Segurança da Informação

Entendendo a criptografia do *Whatsapp* e a possibilidade de sua interceptação

Felipe Benali

fbenali@trf3.jus.br

Acompanhe os slides

👉 http://tiny.cc/emag-seguranca

05/04/2016

Whatsapp anuncia criptografia ponta a ponta

https://blog.whatsapp.com/10000618/end-to-end-encryption
https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

1.5 bilhões

De usuários no mundo

127 milhões

De usuários brasileiros

8 em cada 10

Brasileiros conectados está no **Whatsapp**

Resistência do Whatsapp

- Ordens judiciais para retirada do serviço do ar
- Desafio de volume, autenticidade, legitimidade

- O que é criptografia
- O que é criptografia ponta a ponta
  - É inviolável
  - Somente pode ser aberta com a chave criptográfica
  - Chave essa que o Whatsapp não detém
  - **O Whatsapp pode cumprir ordens judiciais de interceptação, sem desligar a criptografia nem mesmo para os usuários interceptados**

- Análise técnica, e não jurídica;
  - **Não há novidades no plano jurídico;**

CF/88

Art. 5º, inc. XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, **salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal**;

Lei 9296/96

Art. 1º A interceptação de **comunicações telefônicas**, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de **ordem do juiz competente** da ação principal, sob segredo de justiça.

Parágrafo único. **O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática**.

Marco Civil da Internet (Lei 12.965/2014)

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

(...)

II - **inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial**, na forma da lei;

Marco Civil da Internet (Lei 12.965/2014)

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

(...)

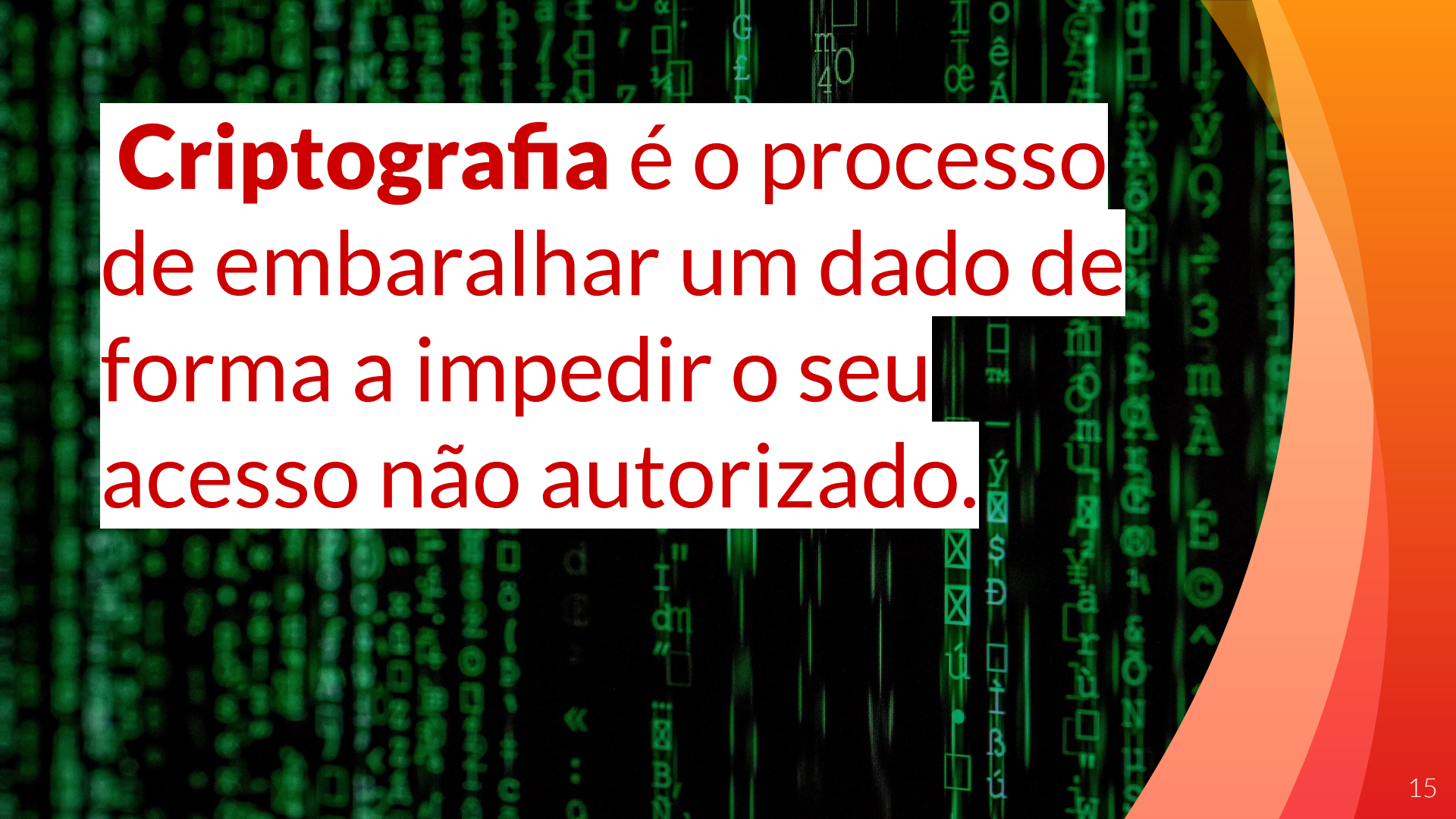
III - **inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial**;

