SECURE COMMUNICATIONS: PAST, PRESENT, FUTURE

Jean-Philippe Aumasson

THE SPEAKER

PhD in cryptography from EPFL & FHNW, 2009

Principal Cryptographer at Kudelski Security

Designed popular algorithms: SipHash, BLAKE2

Talked at Black Hat, DEFCON, RSA, etc.

Designed and reviewed secure com technos

http://aumasson.jp

https://twitter.com/veorq

SECURE COMMUNICATIONS

Internet-based communications, over-IP

VoIP

Real-time text + data, instant messaging-like

Asynchronous text + data, email-like

Out of scope: PSTN phone, satphones, radio coms, etc.

SECURE COMMUNICATIONS

Confidentiality of the **content**

- Is it securely encrypted? Who has the keys?

Privacy and **anonymity** of **parties**

- Who talks with whom? What is stored by the provider?

Authentication of **parties** and **content**

- Am I sure I talk with Alice? Were messages modified?

Assurance and **confidence**

- Can designers be trusted? How secure is the software?

WHY SHOULD WE CARE?

Corporate espionnage, especially when traveling

Nation-state agencies surveillance and recording

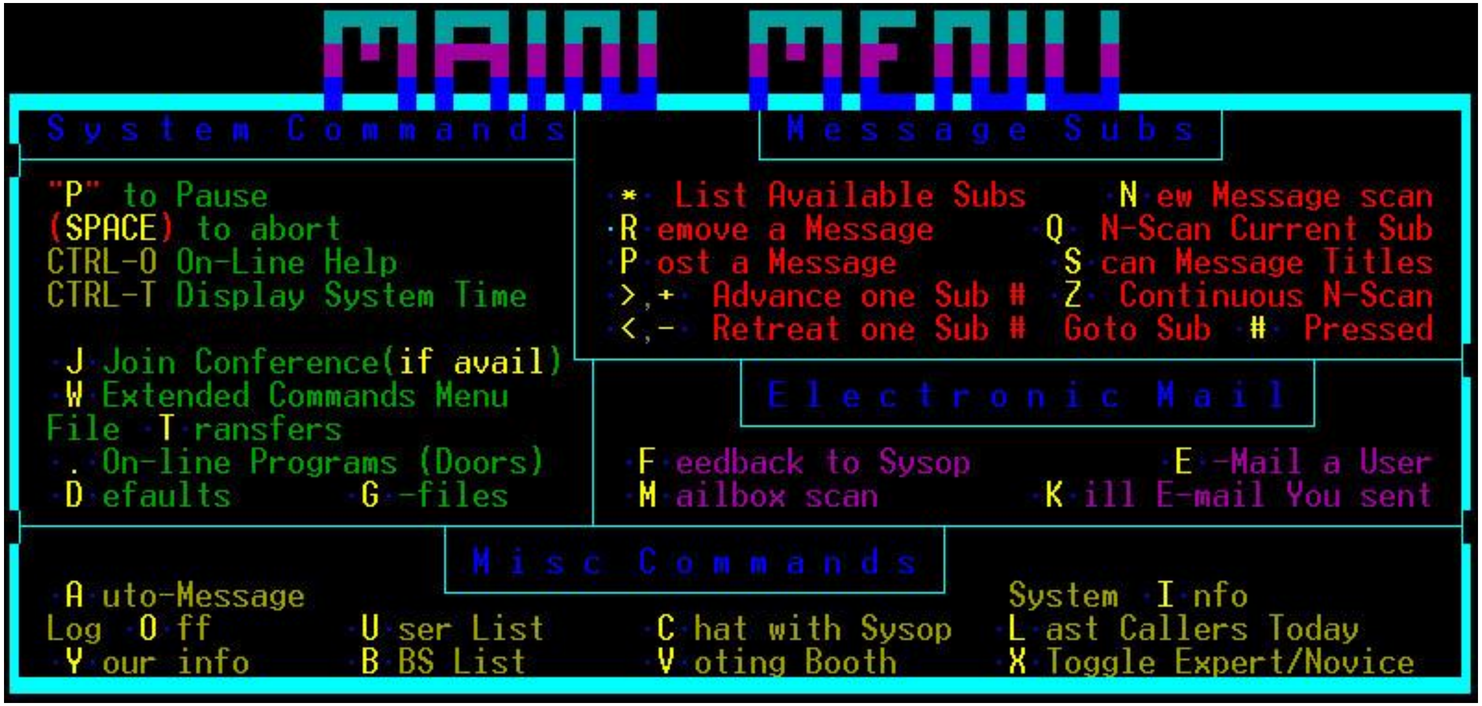
Reduce need for trust in ISPs, admins, etc.

Mere desire for privacy

Past: 1980s–2012

1980-1990

Bulletin boards, email, IRC; **no security**



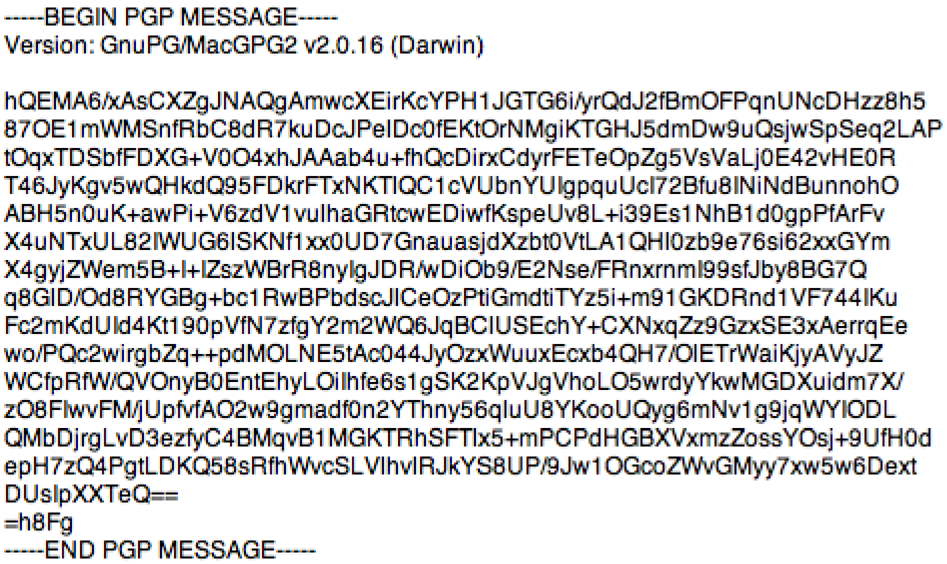
```
                         MAIN MENU
 System Commands                   Message Subs

 "P" to Pause                  * List Available Subs     N ew Message scan
 (SPACE) to abort              R emove a Message       Q  N-Scan Current Sub
 CTRL-O On-Line Help           P ost a Message          S can Message Titles
 CTRL-T Display System Time    >,+ Advance one Sub #    Z  Continuous N-Scan
                               <,- Retreat one Sub #   Goto Sub  #  Pressed
  J Join Conference(if avail)
  W Extended Commands Menu               Electronic Mail
 File  T ransfers
  . On-line Programs (Doors)    F eedback to Sysop               E -Mail a User
  D efaults         G -files    M ailbox scan              K ill E-mail You sent

                         Misc Commands
  A uto-Message                                      System  I nfo
 Log  O ff        U ser List      C hat with Sysop   L ast Callers Today
  Y our info      B BS List       V oting Booth      X Toggle Expert/Novice
```

