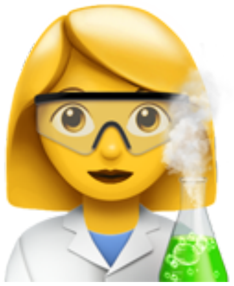
Secure Messaging

36C3. Will Scott

Secure Messaging

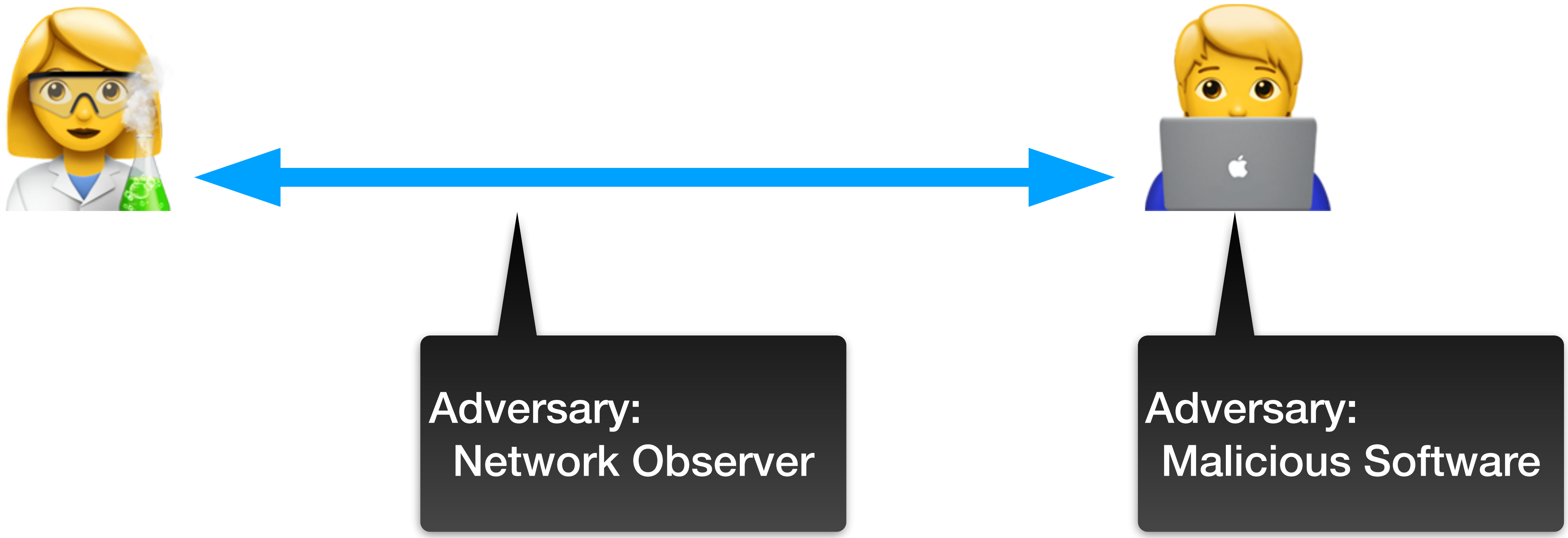
- Identify Adversaries & Threats
- Existing Mechanisms
- Remaining Challenges

ALICE & BOB



TOPOLOGY

Direct



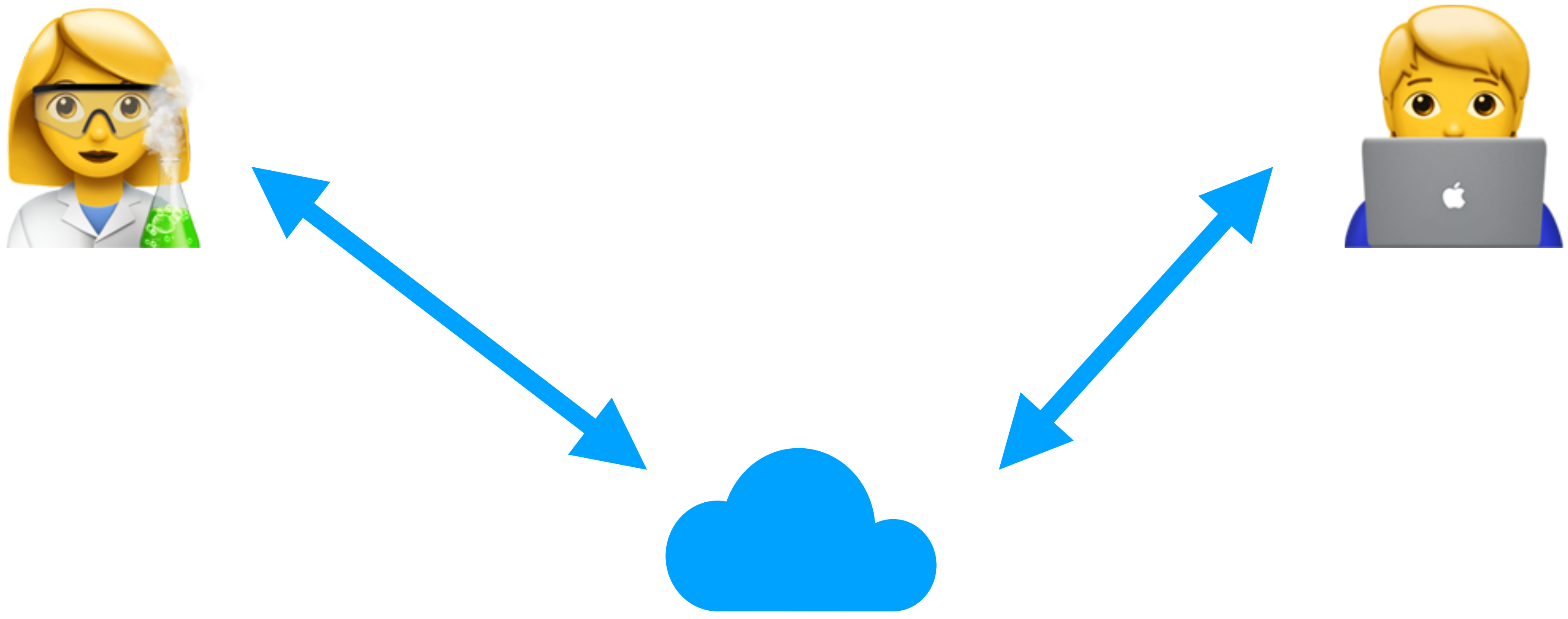
Adversary:
Network Observer

Adversary:
Malicious Software

MECHANISMS

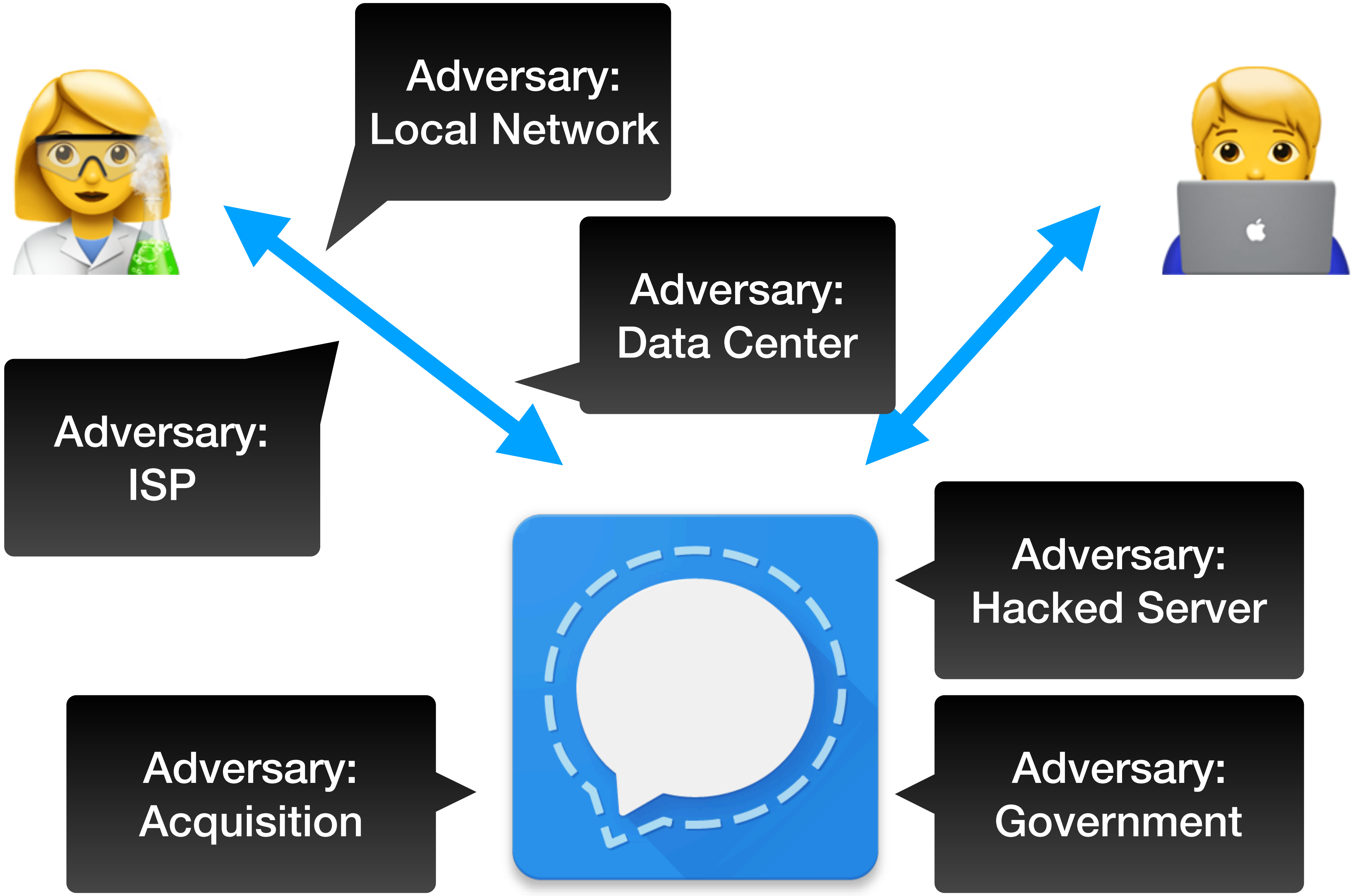
- Encryption
- Message Expiry
- OS Sandboxing / Isolation

Centralized



Facebook, whatsapp, slack, irc, wire, threema, etc.

Centralized



Adversary: Local Network

Adversary: Data Center

Adversary: ISP

Adversary: Hacked Server

Adversary: Acquisition

Adversary: Government

MECHANISMS

- Encryption
- Message Expiry
- OS Sandboxing / Isolation
- Traffic Obfuscation
- Server Hardening

Centralized

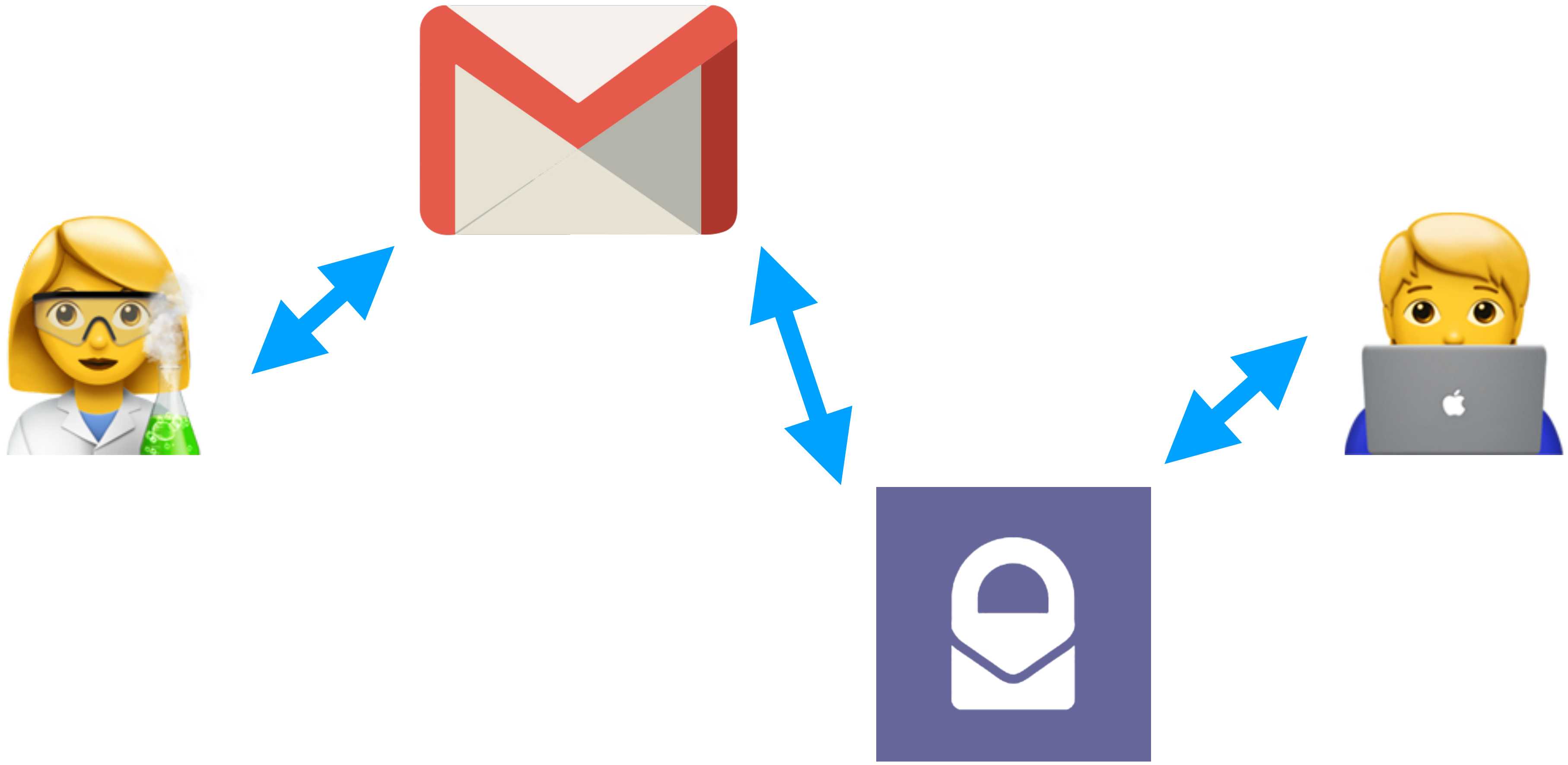
PROS.

