CryptoParty: Rip off the bandaid!

@shiromarieke

PGP

TOR

OTR

WTF


FROM ACADEMY-AWARD®
NOMINATED DIRECTOR
LAURA POITRAS
AND EXECUTIVE PRODUCER
STEVEN SODERBERGH


GO HOME N.S.A...
...YOU'RE DRUNK.


CRYPTO
ALL THE PARTIES
memegenerator.net


CRYPTO
PARTY


corbis
OH LOOK
OUR PRIVACY IS BEING VIOLATED
quickmeme.com


ONE DOES NOT
SIMPLY
SEND UNENCRYPTED MESSAGES

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
gciINxMhXZ4nPt7kXLBrwDYue6U/WYSGGONxzBnz0O91DhBqxM84hdfhmn
Ajgz0W5iYHhecI6OoJRc69MS9gHcztIsTv5KVJItgFphQFXnK&sd9g6/sv
wzsw32 f/ __| '__| | | | '_ \| __/ _ \n98sau98u98a98798782
xxccdsd| (__| |  | |_| | |_) | || (_) |a86K2Mzwj+99uhjk1hj
vdkm0d8h\___|_|   \__, | .__/ \__\___/jd99s0a9l0990avvdakn
sRaC1JJKJadsakkj0c|___/|_|-09jdalkjlkadIGsyORCWDORl+PVMweg
7VyjDD99AgZIuKpVllCDjtOMKJAuA9bgZODci2vmaVRzAVEoXkfM3IOGsE
r8Xe0sRaCqRtaQNTGFH86RJo0dyKqBt7FvwktWGC127dkPC2xsczHpf8hB
n18LOmsklnsdv3m91ncmtn4I| '_ \ / _` | '__| __| | | |BhaLku
seDshJkLKjkal+1dsVcfgDsS| |_) | (_| | |  | |_| |_| |Nz878z
vbdfM09A8Ka87HJkadnM+dVf| .__/ \__,_|_|   \__|\__, |10Klau
23kscmMN1Jan2HgdfG81445n|_|0Kla/sHaj243676HaK1|___/aZdhjk5
W/Nvk160MVSedqdgVxxm3NjMV0cXyCa1DR3BwEwSoxV2oOYk0TY9pIhWCe
OY5252ShsI7+nLDxV6sIuhOqZSLgjijS/ykpVLowKN2hgNHzIWZ4b2Ub02
5Vdhcc8qG0GsHm1F0FTUTKaS7Cr+D9grvyhIGsyORCWDORl+PVMrc2TAo2
PEeXMrdseDv/|  ___ \+2|  ___ \bTYmQXERZ6PG0xifM0kYev3/wzdi
ykLcceFa/CLt| |   | |X| |   | |J1IE5lZWxpY2F0dHUgKFJlZCBIY
aGF0LmNvbT6I| |   | |g| |   | |bAwYLCQgHAwIGFQgCCQoLBBYCAw
wANaP7NetqTb| |___| |g| |___| |r8h+Ta7AFWR1uAecHqnGPNFykA/
EGf7Vn2fK1q7|      /oP|      /uQMNBFBjyUwQDADm8MhSe1705+DZ
Yl9Rhv6Ok6PZ8GEyWCrtRsxxh/VZtmxC3AFN+nF223z7iUjj059wBGmNTB
3DpsZpTmr4sXurX0v17mCFDn7TrH1uxxuuVVnAtARTs4dMs5atxzeOusyy
-----END PGP PUBLIC KEY BLOCK-----
```

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy.
A private matter is something one doesn't want the whole world to know, but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

A Cypherpunk's Manifesto by Eric Hughes, 1993

6. Dezember 2012
18:30 Uhr
Fakultät Informatik (E07)
Nöthnitzer Str. 46, Dresden

Was? Diskussion und Workshops zu Kryptographie, Installation und Ausprobieren von u.a.:

> Anonymes Surfen im Netz mit TOR
> E-Mail-Verschlüsselung mit PGP und Co.
> Sichere Kommunikation, u.v.m.

Mitbringen?

0. Neugierde und Interesse
1. Laptop u.ä. (wenn vorhanden)

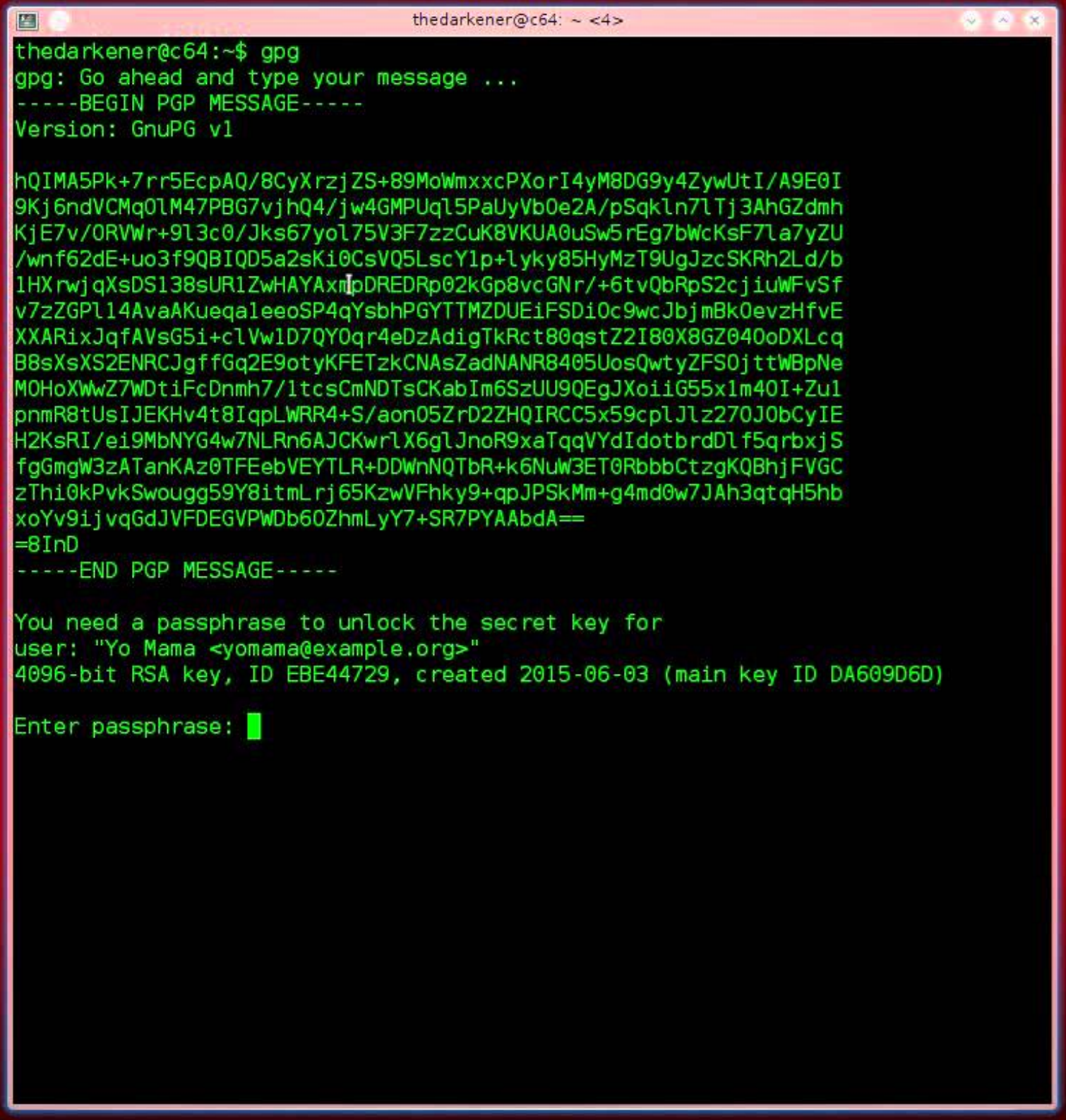
Wer?

C3D2 [https://www.c3d2.de/]
FSR Informatik [https://www.ifsr.de/]
Du!

Für wen? Jeden mit Interesse an Kryptographie, sicherem und anonymem Datenverkehr. Egal, ob mit Vorkenntnissen oder nicht, kommt vorbei!


WX210


I STREET VIEW
ASYL
bizhub C350

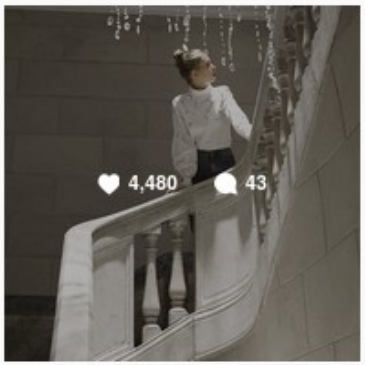

thedarkener@c64: ~ <4>
thedarkener@c64:~$ gpg
gpg: Go ahead and type your message ...