1991: PGP

Confidentiality and authenticity of files, emails

No forward secrecy, no/low anonymity

Complex and error prone



```
-----BEGIN PGP MESSAGE-----
Version: GnuPG/MacGPG2 v2.0.16 (Darwin)

hQEMA6/xAsCXZgJNAQgAmwcXEirKcYPH1JGTG6i/yrQdJ2fBmOFPqnUNcDHzz8h5
87OE1mWMSnfRbC8dR7kuDcJPelDc0fEKtOrNMgiKTGHJ5dmDw9uQsjwSpSeq2LAP
tOqxTDSbfFDXG+V0O4xhJAAab4u+fhQcDirxCdyrFETeOpZg5VsVaLj0E42vHE0R
T46JyKgv5wQHkdQ95FDkrFTxNKTlQC1cVUbnYUlgpquUcl72Bfu8INiNdBunnohO
ABH5n0uK+awPi+V6zdV1vulhaGRtcwEDiwfKspeUv8L+i39Es1NhB1d0gpPfArFv
X4uNTxUL82lWUG6ISKNf1xx0UD7GnauasjdXzbt0VtLA1QHl0zb9e76si62xxGYm
X4gyjZWem5B+l+lZszWBrR8nylgJDR/wDiOb9/E2Nse/FRnxrnml99sfJby8BG7Q
q8GlD/Od8RYGBg+bc1RwBPbdscJlCeOzPtiGmdtiTYz5i+m91GKDRnd1VF744lKu
Fc2mKdUld4Kt190pVfN7zfgY2m2WQ6JqBClUSEchY+CXNxqZz9GzxSE3xAerrqEe
wo/PQc2wirgbZq++pdMOLNE5tAc044JyOzxWuuxEcxb4QH7/OlETrWaiKjyAVyJZ
WCfpRfW/QVOnyB0EntEhyLOilhfe6s1gSK2KpVJgVhoLO5wrdyYkwMGDXuidm7X/
zO8FlwvFM/jUpfvfAO2w9gmadf0n2YThny56qluU8YKooUQyg6mNv1g9jqWYlODL
QMbDjrgLvD3ezfyC4BMqvB1MGKTRhSFTlx5+mPCPdHGBXVxmzZossYOsj+9UfH0d
epH7zQ4PgtLDKQ58sRfhWvcSLVlhvlRJkYS8UP/9Jw1OGcoZWvGMyy7xw5w6Dext
DUslpXXTeQ==
=h8Fg
-----END PGP MESSAGE-----
```

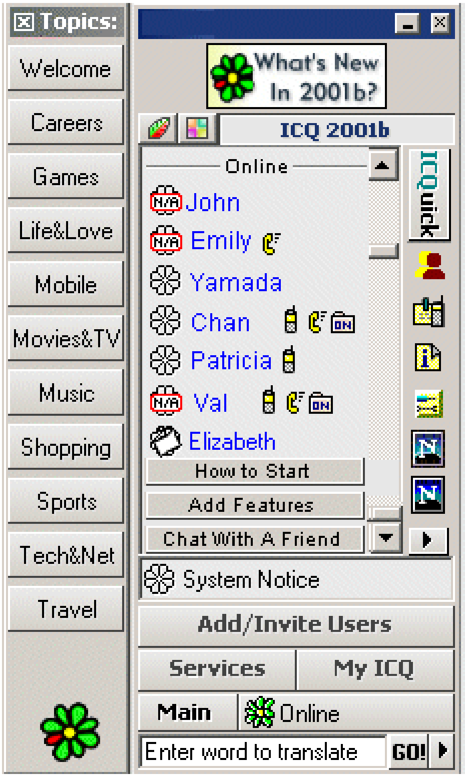
INSTANT MESSAGING SYSTEMS

ICQ, AIM, Gaim/Pidgin, MSN, Jabber, Google talk, etc.

Commercial corporate solutions

Little or no concern for security

- □ At best client-server encryption
- □ Frequent protocol and software flaws



Online

John

Emily

Yamada

Chan

Patricia

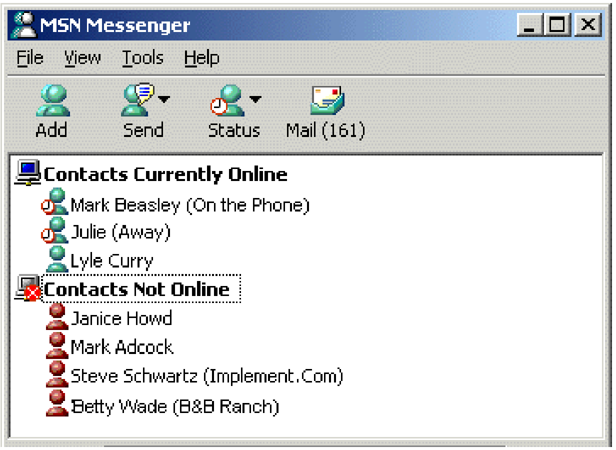
Val

Elizabeth

System Notice

Online

Enter word to translate



Contacts Currently Online

Mark Beasley (On the Phone)

Julie (Away)

Lyle Curry

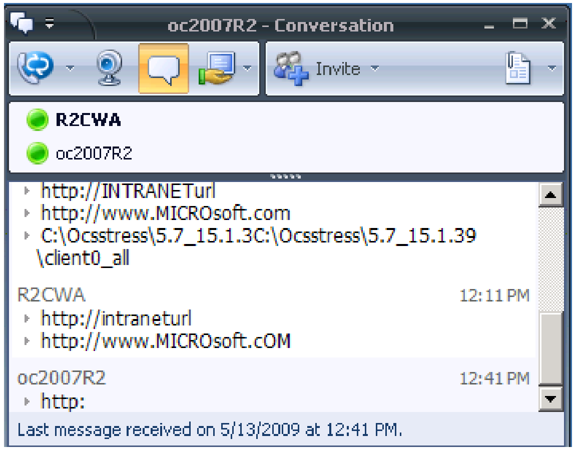
Contacts Not Online

Janice Howd

Mark Adcock

Steve Schwartz (Implement.Com)

Betty Wade (B&B Ranch)



R2CWA

oc2007R2

- http://INTRANETurl
- http://www.MICROsoft.com
- C:\Ocsstress\5.7_15.1.3C:\Ocsstress\5.7_15.1.39 \client0_all

R2CWA 12:11 PM
- http://intraneturl
- http://www.MICROsoft.cOM

oc2007R2 12:41 PM
- http:

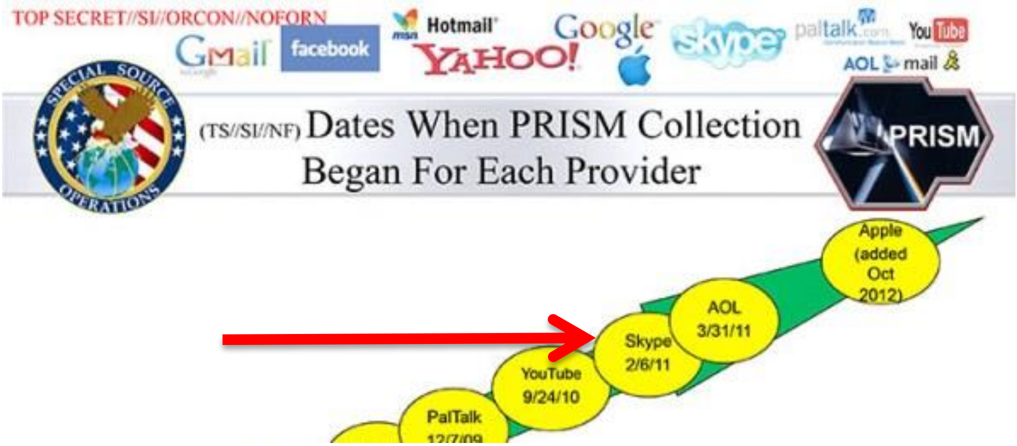
Last message received on 5/13/2009 at 12:41 PM.

2003: SKYPE

Initially based on a peer-to-peer network

2005 audit: standard algorithms, proprietary protocol

Acquired by MS in 2011 (...) NSA eavesdropping...