- Availability
- Multiple devices, mobile push

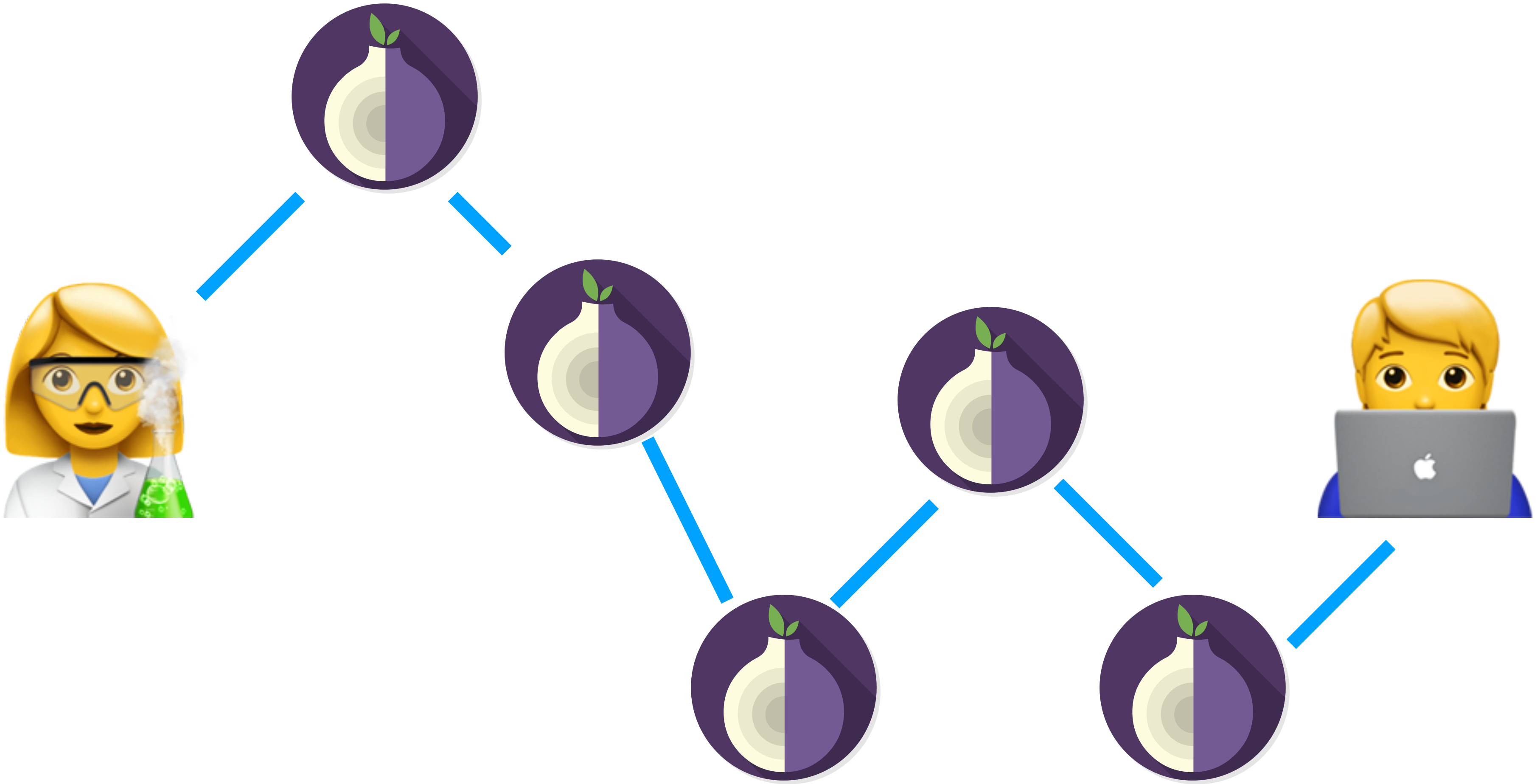
CONS.

- Centralized Costs
- Legal/Regulatory

Federated



'Decentralized'



'Decentralized'

Ricochet.im

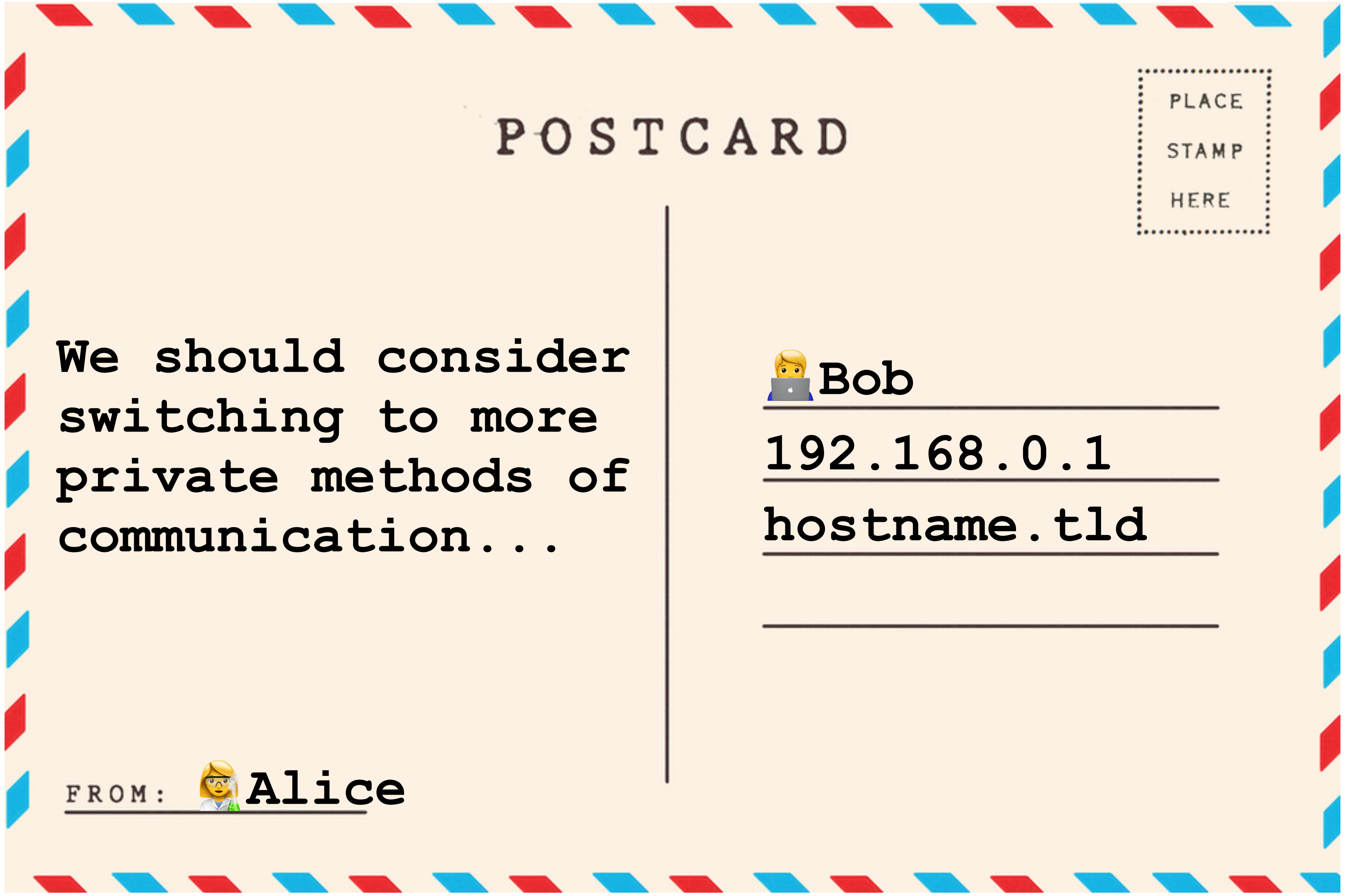
Tox.chat

MECHANISMS

- **Encryption**
- Message Expiry
- OS Sandboxing / Isolation
- Traffic Obfuscation
- Server Hardening

ENCRYPTION

No Encryption

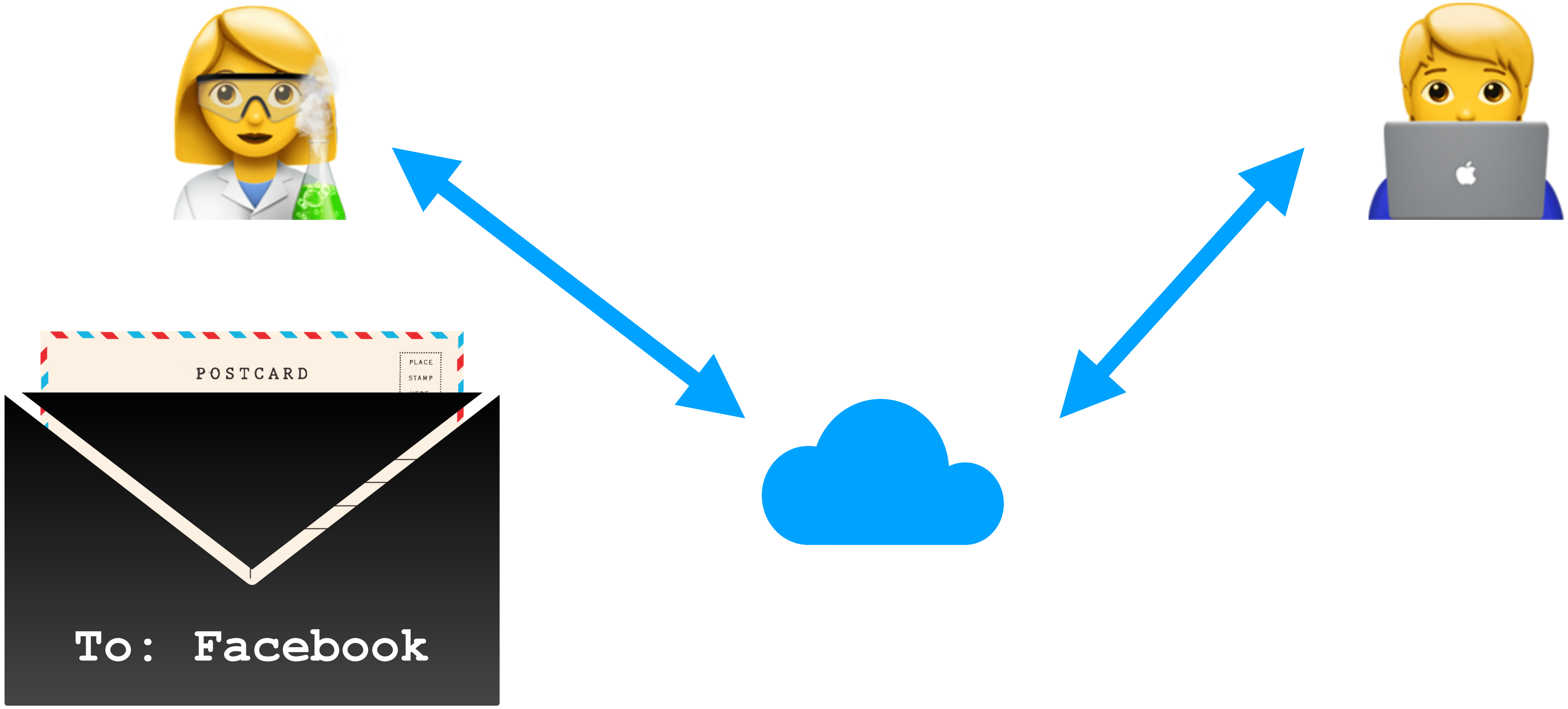


We should consider switching to more private methods of communication...

