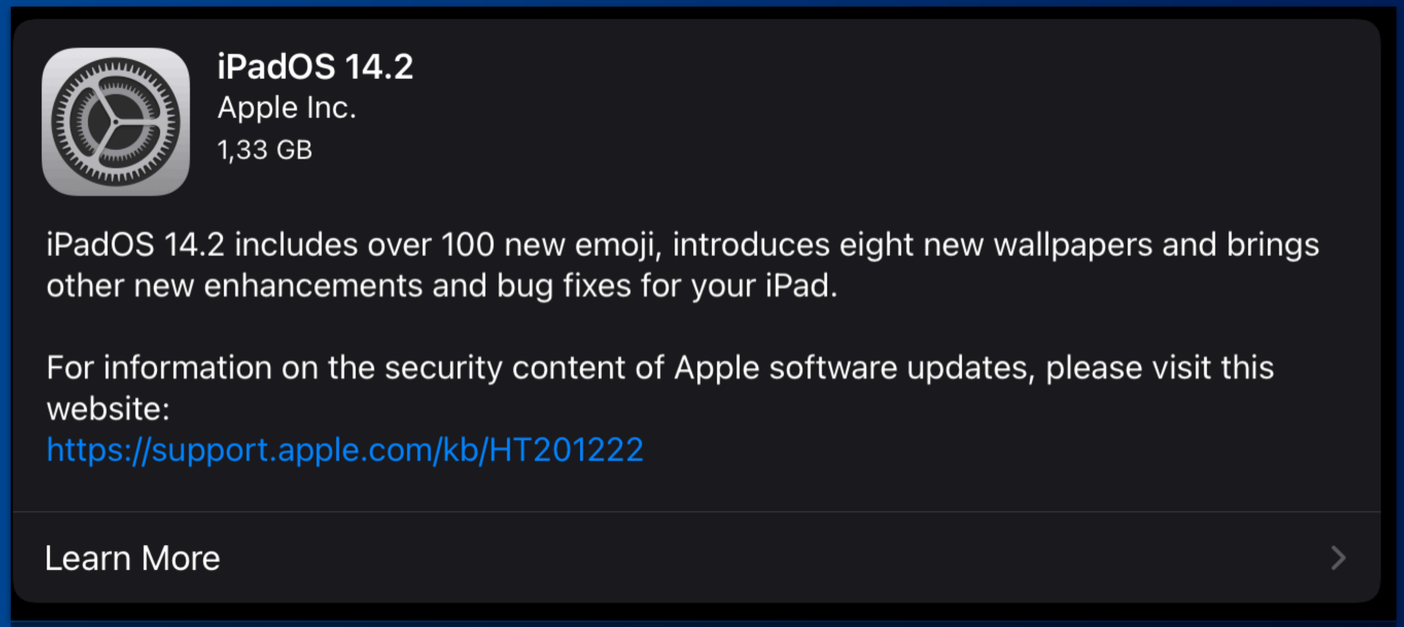
How far can facial recognition go? It is not a stretch to say that, in the not-too-distant future, different methods of biometric identification have the potential to transform the way we live, work and play. For instance, you won't need cash, ATMs, credit cards or even any kind of formal identification, because your face or other unique characteristics like your iris or hand veins will be your ID. You will be able to walk into the grocery store, pick up your food and walk out, because by using IR cameras and sensors, the store will know who you are, what you bought and how you're going to pay for it.

[870]