TOP SECRET//SI//ORCON//NOFORN
GMail
facebook
Hotmail
Google
YAHOO!
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
PRISM
Apple (added Oct 2012)
AOL 3/31/11
Skype 2/6/11
YouTube 9/24/10
PalTalk 12/7/09

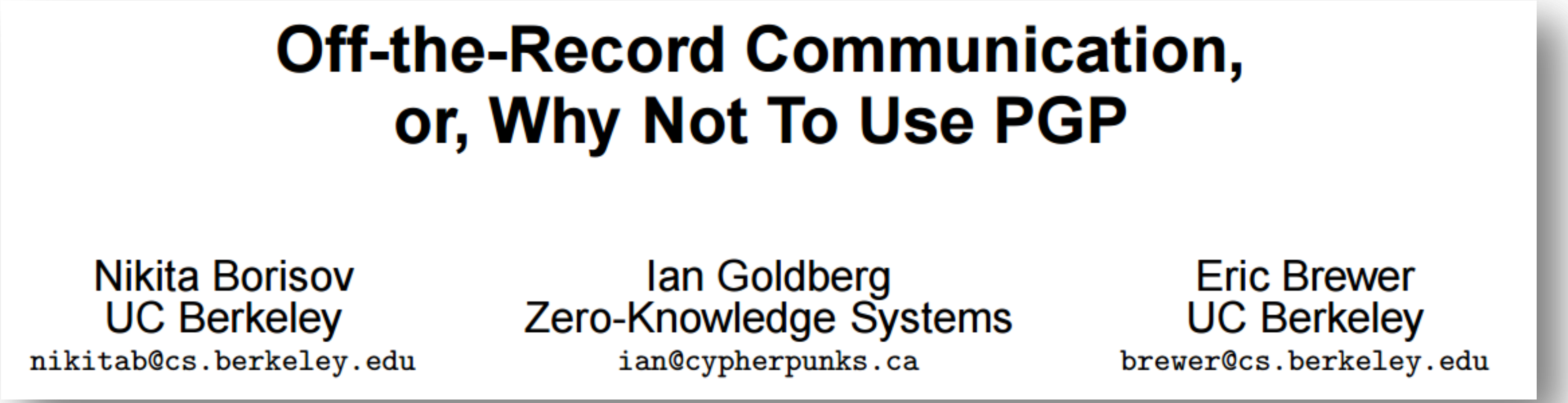
(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

2004: OFF-THE-RECORD (OTR) PROTOCOL

End-to-end encryption, forward secrecy

Runs on top of existing messaging protocols

Trusted by Snowden to chat with journalists



Off-the-Record Communication,
or, Why Not To Use PGP

Nikita Borisov
UC Berkeley
nikitab@cs.berkeley.edu

Ian Goldberg
Zero-Knowledge Systems
ian@cypherpunks.ca

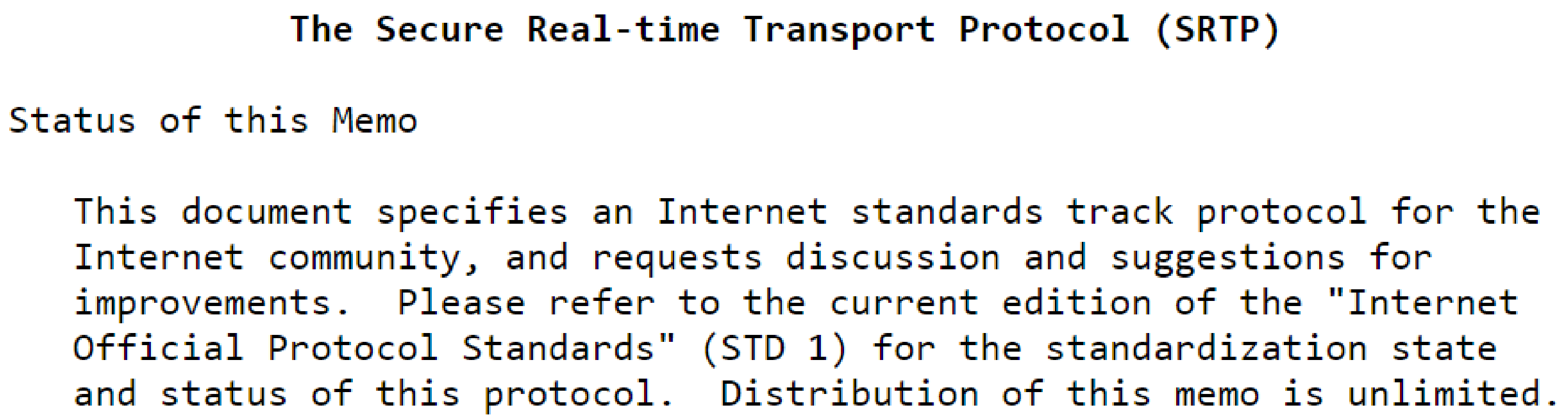
Eric Brewer
UC Berkeley
brewer@cs.berkeley.edu

2004: SRTP

“Secure RTP”, encrypted VoIP (RFC 3711)

Specs on how to protect RTP packets

First step towards secure VoIP



The Secure Real-time Transport Protocol (SRTP)

Status of this Memo

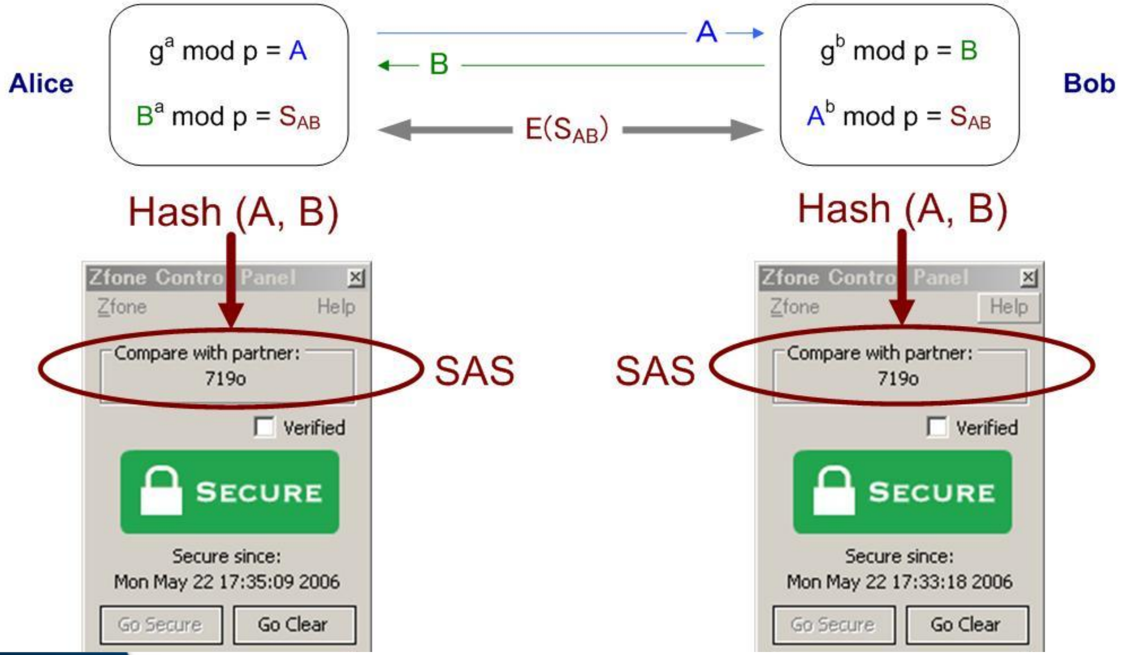
This document specifies an Internet standards track protocol for the Internet community, and requests discussion and suggestions for improvements. Please refer to the current edition of the "Internet Official Protocol Standards" (STD 1) for the standardization state and status of this protocol. Distribution of this memo is unlimited.