🧑‍💻Bob
192.168.0.1
hostname.tld

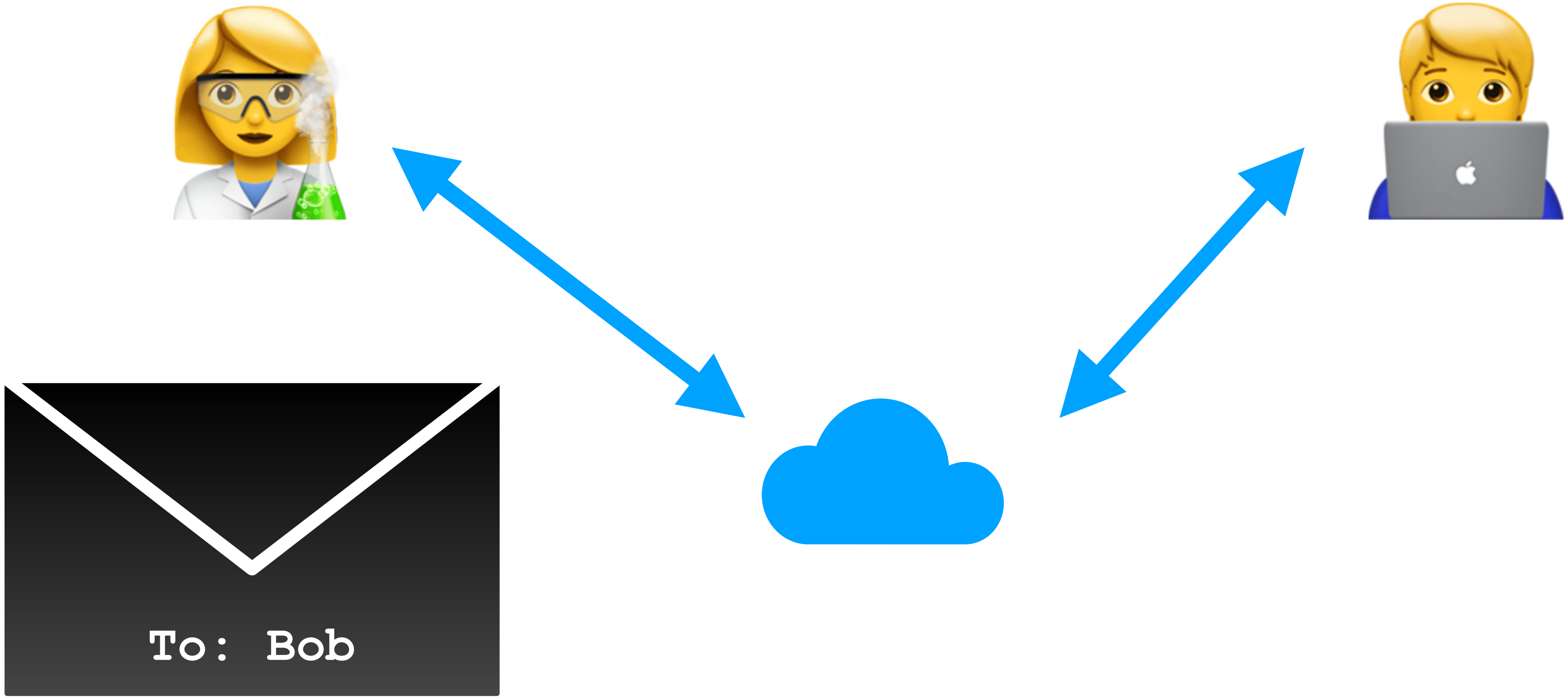
FROM: 👩‍🔬Alice

Transport Encryption



E2E

E2E Encryption



E2E Encryption

Signal Protocol

https://signal.org/docs/

OTR

https://otr.cypherpunks.ca/

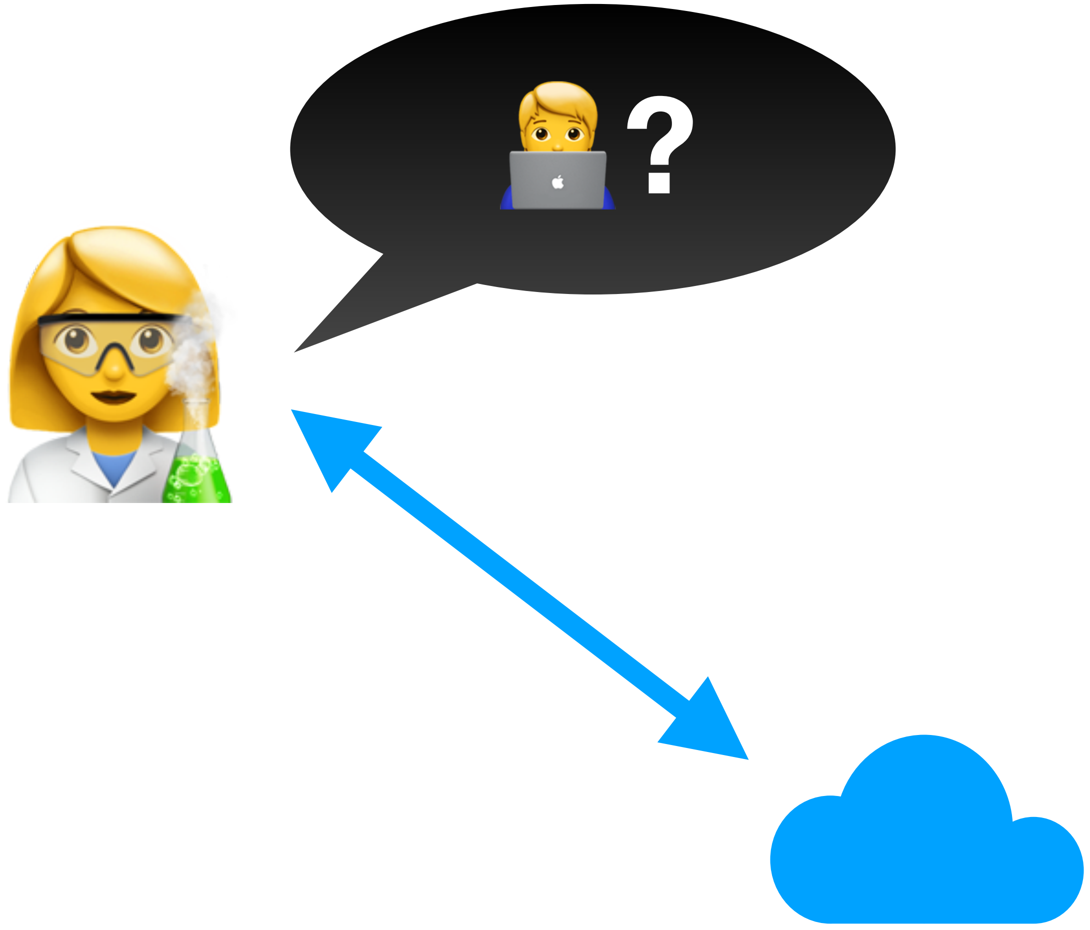
OMEMO

https://conversations.im/omemo/

E2E NEW PROBLEMS

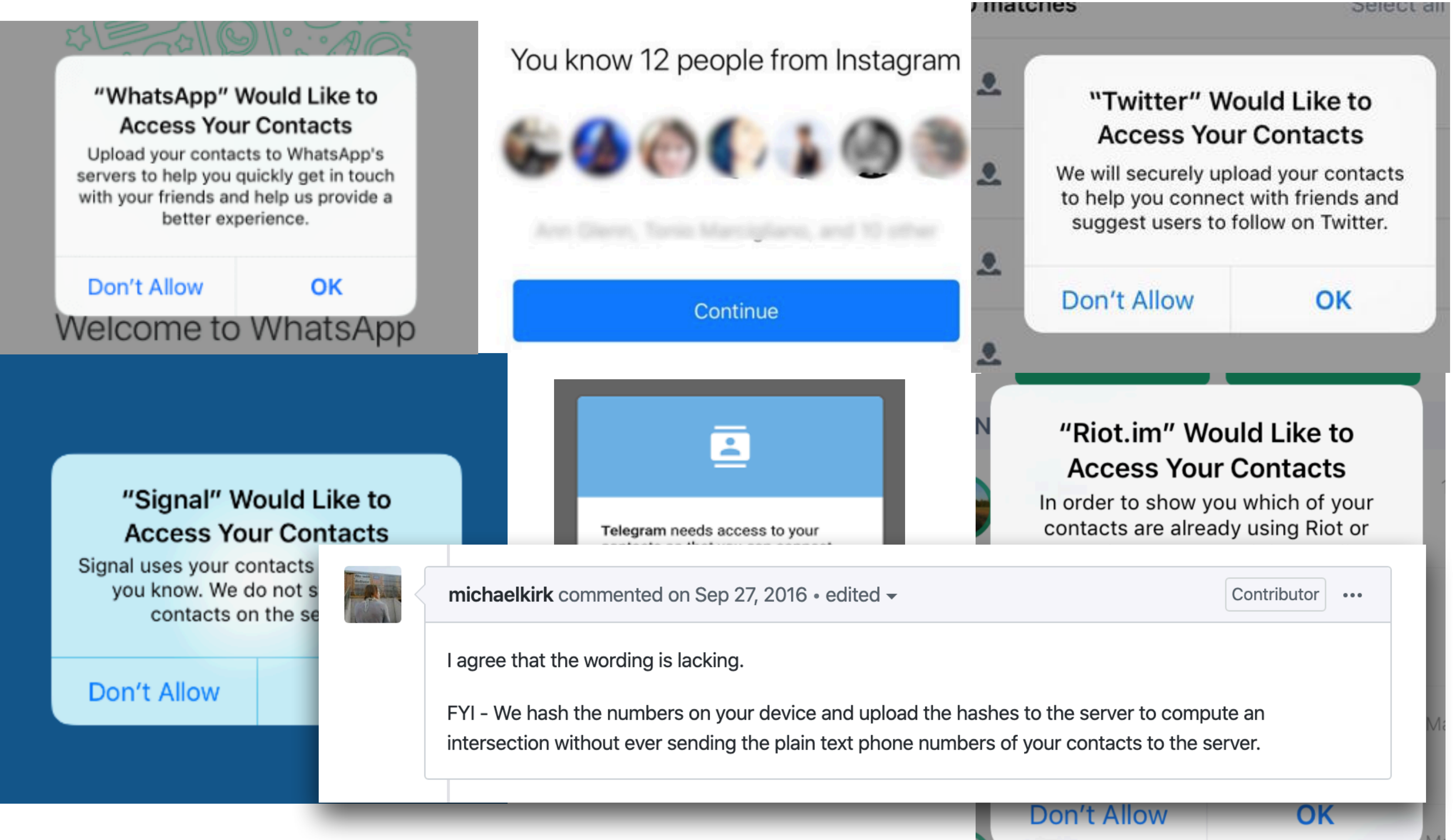
- Connection Establishment
- Deniability

Connecting



Who is bob? who do I trust to map "bob" to an identity?

Connecting



"WhatsApp" Would Like to Access Your Contacts

Upload your contacts to WhatsApp's servers to help you quickly get in touch with your friends and help us provide a better experience.

Don't Allow | OK

Welcome to WhatsApp

You know 12 people from Instagram

Continue

matches | Select all

"Twitter" Would Like to Access Your Contacts

We will securely upload your contacts to help you connect with friends and suggest users to follow on Twitter.

Don't Allow | OK

"Signal" Would Like to Access Your Contacts

Signal uses your contacts you know. We do not s contacts on the se

Don't Allow

Telegram needs access to your

"Riot.im" Would Like to Access Your Contacts

In order to show you which of your contacts are already using Riot or

Don't Allow | OK

michaelkirk commented on Sep 27, 2016 • edited | Contributor

I agree that the wording is lacking.

FYI - We hash the numbers on your device and upload the hashes to the server to compute an intersection without ever sending the plain text phone numbers of your contacts to the server.

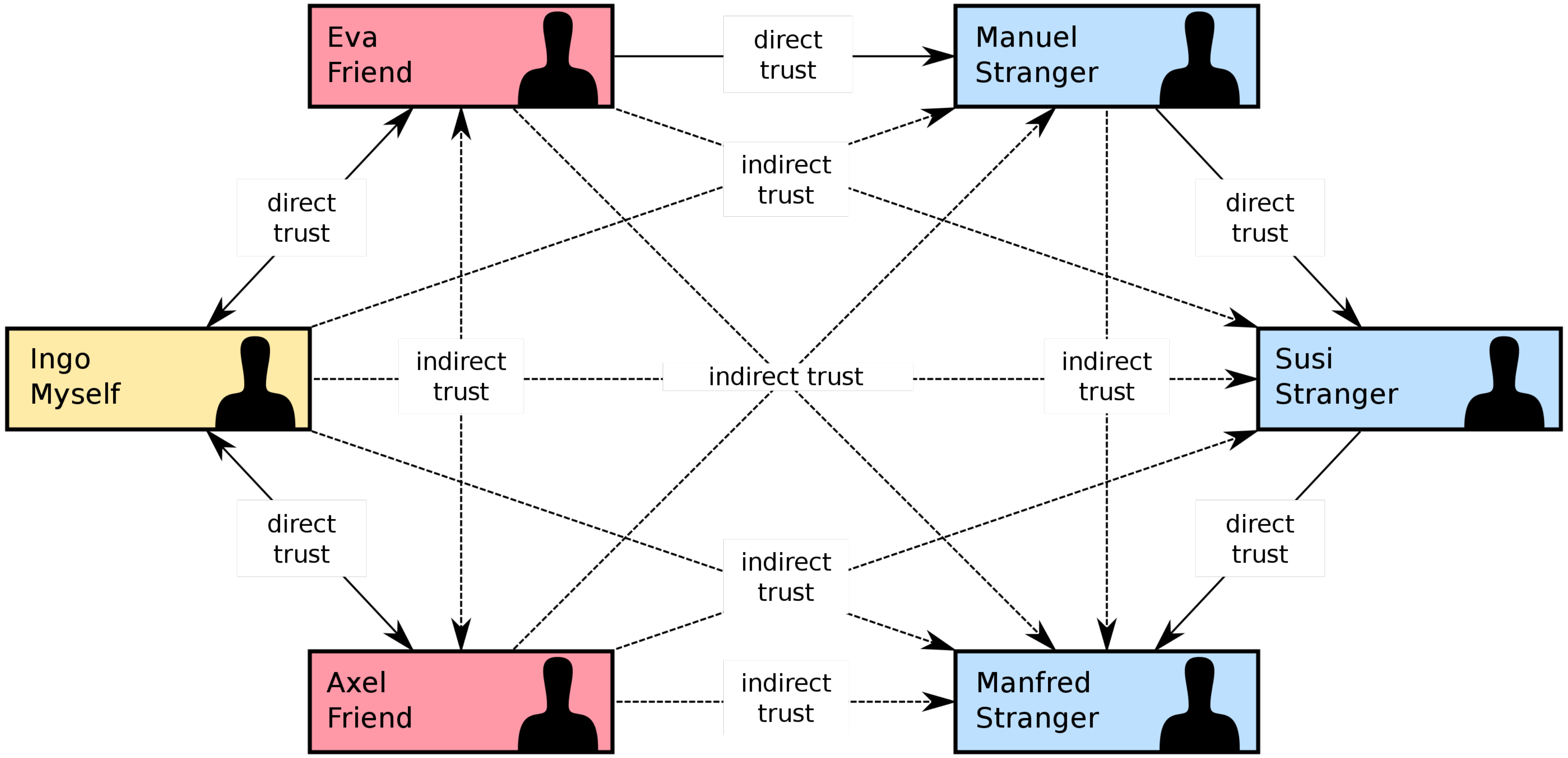
Connecting

intel SGX + ORAM

Pseudonyms

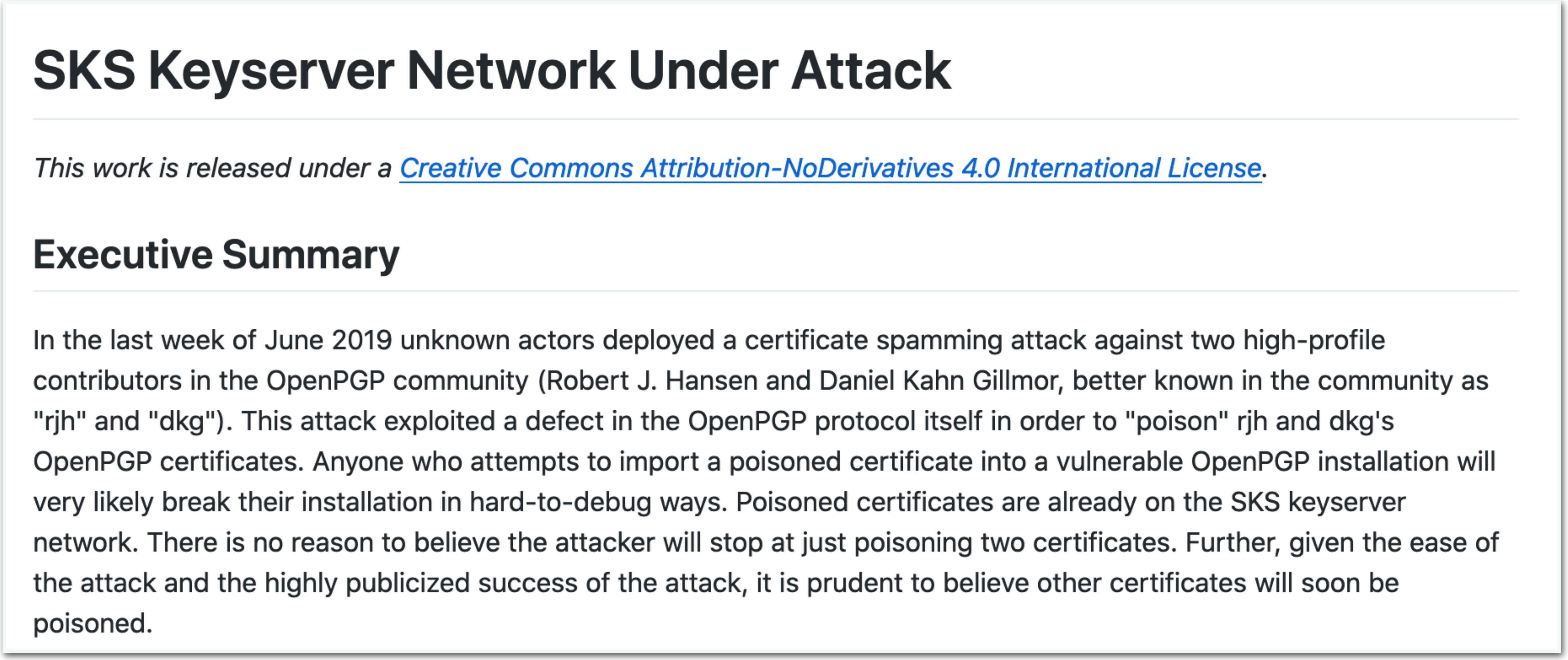
https://github.com/signalapp/contactdiscoveryservice