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1
hQIMA5Pk+7rr5EcpAQ/8CyXrzjZS+89MoWmxxcPXorI4yM8DG9y4ZywUtI/A9E0I
9Kj6ndVCMqOlM47PBG7vjhQ4/jw4GMPUql5PaUyVbOe2A/pSqkln7lTj3AhGZdmh
KjE7v/ORVWr+9l3c0/Jks67yol75V3F7zzCuK8VKUA0uSw5rEg7bWcKsF7la7yZU
/wnf62dE+uo3f9QBIQD5a2sKi0CsVQ5LscY1p+lyky85HyMzT9UgJzcSKRh2Ld/b
1HXrwjqXsDS138sUR1ZwHAYAxmpDREDRp02kGp8vcGNr/+6tvQbRpS2cjiuWFvSf
v7zZGPl14AvaAKueqa1eeoSP4qYsbhPGYTTMZDUEiFSDiOc9wcJbjmBkOevzHfvE
XXARixJqfAVsG5i+clVw1D7QYOqr4eDzAdigTkRct80qstZ2I80X8GZ040oDXLcq
B8sXsXS2ENRCJgffGq2E9otyKFETzkCNAsZadNANR8405UosQwtyZFSOjttWBpNe
MOHoXWwZ7WDtiFcDnmh7/1tcsCmNDTsCKabIm6SzUU9QEgJXoiiG55x1m40I+Zu1
pnmR8tUsIJEKHv4t8IqpLWRR4+S/aon05ZrD2ZHQIRCC5x59cplJlz27OJ0bCyIE
H2KsRI/ei9MbNYG4w7NLRn6AJCKwrlX6glJnoR9xaTqqVYdIdotbrdDlf5qrbxjS
fgGmgW3zATanKAz0TFEebVEYTLR+DDWnNQTbR+k6NuW3ET0RbbbCtzgKQBhjFVGC
zThi0kPvkSwougg59Y8itmLrj65KzwVFhky9+qpJPSkMm+g4md0w7JAh3qtqH5hb
xoYv9ijvqGdJVFDEGVPWDb60ZhmLyY7+SR7PYAAbdA==
=8InD
-----END PGP MESSAGE-----
You need a passphrase to unlock the secret key for
user: "Yo Mama <yomama@example.org>"
4096-bit RSA key, ID EBE44729, created 2015-06-03 (main key ID DA609D6D)
Enter passphrase:

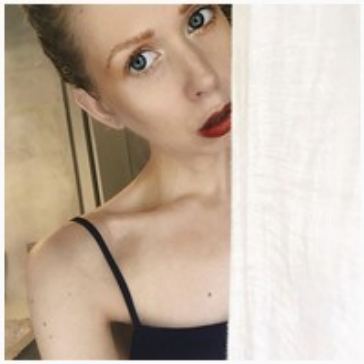
jennymustard

Follow

1,303 posts **85.4k** followers **528** following

jenny mustard swedish vegan feminist in berlin lover of everything deliciously designed info@jennymustard.com youtube : jenny mustard **jennymustard.com**

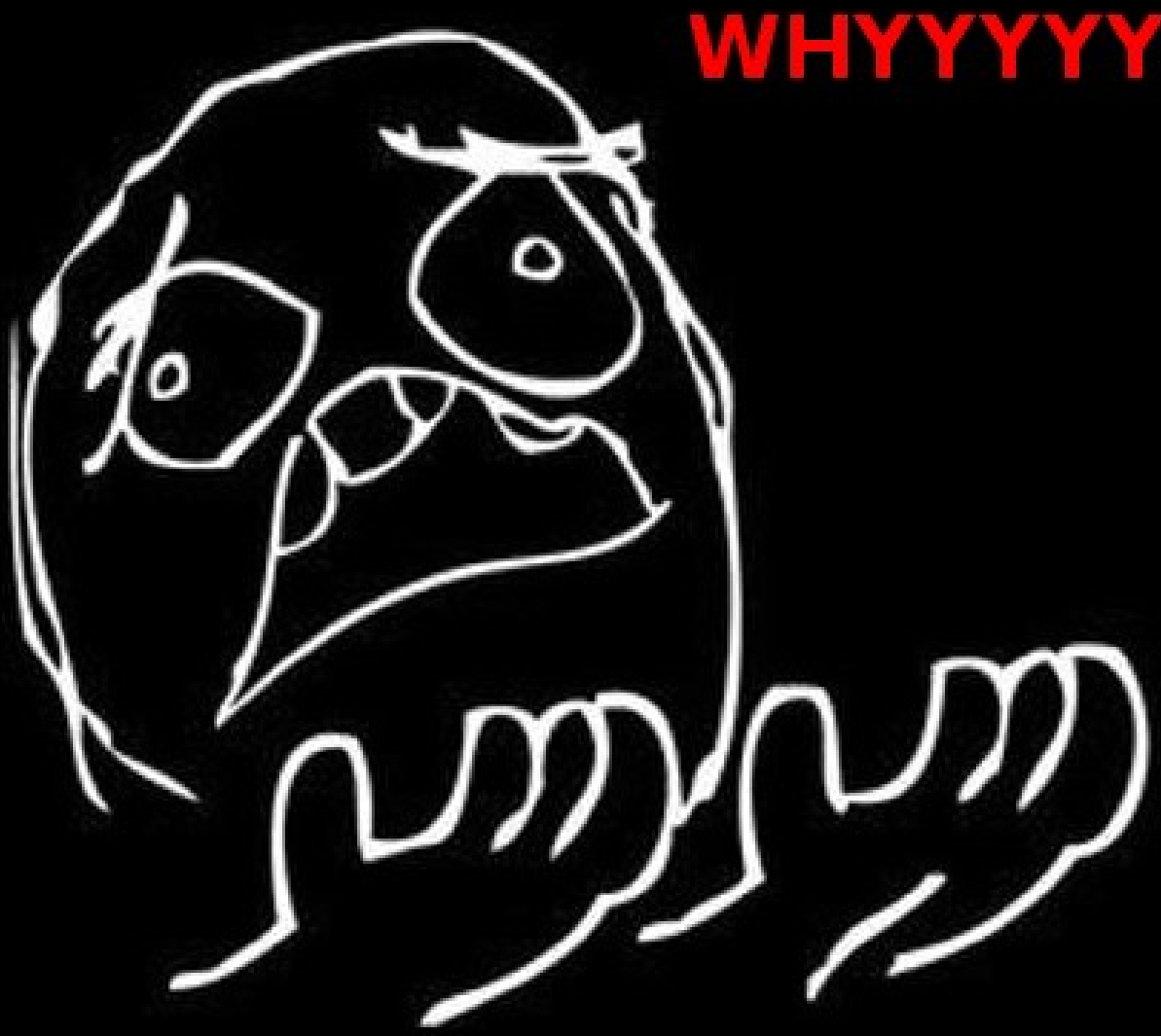




¯_(ツ)_/¯

Crypto for people who don't encrypt.

```
>>> Sent from my iPhone
>>>
>>>
>>> CONFIDENTIALITY NOTICE: This e-mail message (including attachments) is
>>> covered by the Electronic Communications Privacy Act, 18 U.S.C. §§
>>> 2510-2521, and is intended only for the person or entity to which it is
>>> addressed and may contain confidential and/or privileged material. Any
>>> unauthorized review, use, disclosure dissemination, copying, forwarding or
>>> distribution is prohibited. If you are not the intended recipient, please
>>> contact the sender by reply e-mail and destroy all copies of the original
>>> message.
>
>
>
> --
> Robert Russo
> Director of Correspondence and Briefings
> Hillary for America
> rrusso@hillaryclinton.com
```


WHYYYYY


Whatsapp

TIN FOIL

FREE YOUR MIND


BuzzFeed

Just 19 Perfect Tweets About Taylor Swift's "Call It What You Want"

We stan Joe Alwyn.

Posted on November 3, 2017, at 6:39 a.m.

Jemima Skelley
BuzzFeed Staff, Australia

Our queen of making 2017 worth living, Taylor Swift, has dropped another single.

QUIZ

Order A Taco And Build A Hot Guy And We'll Reveal A Deep Truth About You

It's always Taco Tuesday here at BuzzFeed.

Posted on November 2, 2017, at 11:46 p.m.

Matthew Perpetua
BuzzFeed Staff

OK, let's start off with the tortilla. What kind would you like?