Marco Civil da Internet (Lei 12.965/2014)

Art. 10. (...) § 2º O **conteúdo das comunicações privadas** somente **poderá ser disponibilizado mediante ordem judicial**, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º

- **Os argumentos trazidos pela empresa são técnicos e também *geopolíticos*;**
  - Brasil vulnerável no plano internacional
  - Redução da privacidade dos usuários brasileiros


ENCRYPT
ALL THE THINGS


Criptografia é o processo de embaralhar um dado de forma a impedir o seu acesso não autorizado.

O curso de segurança da informação ocorrerá no dia 10/09/2019.

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011

ubXW0BTLJf+XQxH3QTfSLTPjjDJPlFk+N/1KAymNxZnoAJ9/kHaaDmjxJe7q5RpUr4qCKILINhSGj9MhfOiQvyzyhK5dr79JNG7es6JzM00=

ubXW0BTLJf+XQxH3QTfSLTPjjDJPlFk+N/1KAy
mNxZnoAJ9/kHaaDmjxJe7q5RpUr4qCKILINhS
Gj9MhfOiQvyzyhK5dr79JNG7es6JzM00=

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110
01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100
01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011
00111100 01001110 01011111 00011010 00101011

O curso de segurança da informação ocorrerá no dia 10/09/2019.

https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

Ao criptografar um dado, nós reescrevemos o dado na sua origem

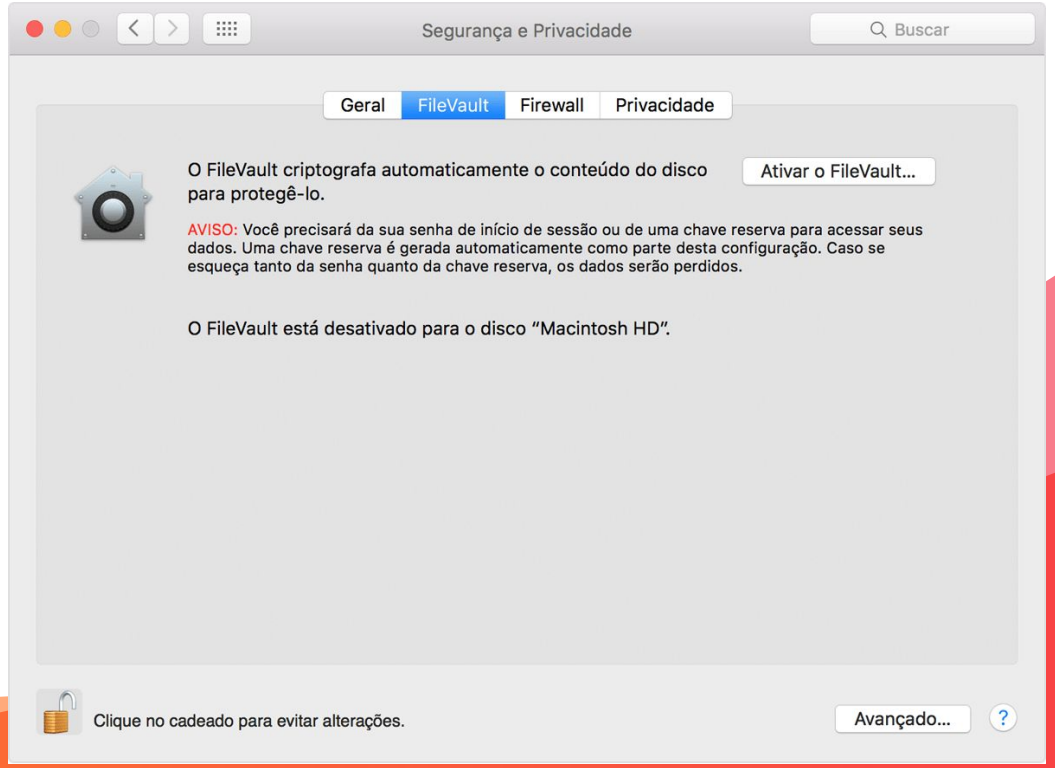
Para descriptografar um dado, precisamos obter a chave criptográfica