Connecting



https://en.wikipedia.org/wiki/Web_of_trust

Connecting



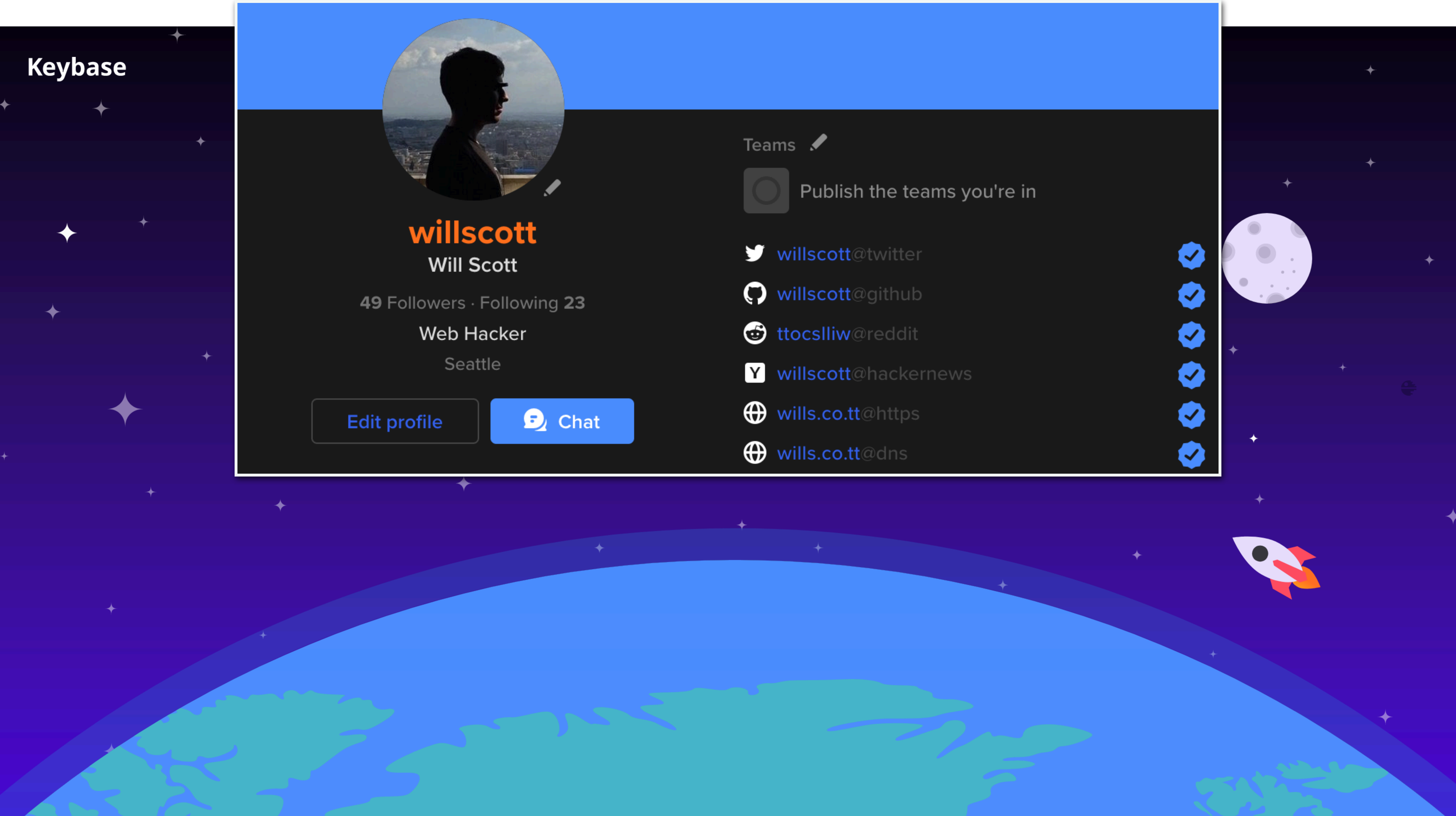
SKS Keyserver Network Under Attack

Executive Summary

In the last week of June 2019 unknown actors deployed a certificate spamming attack against two high-profile contributors in the OpenPGP community (Robert J. Hansen and Daniel Kahn Gillmor, better known in the community as "rjh" and "dkg"). This attack exploited a defect in the OpenPGP protocol itself in order to "poison" rjh and dkg's OpenPGP certificates. Anyone who attempts to import a poisoned certificate into a vulnerable OpenPGP installation will very likely break their installation in hard-to-debug ways. Poisoned certificates are already on the SKS keyserver network. There is no reason to believe the attacker will stop at just poisoning two certificates. Further, given the ease of the attack and the highly publicized success of the attack, it is prudent to believe other certificates will soon be poisoned.

`https://gist.github.com/rjhansen/67ab921ffb4084c865b3618d6955275f`

Connecting



Keybase

willscott

Will Scott

49 Followers · Following 23

Web Hacker

Seattle

Edit profile

Chat

Teams

Publish the teams you're in

willscott@twitter ✓

willscott@github ✓

ttocslliw@reddit ✓

willscott@hackernews ✓

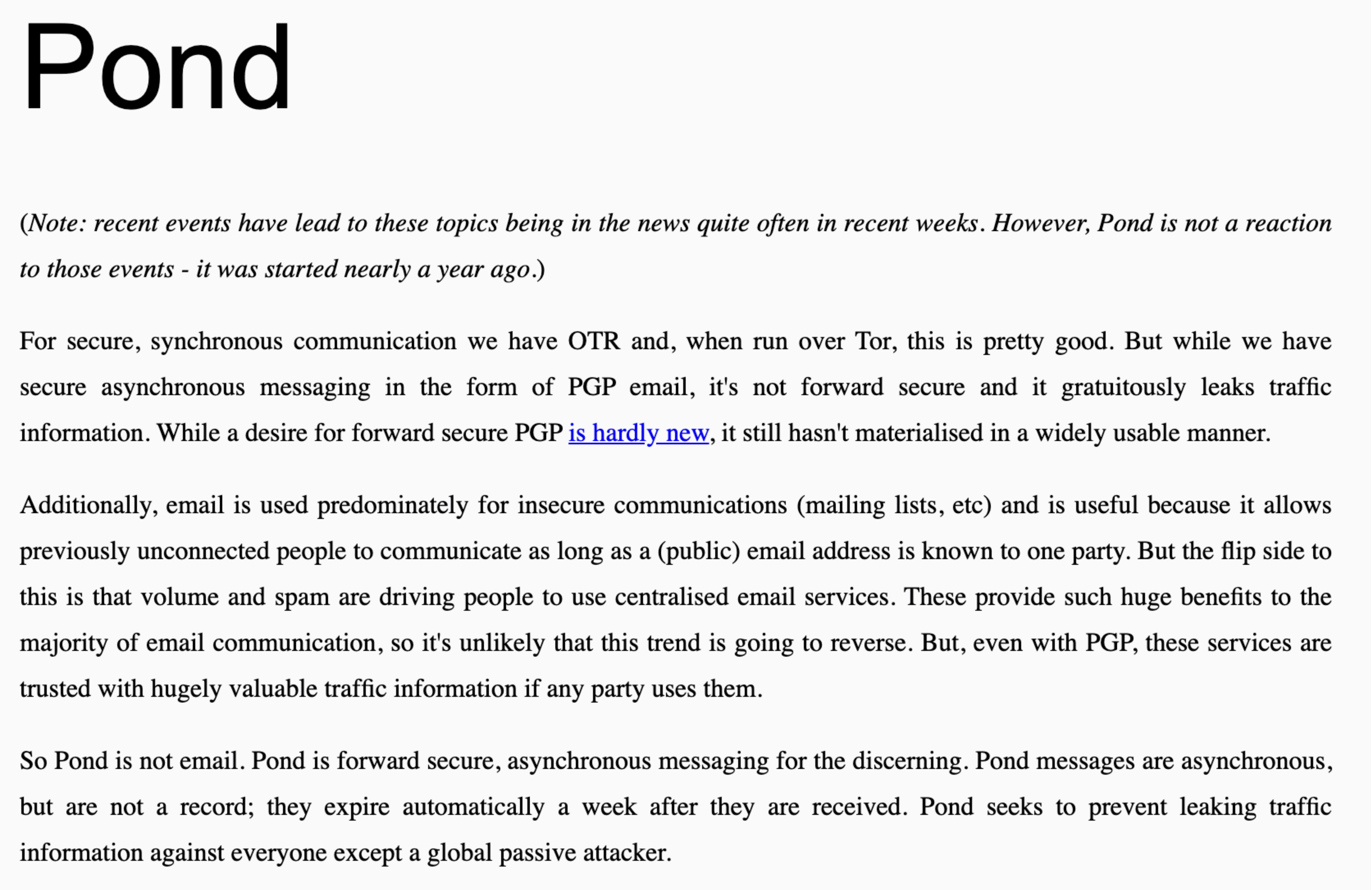
wills.co.tt@https ✓

wills.co.tt@dns ✓

Connecting

TOFU

https://en.wikipedia.org/wiki/Tofu



Pond

(*Note: recent events have lead to these topics being in the news quite often in recent weeks. However, Pond is not a reaction to those events - it was started nearly a year ago*.)

For secure, synchronous communication we have OTR and, when run over Tor, this is pretty good. But while we have secure asynchronous messaging in the form of PGP email, it's not forward secure and it gratuitously leaks traffic information. While a desire for forward secure PGP is hardly new, it still hasn't materialised in a widely usable manner.

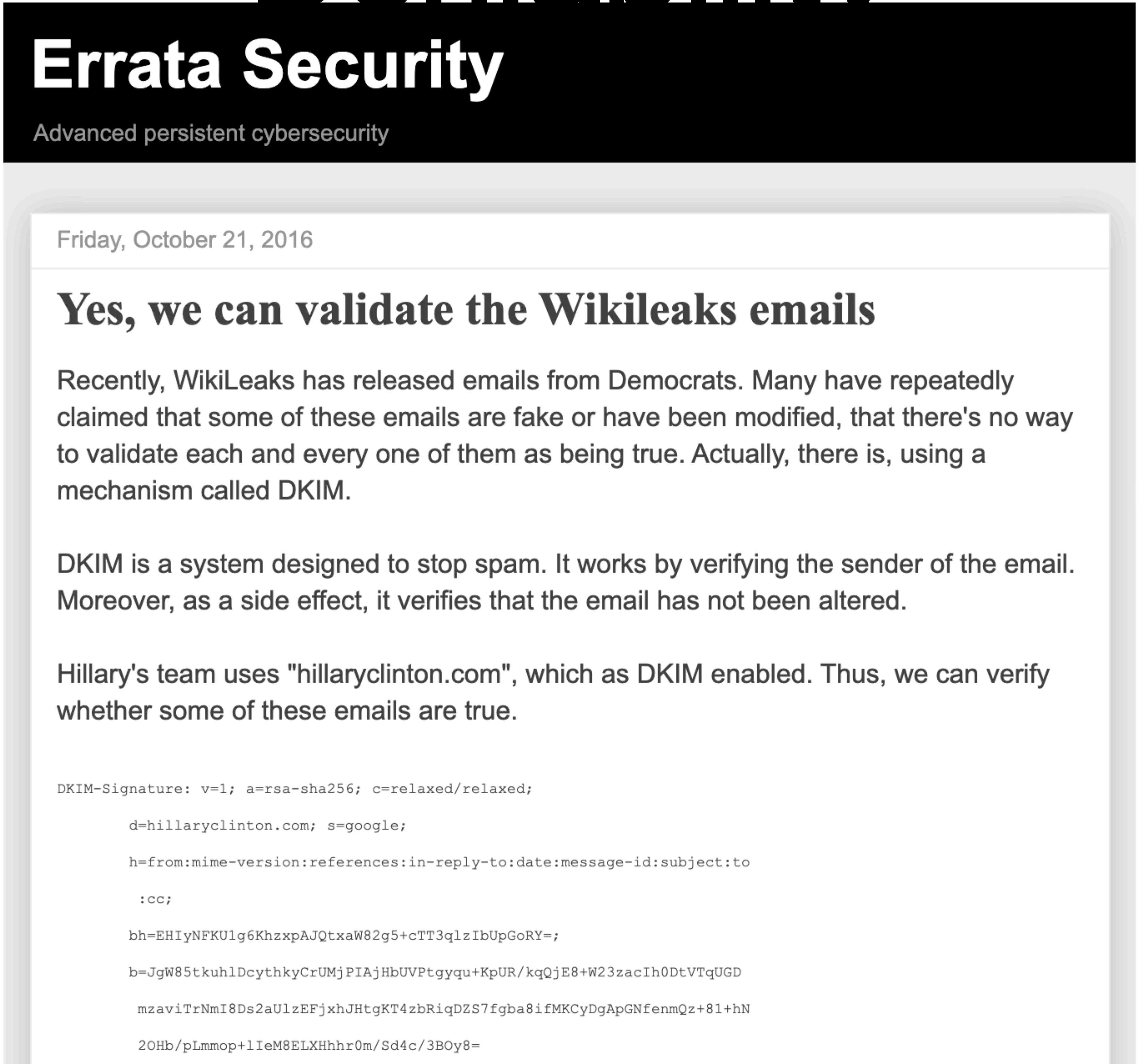
Additionally, email is used predominately for insecure communications (mailing lists, etc) and is useful because it allows previously unconnected people to communicate as long as a (public) email address is known to one party. But the flip side to this is that volume and spam are driving people to use centralised email services. These provide such huge benefits to the majority of email communication, so it's unlikely that this trend is going to reverse. But, even with PGP, these services are trusted with hugely valuable traffic information if any party uses them.