2006: ZRTP

End-to-end encrypted VoIP

MitM defense: **SAS** and **key continuity**

No PKI, implicit user authentication



Compare with partner: 719o

□ Verified

SECURE

Secure since: Mon May 22 17:35:09 2006

Go Secure | Go Clear

Compare with partner: 719o

□ Verified

SECURE

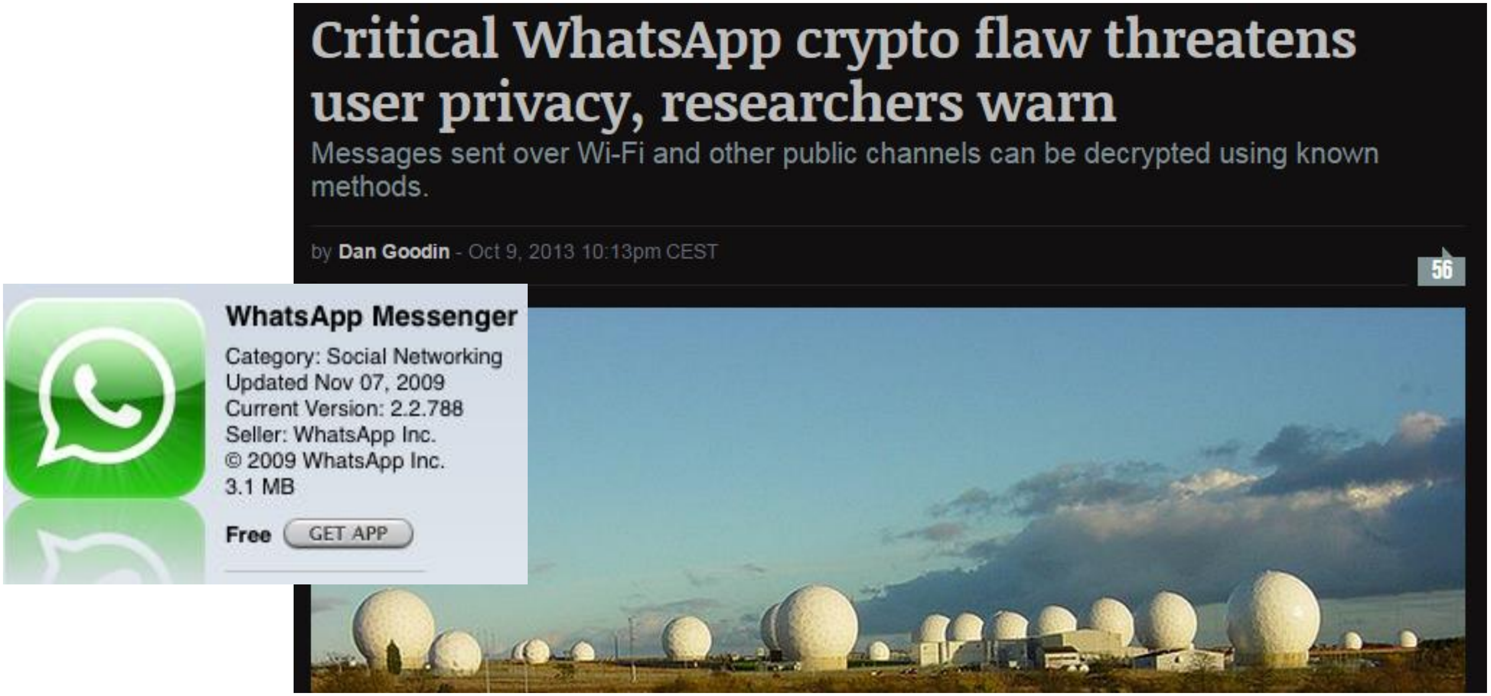
Secure since: Mon May 22 17:33:18 2006

Go Secure | Go Clear

2009: WHATSAPP

One of the first popular **mobile messaging** apps

Initially low security, proprietary protocols...



Critical WhatsApp crypto flaw threatens user privacy, researchers warn

Messages sent over Wi-Fi and other public channels can be decrypted using known methods.

by **Dan Goodin** - Oct 9, 2013 10:13pm CEST

WhatsApp Messenger

Category: Social Networking
Updated Nov 07, 2009
Current Version: 2.2.788
Seller: WhatsApp Inc.
© 2009 WhatsApp Inc.
3.1 MB

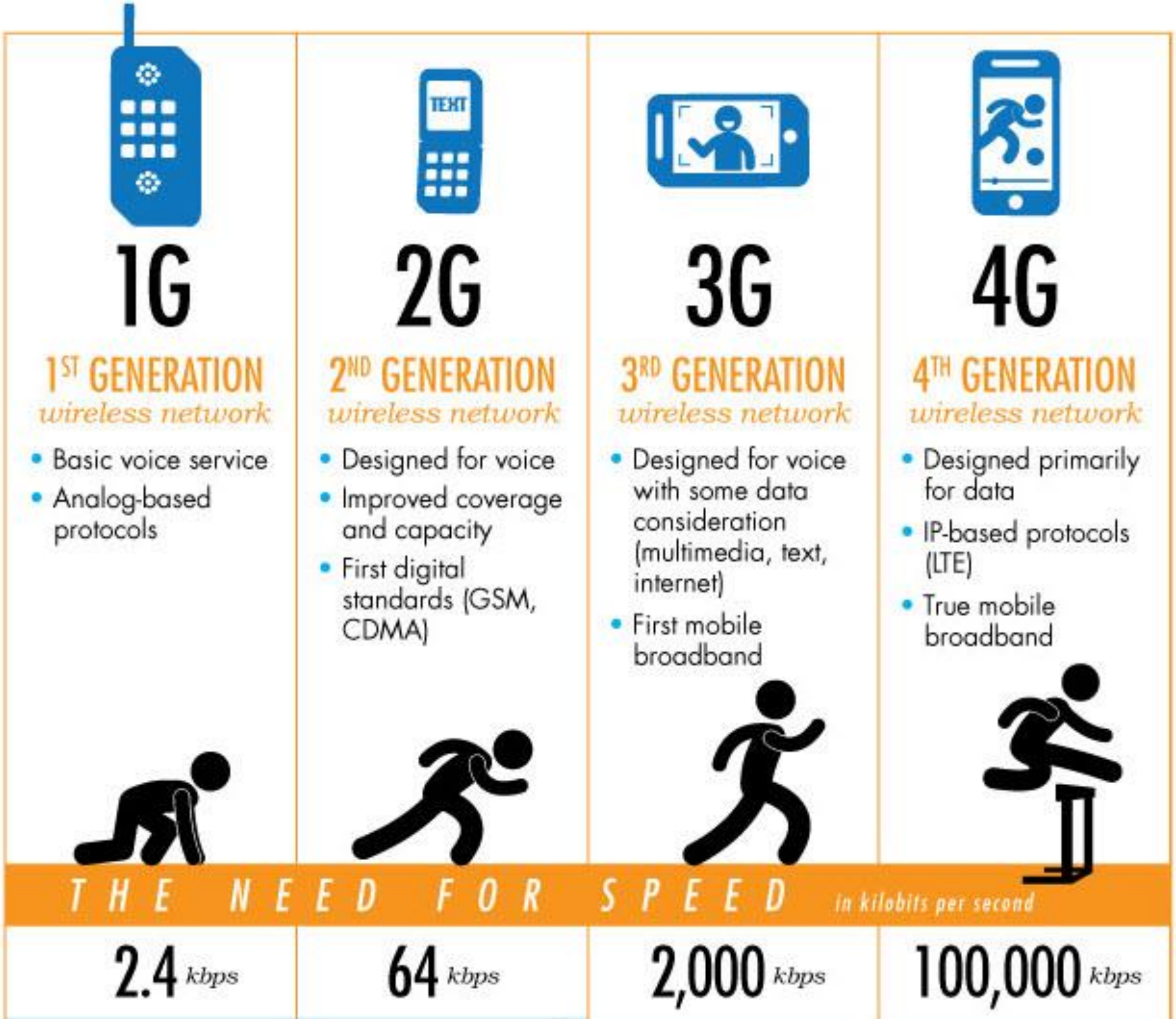
Present: 2012–2015

FACTORS OF CHANGE...

FACTORS OF CHANGE...

FACTORS OF CHANGE...

FACTORS OF CHANGE...



