Post-Snowden Communication

An Analysis of Secure Mobile Messengers

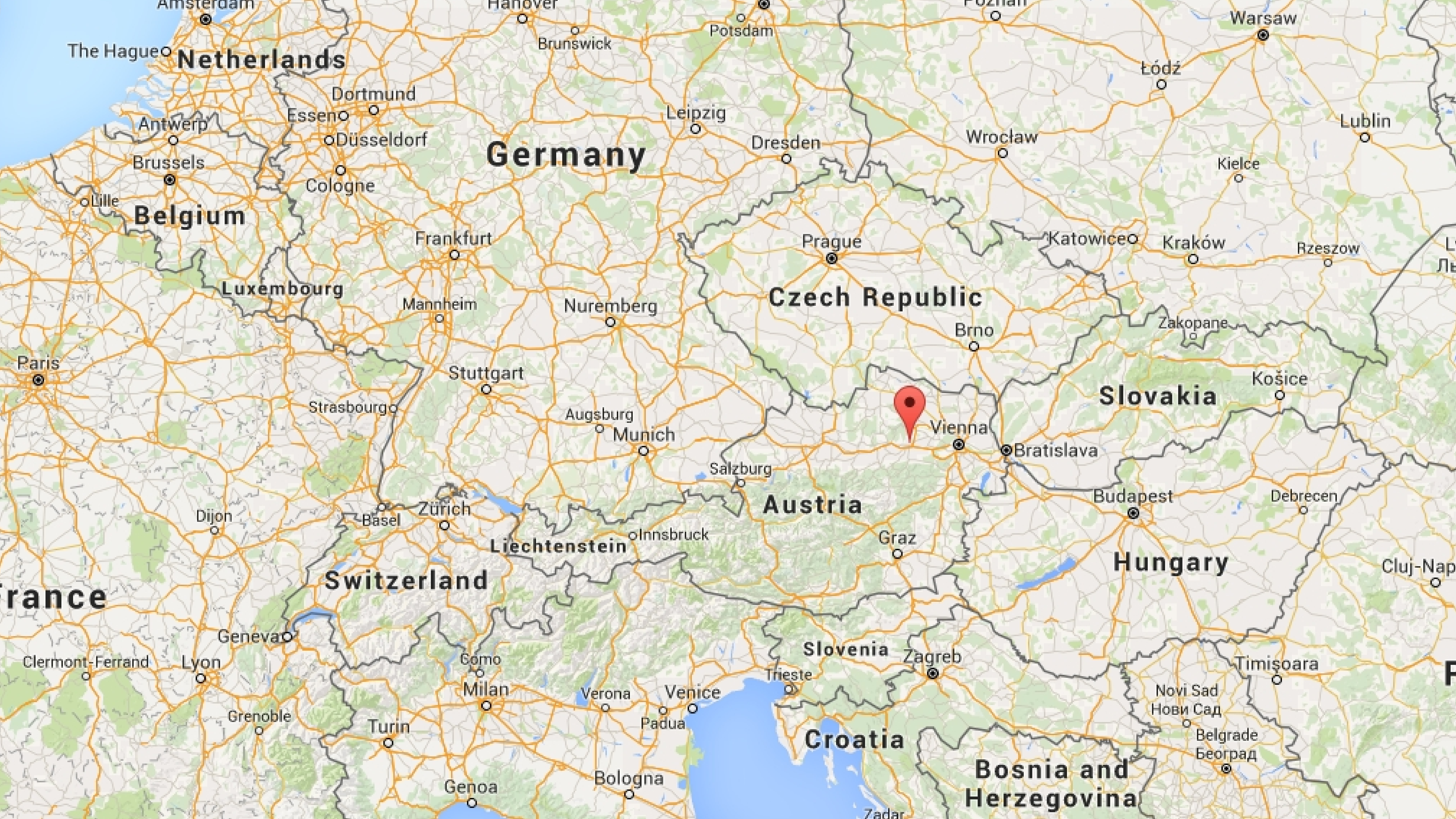
Securi-Tay V

26th February 2016

@slashcrypto @Ra5pS3c

\$whoami^2

- David Wind & Christoph Rottermanner
- Bachelor degree in IT Security at the University of Applied Sciences St. Pölten
- Currently Master in Information Security
- Working for XSEC in Vienna (mainly doing Pentesting)


Amsterdam
Hanover
Potsdam
Poznań
Warsaw
The Hague
Netherlands
Brunswick
Łódź
Dortmund
Essen
Antwerp
Düsseldorf
Leipzig
Lublin
Germany
Dresden
Wrocław
Brussels
Kielce
Cologne
Lille
Belgium
Frankfurt
Prague
Katowice
Kraków
Rzeszow
Luxembourg
Czech Republic
Mannheim
Nuremberg
Zakopane
Brno
Paris
Stuttgart
Košice
Slovakia
Strasbourg
Augsburg
Vienna
Munich
Bratislava
Salzburg
Austria
Budapest
Debrecen
Zürich
Basel
Dijon
Innsbruck
Liechtenstein
Graz
Hungary
Cluj-Nap
Switzerland
France
Geneva
Slovenia
Zagreb
Clermont-Ferrand
Lyon
Como
Trieste
Timișoara
Milan
Verona
Venice
Novi Sad
Нови Сад
Padua
Grenoble
Turin
Croatia
Belgrade
Београд
Bosnia and
Herzegovina
Genoa
Bologna
Zadar

University of Applied Sciences St. Pölten

- 2560 Students
- IT Security Bachelor (3 years)
  - Forensics
  - Networking
  - Management
- Information Security Master (2 years)
- More info: https://www.fhstp.ac.at/en

Secure Messengers

- WhatsApp
- iMessage
- Telegram
- Signal
- Line

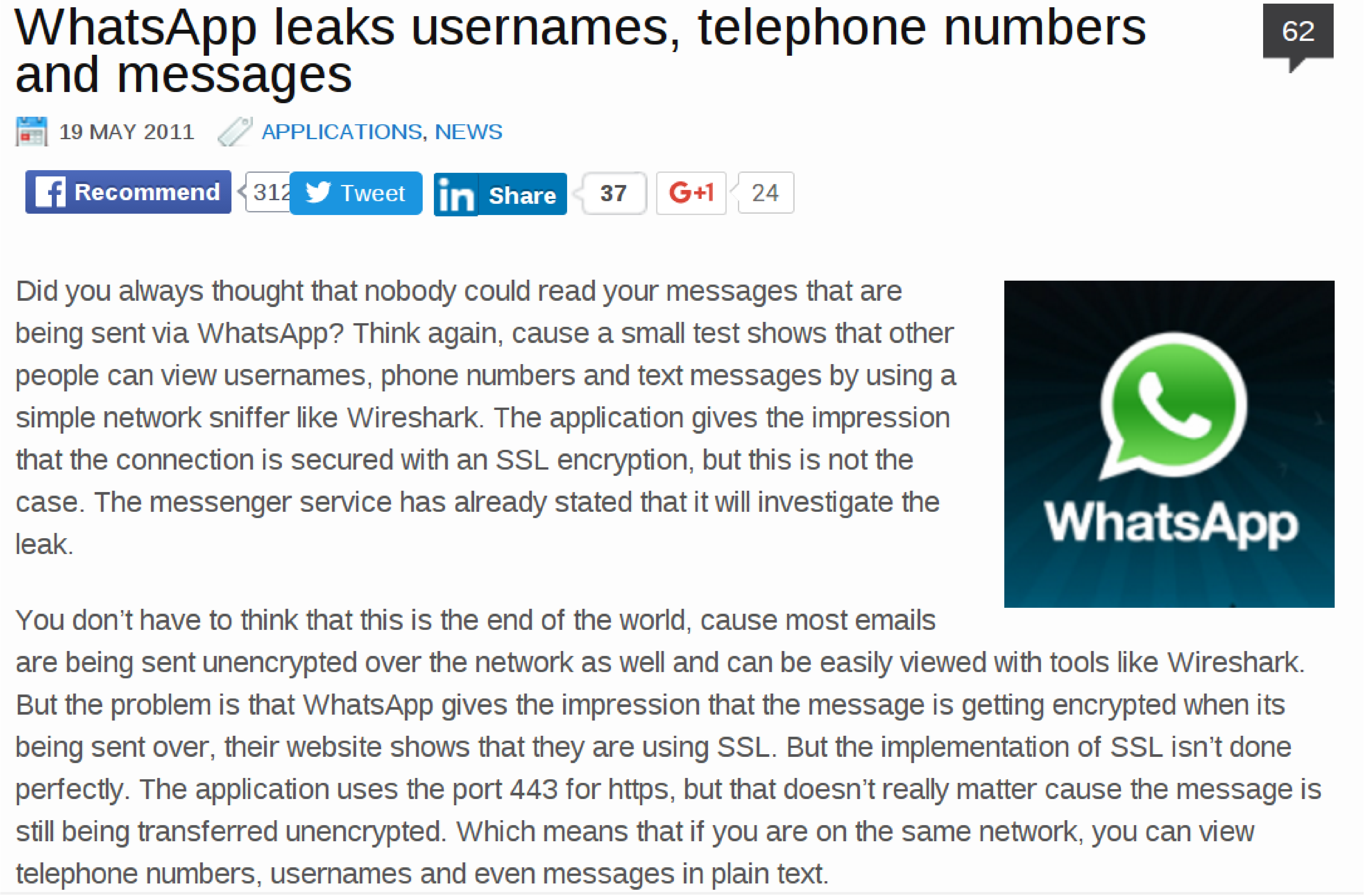
What "Secure" means to us

- Possibility to create end-to-end encrypted conversations ?
- Strong Crypto in use ?
- Possibility to verify each other ?
- Secure storage ?
- Privacy ?