○ Soft corn tortilla

○ Soft flour tortilla

The Cast Of "Rough Night" Your Most Burning Questions

Scarlett, Kate McKinnon, Zoë Kravitz, Ilana Glazer, and Jillian Bell are coming to BuzzFeed!

Kristin Harris

Trending

Build A Smoothie Bowl And We'll Reveal Your Age And College Major

We'll try our berry best.

Sarah Aspler • 6 hours ago

It's Easy To Fall For Email Phishing Scams. Here's How To Protect Yourself.

What "phishing" is, how to identify it, and what to do if hackers trick you.

Nicole Nguyen • 3 hours ago

Pippa Middleton's Wedding Rules Are So Extra And I'm Not Here For It

Who said this was okay?

Delaney Strunk • 5 hours ago

What's The Perfect Dog For You, Based On Your Horoscope?

This "Wheel Of Fortune" Puzzle Is Confusing The Hell Out Of People

Mama June's Makeover Was Actually Damage Control

SHOPPING

21 Insane Gadgets To Make Your iPhone Even Cooler

Because carrying a handheld computer isn't high-tech enough.

Posted on February 11, 2016, at 12:02 a.m.

Katherine Fiorillo
BuzzFeed Staff

More

We hope you love the products we recommend! Just so you know, BuzzFeed may collect a small share of sales from the links on this page.

1. This gooseneck lazy wall mount ($48).

Trending on Shopping


1
19 Geeky Beauty Products That'll Make You Say "Need!"

2
All Of The Best Deals On Amazon Today

3
All The Best Deals On The Internet This Weekend


4
19 Ridiculously Simple Ways To Look And Feel More Awake


5
14 Products On Amazon Our

— THE ANATOMY OF A —
SKETCHY EMAIL

FROM: Your Bank [ur.bank@gmail.com]
SUBJECT: Irregular Activity
DATE: 5/1/2017 8:02 AM

Incorrect domain

Invokes fear

We have detected irregular activity on your account on the date 4/20/2017. For your protection, we have temporarily limited your account.

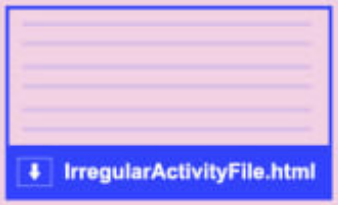
Urgency

In order to regain full access to your account, you must verify this activity before you can continue using your account. We have sent you an attachment ,open it and follow the steps to verify your account.Once completed, please allow up to 48h to update.

Punctuation error

Copyright BankOfYours, All rights reserve

Typo



Malicious attachment

TECH

How to Keep Messages Secure

Security experts give their best advice for keeping messages secure, whether you're at a protest or just want to keep out snooping siblings.

Nicole Kobie
MAR 2, 2017 6:06PM EST

iOS

iOS is a proprietary operating system whose source code is not available for auditing by third parties. You should entrust neither your communications nor your data to a closed source device (better use android or any of these alternatives).

Edit

Messenger

- Signal
- Telegram (choose "secret chat" for encryption that's end-to-end and to use self-destructing messages; add two-factor-authentication and a pin-lock via the app's settings)
- Wire
- ChatSecure

Edit

Calls

- Signal provides ZRTP / end-to-end encryption for your calls, securing your conversations so that nobody can listen in.
- The app "Wire" offers encrypted calls with excellent quality and the option to have video chats.
- More information: https://whispersystems.org/blog/signal

Edit

Web Browsing

- Ghostery stops third-party sites from tracking you.
- Onion browser is a Tor-capable web browser that lets you access the internet privately and anonymously.

Edit

Chat

- See **ChatSecure here**

Edit

Disc Encryption

Edit

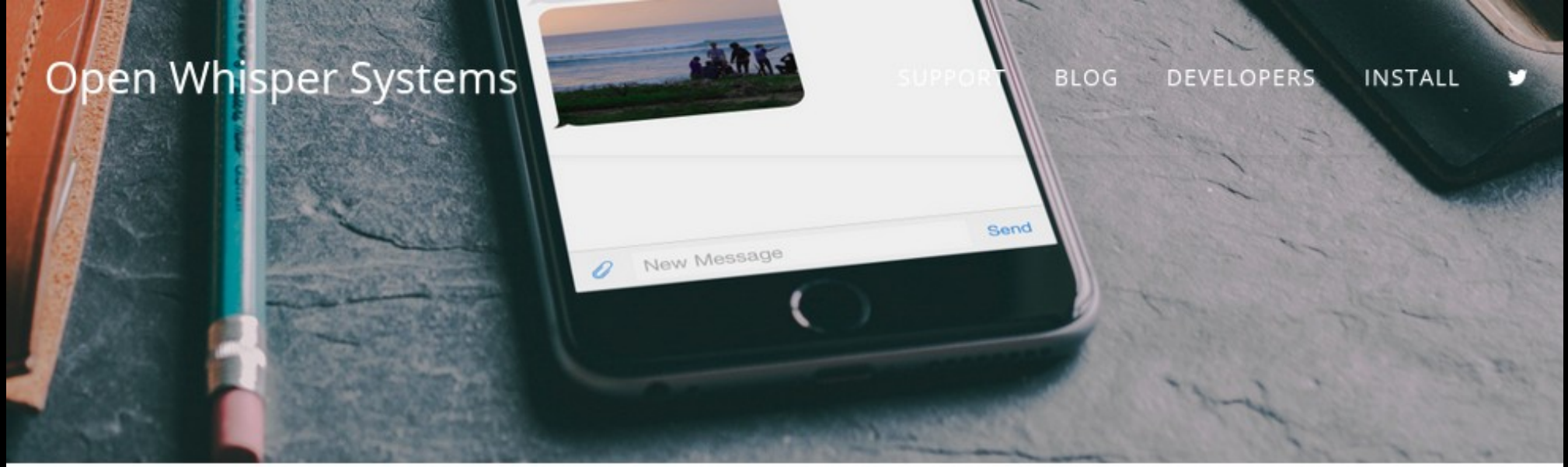
VeraCrypt

VeraCrypt is an on-the-fly disk encryption system and the successor of the discontinued TrueCrypt. The software is freely available, runs on **multiple operating systems**, and is very easy to learn how to use. VeraCrypt also plays nicely with dual-boot systems (such as Windows and Linux). VeraCrypt options include either full disk encryption or the creation of cryptographic container files, which mount as additional drive volumes.

VeraCrypt can also be used to encrypt USB flash memory sticks or digital camera or mobile phone memory cards. The caveat is that it is almost impossible to guarantee to securely wipe or overwrite the data from these devices due to their wear leveling algorithms. Therefore you should use a fresh USB device to re-encrypt the data with a new secret key. VeraCrypt also includes a few options which theoretically provide plausible deniability to the user.

Edit

Learn and Use



PRIVACY THAT FITS IN YOUR POCKET

“Use anything by Open Whisper Systems.

— **Edward Snowden**, Whistleblower and privacy advocate

“Signal is the most scalable encryption tool we have. It is free and peer reviewed. I encourage people to use it everyday.