1G

1ST GENERATION wireless network

- Basic voice service
- Analog-based protocols

2G

2ND GENERATION wireless network

- Designed for voice
- Improved coverage and capacity
- First digital standards (GSM, CDMA)

3G

3RD GENERATION wireless network

- Designed for voice with some data consideration (multimedia, text, internet)
- First mobile broadband

4G

4TH GENERATION wireless network

- Designed primarily for data
- IP-based protocols (LTE)
- True mobile broadband

THE NEED FOR SPEED in kilobits per second

1G	2G	3G	4G
2.4 kbps	64 kbps	2,000 kbps	100,000 kbps

IMPACT

New secure voice/chat/email app every week

- **Some innovative protocols and secure apps**, but also...
- Opportunistic and profit-driven systems, often lower-quality
- Ditto for well-intended but inexperienced developers

Better **awareness and understanding**

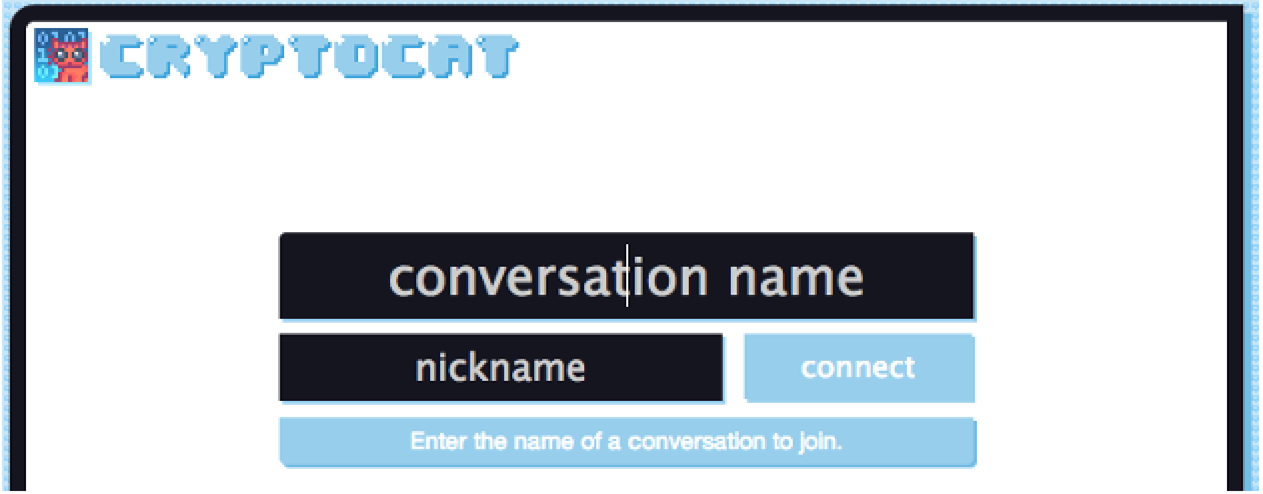
Efforts in terms of **UI and usability**

CRYPTOCAT

Web and mobile chat, free and open-source

Software reviewed and audited

OTR for 2-party chats, custom group protocol



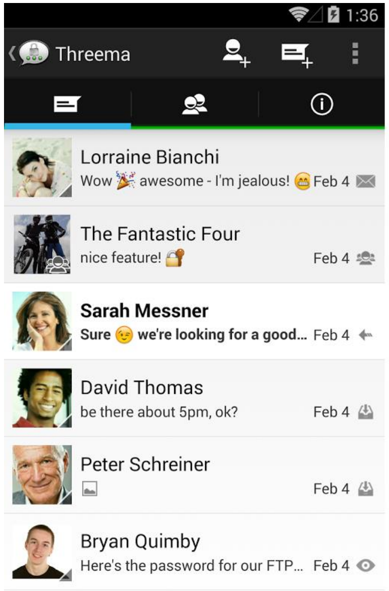
Enter the name of a conversation to join.

THREEMA

Swiss, end-to-end encryption, good track record

Explicit identity verification (QR codes scan)

Not open-source, partial forward secrecy only



1:36

Threema

Lorraine Bianchi
Wow 🎉 awesome - I'm jealous! 😁 Feb 4

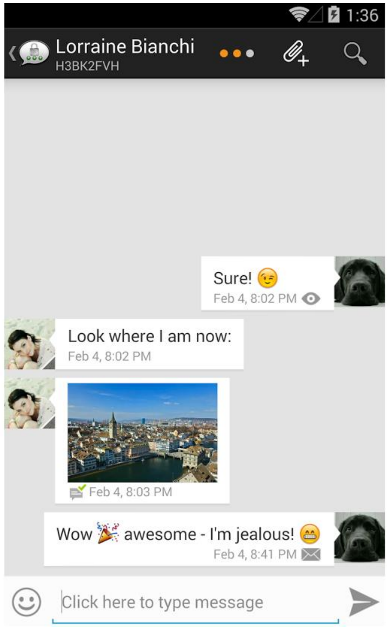
The Fantastic Four
nice feature! 🔐 Feb 4

Sarah Messner
Sure 😉 we're looking for a good... Feb 4

David Thomas
be there about 5pm, ok? Feb 4

Peter Schreiner
Feb 4

Bryan Quimby
Here's the password for our FTP... Feb 4



1:36

Lorraine Bianchi
H3BK2FVH

Sure! 😉
Feb 4, 8:02 PM

Look where I am now:
Feb 4, 8:02 PM

Feb 4, 8:03 PM

Wow 🎉 awesome - I'm jealous! 😁
Feb 4, 8:41 PM

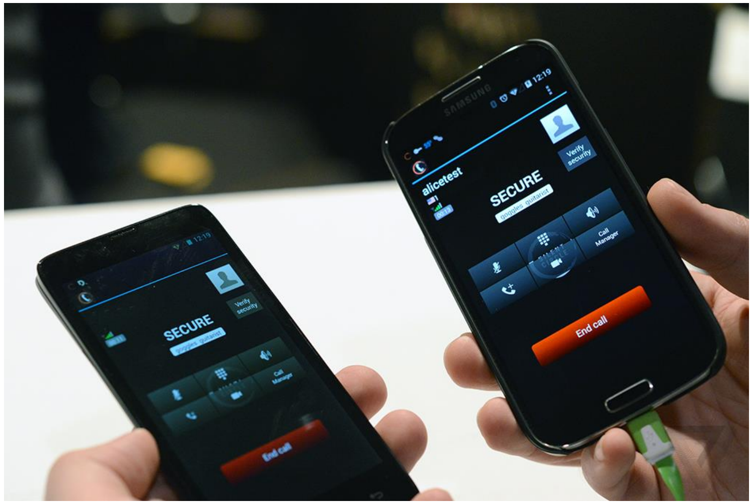
Click here to type message

SILENT CIRCLE

Commercial products from PGP/ZRTP inventor

ZRTP-based VoIP

“SCIMP” messaging protocol, OTR-inspired



Blackphone device integrating Silent Circle apps

OPEN WHISPER SYSTEMS

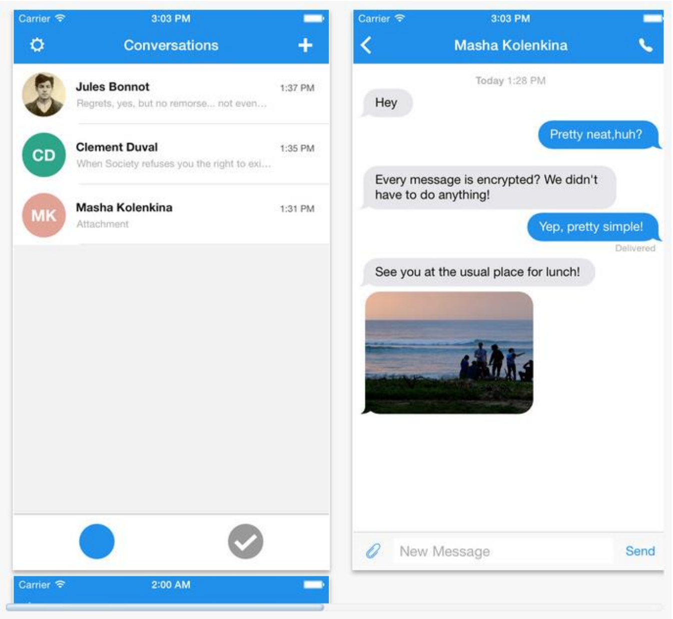
Free & open-source mobile apps, solid engineering

ZRTP-based voice

“Axolotl ratchet” messaging protocol, OTR-inspired

“ Use anything by Open Whisper Systems.