What we were looking at

1) General & Crypto
2) End-to-end encryption & MITM
3) Account Hijacking
4) Privacy
5) Insecure Transmission & Storage

History



WhatsApp leaks usernames, telephone numbers and messages

19 MAY 2011 APPLICATIONS, NEWS

Did you always thought that nobody could read your messages that are being sent via WhatsApp? Think again, cause a small test shows that other people can view usernames, phone numbers and text messages by using a simple network sniffer like Wireshark. The application gives the impression that the connection is secured with an SSL encryption, but this is not the case. The messenger service has already stated that it will investigate the leak.

You don't have to think that this is the end of the world, cause most emails are being sent unencrypted over the network as well and can be easily viewed with tools like Wireshark. But the problem is that WhatsApp gives the impression that the message is getting encrypted when its being sent over, their website shows that they are using SSL. But the implementation of SSL isn't done perfectly. The application uses the port 443 for https, but that doesn't really matter cause the message is still being transferred unencrypted. Which means that if you are on the same network, you can view telephone numbers, usernames and even messages in plain text.

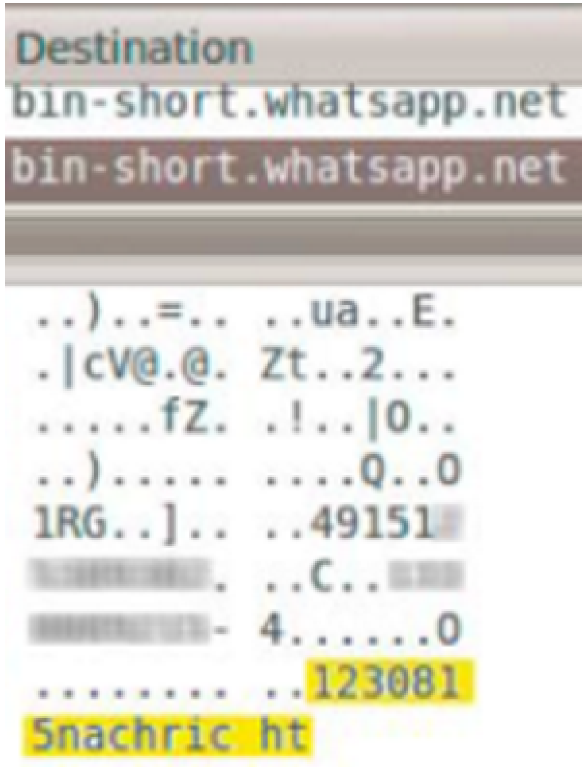
http://www.yourdailymac.net/2011/05/whatsapp-leaks-usernames-telephone-numbers-and-messages/

24 August 2012, 16:21

« previous | next »

WhatsApp no longer sends plain text

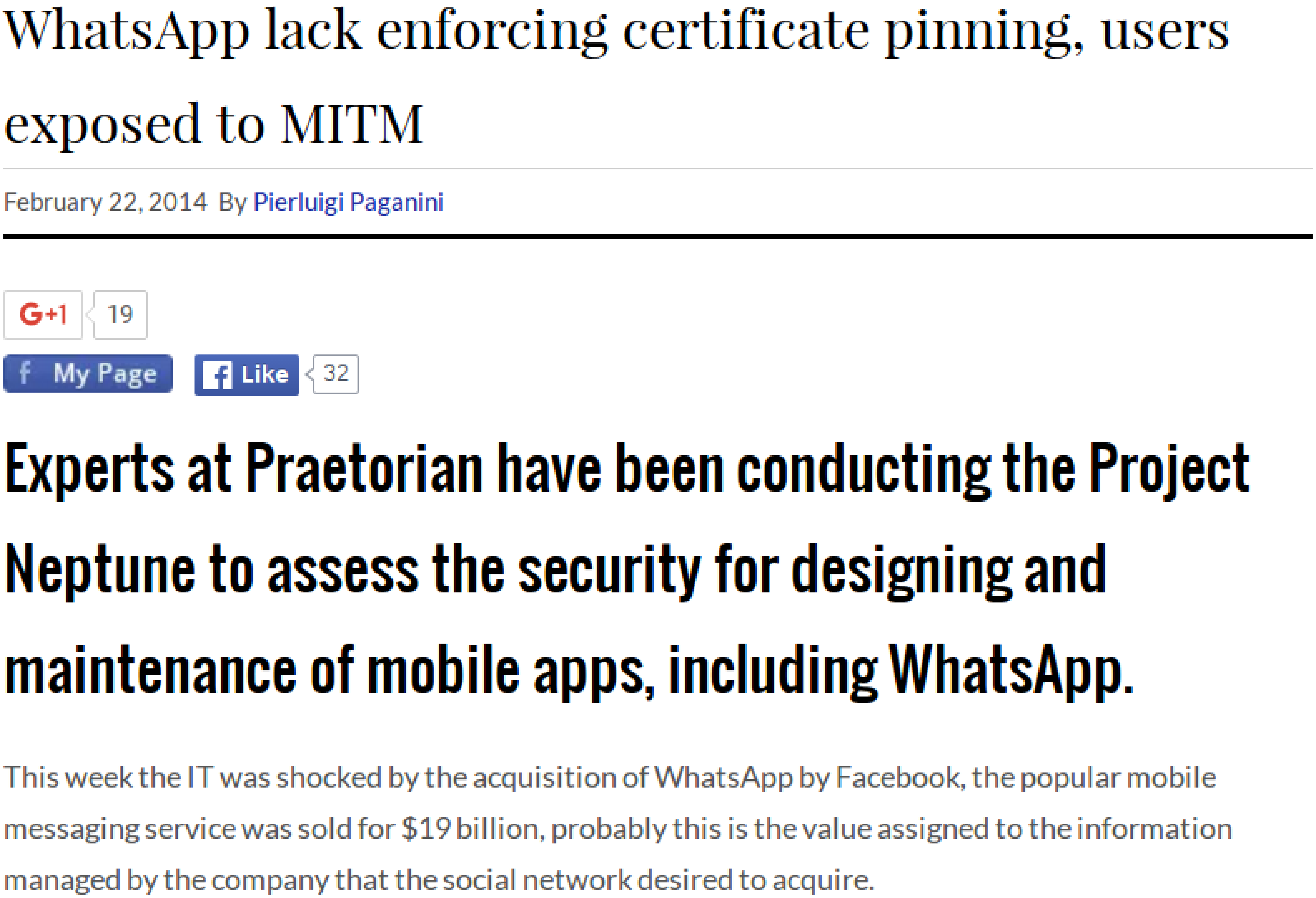
Popular messaging service WhatsApp no longer sends its users' messages in plain text. WhatsApp, which supports all major smartphone platforms, has established itself as an SMS replacement for many users over the past few years. An FAQ entry from the company behind the application states that the latest version of the WhatsApp client now uses encryption.



```
Destination
bin-short.whatsapp.net
bin-short.whatsapp.net
```

```
..)..=..  ..ua..E.
.|cV@.@.  Zt..2...
.....fZ.  .!..|O..
..)......  ....Q..O
1RG..]..  ..49151[redacted]
[redacted].  ..C..[redacted]
[redacted]-  4......O
........  ..123081
Snachric ht
```

It is unclear how long the service has been encrypting messages and which algorithms it uses, and **The H**'s associates at heise Security have yet to receive a response to their request for more information. The change logs of the Android and iOS apps don't mention the introduction of an encryption function.



WhatsApp lack enforcing certificate pinning, users exposed to MITM

February 22, 2014 By Pierluigi Paganini

Experts at Praetorian have been conducting the Project Neptune to assess the security for designing and maintenance of mobile apps, including WhatsApp.