Dica

Ligue o **Filevault** no Mac ou **Bitlocker** no Windows

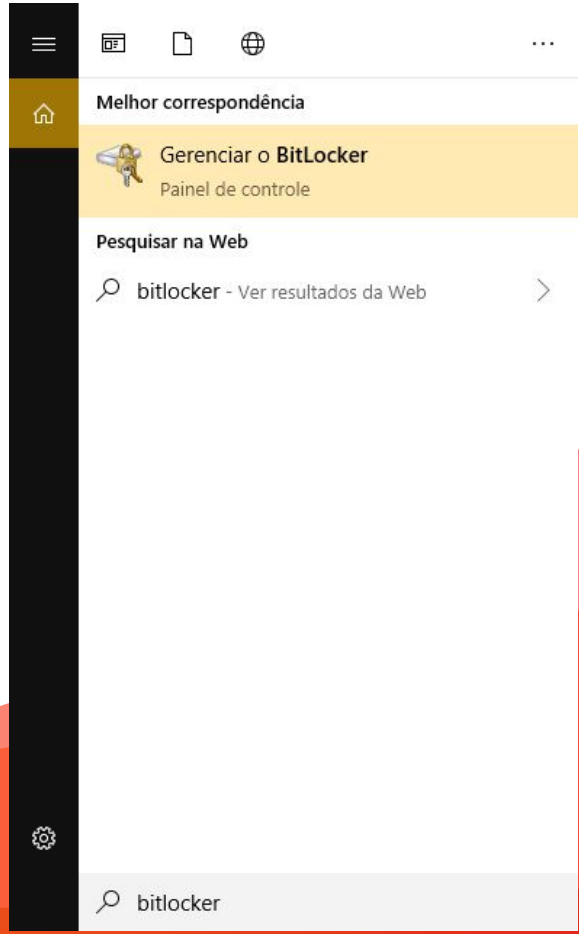
Filevault

https://support.apple.com/pt-br/HT204837



Bitlocker

https://support.apple.com/pt-br/HT204837



00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011

Fonte: https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

Ataques de força bruta

Tentativa e erro

- John the Ripper
- Hashcat
  - Bilhões de tentativas por segundo em um PC doméstico

AES-256

2^{256}

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011

Fonte: https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

$$2^8 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 = \mathbf{256}$$

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011

Fonte: https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

$2^{16} = 65.536$

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110
01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100
01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011
00111100 01001110 01011111 00011010 00101011

Fonte: https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

$2^{72} = 4.722.366.482.869.645.213.696$

00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100 01001110
01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011 00111100
01001110 01011111 00011010 00101011 00111100 01001110 01011111 00011010 00101011
00111100 01001110 01011111 00011010 00101011

Fonte: https://cryptii.com | AES-256 | Chave Binária convertida em Hexadecimal | IV 00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f | Base64 encoded

Supercomputador *Summit*

200.000 **trilhões** de cálculos **por segundo**

https://www.top500.org/lists/2019/06/

1.000.000.000.000.00
0.000.000.000.000.00
0.000.000

destes supercomputadores rodando por **todo o tempo de existência do universo** (14 bilhões de anos) para esgotar *metade* das possibilidades de uma chave de 256 bits

https://www.reddit.com/r/theydidthemath/comments/1x50xl/time_and_energy_required_to_bruteforce_a_aes256/

154

The average cost of electricity in the US is $\$0.12$ per kWh. For a single server, I'll use 3741 kWh annually as an estimate. That would be about $\$450$ per year for one machine.

Let's say you can do 10^{14} decryptions per second. That is 3.15×10^{21} decrypts per year for one machine. You need to do (on average) 2^{255} decryptions in a year, so you would need $\frac{2^{255}}{3.15 \times 10^{21}} \approx 1.84 \times 10^{55}$ machines. To figure your cost you would multiply that by $\$450$ and get about $\$8 \times 10^{57}$ or 8 octodecillion dollars. Gross world product, or GWP, is about 63×10^{12}, so brute-forcing a 256-bit key would cost about 10^{44} times the GWP.

You can follow similar math to get the cost of brute forcing a 128-bit key.

1.000.000.000.000.000.000.000.000.000.000.000.000.000.000.000 x PIB global

https://crypto.stackexchange.com/questions/1145/how-much-would-it-cost-in-u-s-dollars-to-brute-force-a-256-bit-key-in-a-year

É fisicamente impossível

obter uma chave de **256 bits**
por ataque de força bruta

Nós esgotaríamos toda a energia
do **SOL** 

https://www.schneier.com/blog/archives/2009/09/the_doghouse_cr.html

Ninguém

Nem a Polícia Federal, nem o FBI, nem a NSA, nem a CIA...

Qual a utilidade de um ataque de força bruta?