So Pond is not email. Pond is forward secure, asynchronous messaging for the discerning. Pond messages are asynchronous, but are not a record; they expire automatically a week after they are received. Pond seeks to prevent leaking traffic information against everyone except a global passive attacker.

https://github.com/agl/pond

https://blog.erratasec.com/2016/10/yes-we-can-validate-wikileaks-emails.html

Deniability



Errata Security

Advanced persistent cybersecurity

Friday, October 21, 2016

Yes, we can validate the Wikileaks emails

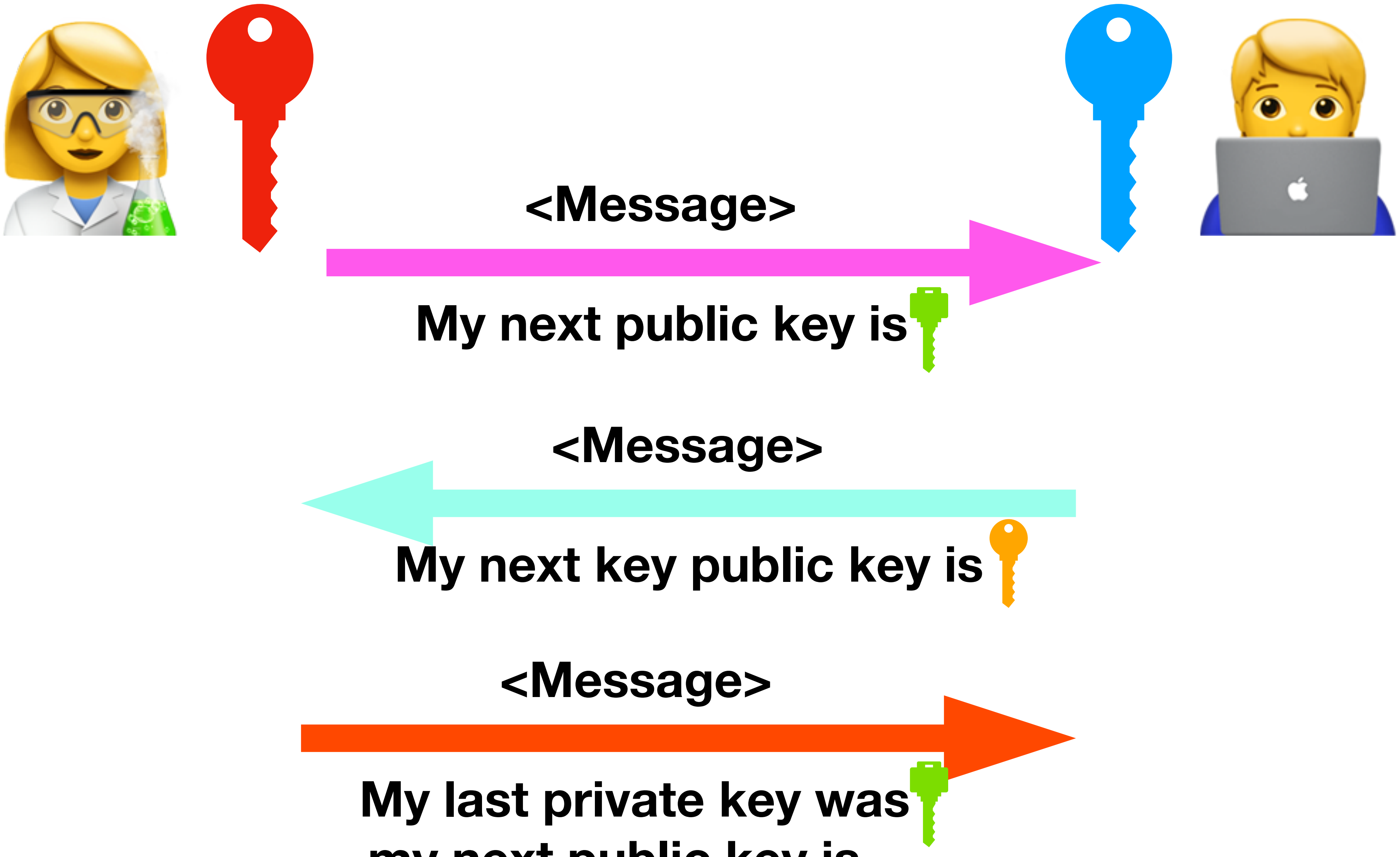
Recently, WikiLeaks has released emails from Democrats. Many have repeatedly claimed that some of these emails are fake or have been modified, that there's no way to validate each and every one of them as being true. Actually, there is, using a mechanism called DKIM.

DKIM is a system designed to stop spam. It works by verifying the sender of the email. Moreover, as a side effect, it verifies that the email has not been altered.

Hillary's team uses "hillaryclinton.com", which as DKIM enabled. Thus, we can verify whether some of these emails are true.