This week the IT was shocked by the acquisition of WhatsApp by Facebook, the popular mobile messaging service was sold for $19 billion, probably this is the value assigned to the information managed by the company that the social network desired to acquire.

http://securityaffairs.co/wordpress/22449/hacking/whatsapp-lack-certificate-pinning.html

History … The End

1) **General & Crypto**

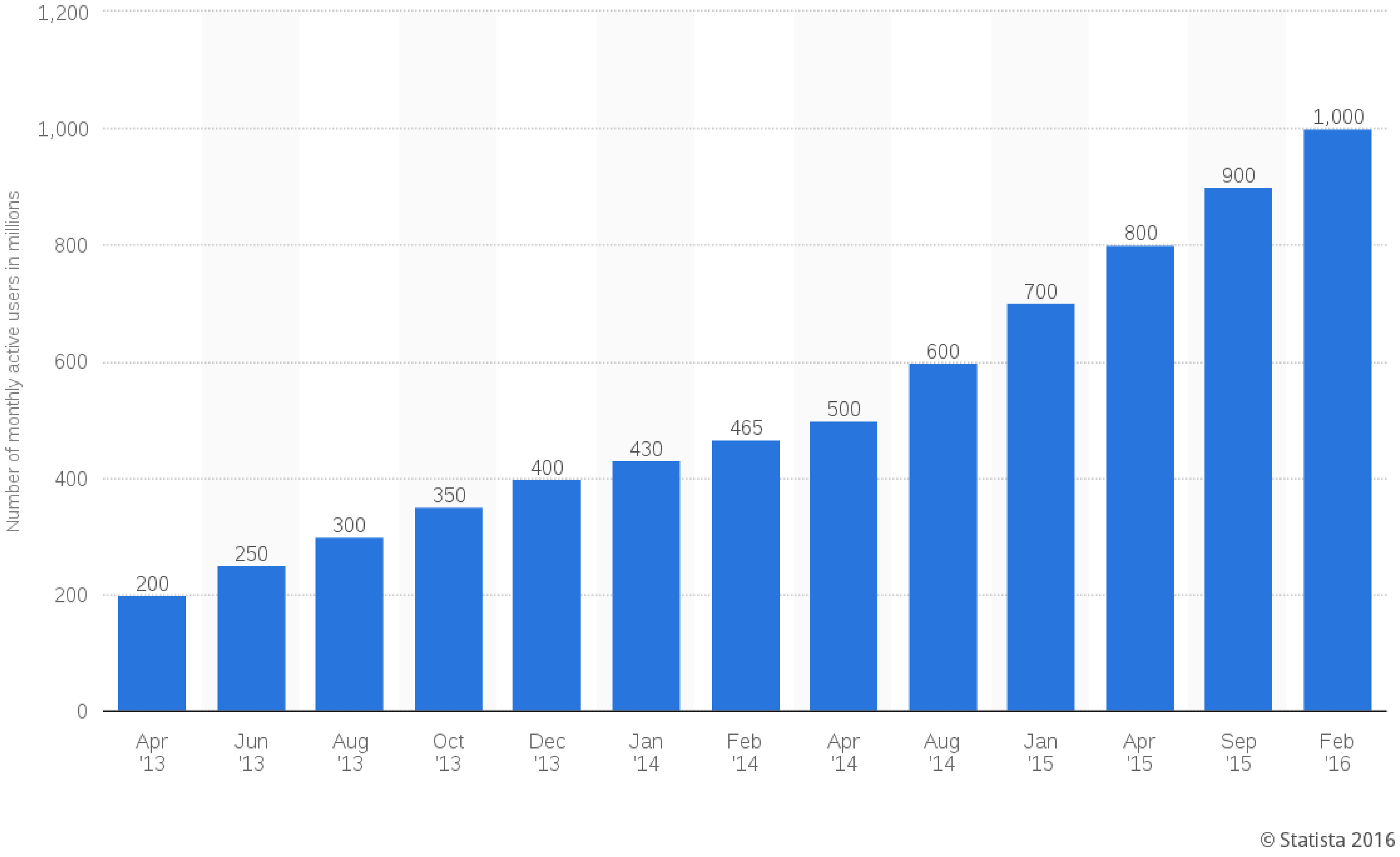
2) End-to-end encryption & MITM

3) Account Hijacking

4) Privacy

5) Insecure Transmission & Storage

WhatsApp General



http://www.statista.com/statistics/260819/number-of-monthly-active-whatsapp-users/

WhatsApp Crypto

- Partnered with Open Whisper Systems (2014)
- Same as Signal (**??**) - Closed source
- "Security Indicators" in Beta version

iMessage General

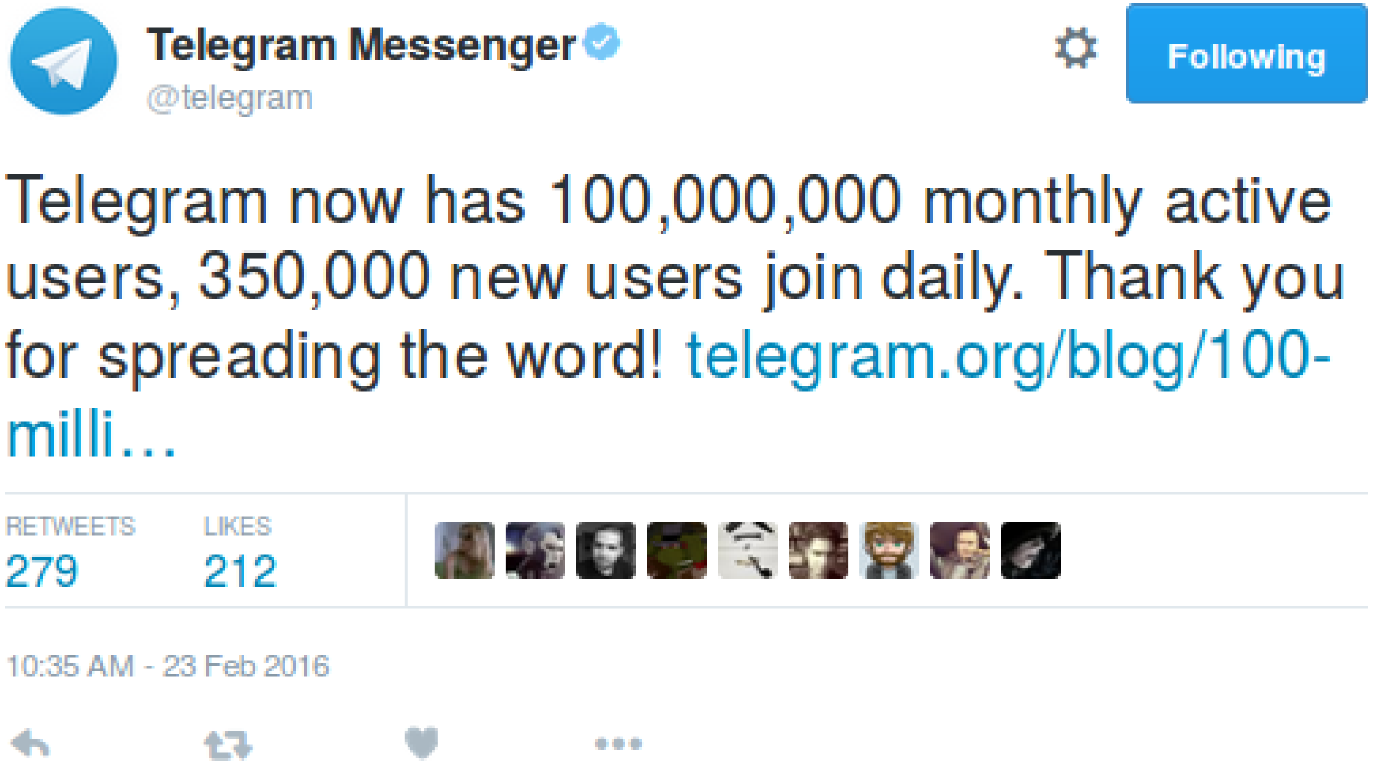
- End-to-end encryption by default (even group chats)
- Default iPhone messaging application
- ~ 200.000 iMessages sent per second

iMessage Crypto

- RSA 1280-bit key (encryption)
- ECDSA 256-bit key on NIST P-256 curve (signing)
- AES128 in CTR mode
- SHA-1 for hashing (**!!**)
- No PFS

https://www.apple.com/business/docs/iOS_Security_Guide.pdf

Telegram General



Telegram Messenger

@telegram

Following

Telegram now has 100,000,000 monthly active users, 350,000 new users join daily. Thank you for spreading the word! telegram.org/blog/100-milli…

RETWEETS 279

LIKES 212

10:35 AM - 23 Feb 2016

https://twitter.com/telegram/status/702064118350659584

Telegram Crypto

- Some "homemade" Crypto
- RSA 2048-bit key (encryption)
- AES 256 in IGE mode (**no integrity protection!!**)
- Plain SHA-1 for "signing" (pseudoMAC-Then-Encrypt)
- **Homemade** KDF for IV & AES key

http://unhandledexpression.com/2013/12/17/telegram-stand-back-we-know-maths/

Signal General

- End-to-end encryption by default (even group chats)
- Open source
- ~ 1 million downloads via Google Play

Signal Crypto

- ECDH with Curve25519
- HMAC with SHA256
- AES256 in CTR and CBC mode

Line General

- Since Oct. 2015 end-to-end encrypted single chat per default
- ~ 215 million active users in 2015
  - mainly in Japan
- Encrypted group chat in development

Line Crypto

- ECDH-256
- AES256 in CBC mode
- No PFS (??) → not documented
- Bad documentation