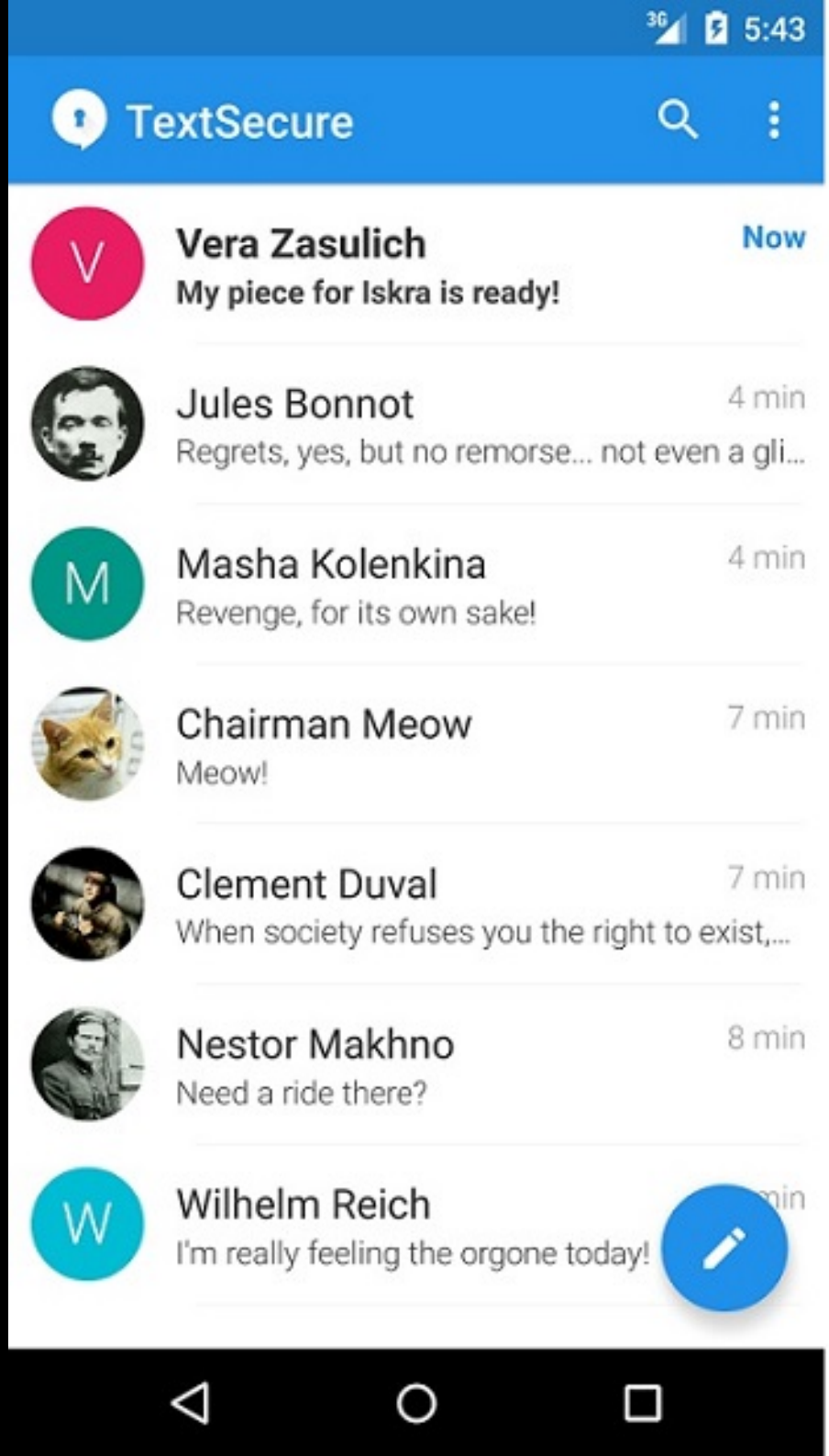
— **Laura Poitras**, Oscar winning filmmaker and journalist

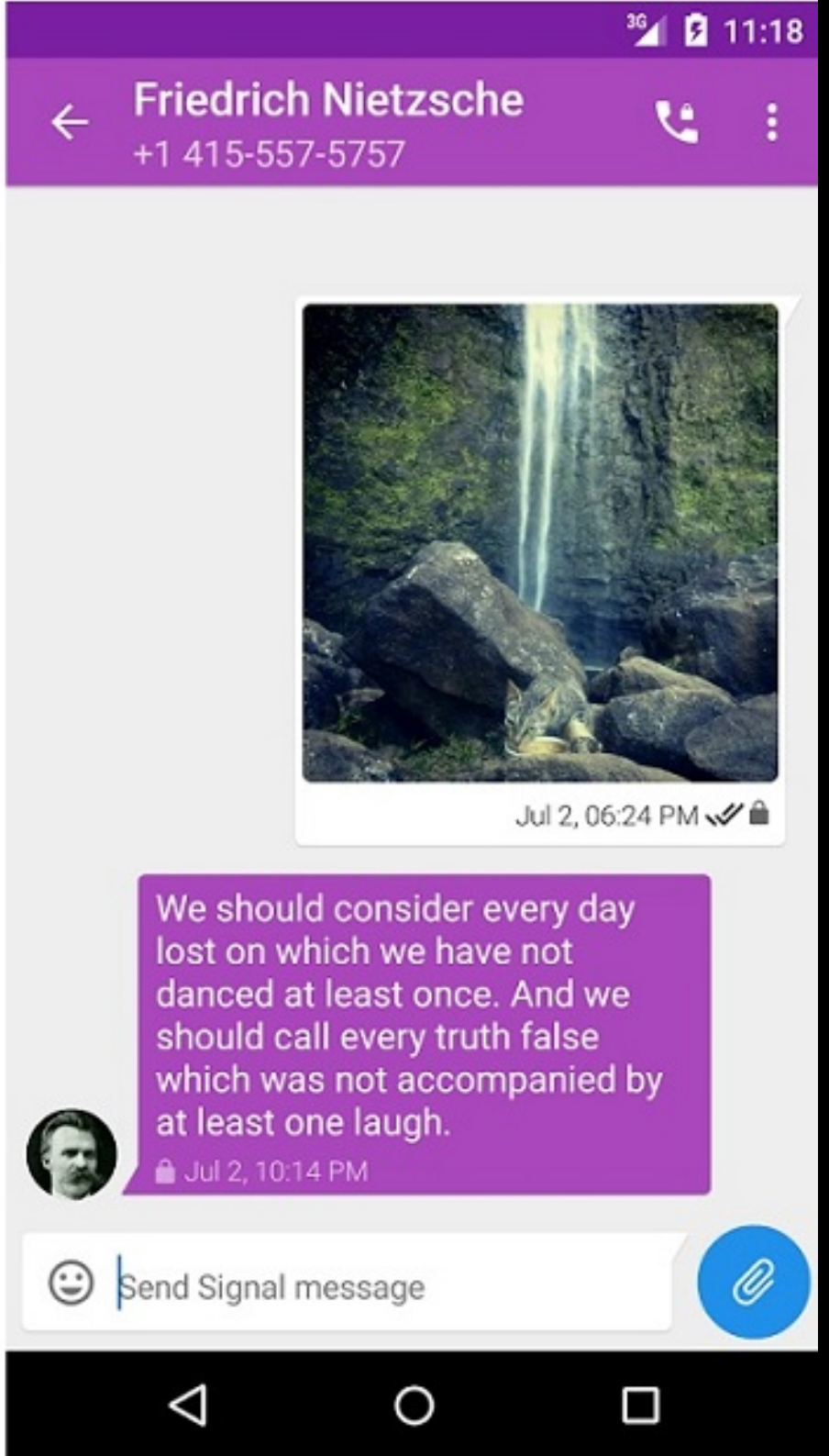
“I am regularly impressed with the thought and care put into both the security and the usability of this app. It's my first choice for an encrypted conversation.

— **Bruce Schneier**, internationally renowned security technologist

“After reading the code, I literally discovered a line of drool running down my face. It’s really nice.

— **Matt Green**, Cryptographer, Johns Hopkins University


5:43
TextSecure
Vera Zasulich
Now
My piece for Iskra is ready!
Jules Bonnot
4 min
Regrets, yes, but no remorse... not even a gli...
Masha Kolenkina
4 min
Revenge, for its own sake!
Chairman Meow
7 min
Meow!
Clement Duval
7 min
When society refuses you the right to exist,...
Nestor Makhno
8 min
Need a ride there?
Wilhelm Reich
I'm really feeling the orgone today!


11:18
Friedrich Nietzsche
+1 415-557-5757
Jul 2, 06:24 PM
We should consider every day lost on which we have not danced at least once. And we should call every truth false which was not accompanied by at least one laugh.
Jul 2, 10:14 PM
Send Signal message

Off-the-Record Messaging

Donate

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. However, *during* a conversation, your correspondent is assured the messages he sees are authentic and unmodified.

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Primary download: Win32 installer for pidgin-otr 4.0.1 (sig) [other downloads]

News

21 Oct 2014

pidgin-otr 4.0.1 released

This point-release includes the following updates:

- Fix max message size for Novell Groupwise
- New Czech, Finnish, Brazilian Portuguese, Norwegian Bokmål translations. Updated French, Chinese translations.
- The Windows binary has been linked with updated versions of libotr, libgcrypt, and libgpg-error.

libotr 4.1.0 released

This minor-version update includes the following changes:

- Modernized autoconf build system
- Use constant-time comparisons where needed
- Use gcrypt secure memory allocation
- Correctly reject attempts to fragment a message into too many pieces
- Fix a missing opdata when sending message fragments
- Don't lose the first user message when REQUIRE_ENCRYPTION is set
- Fix some memory leaks
- Correctly check for children contexts' state when forgetting a context
- API Changes:
  - Added API functions otrl_context_find_recent_instance and otrl_context_find_recent_secure_instance.

10 Oct 2014

git repos and bugtracker now on otr.im

We now link to the new git repositories and the bugtracker on the community development site, otr.im.