— Edward Snowden, Whistleblower and privacy advocate



Carrier 3:03 PM

Conversations

Jules Bonnot 1:37 PM
Regrets, yes, but no remorse... not even...

CD Clement Duval 1:35 PM
When Society refuses you the right to exi...

MK Masha Kolenkina 1:31 PM
Attachment

Carrier 2:00 AM

Carrier 3:03 PM

Masha Kolenkina

Today 1:28 PM

Hey

Pretty neat,huh?

Every message is encrypted? We didn't have to do anything!

Yep, pretty simple!

Delivered

See you at the usual place for lunch!

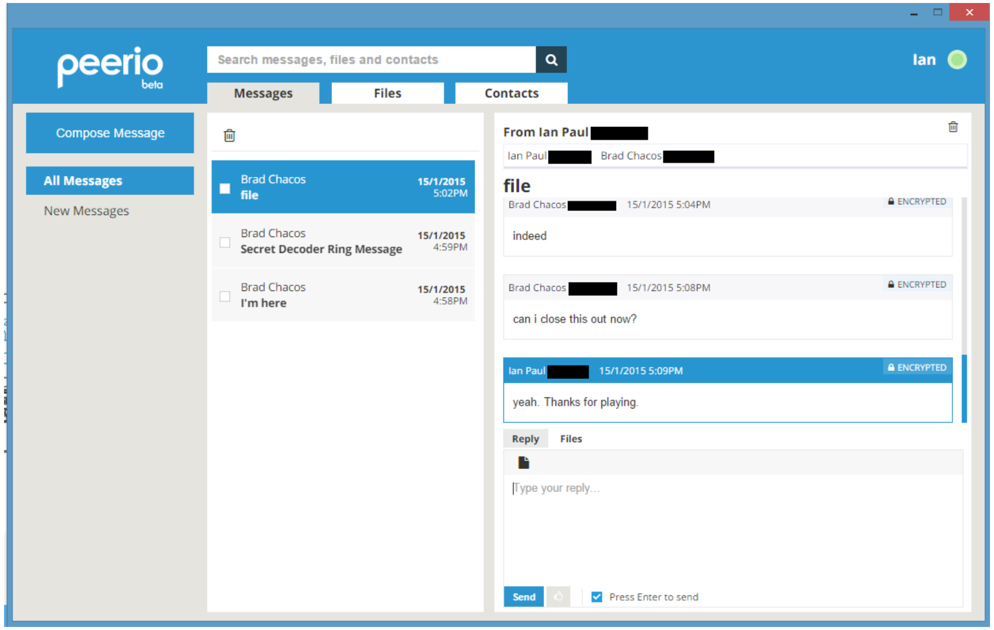
New Message Send

PEERIO

Email-like messaging and file sharing, end-to-end

Browser extensions, mobile apps coming

Minimized user interaction with security parameters



Brad Chacos file 15/1/2015 5:02PM

Brad Chacos Secret Decoder Ring Message 15/1/2015 4:59PM

Brad Chacos I'm here 15/1/2015 4:58PM

From Ian Paul [redacted]

Ian Paul [redacted] Brad Chacos [redacted]

file

Brad Chacos [redacted] 15/1/2015 5:04PM 🔒 ENCRYPTED

indeed

Brad Chacos [redacted] 15/1/2015 5:08PM 🔒 ENCRYPTED

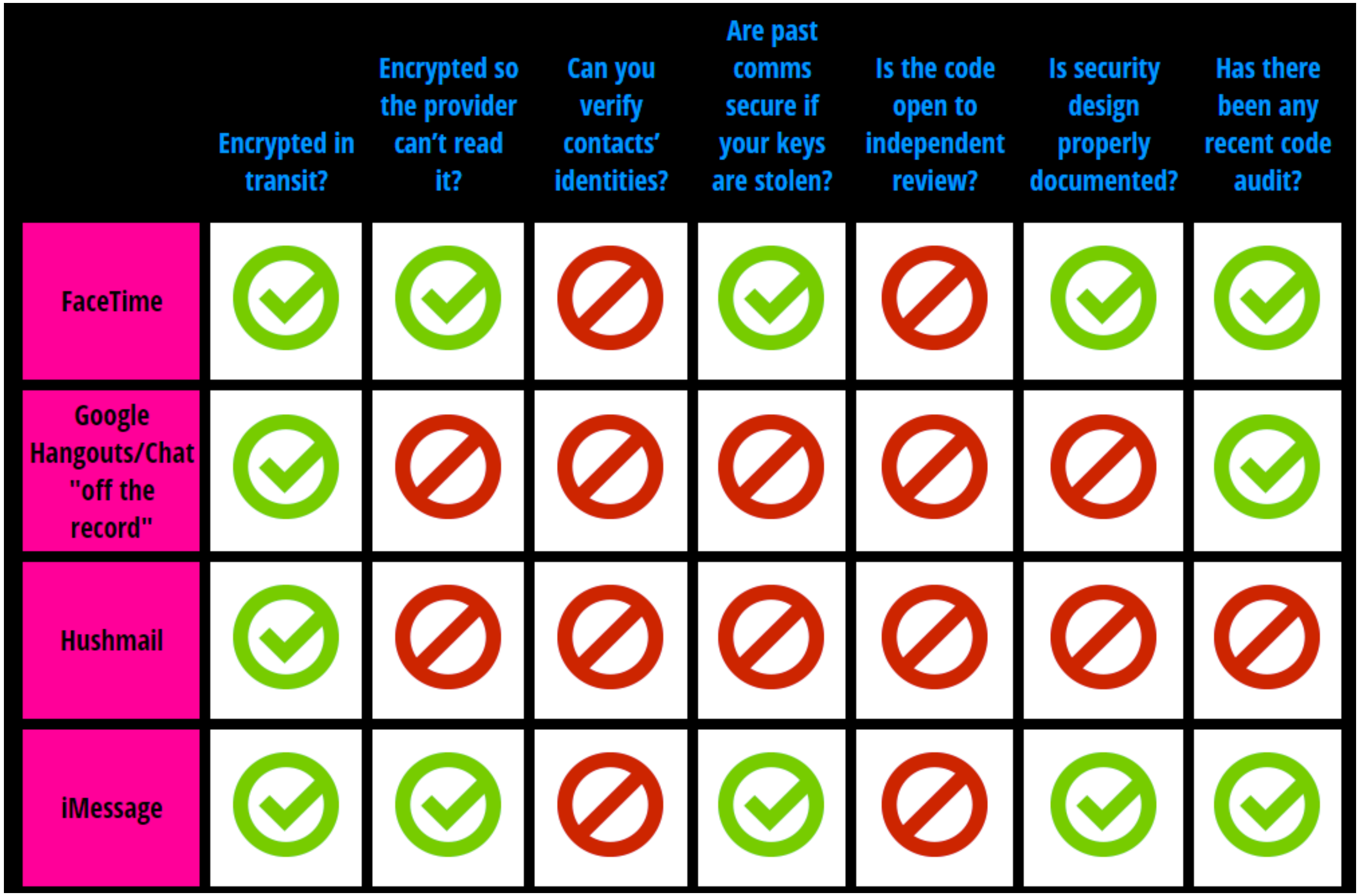
can i close this out now?

Ian Paul [redacted] 15/1/2015 5:09PM 🔒 ENCRYPTED

yeah. Thanks for playing.