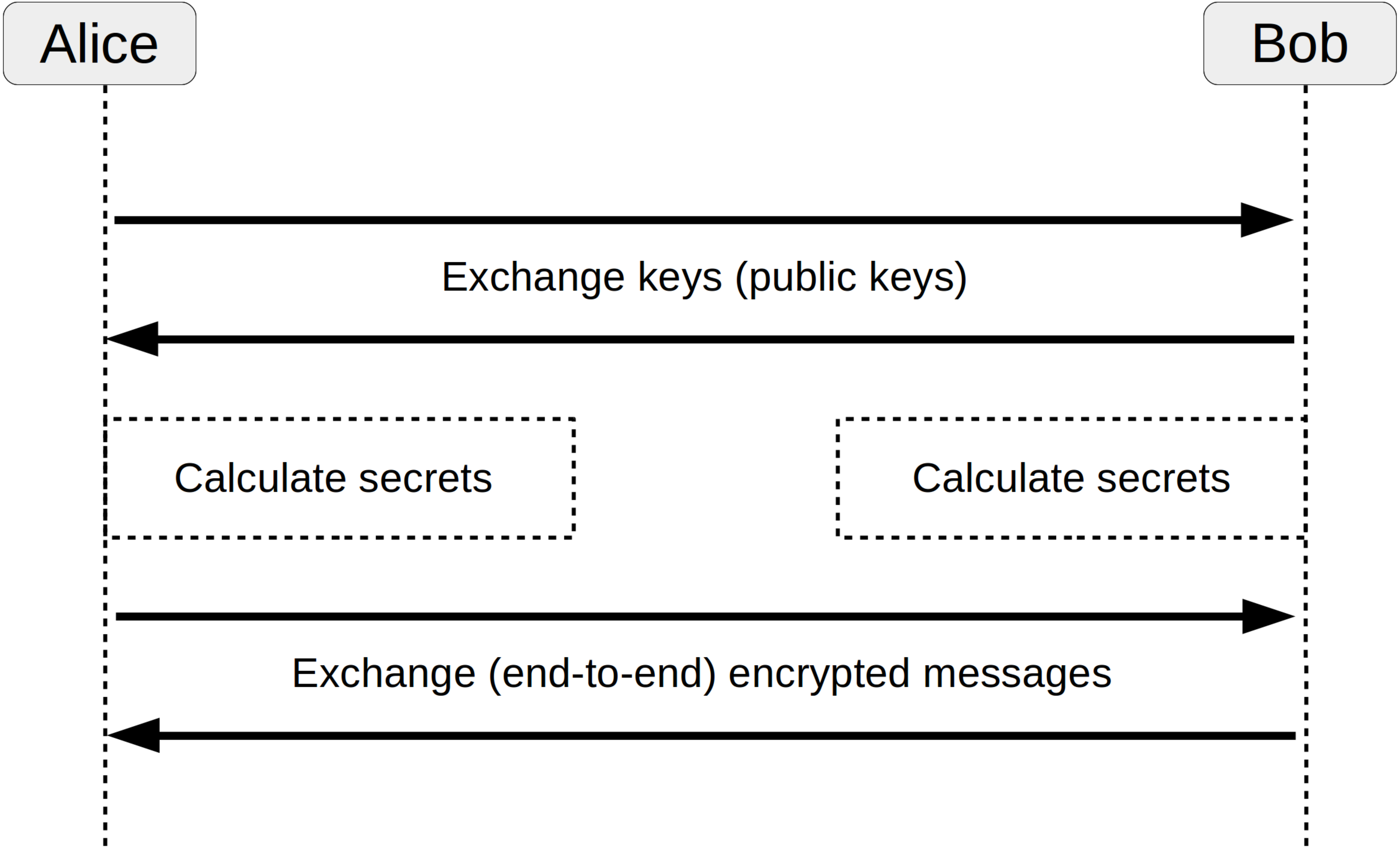
1) General & Crypto

2) End-to-end encryption & MITM

3) Account Hijacking

4) Privacy

5) Insecure Transmission & Storage



Alice

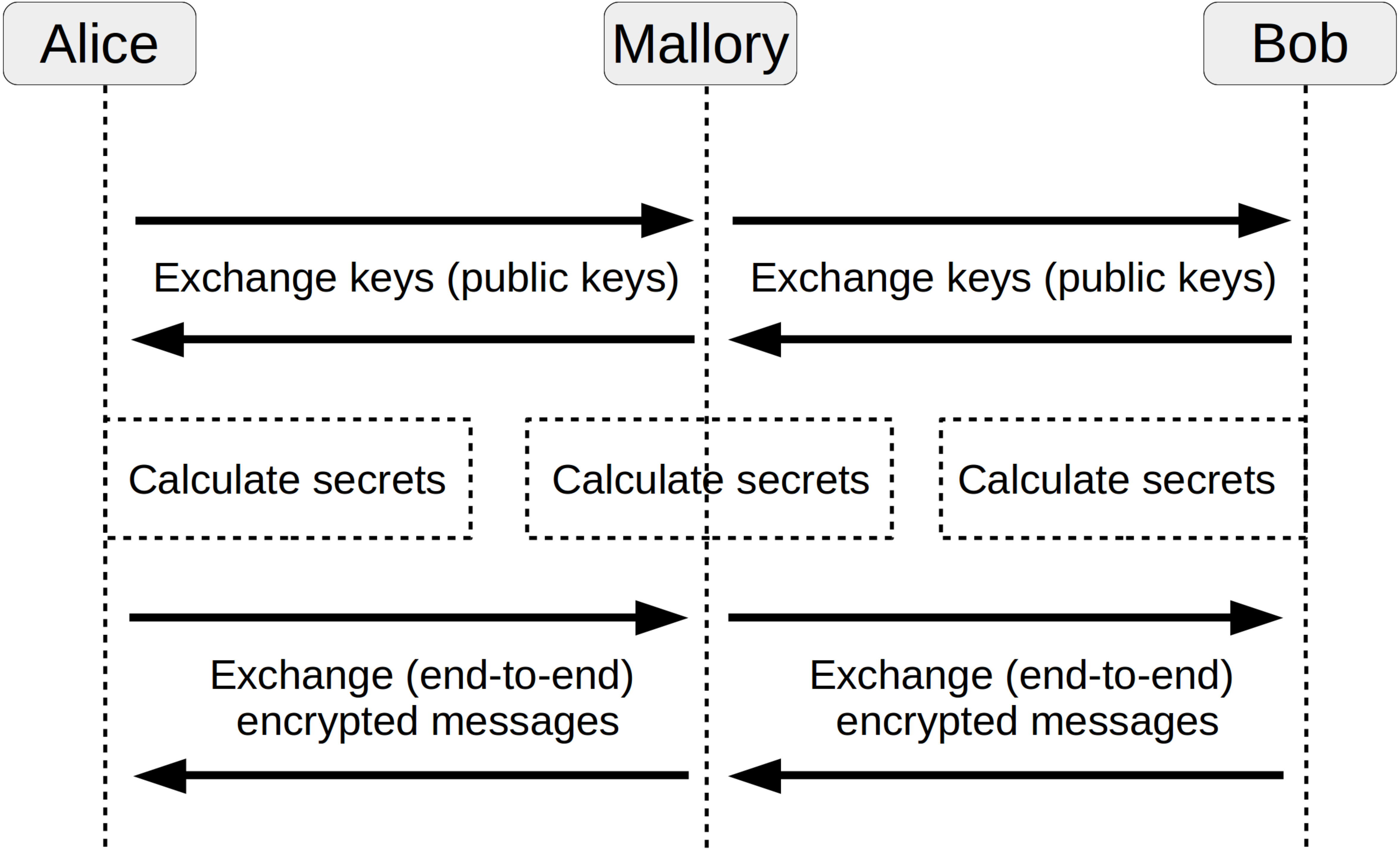
Bob

Exchange keys (public keys)

Calculate secrets

Calculate secrets

Exchange (end-to-end) encrypted messages



Alice

Mallory

Bob

Exchange keys (public keys)

Exchange keys (public keys)