R: ataca-se o *atalho*, a senha

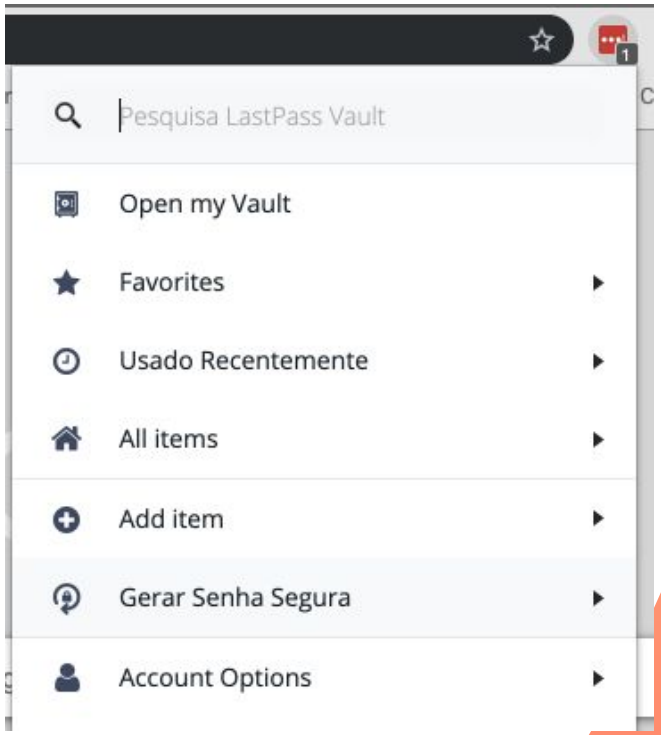
Usuários são péssimos em criar senhas fortes e repetem as senhas

Aumente a complexidade das suas senhas

	Combinações possíveis por caractere
A-Z	**26**
+ a-z	**52**
+ Dígitos (0-9)	**62**
+ Caracteres especiais ($%#@)	**95**

Utilize um gerenciador de senhas!

- Ex: Lastpass
  - Gera senhas seguras e as armazena
  - Notas seguras
  - Preenche formulários



Utilize senhas longas e com caracteres especiais

- felipe2019
  - **37 segundos**

- q#CA0A59ZhrVDa
  - **16 milhões de anos**

http://password-checker.online-domain-tools.com/
https://lastpass.com/howsecure.php

Não utilize dados pessoais nas senhas

- 11/09 - case da **Cantor Fitzgerald**

  - Datas (aniversário, casamento)
  - Nome dos filhos, animais de estimação
  - Universidade que frequentou

https://www.nytimes.com/2014/11/19/magazine/the-secret-life-of-passwords.html

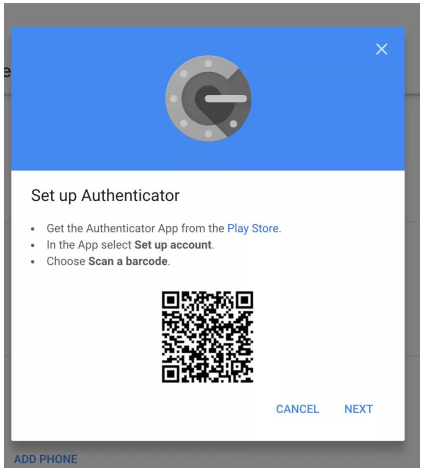
Jamais repita login e senha em diferentes sites

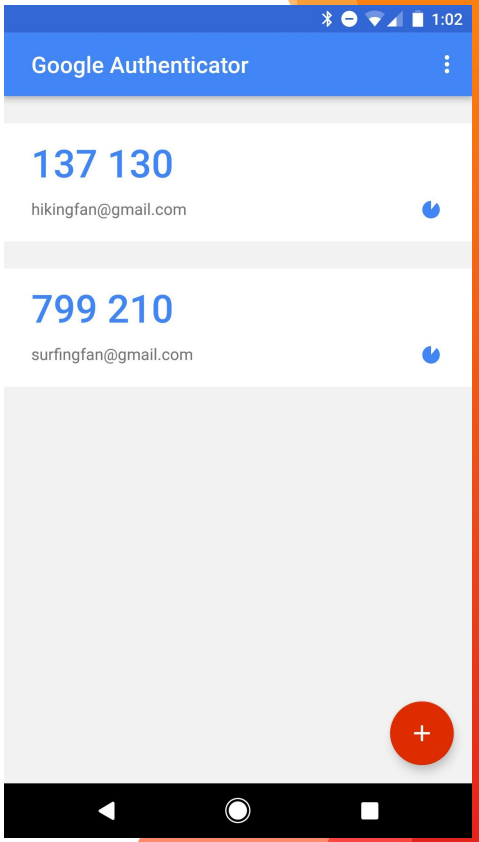
- Google x Floricultura
- Acessou seu e-mail? *Game over*
  - *Recurso esqueci minha senha*
  - *Pecou no passado? Troque **primeiro** a senha do seu e-mail!*