MORE MESSAGING APPS

40 listed on https://www.eff.org/secure-messaging-scorecard



	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
FaceTime	✓	✓	⊘	✓	⊘	✓	✓
Google Hangouts/Chat "off the record"	✓	⊘	⊘	⊘	⊘	⊘	✓
Hushmail	✓	⊘	⊘	⊘	⊘	⊘	⊘
iMessage	✓	✓	⊘	✓	⊘	✓	✓

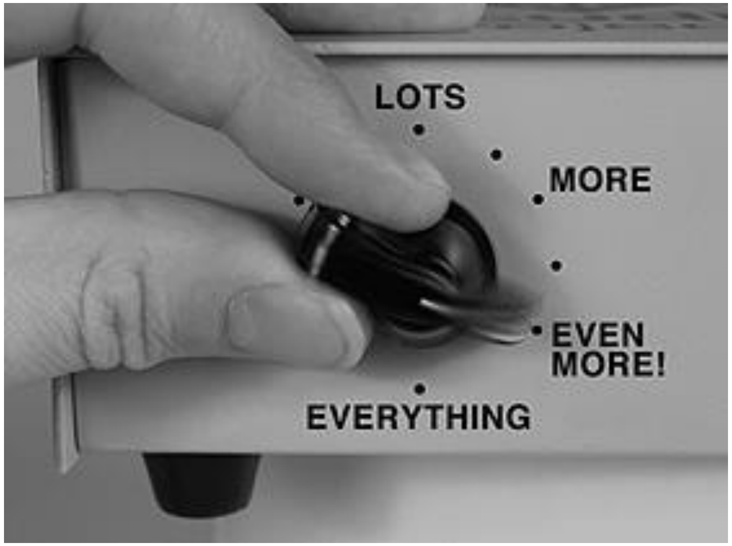
Future 2016+

WHAT WILL CHANGE...

More bandwidth for audio and video content

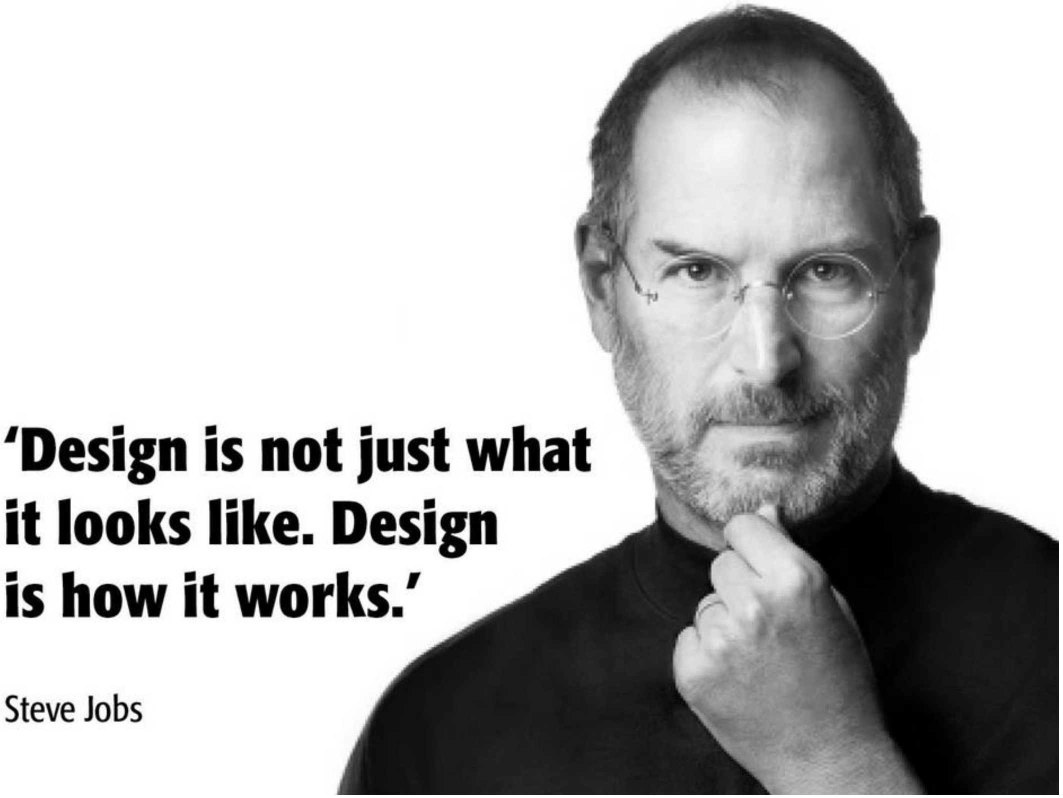
More users of mobile devices

More platforms (watches, etc.)



EXPECT... LESS FRAGMENTATION

Most usable and beautiful apps will survive



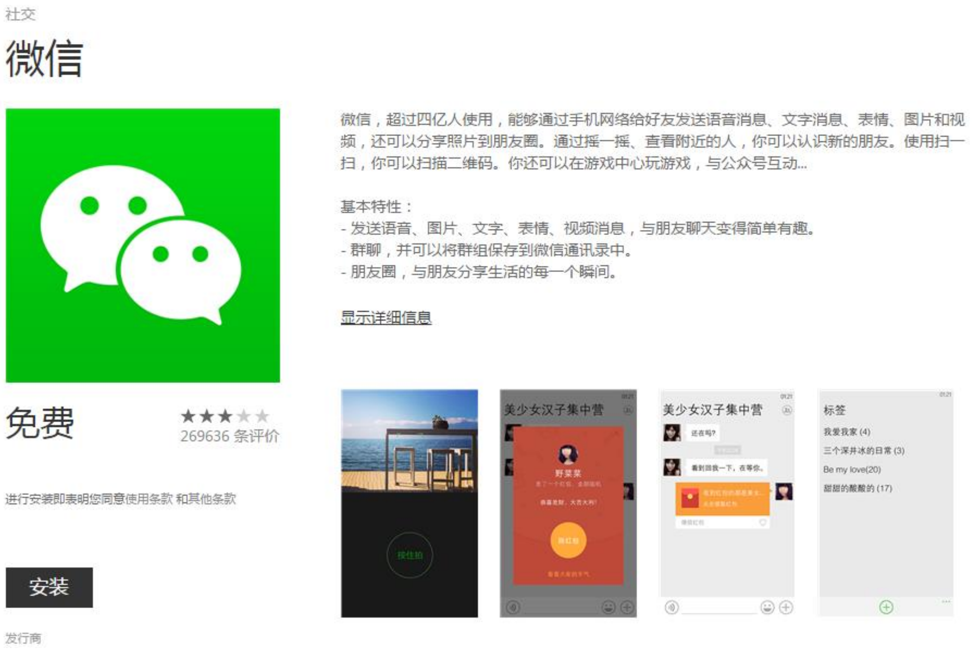
'Design is not just what it looks like. Design is how it works.'

Steve Jobs

EXPECT... REGIONAL DIFFERENCES

Different apps will dominate different markets

Due to different usage, culture, regulations, preference for local apps, etc.



社交

微信

微信，超过四亿人使用，能够通过手机网络给好友发送语音消息、文字消息、表情、图片和视频，还可以分享照片到朋友圈。通过摇一摇、查看附近的人，你可以认识新的朋友。使用扫一扫，你可以扫描二维码。你还可以在游戏中心玩游戏，与公众号互动...

基本特性：
- 发送语音、图片、文字、表情、视频消息，与朋友聊天变得简单有趣。
- 群聊，并可以将群组保存到微信通讯录中。
- 朋友圈，与朋友分享生活的每一个瞬间。