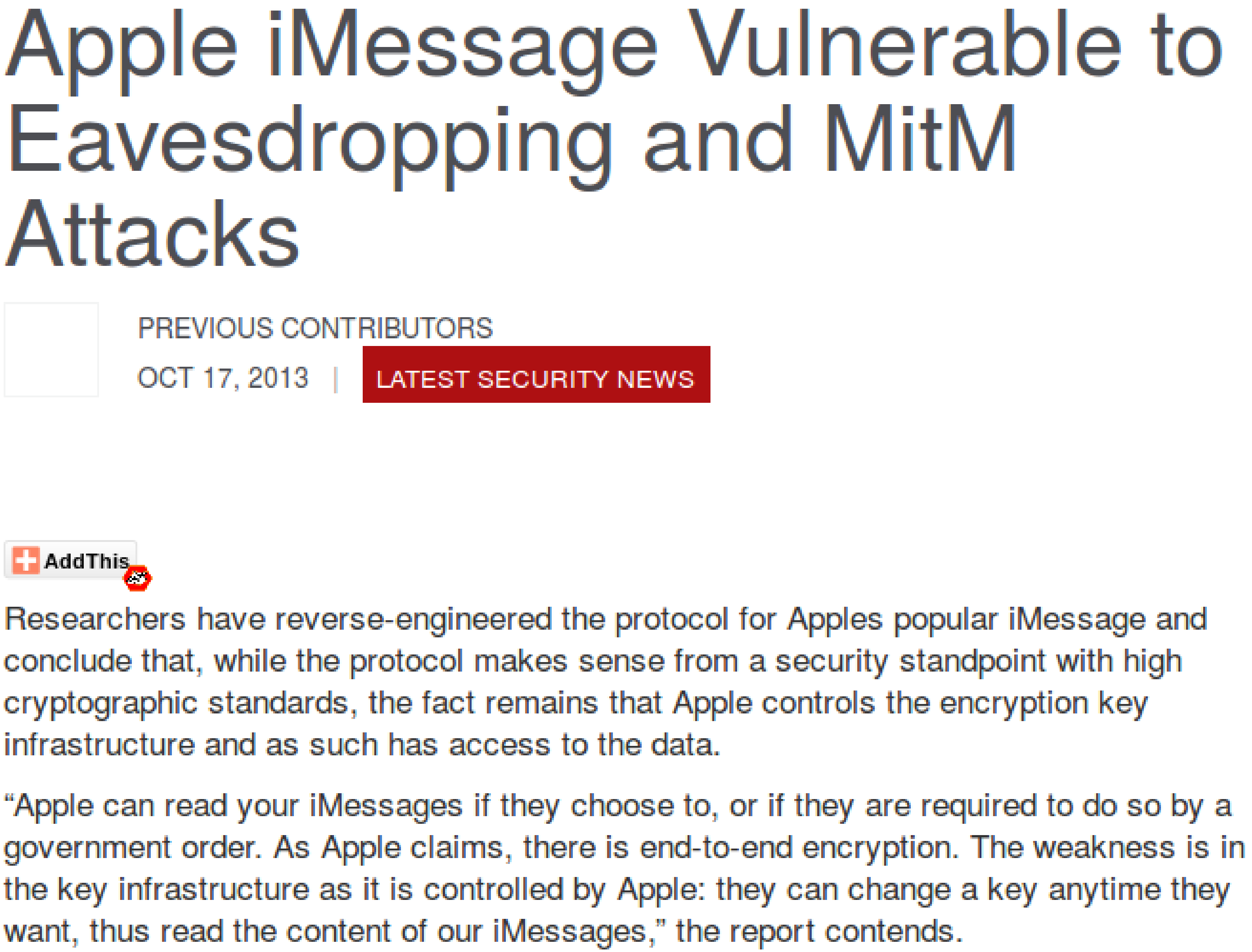
Calculate secrets

Calculate secrets

Calculate secrets

Exchange (end-to-end) encrypted messages

Exchange (end-to-end) encrypted messages



Apple iMessage Vulnerable to Eavesdropping and MitM Attacks

PREVIOUS CONTRIBUTORS

OCT 17, 2013 | LATEST SECURITY NEWS

Researchers have reverse-engineered the protocol for Apples popular iMessage and conclude that, while the protocol makes sense from a security standpoint with high cryptographic standards, the fact remains that Apple controls the encryption key infrastructure and as such has access to the data.

“Apple can read your iMessages if they choose to, or if they are required to do so by a government order. As Apple claims, there is end-to-end encryption. The weakness is in the key infrastructure as it is controlled by Apple: they can change a key anytime they want, thus read the content of our iMessages,” the report contends.

http://www.tripwire.com/state-of-security/latest-security-news/apple-imessage-vulnerable-eavesdropping-mitm-attacks/

"Apple has no way to decrypt iMessage and FaceTime data when it’s in transit between devices."

[..]

"... we wouldn’t be able to comply with a wiretap order even if we wanted to."

https://www.apple.com/privacy/approach-to-privacy/

WhatsApp, iMessage & Line

- No way to verify, if the correct key was exchanged
    - The key infrastructure is controlled by the provider
- Closed-source software
    - Even if there would be a way to verify each other, who says that the software does not return "true" all the time?

Verify your contacts !!

(compare public key hashes via a secure channel)

1) General & Crypto

2) End-to-end encryption & MITM

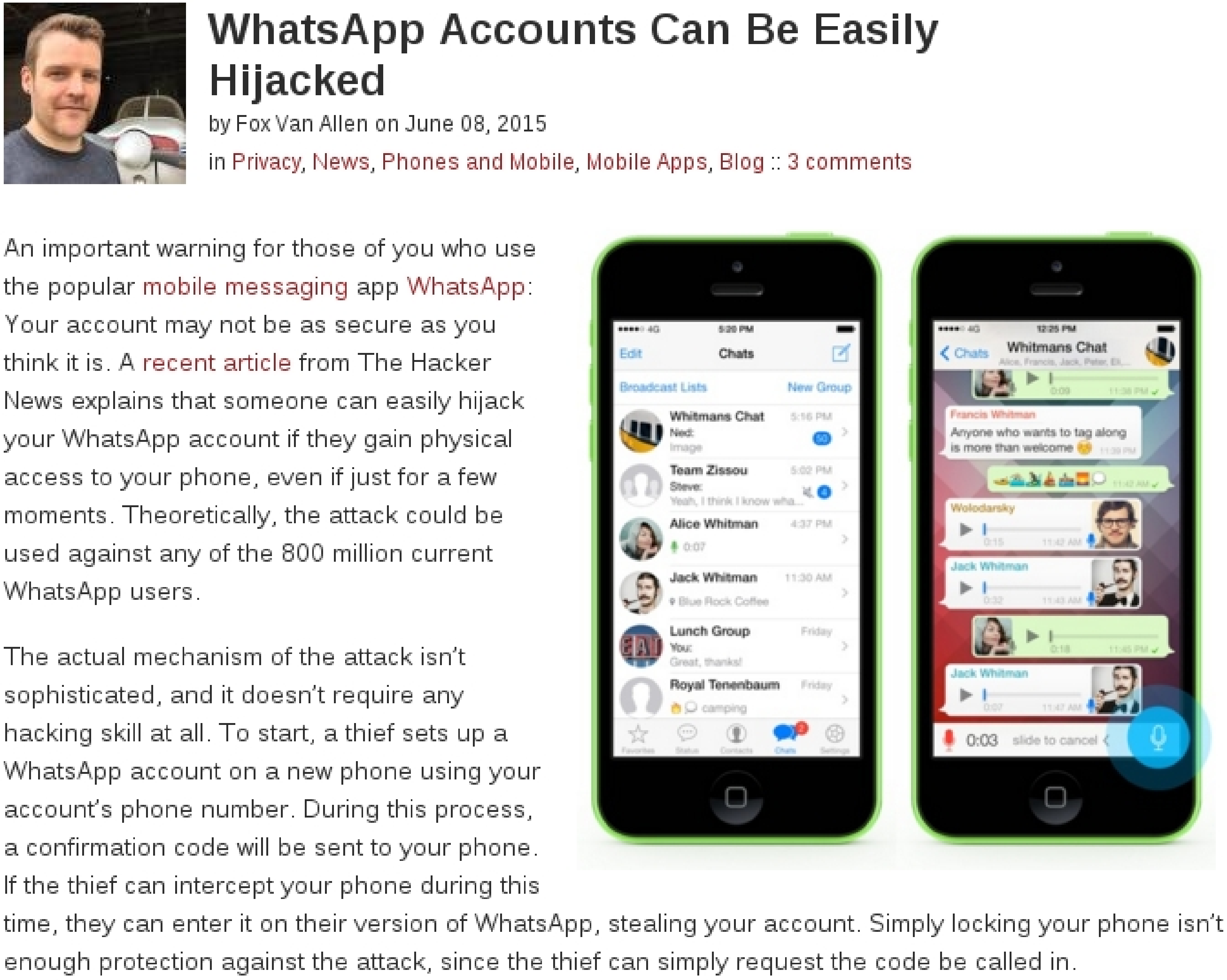
3) Account Hijacking

4) Privacy

5) Insecure Transmission & Storage

Account Hijacking

- Authentication via SMS or phone call
    - WhatsApp, Telegram, Signal, ...
- Intercept SMS or phone call
    - IMSI Catcher, SS7 vulnerability



WhatsApp Accounts Can Be Easily Hijacked

by Fox Van Allen on June 08, 2015

in Privacy, News, Phones and Mobile, Mobile Apps, Blog :: 3 comments

An important warning for those of you who use the popular mobile messaging app WhatsApp: Your account may not be as secure as you think it is. A recent article from The Hacker News explains that someone can easily hijack your WhatsApp account if they gain physical access to your phone, even if just for a few moments. Theoretically, the attack could be used against any of the 800 million current WhatsApp users.