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;
        d=hillaryclinton.com; s=google;
        h=from:mime-version:references:in-reply-to:date:message-id:subject:to
         :cc;
        bh=EHIyNFKU1g6KhzxpAJQtxaW82g5+cTT3qlzIbUpGoRY=;
        b=JgW85tkuhlDcythkyCrUMjPIAjHbUVPtgyqu+KpUR/kqQjE8+W23zacIh0DtVTqUGD
         mzaviTrNmI8Ds2aUlzEFjxhJHtgKT4zbRiqDZS7fgba8ifMKCyDgApGNfenmQz+81+hN
         2OHb/pLmmop+lIeM8ELXHhhr0m/Sd4c/3BOy8=
```

Forward Secrecy



<Message>

My next public key is 🔑

<Message>

My next key public key is 🔑

<Message>

My last private key was 🔑
my next public key is...

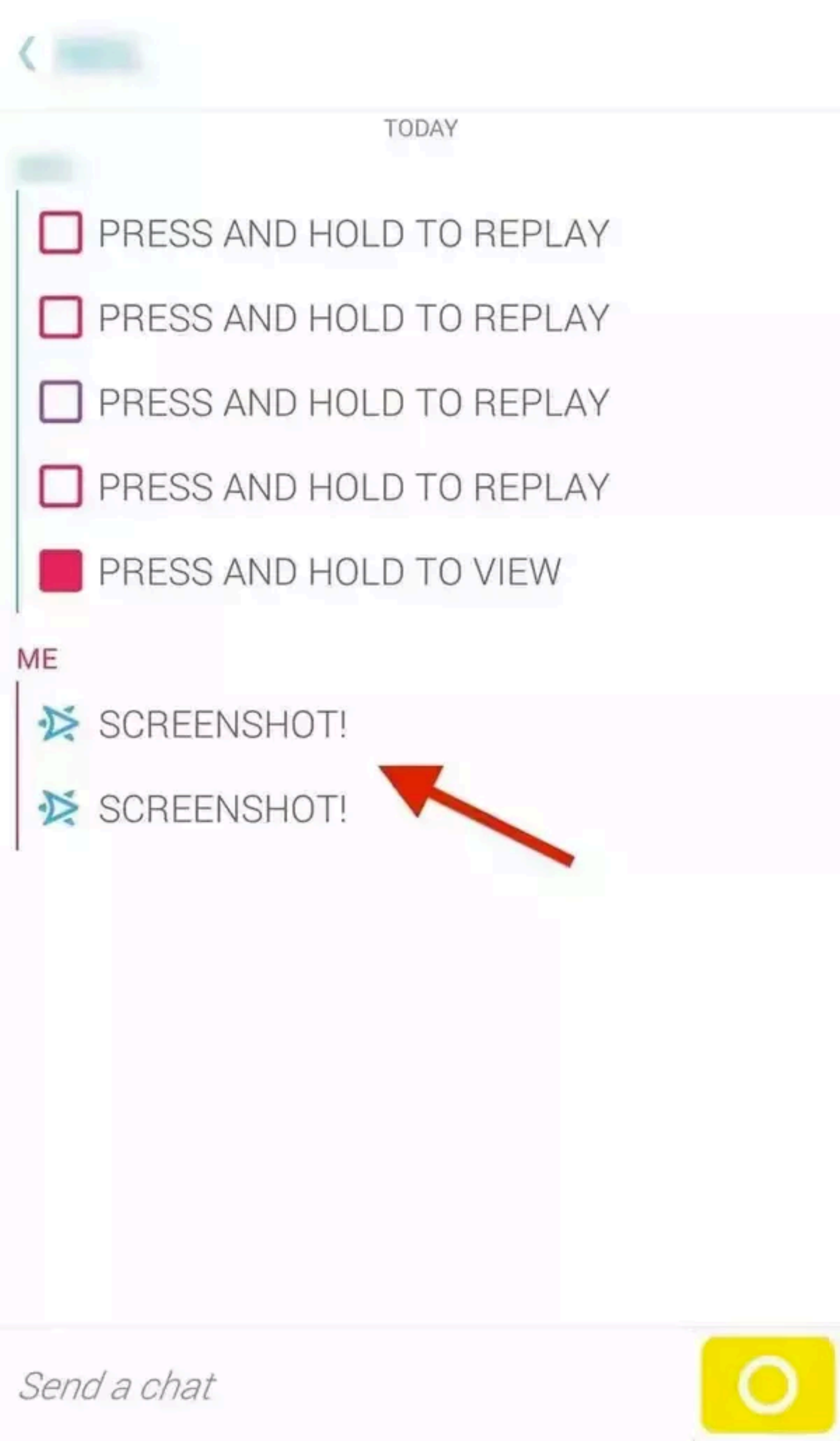
MECHANISMS

- Encryption
- **Message Expiry**
- OS Sandboxing / Isolation
- Traffic Obfuscation
- Server Hardening

EXPIRY

Expiry

The "screenshot" adversary



TODAY

□ PRESS AND HOLD TO REPLAY

□ PRESS AND HOLD TO REPLAY

□ PRESS AND HOLD TO REPLAY

□ PRESS AND HOLD TO REPLAY

■ PRESS AND HOLD TO VIEW

ME

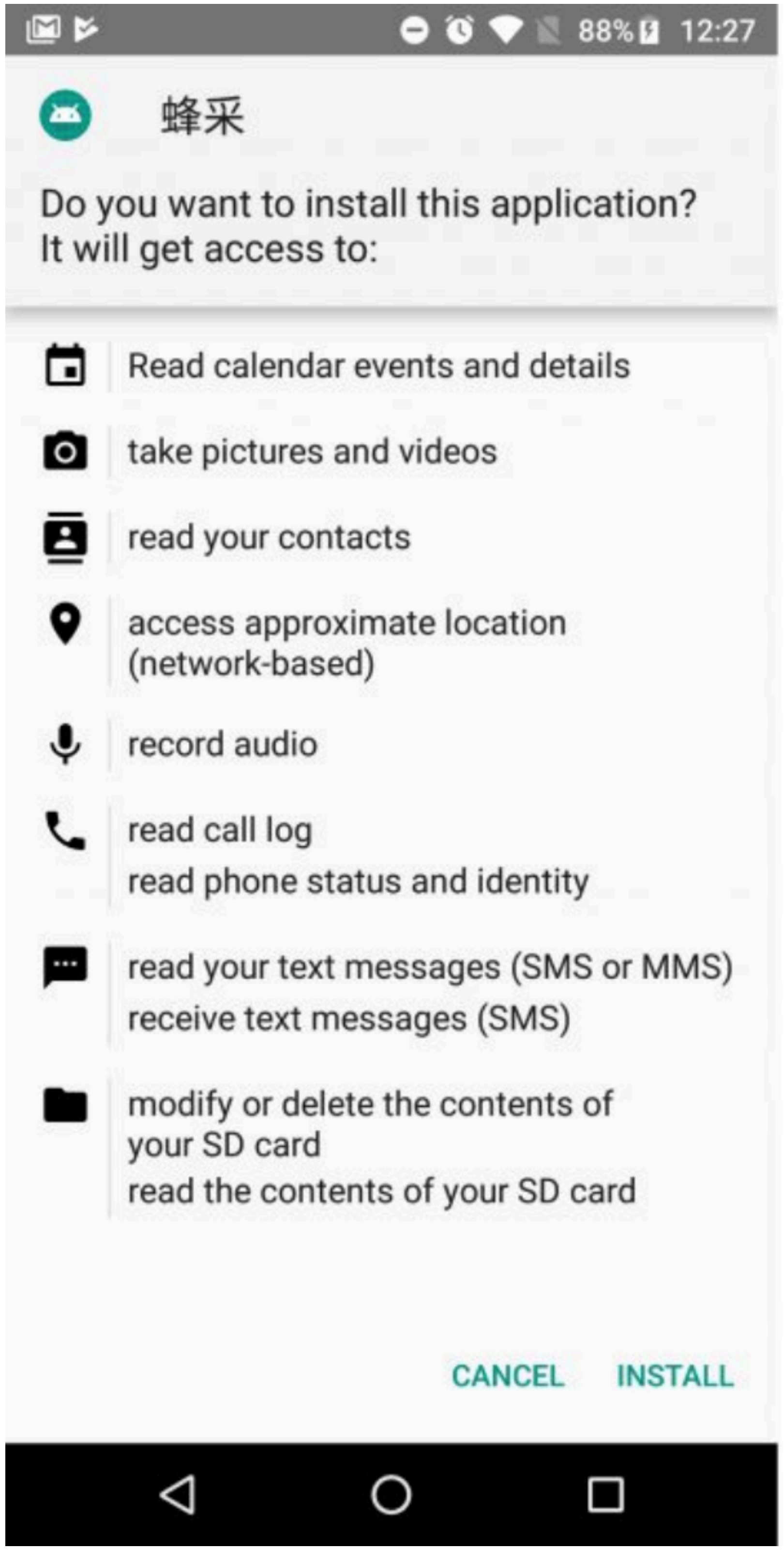
SCREENSHOT!

SCREENSHOT!

Expiry

(the forensic adversary)

**GrayKey / Cellebrite
or "ADB" on android**



蜂采

Do you want to install this application? It will get access to:

- Read calendar events and details
- take pictures and videos
- read your contacts
- access approximate location (network-based)
- record audio
- read call log
  read phone status and identity
- read your text messages (SMS or MMS)
  receive text messages (SMS)
- modify or delete the contents of your SD card
  read the contents of your SD card

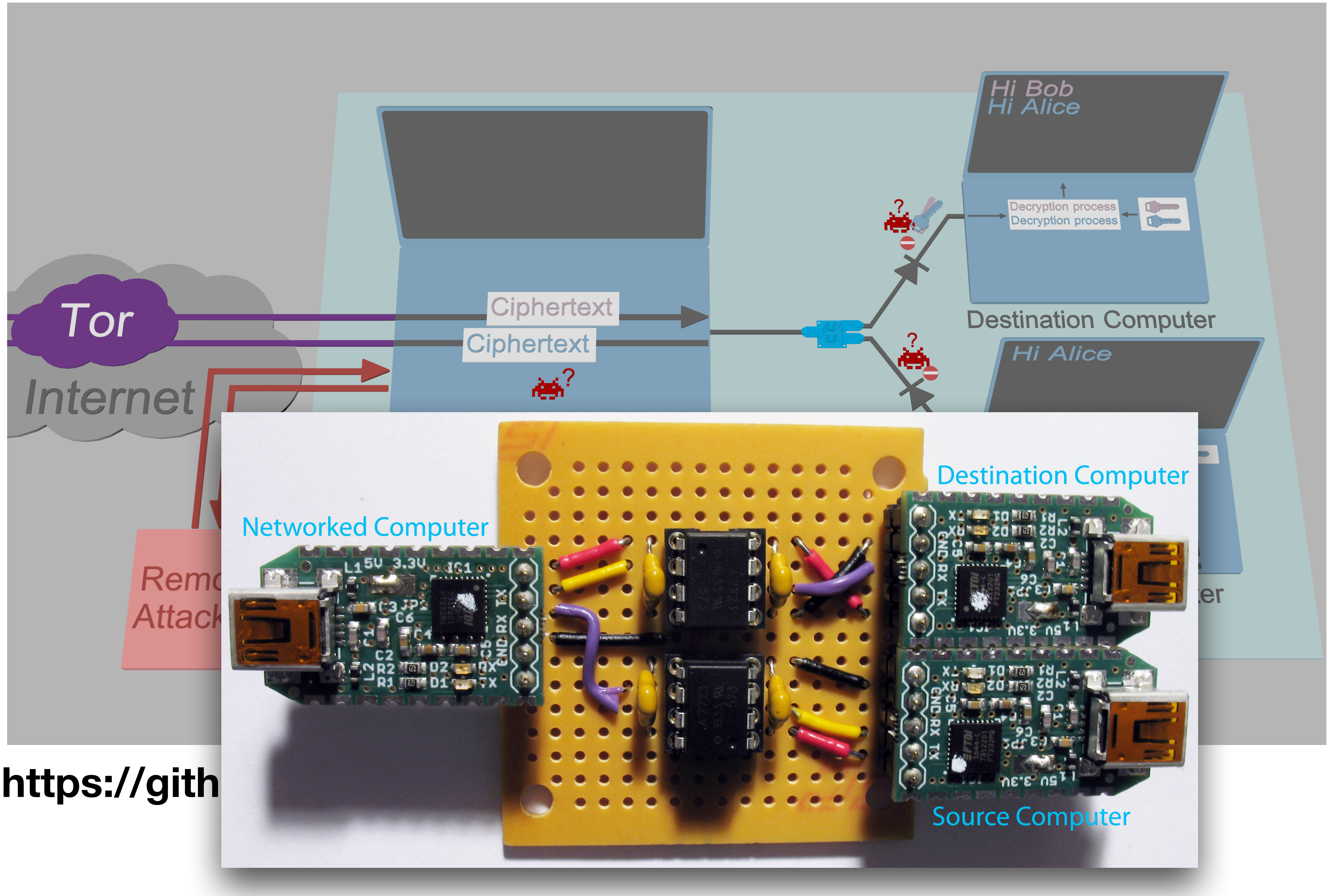
```
https://bit.ly/39dzEDy
https://bit.ly/2EREN66
```

MECHANISMS

- Encryption
- Message Expiry
- **OS Sandboxing / Isolation**
- Traffic Obfuscation
- Server Hardening

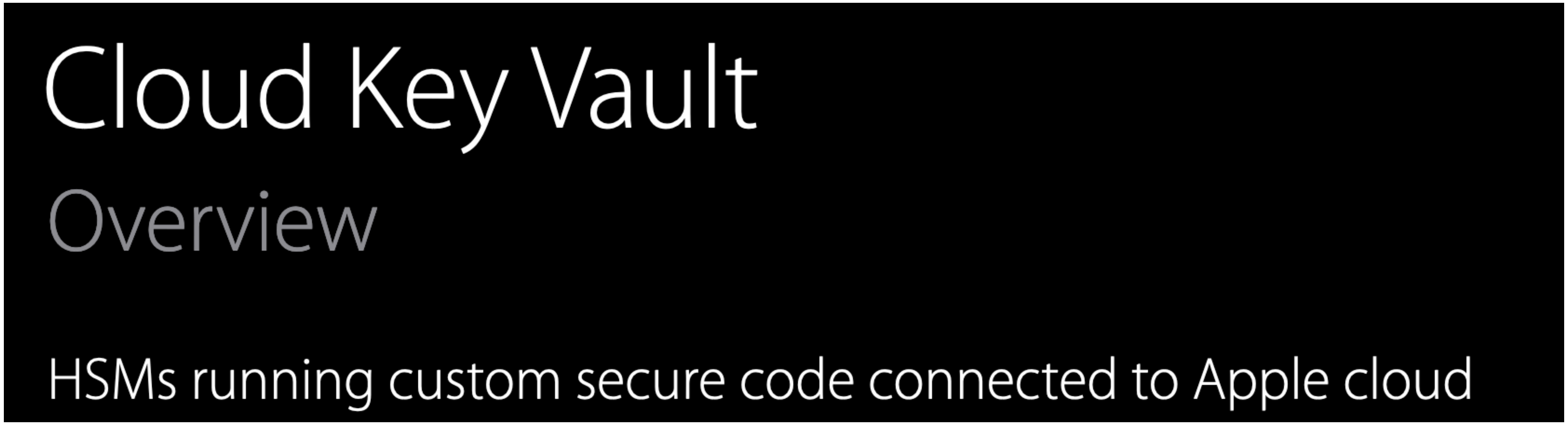
ISOLATION

Tinfoil Chat



https://gith

Recovery & Backups



Cloud Key Vault

Overview

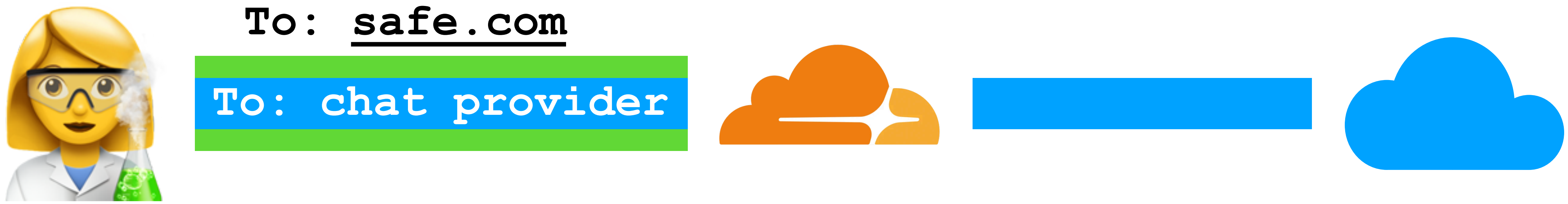