显示详细信息

免费

★★★☆☆
269636 条评价

进行安装即表明您同意使用条款 和其他条款

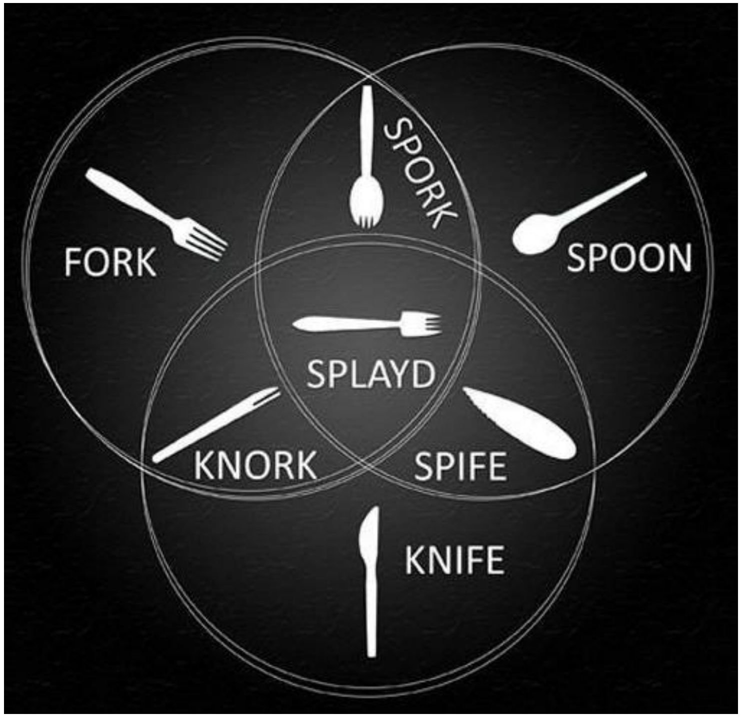
安装

发行商

EXPECT... UNIFICATION

Voice, messaging, and video in a **single app**

Same app in mobile platforms and (mobile) browsers



EXPECT... BETTER INTEGRATION

In **corporate** and **professional** environments

Industry-specific, such as health or finance

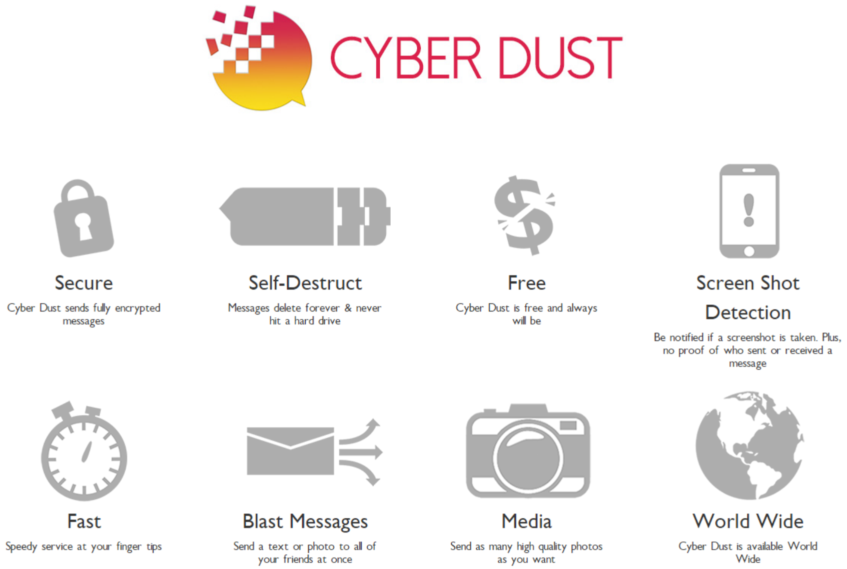
Features for compliance, accountability, auditability

EXPECT... MORE COMMERCIAL APPS

Due to more popular demande for privacy

Usually better marketing and usability than FOSS

Tends to favor time to market over security



CYBER DUST

Secure
Cyber Dust sends fully encrypted messages

Self-Destruct
Messages delete forever & never hit a hard drive

Free
Cyber Dust is free and always will be

Screen Shot Detection
Be notified if a screenshot is taken. Plus, no proof of who sent or received a message

Fast
Speedy service at your finger tips

Blast Messages
Send a text or photo to all of your friends at once

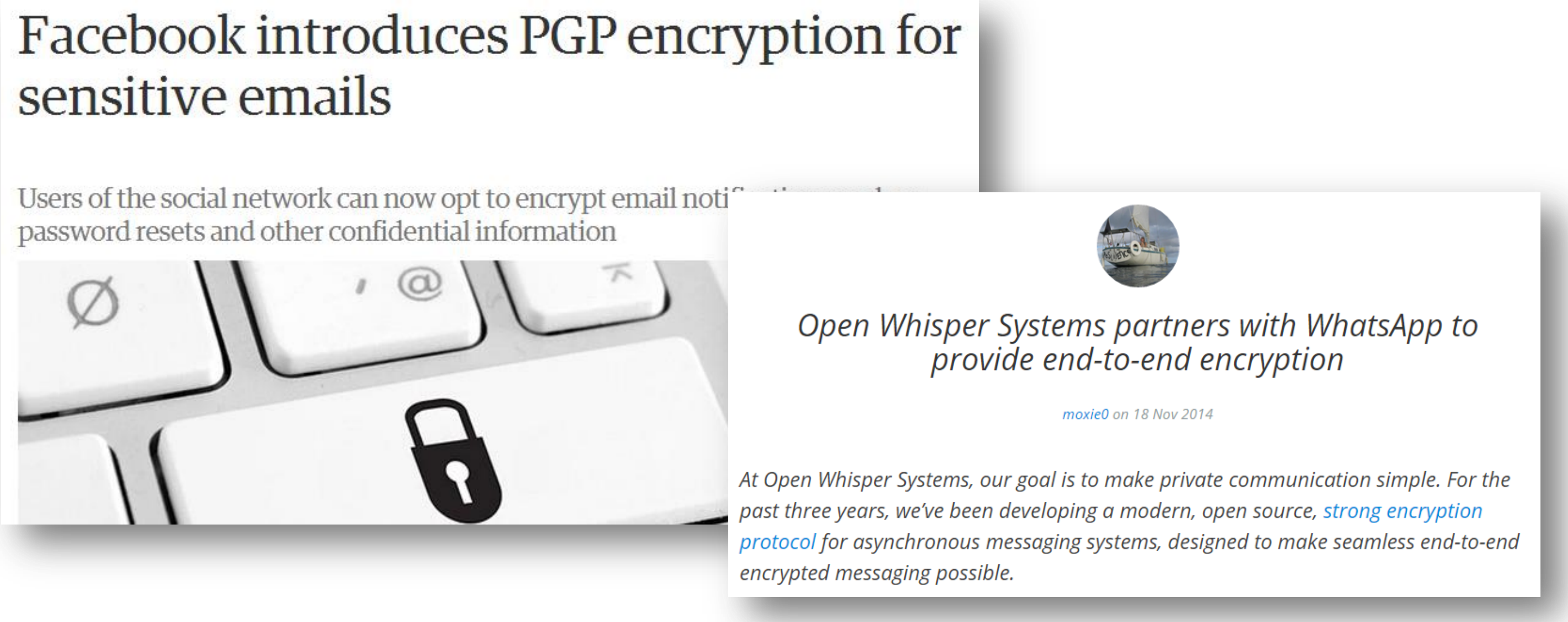
Media
Send as many high quality photos as you want

World Wide
Cyber Dust is available World Wide

EXPECT... MORE GROUP/SOCIAL INTEGRATION

Social network services will use stronger messaging

Secure group communications is a challenge



Facebook introduces PGP encryption for sensitive emails

Users of the social network can now opt to encrypt email noti
password resets and other confidential information

Open Whisper Systems partners with WhatsApp to provide end-to-end encryption

moxie0 on 18 Nov 2014

At Open Whisper Systems, our goal is to make private communication simple. For the past three years, we've been developing a modern, open source, strong encryption protocol for asynchronous messaging systems, designed to make seamless end-to-end encrypted messaging possible.

EXPECT... VULNERABILITIES AND ATTACKS

On the **software, infrastructure, users**

“Bug bounty” initiatives helping bugs discovery

Increasing cost of breaking into mobile platforms...

Conclusions

ON THE TECHNICAL SIDE

We know **the theoretical recipe** of secure systems

But...

- DoS/fallback attacks are effective
- Operational security is also important
- Metadata can leak critical information
- Secure app on a compromised system is insecure

Secure coms solutions are just a **part of a system**

ON THE BUSINESS SIDE

Plenty of vendors, affordable/free mobile solutions...

But...

- Technically state-of-the-art solutions not mature as products
- Unclear security of corporate-friendly, commercial systems
- Non-interoperability limits adoption and effectiveness
- You may want/need hardware-based security

The right solution depends on your assets, threats, platform(s), size, etc.

Buy **actual security**, not a feeling of security

KUDELSKI SECURITY

THANK YOU !

www.kudelskisecurity.com
cyber security unit of Kudelski Group