The actual mechanism of the attack isn't sophisticated, and it doesn't require any hacking skill at all. To start, a thief sets up a WhatsApp account on a new phone using your account's phone number. During this process, a confirmation code will be sent to your phone. If the thief can intercept your phone during this time, they can enter it on their version of WhatsApp, stealing your account. Simply locking your phone isn't enough protection against the attack, since the thief can simply request the code be called in.

http://www.techlicious.com/blog/whatsapp-account-hijackings-authentication-code-hack/

Account Hijacking

- Indicators for hijacked account
  - Telegram → notification, new device linked
  - Signal → new messages fail
  - WhatsApp → old device unlinked
- Impact of Account Hijacking
  - WhatsApp → group chats
  - Telegram …

Account Hijacking

"We store messages, photos, videos and documents from your cloud chats on our servers, so that you can access your data from any of your devices anytime and use our instant server search to quickly access your messages from waaay back. "

https://telegram.org/privacy

https://www.fredericjacobs.com/blog/2016/01/14/sms-login/

Account Hijacking

- Mitigation
    - Password for Telegram
    - No mitigation for other messengers like WhatsApp and Signal

1) General & Crypto

2) End-to-end encryption & MITM

3) Account Hijacking

4) Privacy

5) Insecure Transmission & Storage

Privacy

- Signal hashes contacts

```
https://54.172.208.191/v1/directory/tokens
{
        "contacts": [
                "hr/5JNlZd7AgnQ",
                "lLkSRf60EHM8tA",
                "BprFLzDEJZnJyw",
                "+k6SXgmv1mCQJw",
                "Lroio4/R1J6H9g",
                ...
}
```

Privacy

- Private Information Retrieval (PIR)
  - Send database of all registered users to client
  - Bloom filters
  - Encrypted bloom filters
  - Shared bloom filters

https://whispersystems.org/blog/contact-discovery/

Bloom Filter

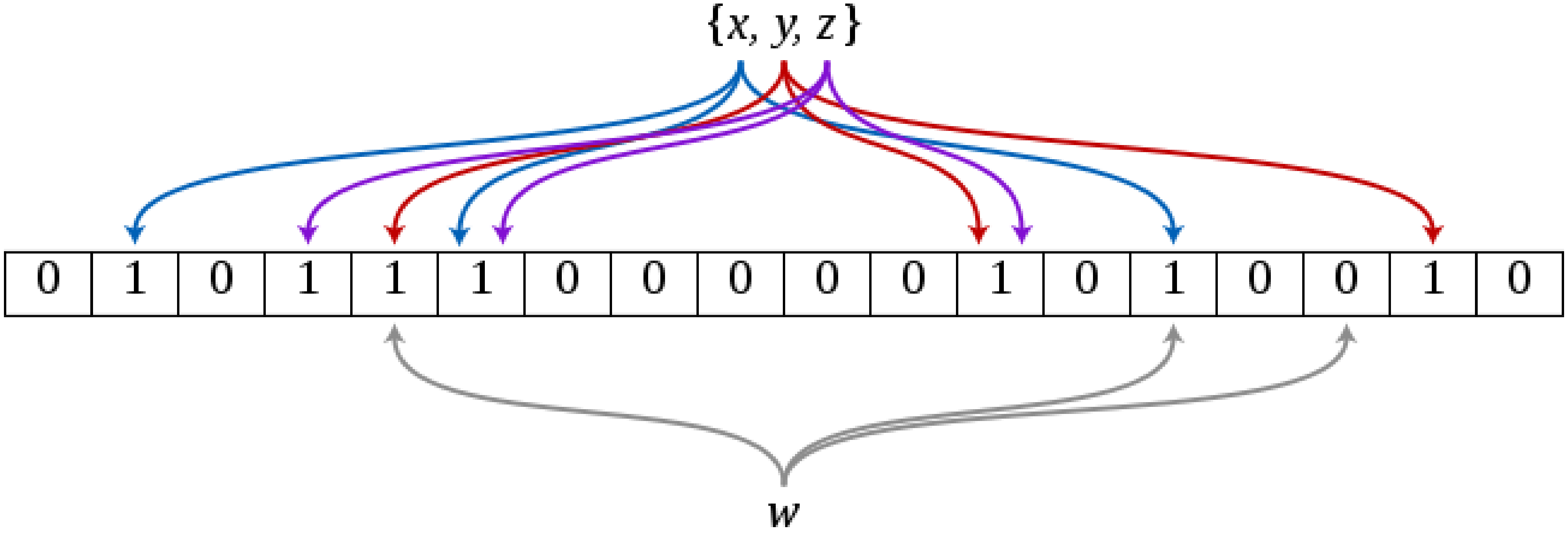
- Test if element is member of a set
- False positives possible, no false negatives
- More elements → higher probability of false positives

Bloom Filter

- Start with empty bloom filter → bit array of m bits, all set to zero
- k different hashing functions → k positions in the array
- Adjusting hashing functions → reduces false positives