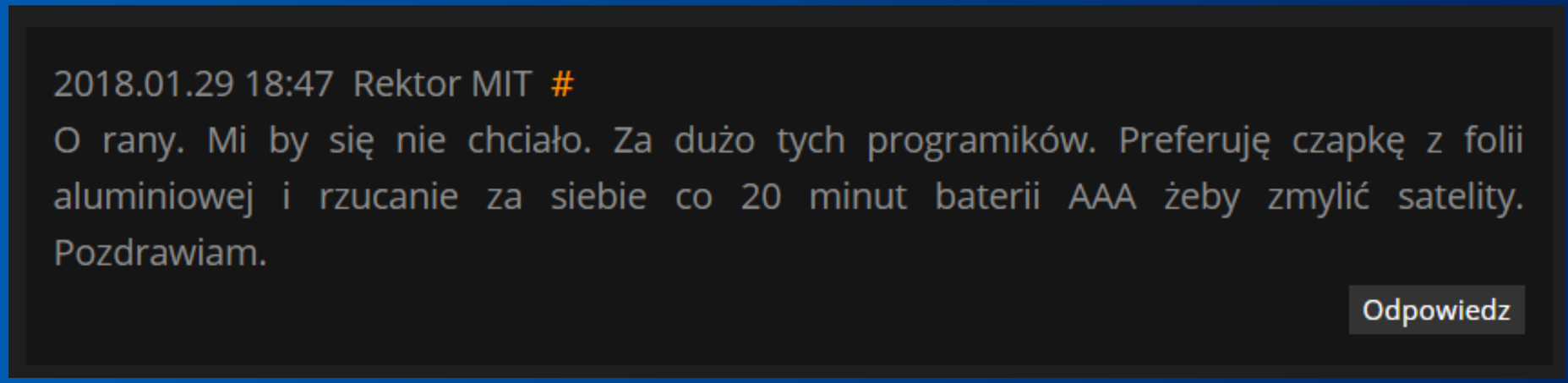
Wyzwania dla programistów

Wyzwania


Paweł Ja ▸ Sekurak
6 mins ·
Taka ciekawostka na dziś
„Bolt" chce uprawnień do śledzenia Cię w aplikacjach i witrynach należących do innych firm.
Twoje dane zostaną wykorzystane do przeanalizowania sposobu w jaki dowiedziałeś się o Bolt
Poproś aplikację o niesledzenie
Pozwalaj na śledzenie
Klonowanie ekranu


iPadOS 14.2
Apple Inc.
1,33 GB
iPadOS 14.2 includes over 100 new emoji, introduces eight new wallpapers and brings other new enhancements and bug fixes for your iPad.
For information on the security content of Apple software updates, please visit this website:
https://support.apple.com/kb/HT201222
Learn More

Wyzwania



„Użytkownicy będą korzystać z zabezpieczeń tylko jeśli będą one całkowicie dla nich transparentne ”

Biblioteka

[5EA] - https://zaufanatrzeciastrona.pl/post/spowiedz-bezpieczenstwa-adama-aktualizacja-czyli-co-zmienilo-sie-przez-dwa-lata/
[4E8] - https://paul.reviews/passwords-why-using-3-random-words-is-a-really-bad-idea/
[A1D] - https://security.stackexchange.com/questions/66989/how-does-a-random-salt-work
[8EA] - https://www.youtube.com/watch?v=50lwOrQW-zY
[D7C] - https://www.youtube.com/watch?v=wDGAkp1sHM4
[E96] - https://www.safetydetectives.com/blog/the-most-hacked-passwords-in-the-world/
[EAA] - https://digitalguardian.com/blog/uncovering-password-habits-are-users-password-security-habits-improving-infographic
[870] - https://www.novuslight.com/why-facial-recognition-is-the-face-of-the-future_N9346.html#:~:text=From%20a%20technical%20standpoint%2C%20facial,image%20with%20an%20IR%20camera.&text=2D%20facial%20recognition%20measures%20such,determine%20if%20the%20images%20match.
[DCE] - https://cqureacademy.com/blog/6-crucial-windows-security-skills-for-2021
[DB2] - https://theintercept.com/2015/03/26/passphrases-can-memorize-attackers-cant-guess/
[CA8] - https://www.thesecuritybuddy.com/data-breaches-prevention/what-is-honeypot/
[E4B] - https://sekurak.pl/chinczycy-jestesmy-w-stanie-obejsc-kazdy-czytnik-palca-w-telefonie-wystarczy-np-zdjecie-kieliszka-z-odciskiem/
[EF4] - https://www.pocket-lint.com/phones/news/apple/142207-what-is-apple-face-id-and-how-does-it-work
[AC4] - https://nypost.com/2017/12/21/chinese-users-claim-iphone-x-face-recognition-cant-tell-them-apart/
[5DF] - https://www.eteknix.com/iphone-x-face-id-unable-tell-two-chinese-women-apart/
[E1D] - https://firebase.google.com/docs/auth
[4E3] - https://www.macrumors.com/2017/09/13/how-iphone-x-face-id-works/#:~:text=Face%20ID%20uses%20infrared%20to,camera%20can%20do%20their%20jobs.
[3BD] - https://securityaffairs.co/wordpress/66964/hacking/win10-hello-facial-recognition-bypass.html