- www.haveibeenpwned.com

Ligue sempre a autenticação de 2 fatores (2 factor authentication)

- Prefira utilizar App (ex: Google Authenticator) do que SMS

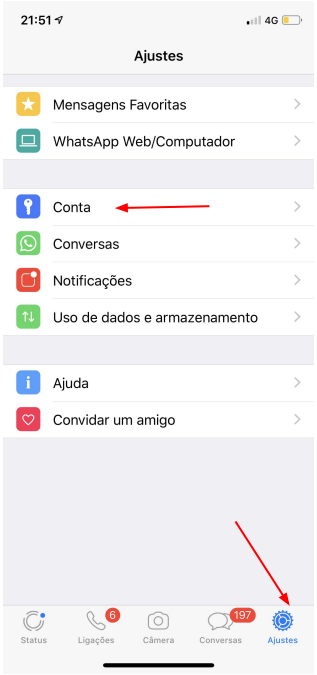


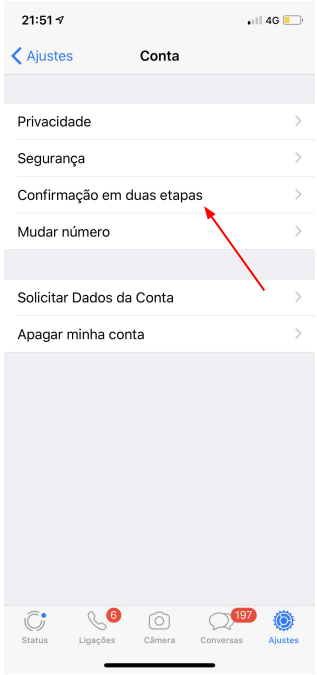


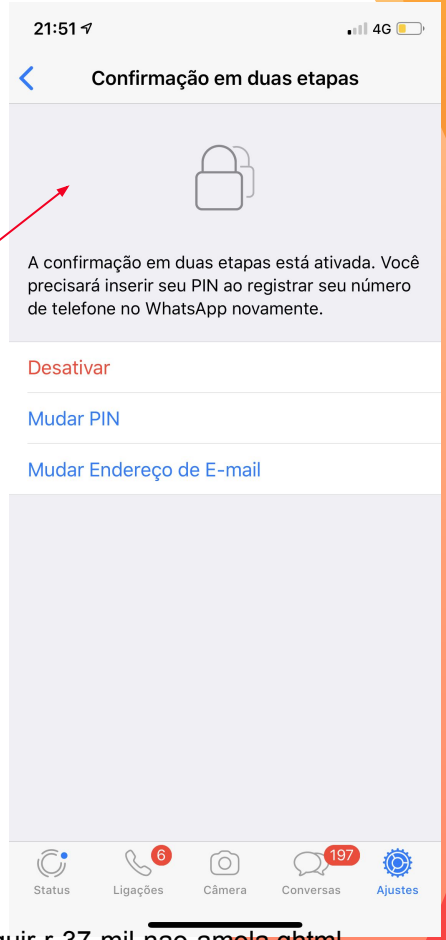
Qual a senha do seu Whatsapp?

Como o Whatsapp não utiliza senha, ele conta com toda a força da chave de 256 bits

Dica: ligue autenticação de 2 fatores no Whatsapp!







https://g1.globo.com/sp/santos-regiao/noticia/2019/08/13/golpista-clona-whatsapp-e-tira-onda-apos-conseguir-r-37-mil-nao-amola.ghtml

Como funciona a criptografia do Whatsapp

Criptografia assimétrica
Criptografia de chaves públicas

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Whitfield Diffie e Martin Hellman

1976 - Criptografia assimétrica (chaves públicas)

CHAVE PÚBLICA

CHAVE PRIVADA

Olá, tudo bem?

Olá, tudo bem?

CHAVE PÚBLICA

CHAVE PRIVADA

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Tudo bem, e aí?

Curiosidade: Whatsapp Web

- Utiliza a chave privada que está fisicamente dentro do seu celular
  - Ao desligar o celular, o Whatsapp Web para de funcionar.

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Olá, tudo bem?

Ataque *MITM*

Man in the middle

A criptografia é inviolável,
só pode ser aberta com a chave,
chave a qual o Whatsapp não detém,
e por isso o Whatsapp não pode ler as mensagens.