28 Sept 2013

Now running on a new server

We've migrated the OTR website to a new and faster server. (Updated 3 Oct 2013): The URL is now https://otr.cypherpunks.ca/, as we have enabled TLS.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. Anyone can forge messages after a conversation to make them look like they came from you. H

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. sation to make them look like they came from you. I

- **Perfect forward secrecy**

  If you lose control of your private keys, no previous conversation is compromised.

Off-the-Record (OTR) Messaging allows you to have private conversations over instant messaging by providing:

- **Encryption**

  No one else can read your instant messages.

- **Authentication**

  You are assured the correspondent is who you think it is.

- **Deniability**

  The messages you send do *not* have digital signatures that are checkable by a third party. sation to make them look like they came from you. I

- **Perfect forward secrecy**

  If you lose control of your private keys us conversation is compromised.

Downloads

OTR library and toolkit

This is the portable OTR Messaging Library, as well as the toolkit to help you forge messages. You need this library in order to use the other OTR software on this page. [Note that some binary packages, particularly Windows, do not have a separate library package, but just include the library and toolkit in the packages below.] The current version is 4.1.0.

README

UPGRADING from version 3.2.x

Source code (4.1.0)

Compressed tarball (sig)

Java OTR library

This is the Java version of the OTR library. This is for developers of Java applications that want to add support for OTR. End users do not require this package. It's still early days, but you can download java-otr version 0.1.0 (sig).

OTR plugin for Pidgin

This is a plugin for Pidgin 2.x which implements Off-the-Record Messaging over any IM network Pidgin supports. The current version is 4.0.1.

README

Source code (4.0.1)

Compressed tarball (sig)

Windows (4.0.1)

Win32 installer for pidgin 2.x (sig)
Win32 zipfile (manual installation) for pidgin 2.x (sig)

OTR localhost AIM proxy

This software is no longer supported. Please use an IM client with native support for OTR.

This is a localhost proxy you can use with almost any AIM client in order to participate in Off-the-Record conversations. The current version is 0.3.1, which means it's still a long way from done. Read the README file carefully. Some things it's still missing:

- Username/password authentication to the proxy
- Having the proxy be able to use *outgoing* proxies itself
- Support for protocols other than AIM/ICQ
- Configurability of the proxy types and ports it uses

But it should work for most people. Please send feedback to the otr-users mailing list, or to the dev team. You may need the above library packages.

README

Source code (0.3.1)

Compressed tarball (sig)

Windows (0.3.1)

Win32 installer (sig)

OS X (0.3.1)

OS X package

Source Code Repository and Bugtracker

You can find a git repository of the OTR source code, as well as the bugtracker, on the otr.im community development site:

- libotr git repo: https://bugs.otr.im/git/libotr.git ; git://git.otr.im/libotr.git
- pidgin-otr git repo: https://bugs.otr.im/git/pidgin_otr.git ; git://git.otr.im/pidgin_otr.git
- Bugtracker: https://bugs.otr.im

Mailing Lists

If you use OTR software, you should join at least the otr-announce mailing list, and possibly otr-users (for users of OTR software) or otr-dev (for developers of OTR software) as well.

Documentation

Installation and Setup Guides

pidgin-otr tutorial from the Security-in-a-Box project
Video OTR tutorial (by Niels)
Adium, Pidgin & OTR (auf Deutsch, by Christian Franke)

Downloads

OTR library and toolkit

This is the portable OTR Messaging Library, as well as the toolkit to help you forge messages. You need this library in order to use the other OTR software on this page. [Note that some binary packages, particularly Windows, do not have a separate library package, but just include the library and toolkit in the packages below.] The current version is 4.1.0.

README

UPGRADING from version 3.2.x

Source code (4.1.0)

Compressed tarball (sig)

Java OTR library

This is the Java version of the OTR library. This is for developers of Java applications that want to add support for OTR. End users do not require this package. It's still early days, but you can download java-otr version 0.1.0 (sig).

OTR plugin for Pidgin

This is a plugin for Pidgin 2.x which implements Off-the-Record Messaging over any IM network Pidgin supports. The current version is 4.0.1.

README

Source code (4.0.1)

Compressed tarball (sig)

Windows (4.0.1)

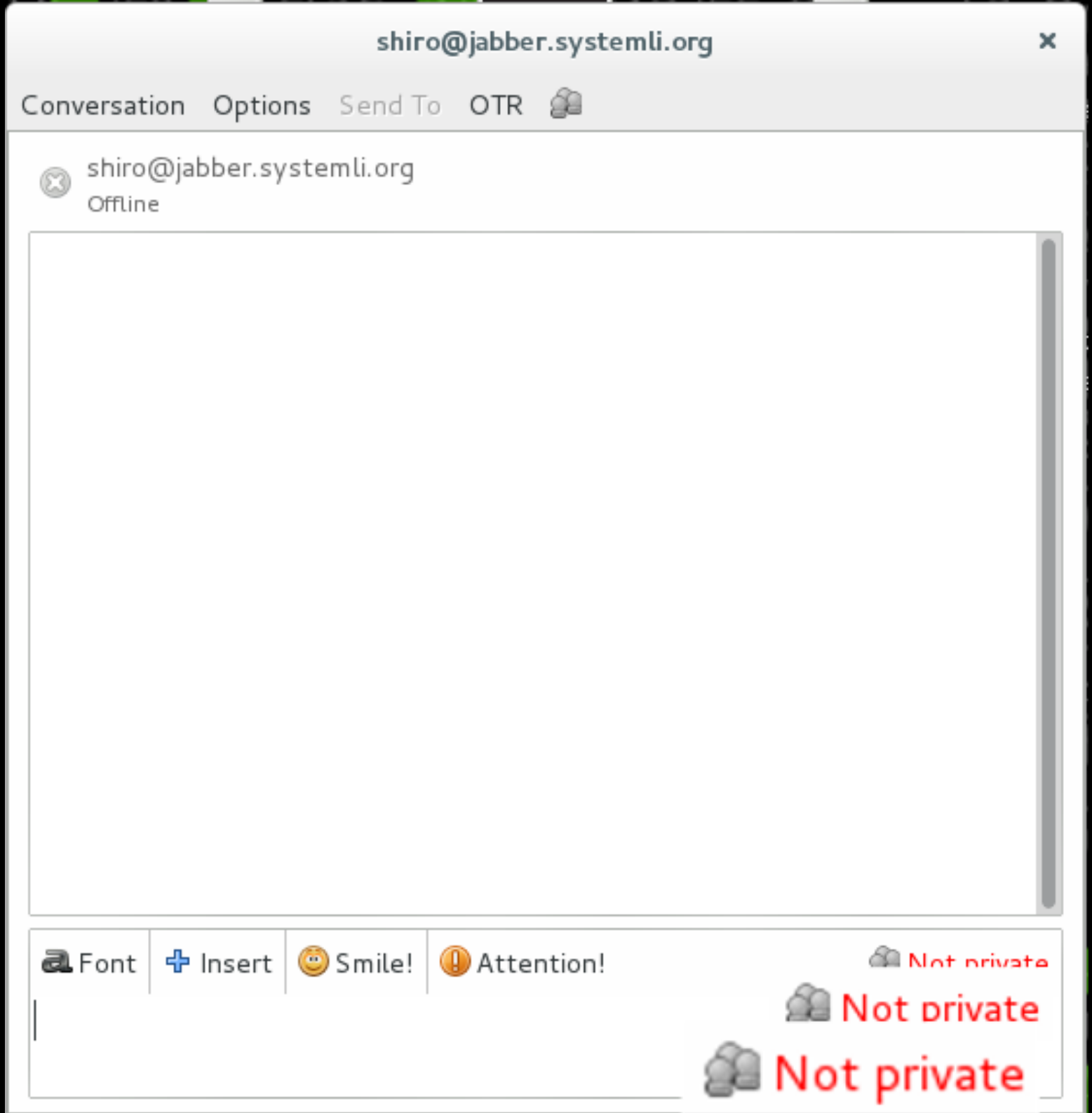
Win32 installer for pidgin 2.x (sig)
Win32 zipfile (manual installation) for pidgin 2.x (sig)

Plugins

Enabled	Name
☐	**Message Notification** 2.10.11 Provides a variety of ways of notifying you of unread messages.
☐	**Message Timestamp Formats** 2.10.11 Customizes the message timestamp formats.
☐	**Mouse Gestures** 2.10.11 Provides support for mouse gestures
☐	**Music Messaging** 2.10.11 Music Messaging Plugin for collaborative composition.
☐	**New Line** 2.10.11 Prepends a newline to displayed message.
☐	**NSS Preferences** 2.10.11 Configure Ciphers and other Settings for the NSS SSL/TLS Plugin
☐	**Offline Message Emulation** 2.10.11 Save messages sent to an offline user as pounce.