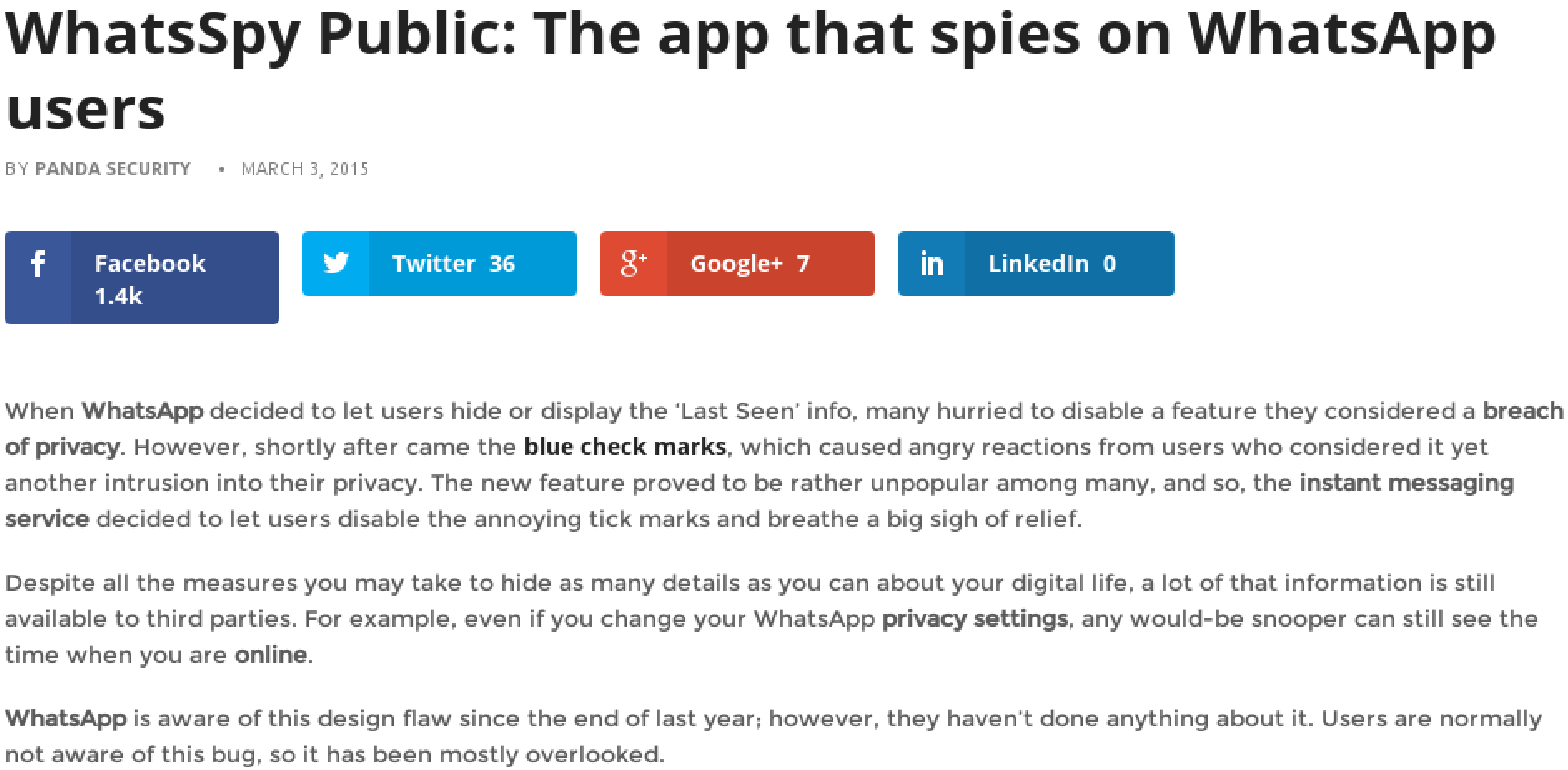
Bloom Filter

m = 18, k = 3



0	1	0	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0

https://en.wikipedia.org/wiki/Bloom_filter#/media/File:Bloom_filter.svg



WhatsSpy Public: The app that spies on WhatsApp users

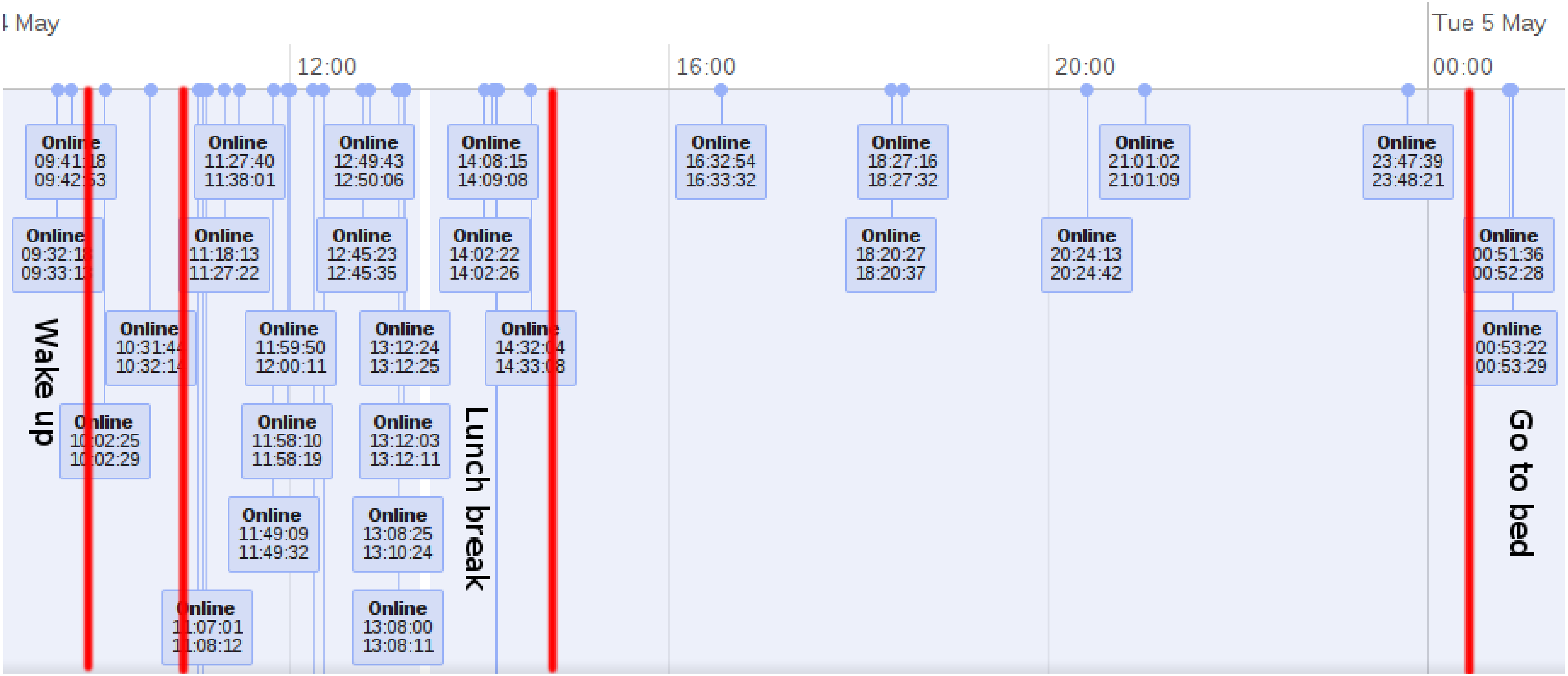
BY **PANDA SECURITY** • MARCH 3, 2015

When **WhatsApp** decided to let users hide or display the 'Last Seen' info, many hurried to disable a feature they considered a **breach of privacy**. However, shortly after came the **blue check marks**, which caused angry reactions from users who considered it yet another intrusion into their privacy. The new feature proved to be rather unpopular among many, and so, the **instant messaging service** decided to let users disable the annoying tick marks and breathe a big sigh of relief.

Despite all the measures you may take to hide as many details as you can about your digital life, a lot of that information is still available to third parties. For example, even if you change your WhatsApp **privacy settings**, any would-be snooper can still see the time when you are **online**.

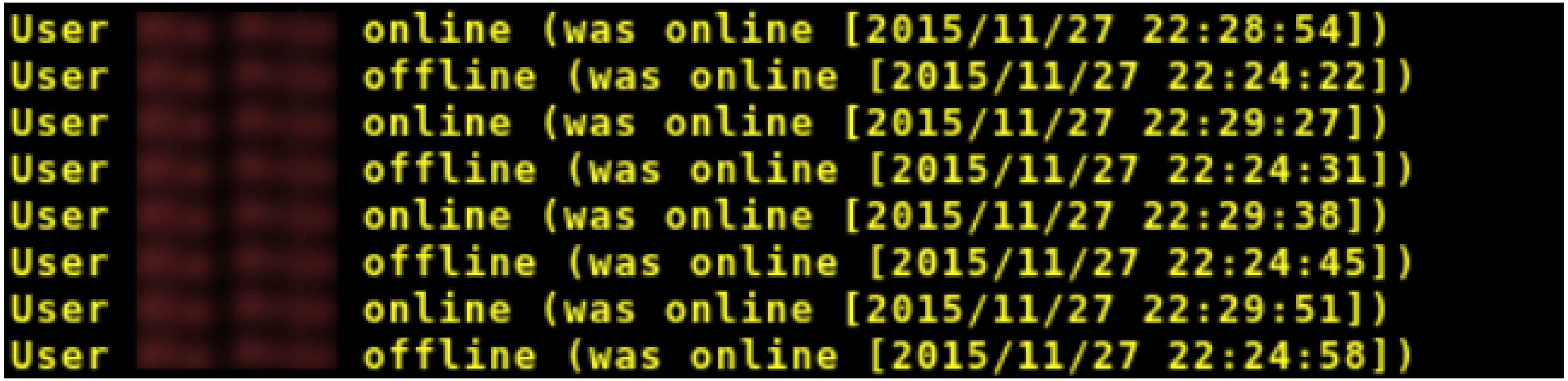
WhatsApp is aware of this design flaw since the end of last year; however, they haven't done anything about it. Users are normally not aware of this bug, so it has been mostly overlooked.

http://www.pandasecurity.com/mediacenter/mobile-security/whatsspy-public-app-spies-whatsapp-users/



https://gitlab.maikel.pro/maikeldus/WhatsSpy-Public/wikis/home

After having read that I was surprised to see the amount of metadata received from my contacts. Most of the metadata is not directly visible in the web and mobile clients, but using a third party client such as vysheng's CLI client any received metadata is displayed:



```
User [redacted] online (was online [2015/11/27 22:28:54])
User [redacted] offline (was online [2015/11/27 22:24:22])
User [redacted] online (was online [2015/11/27 22:29:27])
User [redacted] offline (was online [2015/11/27 22:24:31])
User [redacted] online (was online [2015/11/27 22:29:38])
User [redacted] offline (was online [2015/11/27 22:24:45])
User [redacted] online (was online [2015/11/27 22:29:51])
User [redacted] offline (was online [2015/11/27 22:24:58])
```

The Telegram android app sends a notification to all contacts when it becomes or stops being the "foreground" app on the device. Using that information alone it's at times easy to make guesses about who's talking to who if you have several contacts in common with a "victim". An "attacker" will sometimes see the victim and another contact taking turns going active/inactive as they pass messages back and forth.

https://oflisback.github.io/telegram-stalking/

1) General & Crypto

2) End-to-end encryption & MITM

3) Account Hijacking

4) Privacy

5) Insecure Transmission & Storage

Insecure Storage

- Signal
    - Local database encrypted with master key → encrypted with user-defined password
- Telegram
    - Database not encrypted → only protected by file permissions
    - PIN doesn't affect database encryption

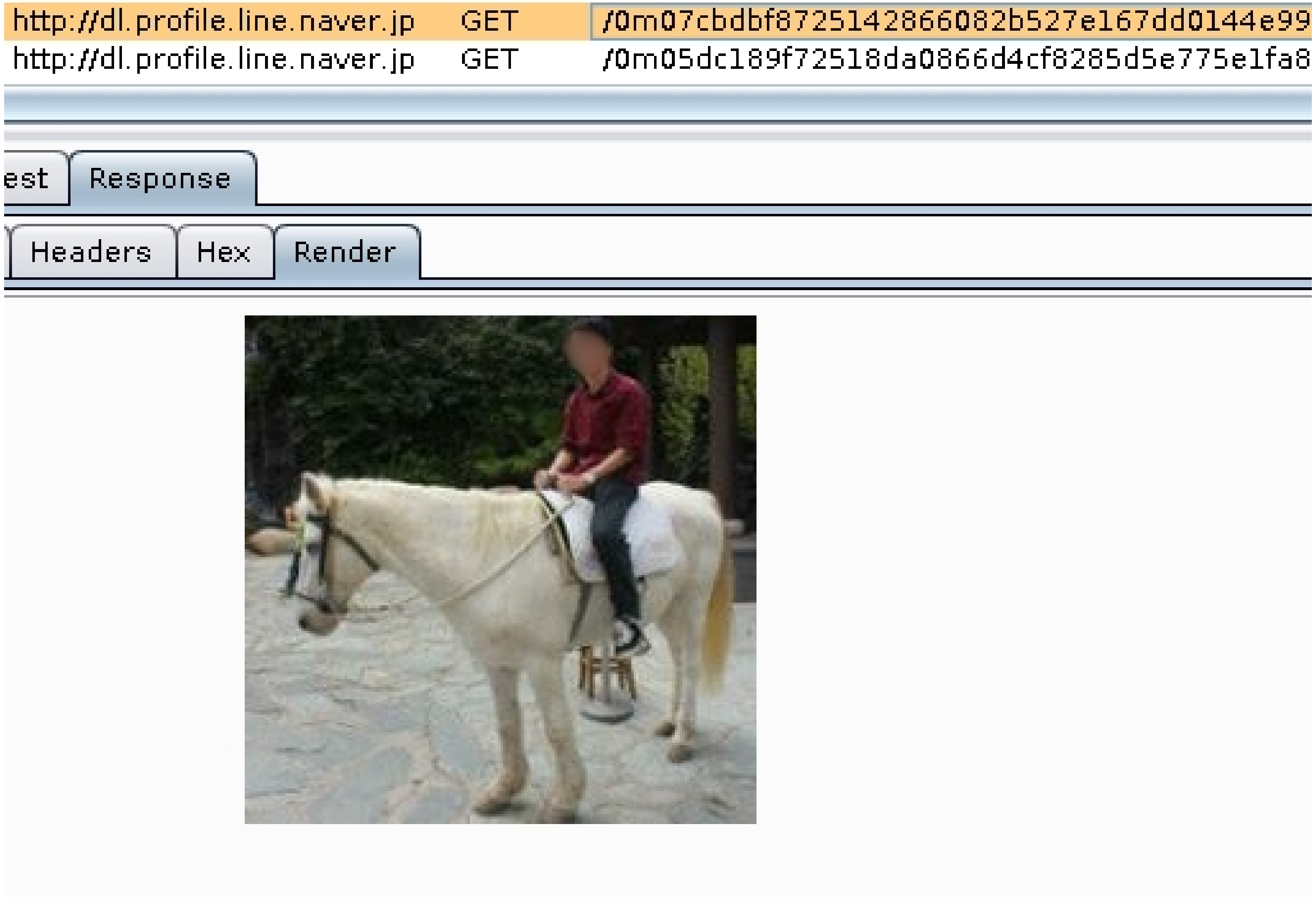
Insecure Storage

- WhatsApp
  - Local database unencrypted → only protected by file permissions
  - Backup encrypted → key and IV on local storage
  - Backup stored on SD card → world readable
- Line
  - Local database unencrypted → only protected by file permissions