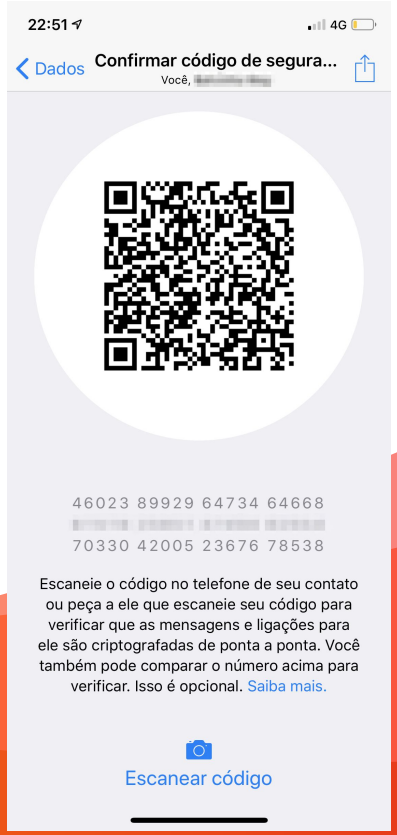
A criptografia é inviolável,
só pode ser aberta com a chave,
chave a qual o Whatsapp não detém,
e por isso o Whatsapp não pode ler as mensagens.

A criptografia é inviolável,
só pode ser aberta com a chave,
chave a qual o Whatsapp não detém,
e por isso o Whatsapp não pode ler as mensagens.

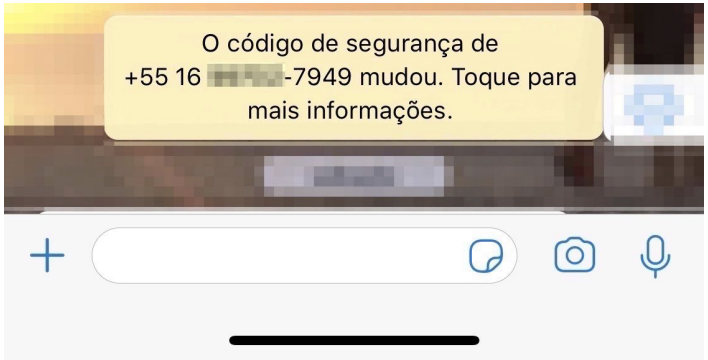
A criptografia é inviolável,
só pode ser aberta com a chave,
chave a qual o Whatsapp não detém,
e por isso o Whatsapp não pode ler as mensagens.

A criptografia é inviolável,
só pode ser aberta com a chave,
chave a qual o Whatsapp não detém,
e por isso o Whatsapp não pode ler as mensagens.

Conferência de chaves



Aviso quando da mudança de chaves



Desligada por padrão!

Confissões da empresa

Artigo The Guardian

13/01/2017

E a resposta de **Moxie Marlinspike**

https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/

“

This is called a “man in the middle” attack, or MITM, and ***is endemic to public key cryptography****, not just WhatsApp.*

https://signal.org/blog/there-is-no-whatsapp-backdoor/

“

WhatsApp could try to “man in the middle” a conversation, just like with any encrypted communication system, but they would risk getting caught by users who verify keys.

https://signal.org/blog/there-is-no-whatsapp-backdoor/

“

moxie on Jan 14, 2017 | parent | favorite | on: There is no WhatsApp 'backdoor'

> This allows WhatsApp to MITM. Whatapps can rekey both Alice and Bob, decrypt both their messages from that point onwards (incl unsent messages) and forward them re-encrypted with their real keys. The only notification might be that rekeying warning, if the users have turned it on. In this scenario even the double-checkmarks are present. This is contrary to WhatsApp's claim that even they cannot snoop.

You've just described a "man in the middle" attack. It is endemic to any public key cryptosystem, including Signal and PGP, not just WhatsApp. The notification that you see in WhatsApp, Signal, SSH, PGP, or whatever is the defense.

https://news.ycombinator.com/item?id=13396129

Audiência pública STF

Fundador do Whatsapp


TV JUSTIÇA
AO VIVO
MARCO CIVIL DA INTERNET E A POSSIBILIDADE DE DECISÕES JUDICIAIS
IMPEDIREM O FUNCIONAMENTO DO APLICATIVO WHATSAPP

“

“Se o Whatsapp modificasse seu servidores, para interferir no sistema de troca de chaves, ***como num ataque de “homem no meio”****,* ***esse tipo de interceptação seria também detectável, devido ao sistema de verificação do código de segurança****, (...)* ***fazendo com que os alvos soubesse imediatamente que estariam sendo monitorados.***”

Brian Acton, fundador do Whatsapp
https://www.youtube.com/watch?v=3TNsQCNIOO0 aos 58:05

E agora?
Multa diária?
Tirar do ar?