☑	**Off-the-Record Messaging** 4.0.1 Provides private and secure conversations
☐	**Pidgin GTK+ Theme Control** 2.10.11 Provides access to commonly used gtkrc settings.
☐	**Pidgin Theme Editor** 2.10.11 Pidgin Theme Editor.
☐	**Psychic Mode** 2.10.11 Psychic mode for incoming conversation
☐	**Send Button** 2.10.11 Conversation Window Send Button.
☐	**Text replacement** 2.10.11 Replaces text in outgoing messages according to user-defined rules.
☐	**Timestamp** 2.10.11 Display iChat-style timestamps
☐	**Voice/Video Settings** 2.10.11 Configure your microphone and webcam.
☐	**XMPP Console** 2.10.11 Send and receive raw XMPP stanzas.
☐	**XMPP Service Discovery** 2.10.11 Allows browsing and registering services.

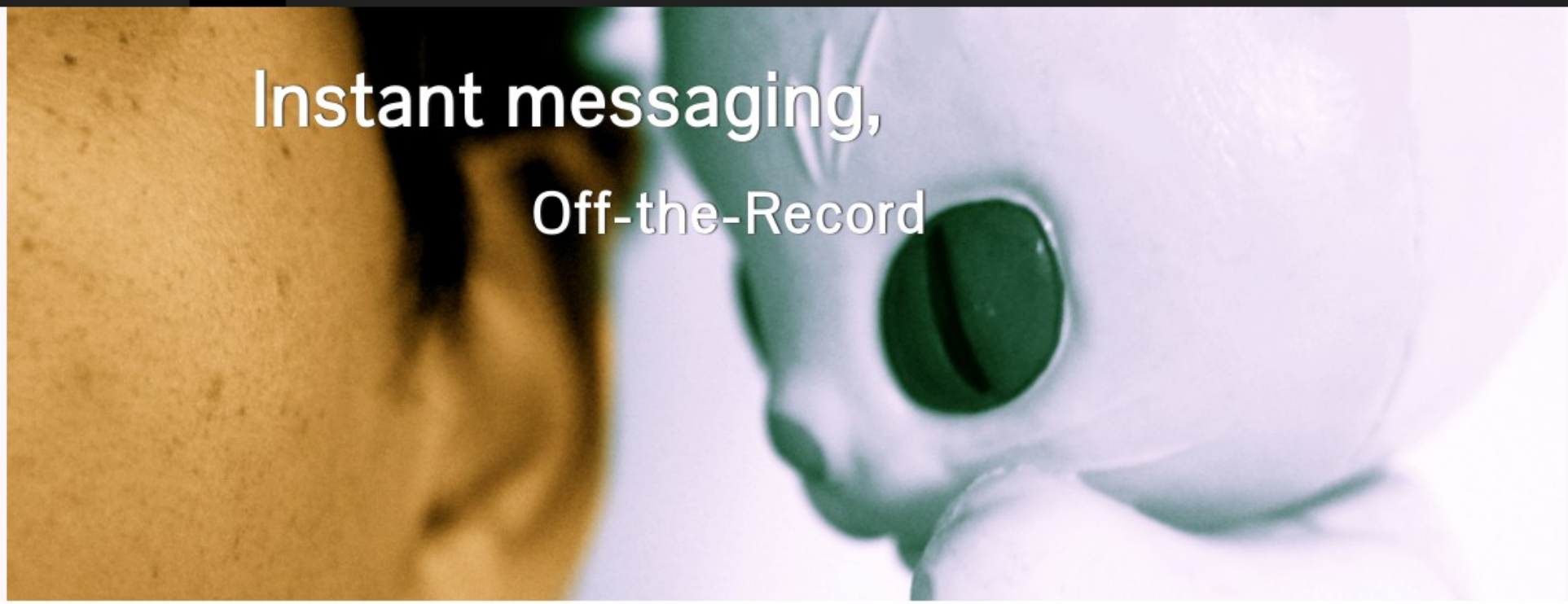
⊞ Plugin Details

Configure Plugin | Close


shiro@jabber.systemli.org
Conversation
Options
Send To
OTR
shiro@jabber.systemli.org
Offline
Font
Insert
Smile!
Attention!
Not private
Not private
Not private

OTR.im

Home Clients Chat About Blog



OTR!

OTR, which stands for Off-the-Record messaging is a cryptographic protocol that provides strong encryption for instant messaging conversations. Originally designed by, among others, Ian Goldberg.

Get to know the OTR protocol »

Bugtracker

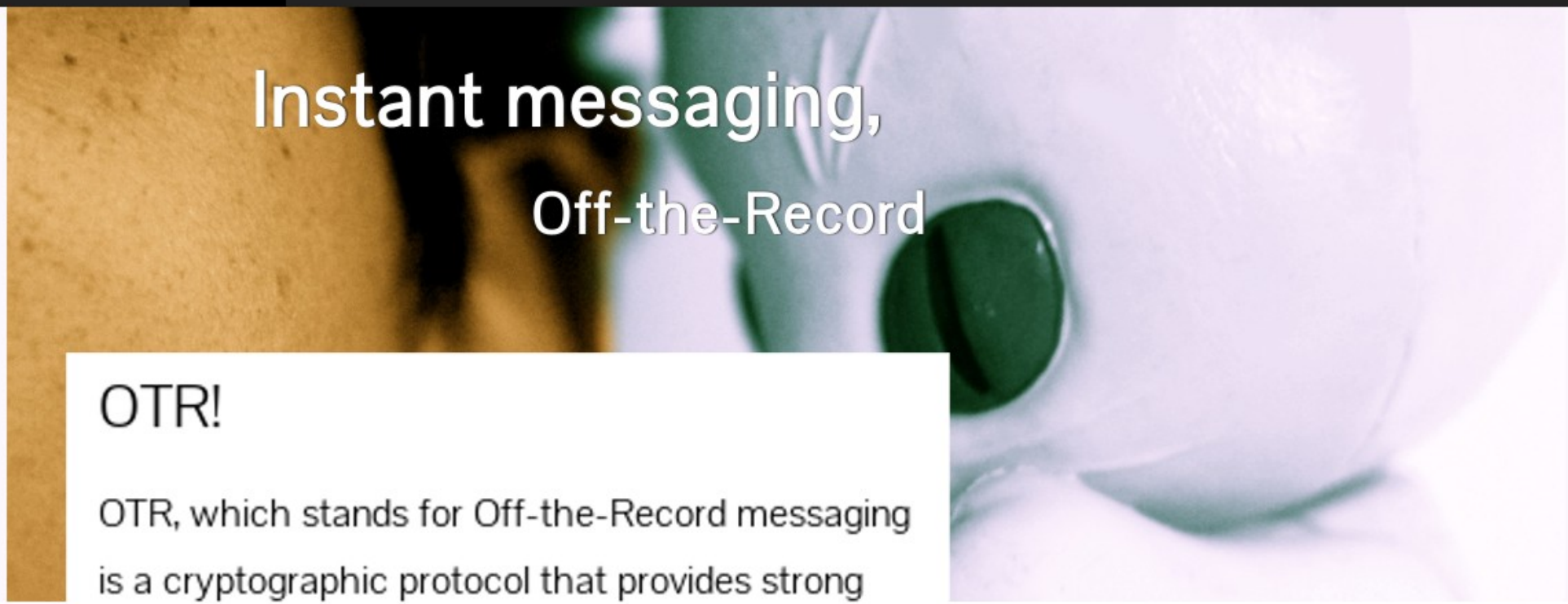
Help us improve OTR software by filing bugs, triaging bugs or submit patches to solve issues.

Contribute to the bugtracker »

Reaching developers

Many of the OTR enthusiasts and developers idle on the #OTR channel on the OFTC IRC network. Feel free to join, lurk or discuss..

IRC webchat »



OTR!

OTR, which stands for Off-the-Record messaging is a cryptographic protocol that provides strong encryption for instant messaging conversations. Originally designed by, among others, Ian Goldberg.

Get to know the OTR protocol »

OTR

OTR, v
is a cry
encryp
Origina
Goldbe

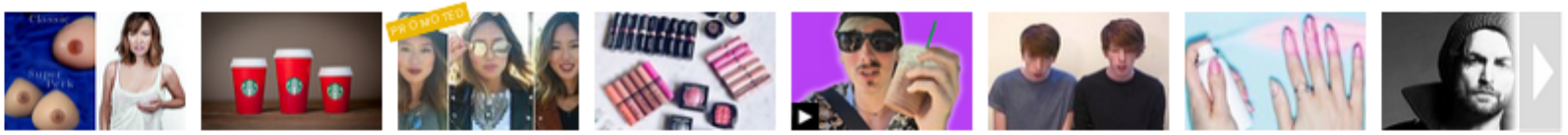
Get to know the OTR protocol »

Reaching developers

Many of the OTR enthusiasts and developers idle on the #OTR channel on the OFTC IRC network. Feel free to join, lurk or discuss..