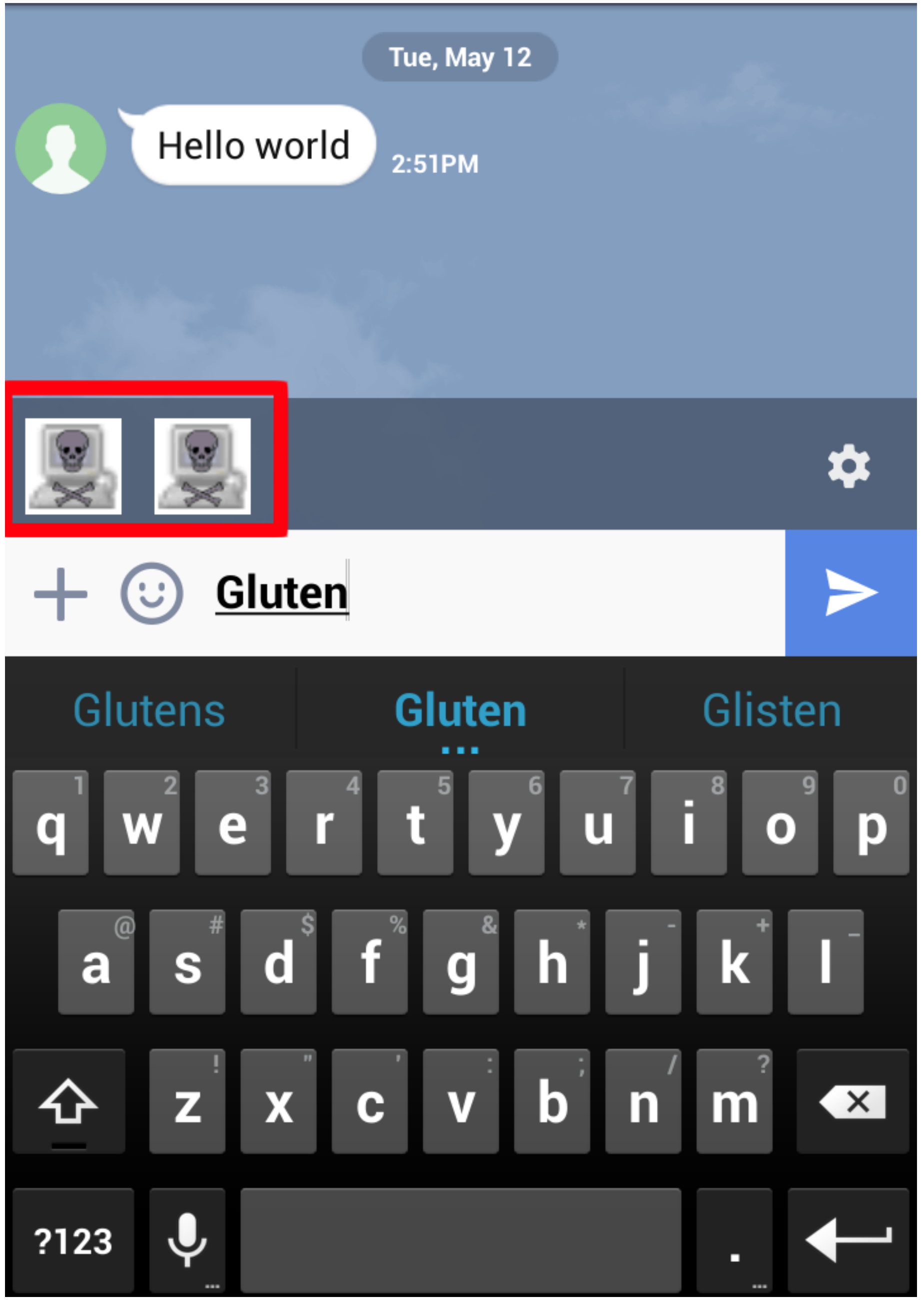
Insecure Storage

- iMessage
  - Modern devices encrypted by default
  - Database encryption → no further research was done

Insecure Transmission



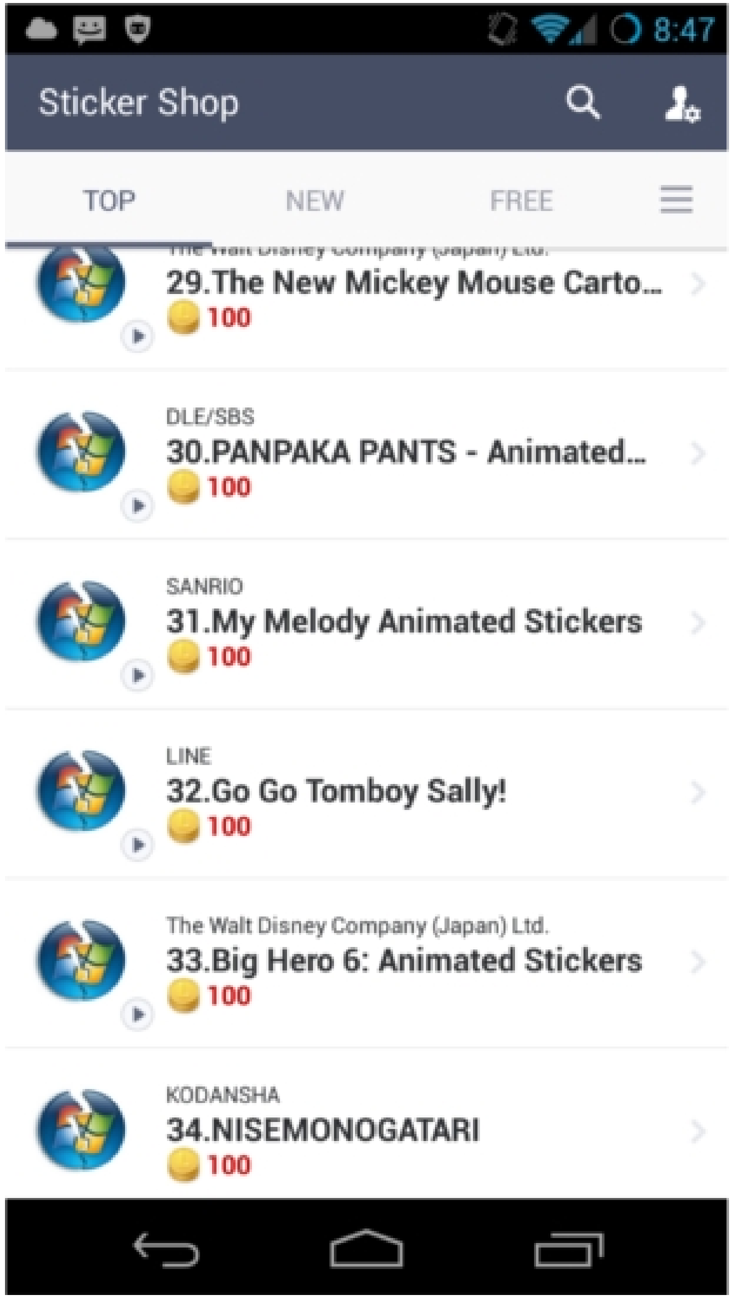
```
http://dl.profile.line.naver.jp    GET    /0m07cbdbf8725142866082b527e167dd0144e99
http://dl.profile.line.naver.jp    GET    /0m05dc189f72518da0866d4cf8285d5e775e1fa8
```



Tue, May 12

Hello world 2:51PM

Gluten



The Walt Disney Company (Japan) Ltd.
29.The New Mickey Mouse Carto...
100

DLE/SBS
30.PANPAKA PANTS - Animated...
100

SANRIO
31.My Melody Animated Stickers
100

LINE
32.Go Go Tomboy Sally!
100

The Walt Disney Company (Japan) Ltd.
33.Big Hero 6: Animated Stickers
100

KODANSHA
34.NISEMONOGATARI
100

Conclusion

- Verify fingerprints
- Don't trust closed source software
- Account hijacking mitigations (Telegram)
- Use state-of-the-art Crypto
- In our opinion, Signal is the best secure messaging application out there!

Q&A

@slashcrypto @Ra5pS3c

http**s**://www.slashcrypto.org for the slides