HSMs running custom secure code connected to Apple cloud

"Behind the Scenes with iOS Security" - Ivan Krstić. Blackhat 2016

MECHANISMS

- Encryption
- Message Expiry
- OS Sandboxing / Isolation
- **Traffic Obfuscation**
- Server Hardening

Obfuscation



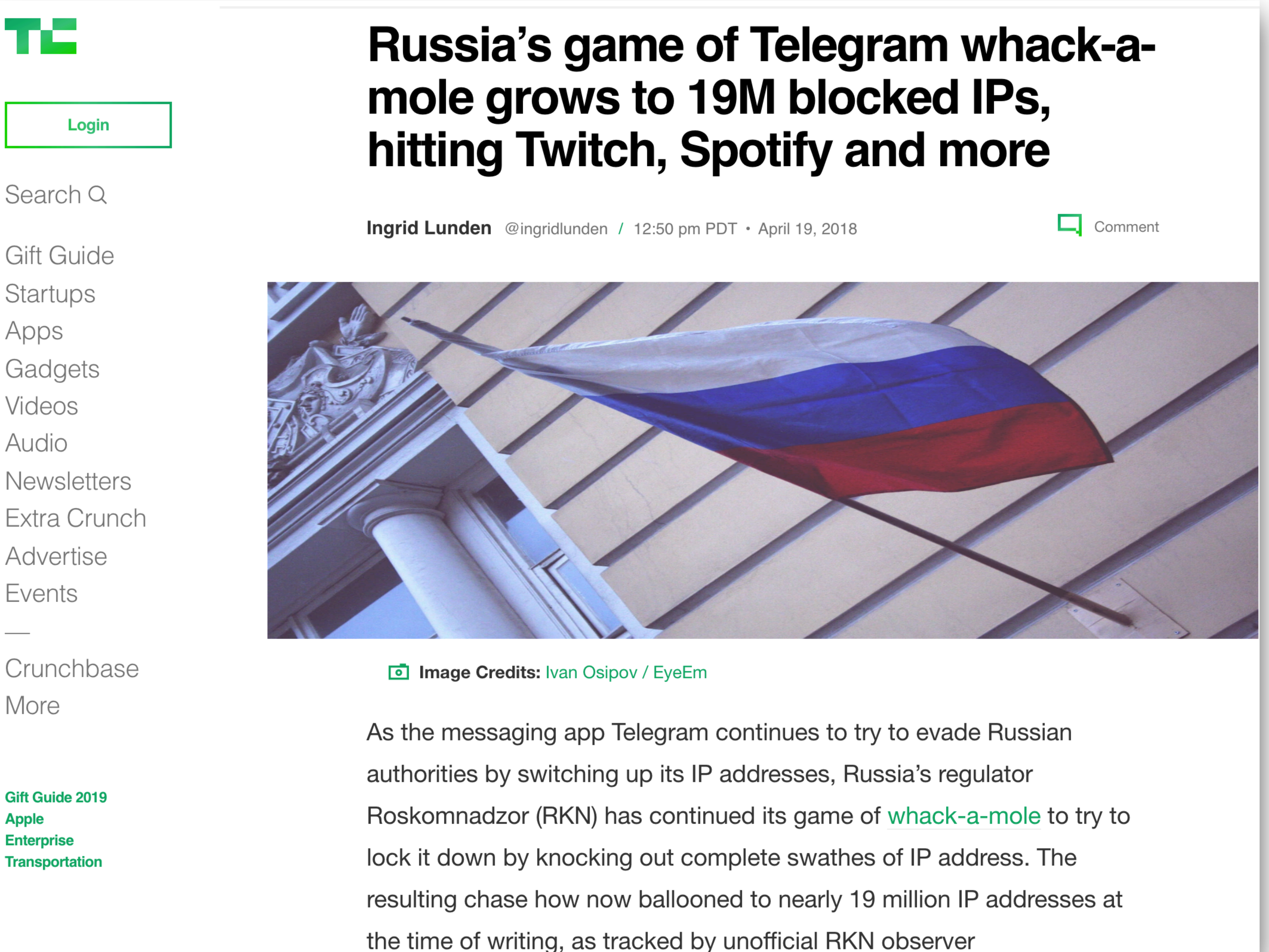
To: safe.com

To: chat provider

DOMAIN FRONTING

https://techcrunch.com/2018/04/19/russias-game-of-telegram-whack-a-mole-grows-to-19m-blocked-ips-hitting-twitch-spotify-and-more/

Obfuscation



Russia's game of Telegram whack-a-mole grows to 19M blocked IPs, hitting Twitch, Spotify and more

Ingrid Lunden @ingridlunden / 12:50 pm PDT • April 19, 2018

Image Credits: Ivan Osipov / EyeEm

As the messaging app Telegram continues to try to evade Russian authorities by switching up its IP addresses, Russia's regulator Roskomnadzor (RKN) has continued its game of whack-a-mole to try to lock it down by knocking out complete swathes of IP address. The resulting chase how now ballooned to nearly 19 million IP addresses at the time of writing, as tracked by unofficial RKN observer

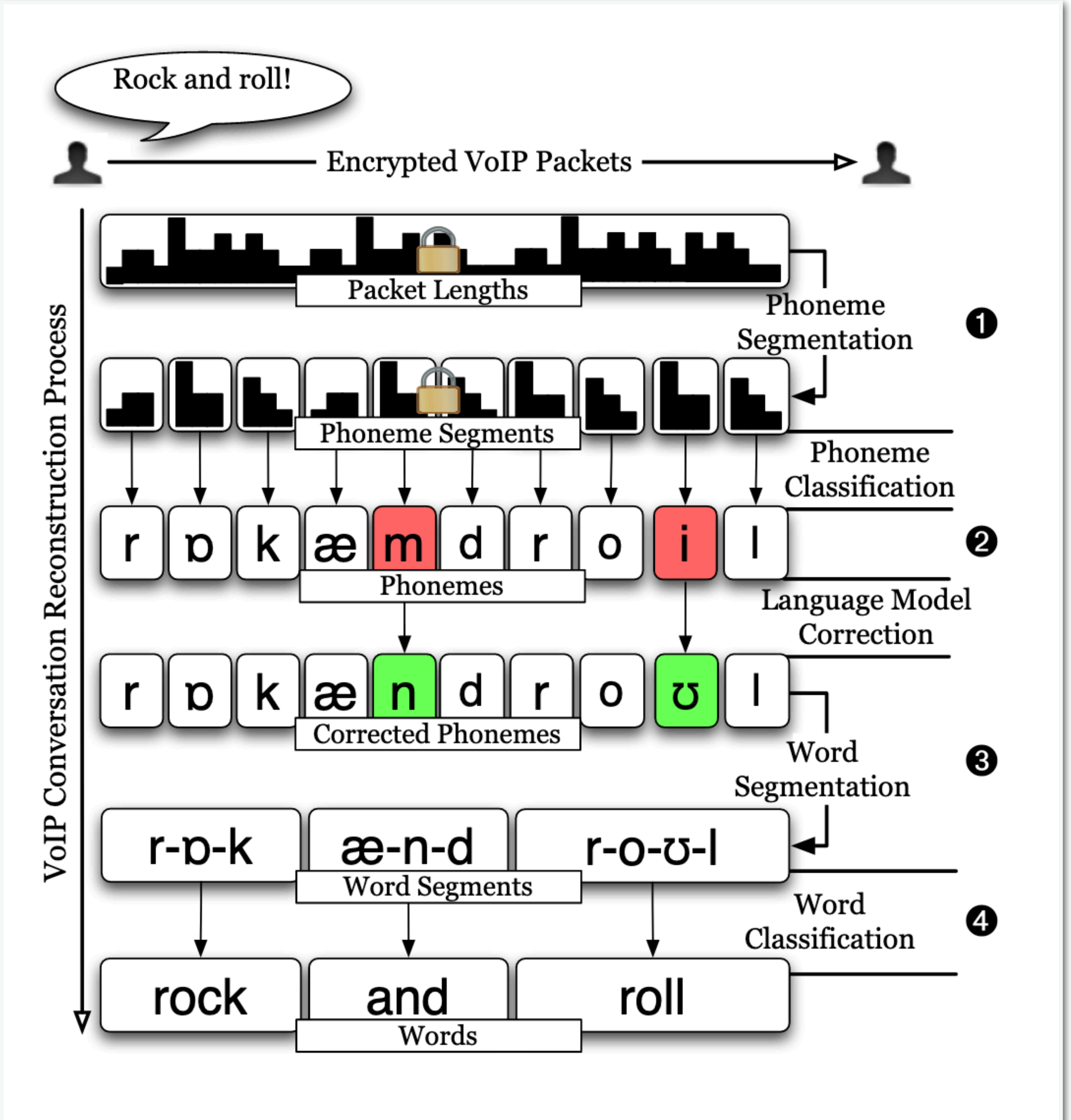
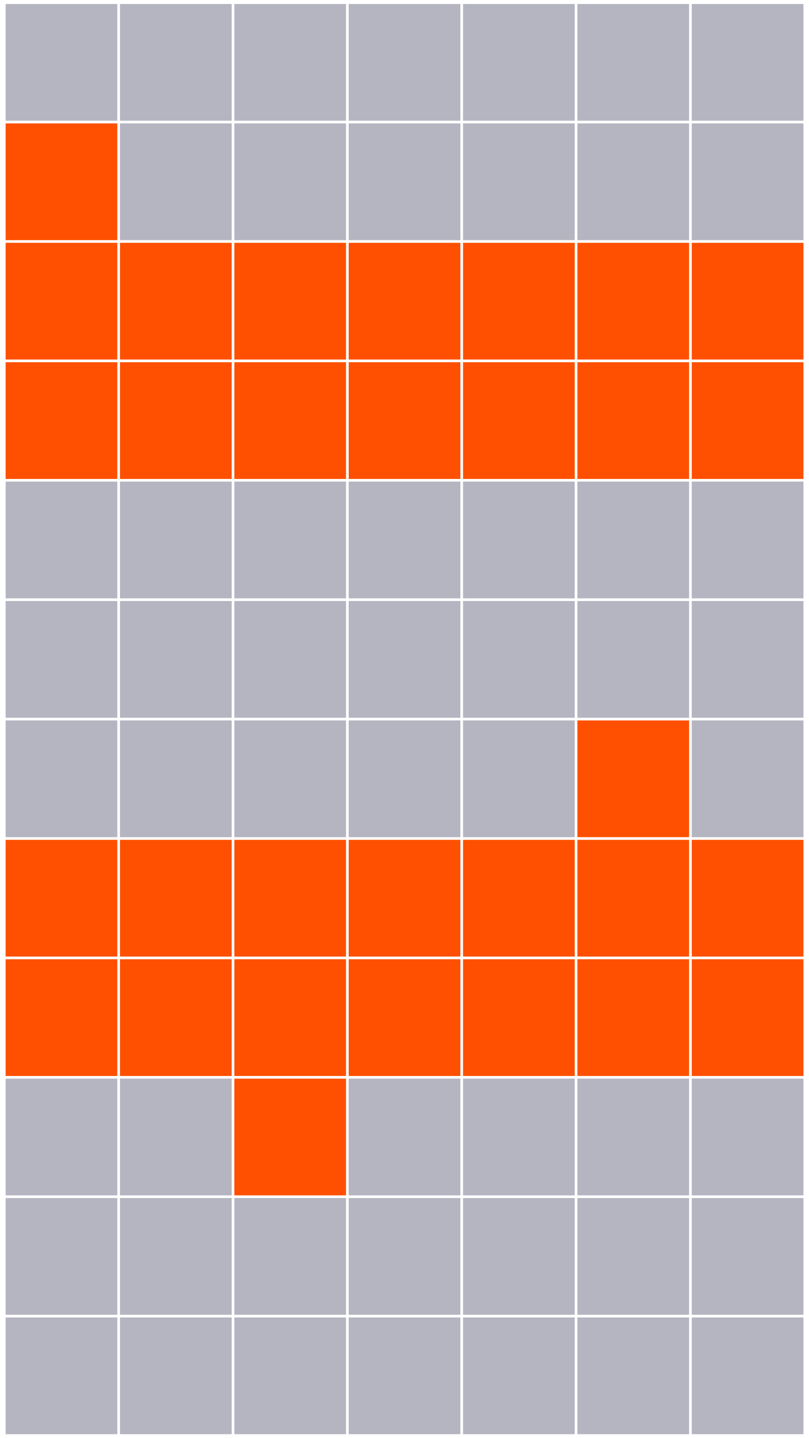


Figure 2. Overall architecture of our approach for reconstructing transcripts of VoIP conversations from sequences of encrypted packet sizes.

White, Andrew M., et al. "Phonotactic reconstruction of encrypted voip conversations: Hookt on fon-iks." IEEE S&P 2011

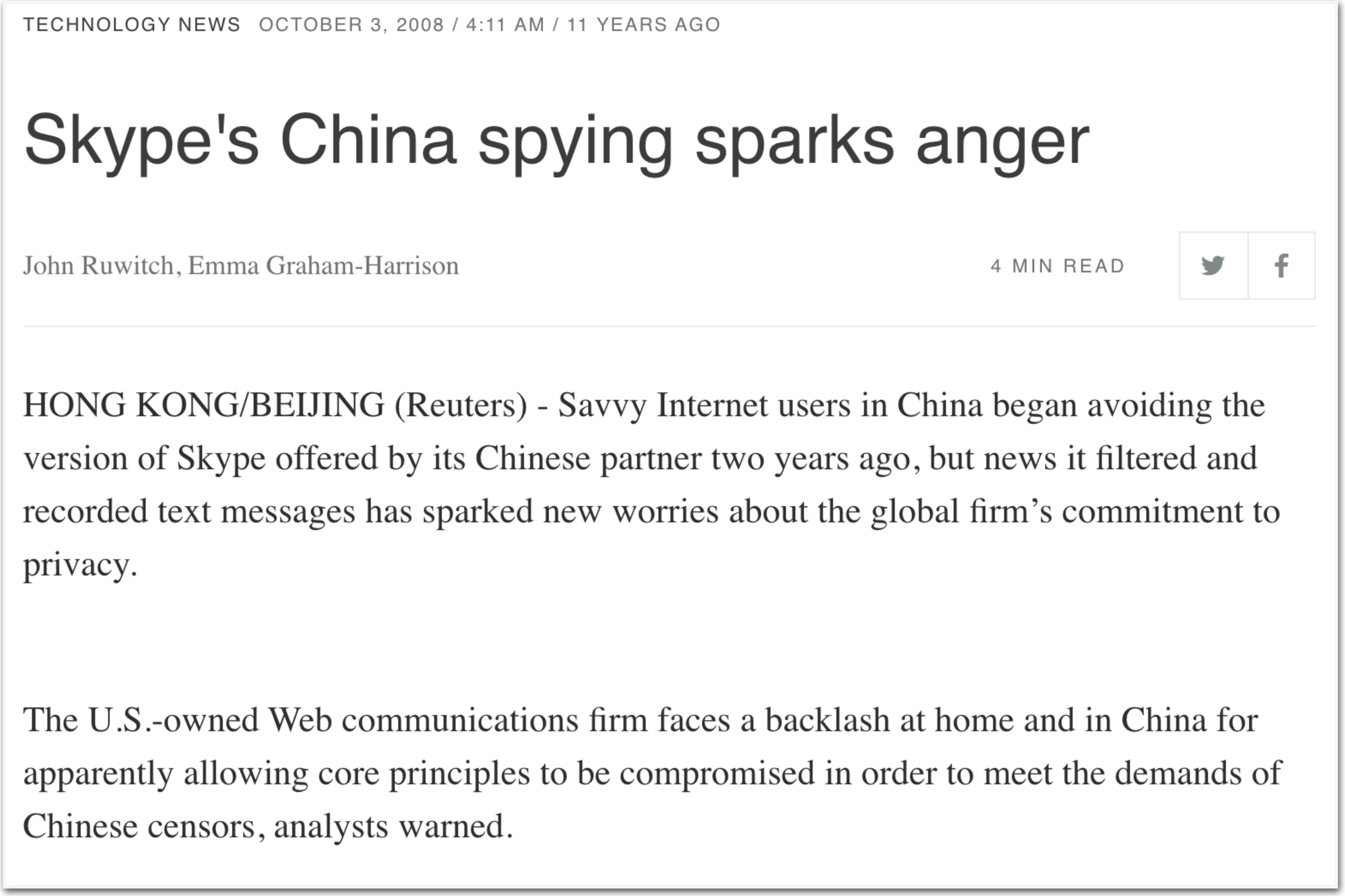
Activity



MECHANISMS

- Encryption
- Message Expiry
- OS Sandboxing / Isolation
- Traffic Obfuscation
- **Server Hardening**

Server Hardening



TECHNOLOGY NEWS OCTOBER 3, 2008 / 4:11 AM / 11 YEARS AGO

Skype's China spying sparks anger

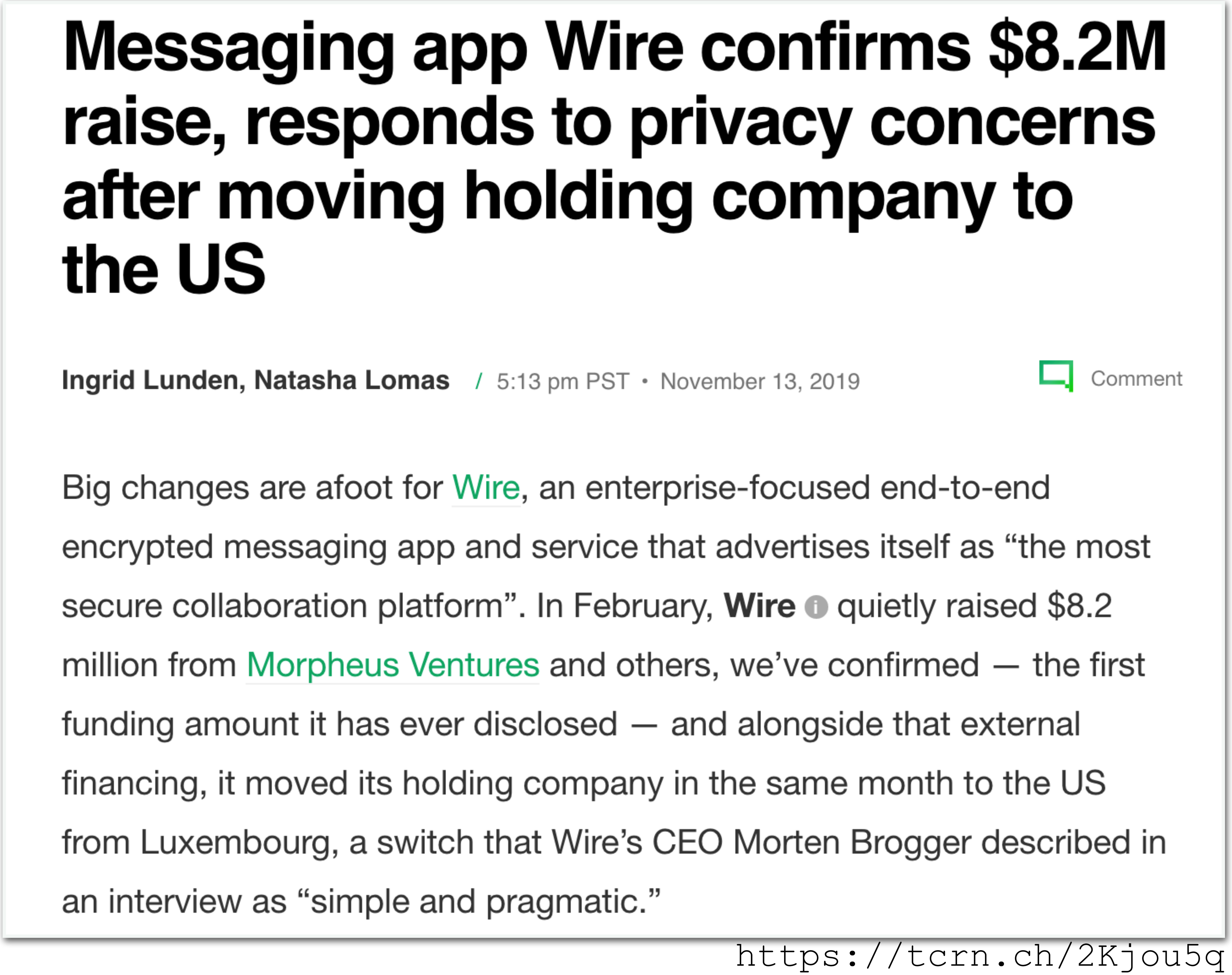
John Ruwitch, Emma Graham-Harrison

HONG KONG/BEIJING (Reuters) - Savvy Internet users in China began avoiding the version of Skype offered by its Chinese partner two years ago, but news it filtered and recorded text messages has sparked new worries about the global firm’s commitment to privacy.