IRC webchat »

User pain level: very high.



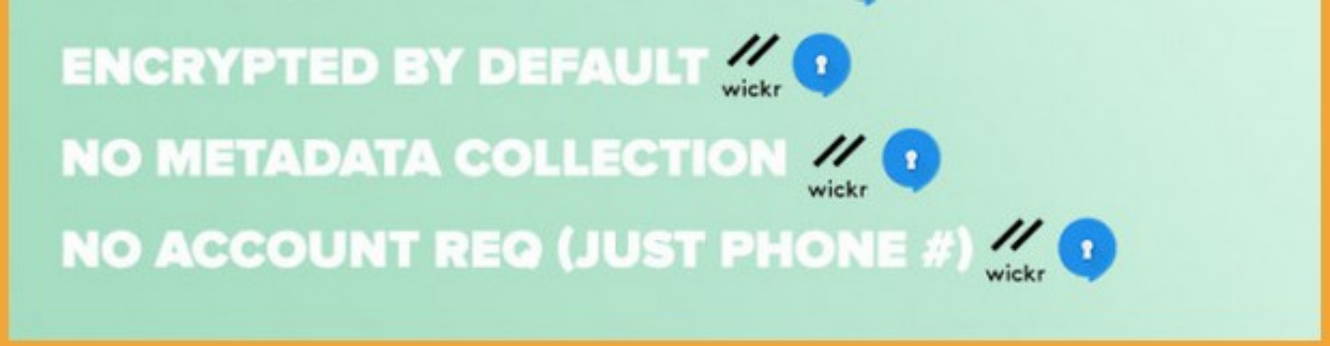
TECH

You Probably Can't Encrypt Anything, Can You?

A new study shows that even the simplest encryption tools are lost on the public.

posted on Nov. 4 2015, at 8:32 p.m.

Joseph Bernstein
BuzzFeed News Reporter



Nicole Nguyen / BuzzFeed News

Looking to stay secure? Good for you!! Here are three suggestions.

Some digital privacy advocates believe that government surveillance – which has grown significantly under Presidents Bush and Obama – will continue to grow under the Trump administration. Furthermore, using fully encrypted messaging will protect your personal information from hackers and corporations, too.

Signal (free, iOS and Android) is an app for messaging and audio calls that saw a 400% increase in downloads after President Trump was elected. The app is encrypted end-to-end, offers Snapchat-style expiring messages, and doesn't store messages or your "metadata" (like the date, timestamp, and phone numbers associated with a message you've sent). Signal leaves their code open to review, so anyone can audit the software and verify that its privacy settings retain strong encryption and best practices. In October 2016, an independent security audit by five researches from the University of Oxford, "found no major flaws" in the design of Signal's cryptographic protocol.

As my colleague Hamza Shaban pointed out, Signal requires your phone number and access to your address book when you sign up, which risks ratting out whistleblowers. Signal's creator, Moxie Marlinspike, suggests signing up with a throwaway Google Voice number as a workaround for concerned parties.

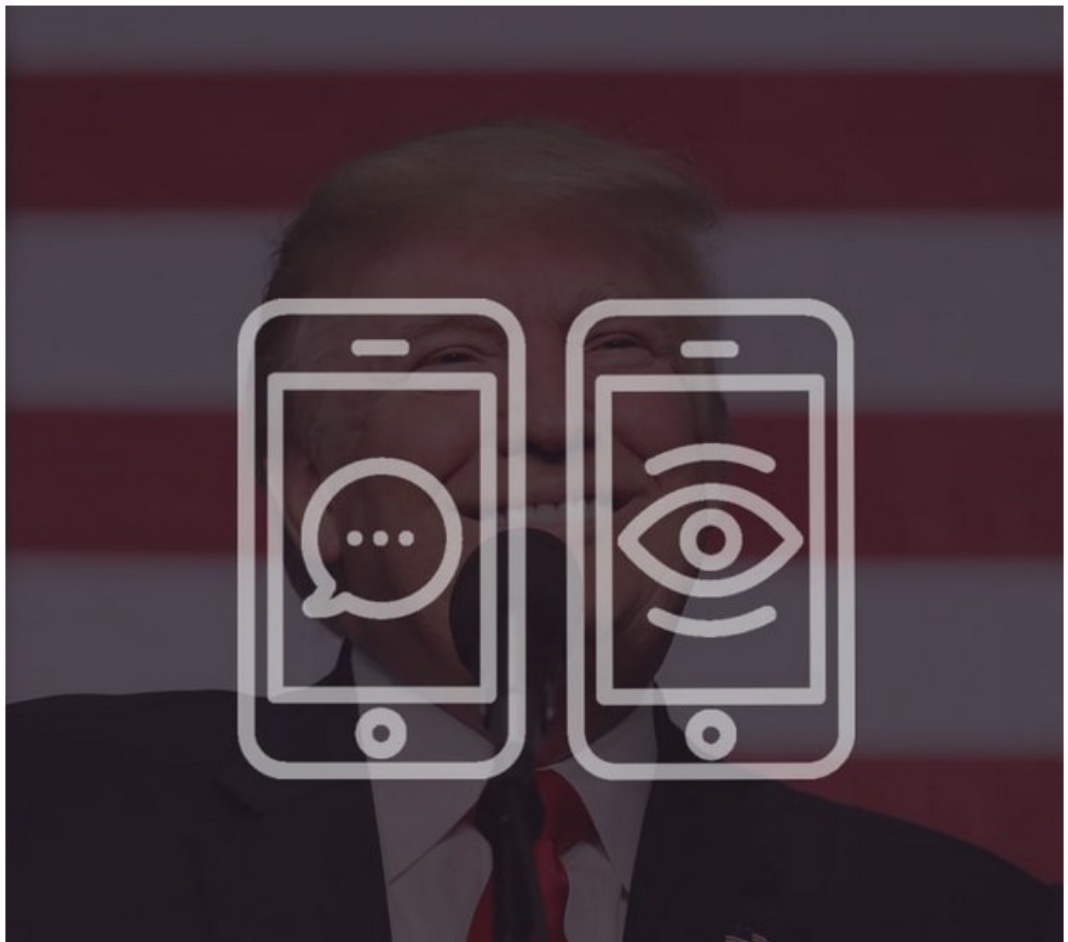
TECH

Here's How To Protect Your Privacy In Trump's America

Easy tips to shield yourself from expanded government surveillance.

Posted on January 20, 2017, at 2:01 p.m.