Análise de razoabilidade

“

E Ademais, a extensão do bloqueio a todo o território nacional, afigura-se, quando menos, ***medida desproporcional*** *ao motivo que lhe deu causa. (...)*

STF, ADPF 403, Min. Ricardo Lewandowski, 19/07/2016

*(...) não se mostra **razoável** permitir que o ato impugnado prospere, quando mais não seja por gerar insegurança jurídica entre os usuários do serviço, **ao deixar milhões de brasileiros sem comunicação entre si**.*

STF, ADPF 403, Min. Ricardo Lewandowski, 19/07/2016

*Em face dos princípios constitucionais, não se mostra **razoável** que **milhões de usuários** sejam afetados em decorrência da inércia da impetrante, mormente quando não esgotados outros meios disponíveis para a obtenção do resultado desejado.*

TJ/SP, Mandado de Segurança nº 2271462- 77.2015.8.26.0000

“

A fim de melhor ilustrar ***a falta de proporcionalidade*** *que emana do ato questionado (...)*

TJ/PI, MS nº 2015.0001.001592-4

Proposta

- Caminho é o diálogo com a empresa, discutindo proporcionalidade não com relação a processo isolado, e sim sistêmica
- Prazo longo e razoável para adaptação (ex: 6 meses, 12 meses)

Proposta

- Mantida a recusa, o livre mercado regulará a sua ausência
- Whatsapp foi adquirido por USD 19bi quando tinha 600 milhões de usuários, valor do mercado brasileiro pode ser estimado em R$ 12 bi

Proposta

- Mantém criptografia ligada
- Não cria nenhuma nova vulnerabilidade, pois a brecha é intrínseca ao modelo criptográfico adotado e já existe hoje
- Passa a cumprir ordens judiciais

Última dica

Mantenha seus dispositivos **sempre atualizados**.

Agosto/2019 - Defcon em Las Vegas

- Cabos de carregador maliciosos

https://www.vice.com/en_us/article/evj4qw/these-iphone-lightning-cables-will-hack-your-computer

Agosto/2019 - iOS Exploits | Project Zero

messages database file uploaded by implant

```
$ sqlite3 ChatStorage.sqlite
SQLite version 3.24.0 2018-06-04 14:10:15
Enter ".help" for usage hints.
sqlite> .tables
ZWABLACKLISTITEM          ZWAGROUPMEMBERSCHANGE     ZWAPROFILEPUSHNAME
ZWACHATPROPERTIES         ZWAMEDIAITEM              ZWAVCARDMENTION
ZWACHATPUSHCONFIG         ZWAMESSAGE                ZWAZ1PAYMENTTRANSACTION
ZWACHATSESSION            ZWAMESSAGEDATAITEM        Z_METADATA
ZWAGROUPINFO              ZWAMESSAGEINFO            Z_MODELCACHE
ZWAGROUPMEMBER            ZWAPROFILEPICTUREITEM     Z_PRIMARYKEY
sqlite> select * from ZWACHATSESSION;
...
2|4|6|0|0|272|0|2|0|4|0|0|-5|0||9||588088153.555802||578764AD-682C-42DE-A19
C-8D83C3B60977:ABPerson|447846412085@s.whatsapp.net|||Kitty|
sqlite> select * from ZWAMESSAGE;
...
8|9|4|0|0|0|3|5|0|0|0|2|0|0|8|0|2|-32768||2||||||588088133|588088136.227191
|447846412085@s.whatsapp.net||||3A1A5EF9D85E2656CBFE|Gruuuuezi Issac!|
9|9|4|0|0|0|3|6|0|0|0|0|1|0|8|0|3|-32768||2||2||1||588088153.555802|5880881
53.599606|||||3AE107207900EEC3C115|MEGA HAMMER|447846412085@s.whatsapp.net
```

https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html

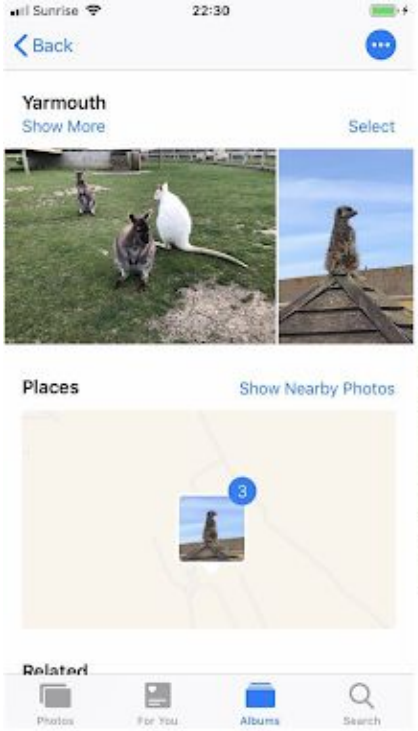
Agosto/2019 - iOS Exploits

gmail email database file uploaded by implant

```
$ sqlite3 "./Library/Application
Support/data/issac.cassi.19929292@gmail.com/sqlitedb" "select
hex(item_summary_proto) from items" | xxd -r -p
...
thread-a:r-3850742854413041744Does your yahoo account work??On Wed, 21 Aug
2019 at 20:56, Issac cassi <issac.cassi.19929292@gmail.com> wrote: On Wed,
21 Aug 2019 at 20:49, Issac cassi <issac.cassi.19929292@gmail.com> wro ?
i?-(????-U F?hqx`??G?x?
...
?thread-f:1642479081486697007NYour Apple ID was used to sign in to FaceTime
and iMessage on an iPhone 8.?Dear Issac Cassi, Your Apple ID
(issac.cassi.19929292@gmail.com)
...
```