The U.S.-owned Web communications firm faces a backlash at home and in China for apparently allowing core principles to be compromised in order to meet the demands of Chinese censors, analysts warned.

https://www.reuters.com/article/us-china-skype-censorship/idUSTRE49238X20081003

Server Hardening



Messaging app Wire confirms $8.2M raise, responds to privacy concerns after moving holding company to the US

Ingrid Lunden, Natasha Lomas / 5:13 pm PST • November 13, 2019 Comment

Big changes are afoot for Wire, an enterprise-focused end-to-end encrypted messaging app and service that advertises itself as "the most secure collaboration platform". In February, **Wire** quietly raised $8.2 million from Morpheus Ventures and others, we've confirmed — the first funding amount it has ever disclosed — and alongside that external financing, it moved its holding company in the same month to the US from Luxembourg, a switch that Wire's CEO Morten Brogger described in an interview as "simple and pragmatic."

https://tcrn.ch/2Kjou5q

Server Hardening

Message Metadata:

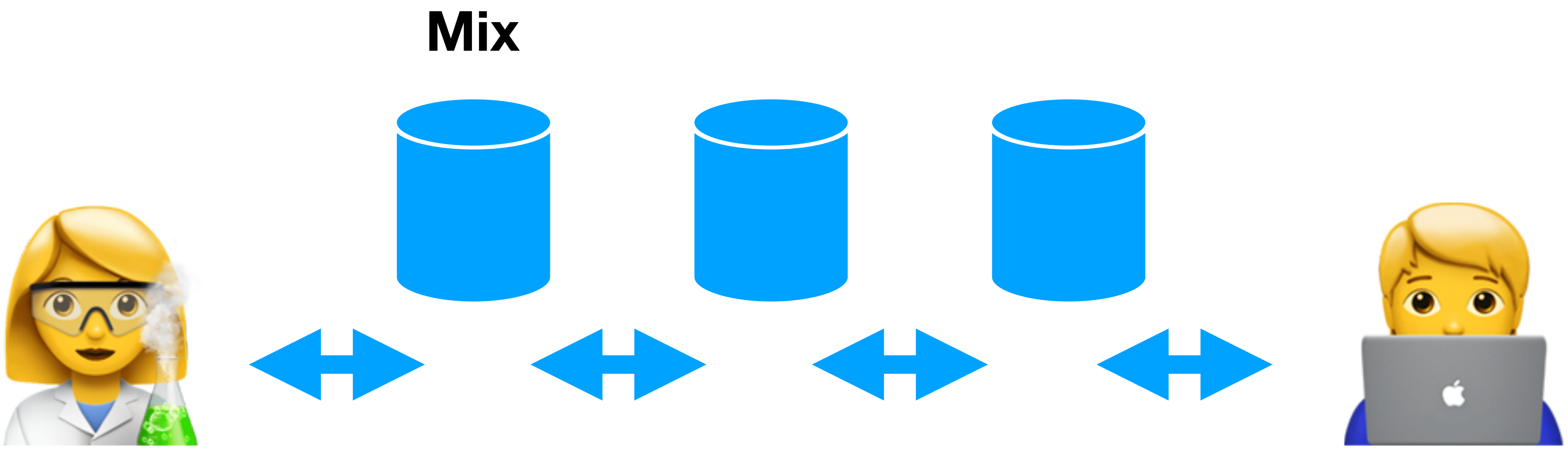
- Size

PADDING

- Source
- Destination

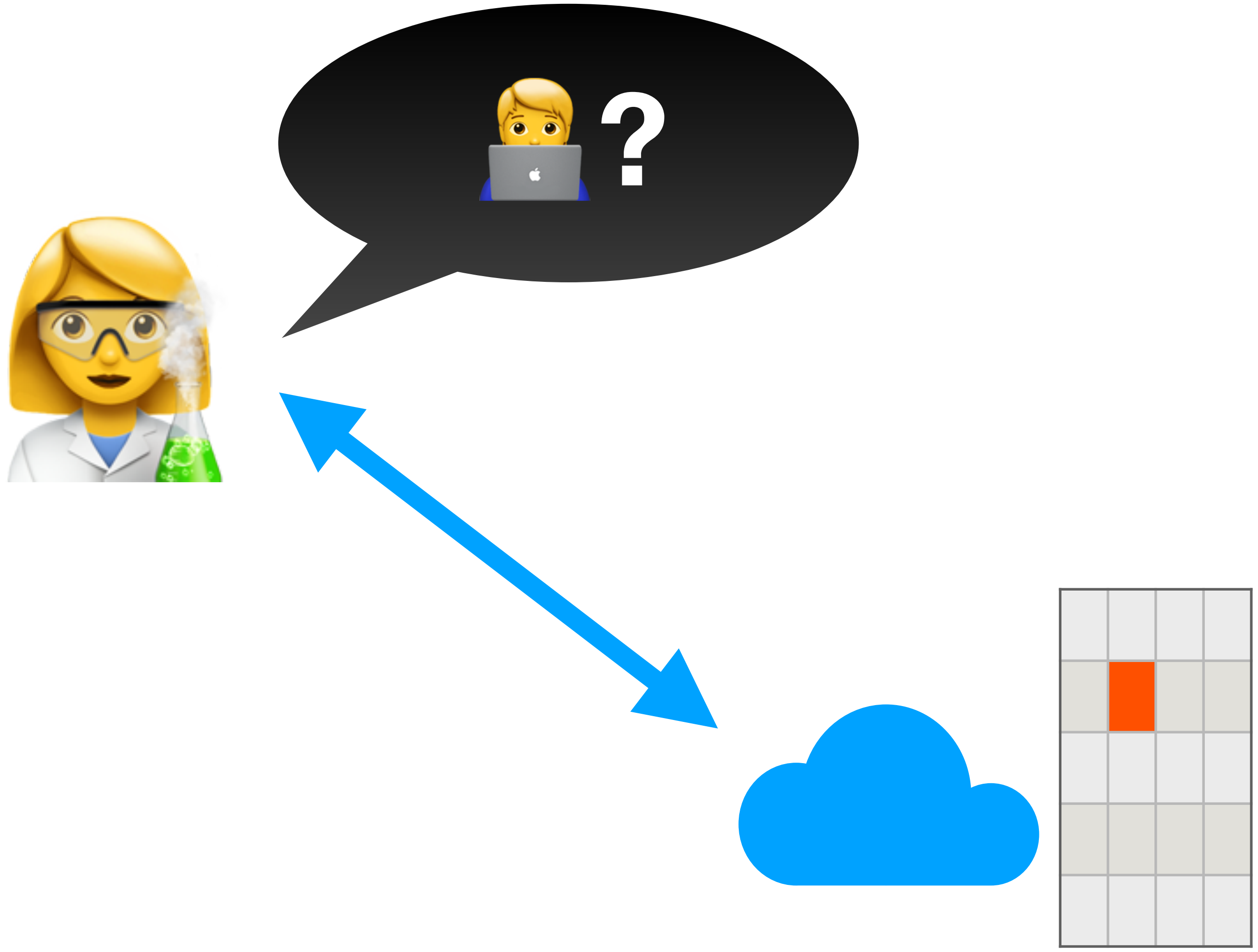
Link-ability

Link-ability



https://katzenpost.mixnetworks.org/

Private Information Retrieval



INFORMATION THEORETIC

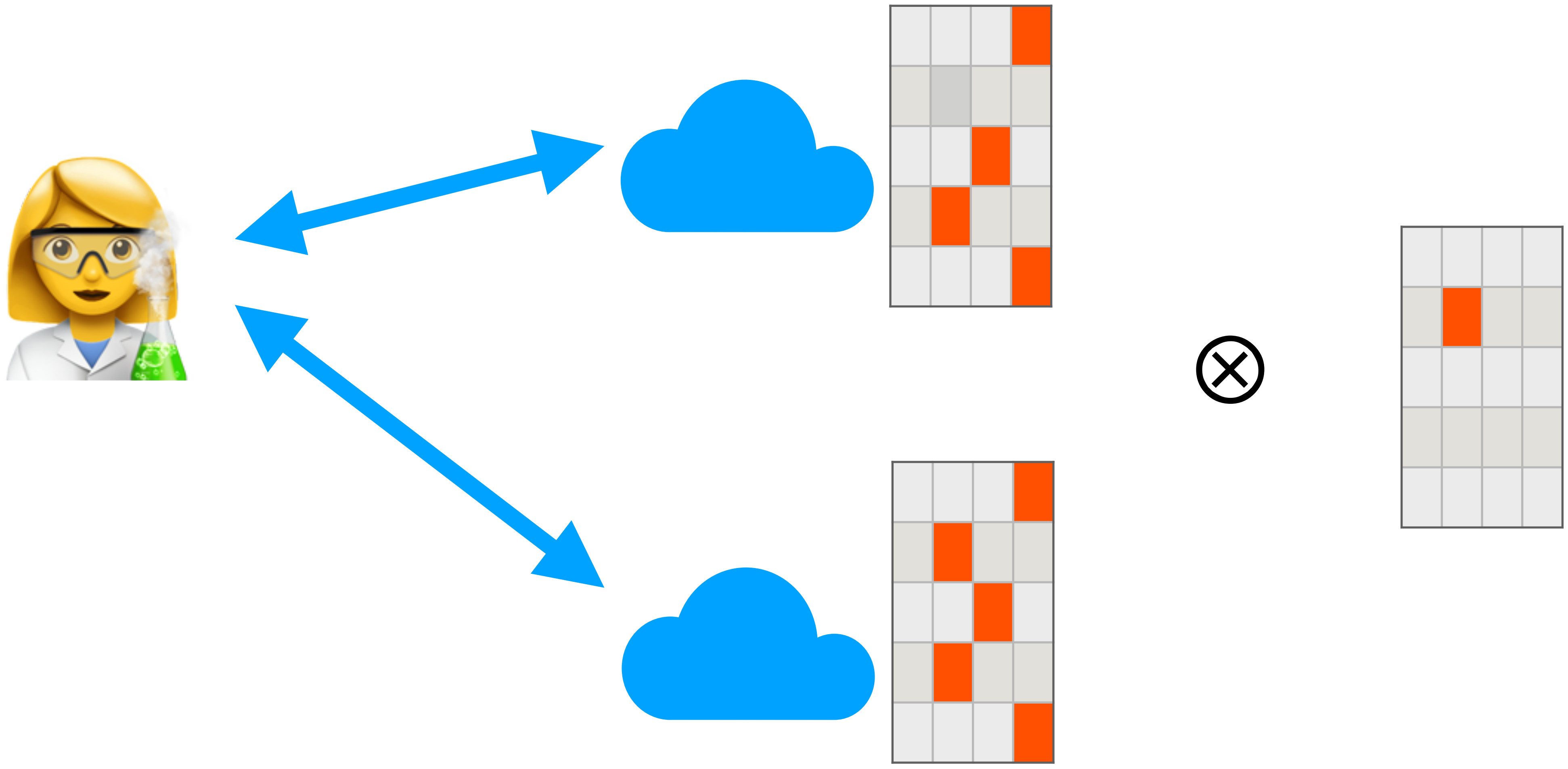
Private Information Retrieval

EXCLUSIVE OR

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

INFORMATION THEORETIC

Private Information Retrieval

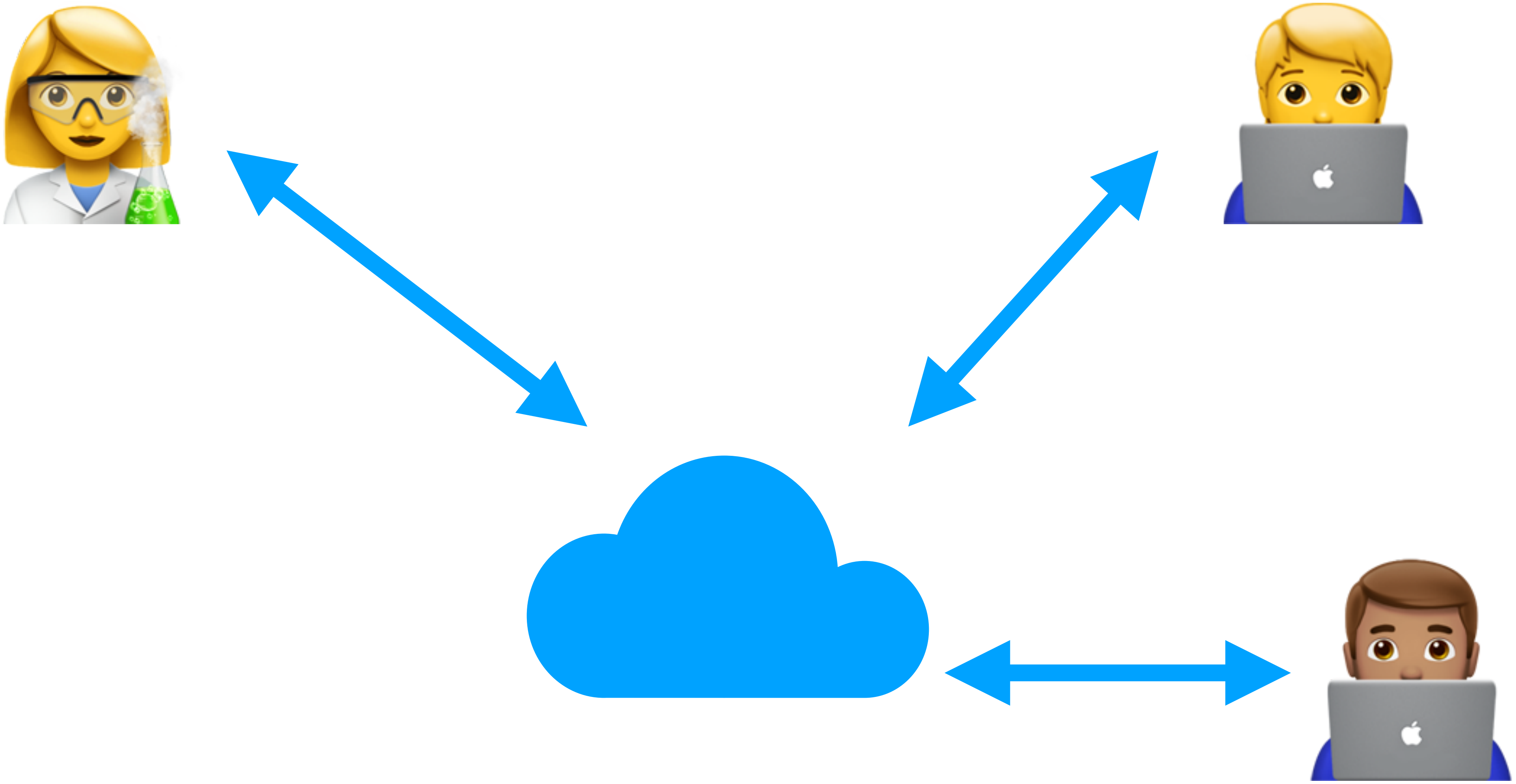


Private Information Retrieval

- (PIR) Talek - https://github.com/privacylab/talek
- (PIS) Express - https://github.com/SabaEskandarian/Express

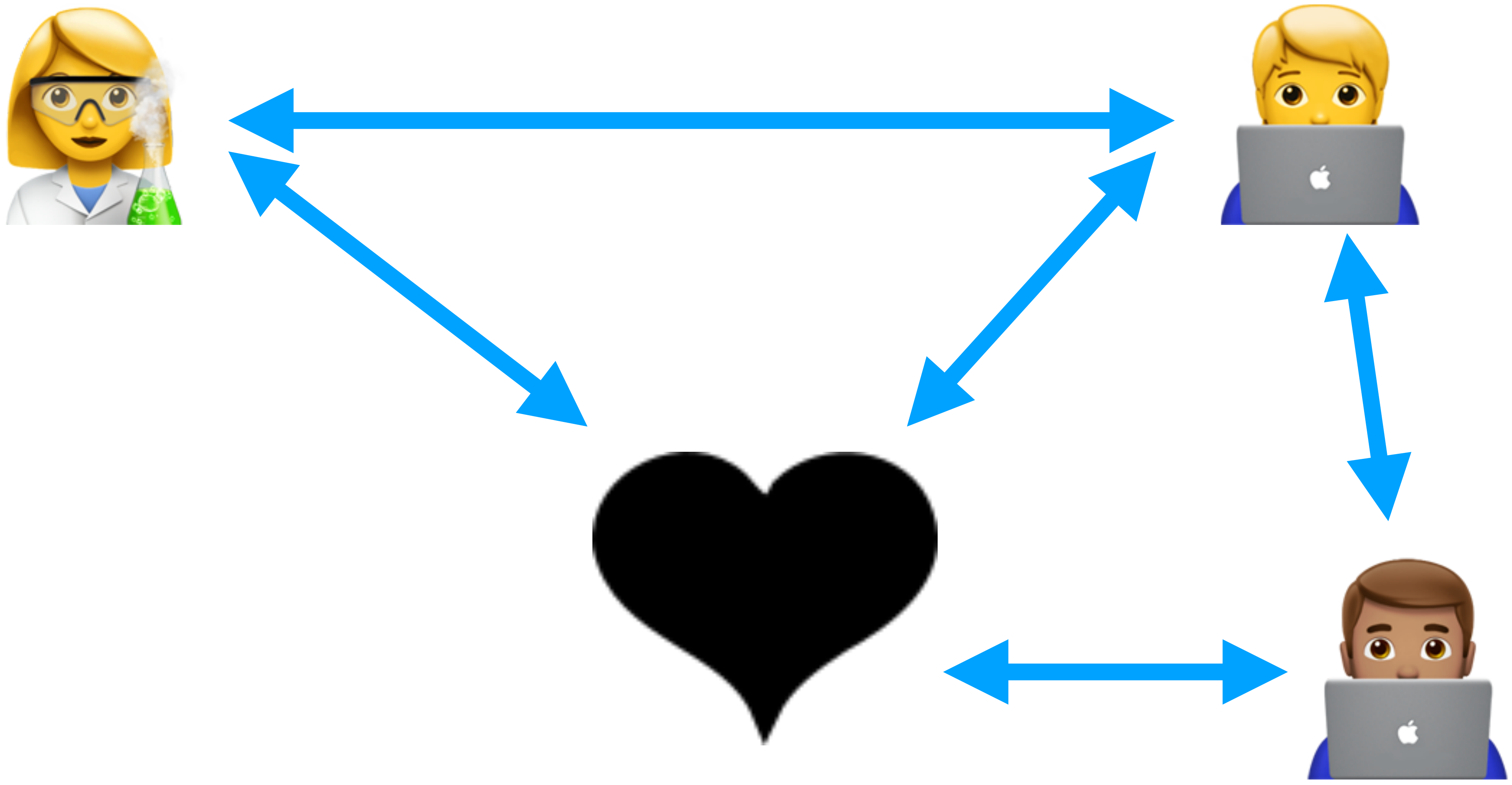
MULTIPARTY

Multiparty



https://signal.org/blog/signal-private-group-system/

cwtch.im



36C3. @WILLSCOTT