Nicole Nguyen
BuzzFeed News Reporter



CHATTING IN SECRET WHILE WE'RE ALL BEING WATCHED

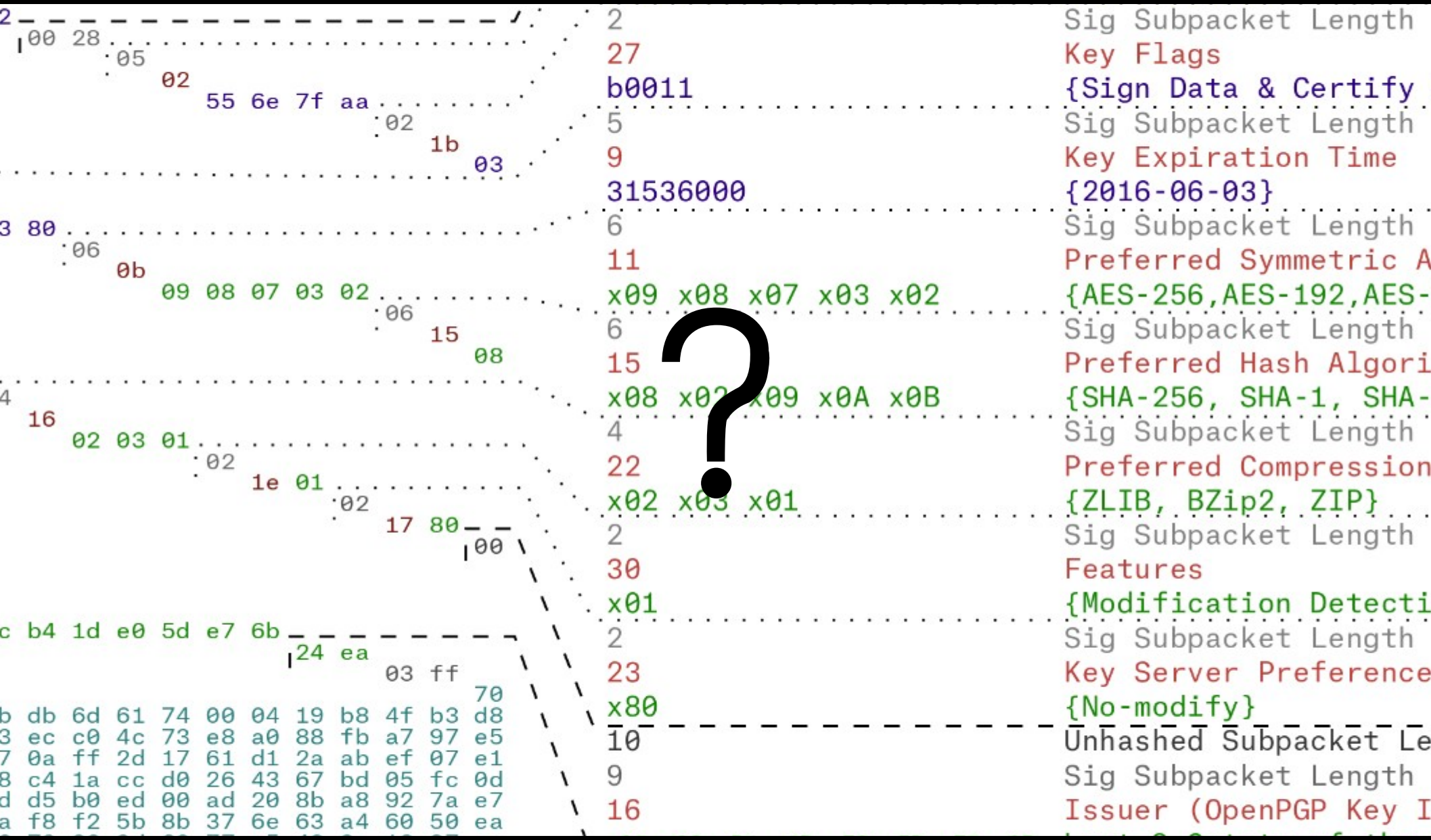
Micah Lee

July 14 2015, 7:08 p.m.

When you pick up the phone and call someone, or send a text message, or write an email, or send a Facebook message, or chat using Google Hangouts, other people find out what you're saying, who you're talking to, and where you're located. Such private data might only be available to the service provider brokering your conversation, but it might also be visible to the telecom companies carrying your Internet packets, to spy and law enforcement agencies, and even to some nearby teenagers monitoring your Wi-Fi network with Wireshark.

But if you take careful steps to protect yourself, it's possible to communicate online in a way that's private, secret and anonymous. Today I'm going to explain in precise terms how to do that. I'll take techniques NSA


PRISM
KEYSCORE
CTO
Internet Cloud
CIA
The Internet
DoD Network


2
00 28
05
02
55 6e 7f aa
02
1b
03
3 80
06
0b
09 08 07 03 02
06
15
08
4
16
02 03 01
02
1e 01
02
17 80
00
c b4 1d e0 5d e7 6b
24 ea
03 ff
70
b db 6d 61 74 00 04 19 b8 4f b3 d8
3 ec c0 4c 73 e8 a0 88 fb a7 97 e5
7 0a ff 2d 17 61 d1 2a ab ef 07 e1
8 c4 1a cc d0 26 43 67 bd 05 fc 0d
d d5 b0 ed 00 ad 20 8b a8 92 7a e7
a f8 f2 5b 8b 37 6e 63 a4 60 50 ea
2
Sig Subpacket Length
27
Key Flags
b0011
{Sign Data & Certify
5
Sig Subpacket Length
9
Key Expiration Time
31536000
{2016-06-03}
6
Sig Subpacket Length
11
Preferred Symmetric A
x09 x08 x07 x03 x02
{AES-256,AES-192,AES-
6
Sig Subpacket Length
15
Preferred Hash Algori
x08 x02 x09 x0A x0B
{SHA-256, SHA-1, SHA-
4
Sig Subpacket Length
22
Preferred Compression
x02 x03 x01
{ZLIB, BZip2, ZIP}
2
Sig Subpacket Length
30
Features
x01
{Modification Detecti
2
Sig Subpacket Length
23
Key Server Preference
x80
{No-modify}
10
Unhashed Subpacket Le
9
Sig Subpacket Length
16
Issuer (OpenPGP Key I
?


the "CryptoParty guys"

the grugq @thegrugq · 13 Dec 2016

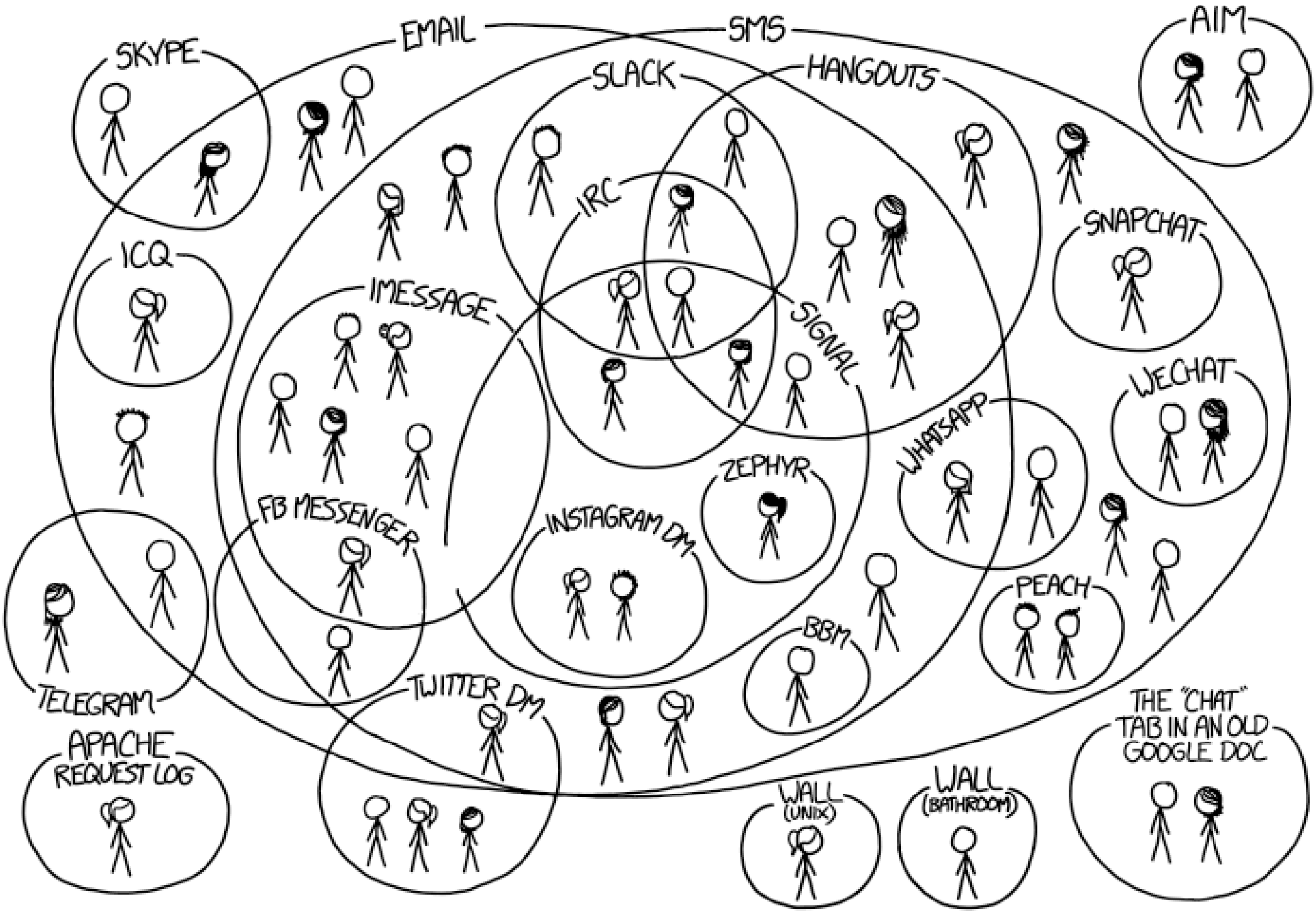
Q: I have to protect against cavities, my threat model is basically candy, sugars, etc. etc.

Privacy Activist: Use Signal. Use Tor.

25 271 513

Theat model


INFOSEC
\\BYTES



I HAVE A HARD TIME KEEPING TRACK OF WHICH CONTACTS USE WHICH CHAT SYSTEMS.

¯_(ツ)_/¯

@shiromarieke