https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html

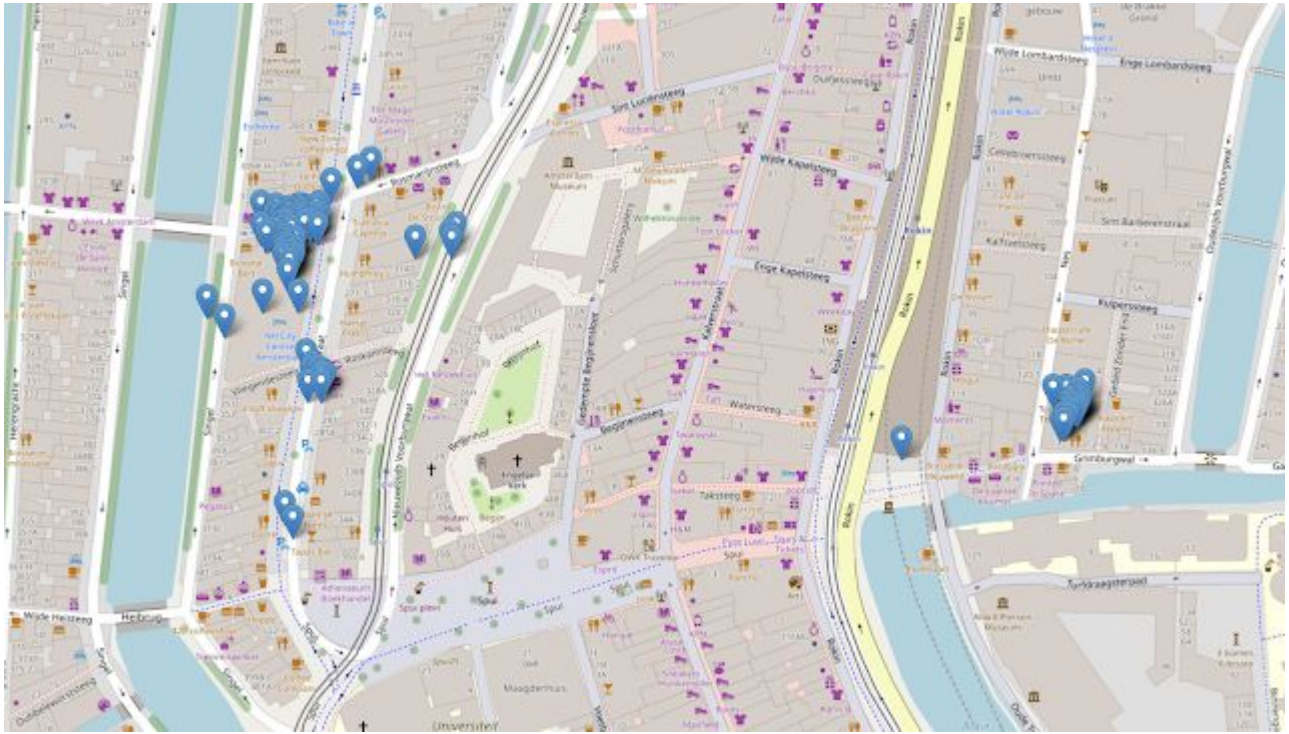
Agosto/2019 - iOS Exploits



photos uploaded by implant

https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html

Agosto/2019 - iOS Exploits



https://googleprojectzero.blogspot.com/2019/08/implant-teardown.html

Julho/2019 - Zero Interaction

- Sem necessidade de qualquer interação com o seu celular.

https://www.wired.com/story/imessage-interactionless-hacks-google-project-zero/

Atualizem seus dispositivos!

- iPhone: Geral > Atualização de Software > Atualizações automáticas
- Android: Configurações > Sobre o telefone > Atualizações de sistema

https://olhardigital.com.br/lu-explica/noticia/saiba-como-atualizar-a-versao-do-android-e-do-ios/59650

1 milhão de dólares

Para quem conseguir hackear um iPhone

https://www.forbes.com/sites/thomasbrewster/2019/08/08/apple-confirms-1-million-reward-for-hackers-who-find-serious-iphone-vulnerabilities/#196080693948

Obrigado!

http://tiny.cc/emag-seguranca

Felipe Benali

- fbenali@trf3.jus.br

1996 x 2019