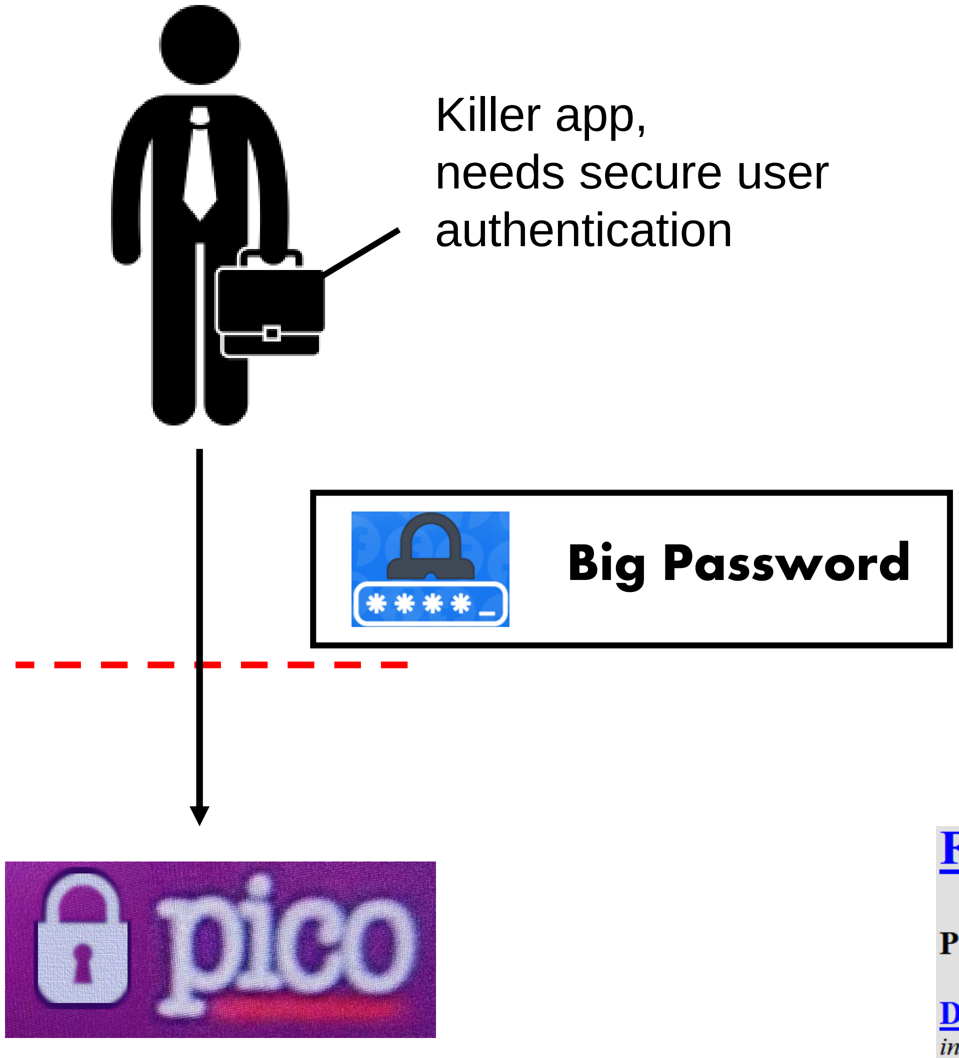
ETH zürich

D-INFK
Network Security Group

Trusted Introductions For Secure Messaging

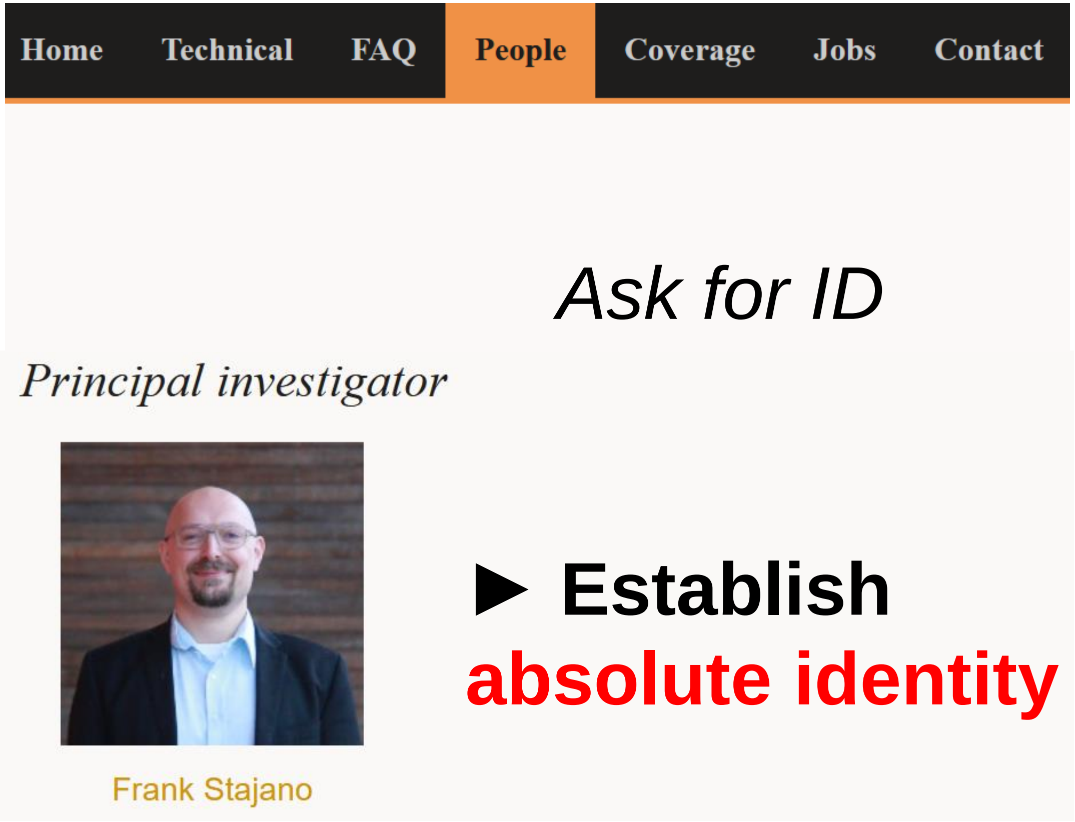
Christelle Gloor & Adrian Perrig

Motivation



Killer app,
needs secure user
authentication

https://www.cl.cam.ac.uk/~fms27/pico/people/index.html



Principal investigator

Frank Stajano

Ask for ID

► **Establish**
absolute identity

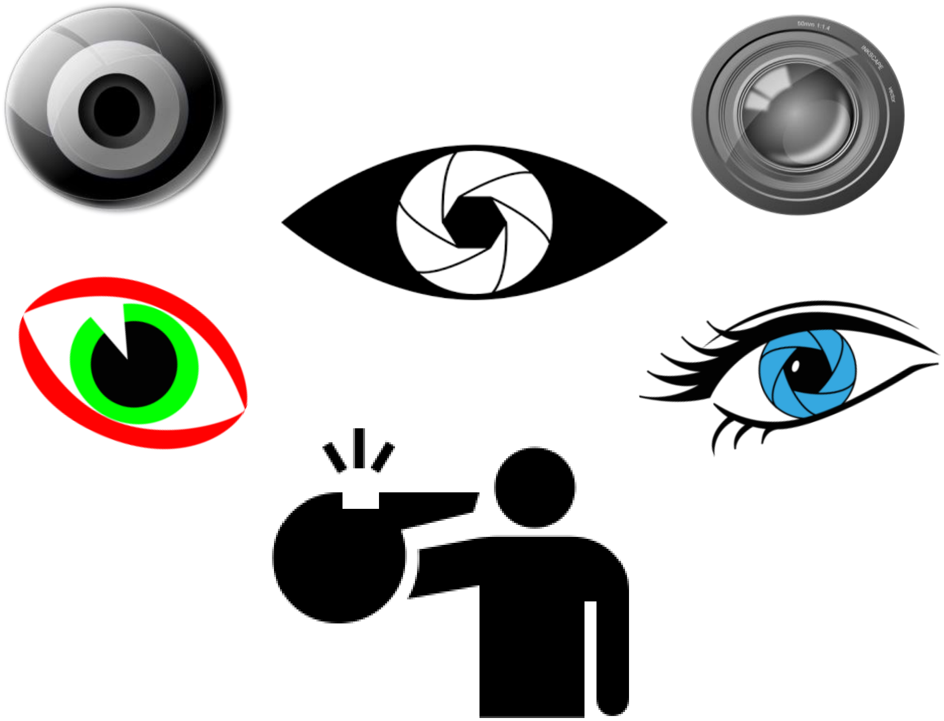
https://www.cl.cam.ac.uk/~fms27/

Frank Stajano, PhD *(filologo disneyano — I used to run a comics podcast)*

Professor of Security and Privacy

Department of Computer {Science and Technology} *(This new name encourages incorrect parsing. Read as "Department of the science and technology of computers", not as "Department of computer science (first topic) and of technology (second topic)".)*
Computer Laboratory, University of Cambridge
Security Group and Digital Technology Group

Motivation



Whistleblower may want to stay **anonymous**

► **Establish relative identity**

© 2023 Christina Atik for Human Rights Watch

HRW report: “All This Terror Because of a Photo”
Feb. 21 2023, p. 14

https://www.hrw.org/sites/default/files/media_2023/02/lgbt_mena0223web_0.pdf

https://www.hrw.org/news/2023/03/09/uganda-new-anti-gay-bill-further-threatens-rights

Motivation

General issue, **IRL** and **online**.

May mean **life or death** for *marginalized* groups.

New *trusted* relationships through **endorsements** by **people we already trust**.

https://zh.wikihow.com/%E4%BB%8B%E7%BB%8D%E5%88%AB%E4%BA%BA

Outline

- Motivation
- The Signal Protocol
- Safety Numbers
- A Trusted Introduction
- Open Questions

The Signal Protocol

Signal

WhatsApp

Secret
Encrypted Chat
on Messenger

Out-of-the-box *opportunistic encryption*

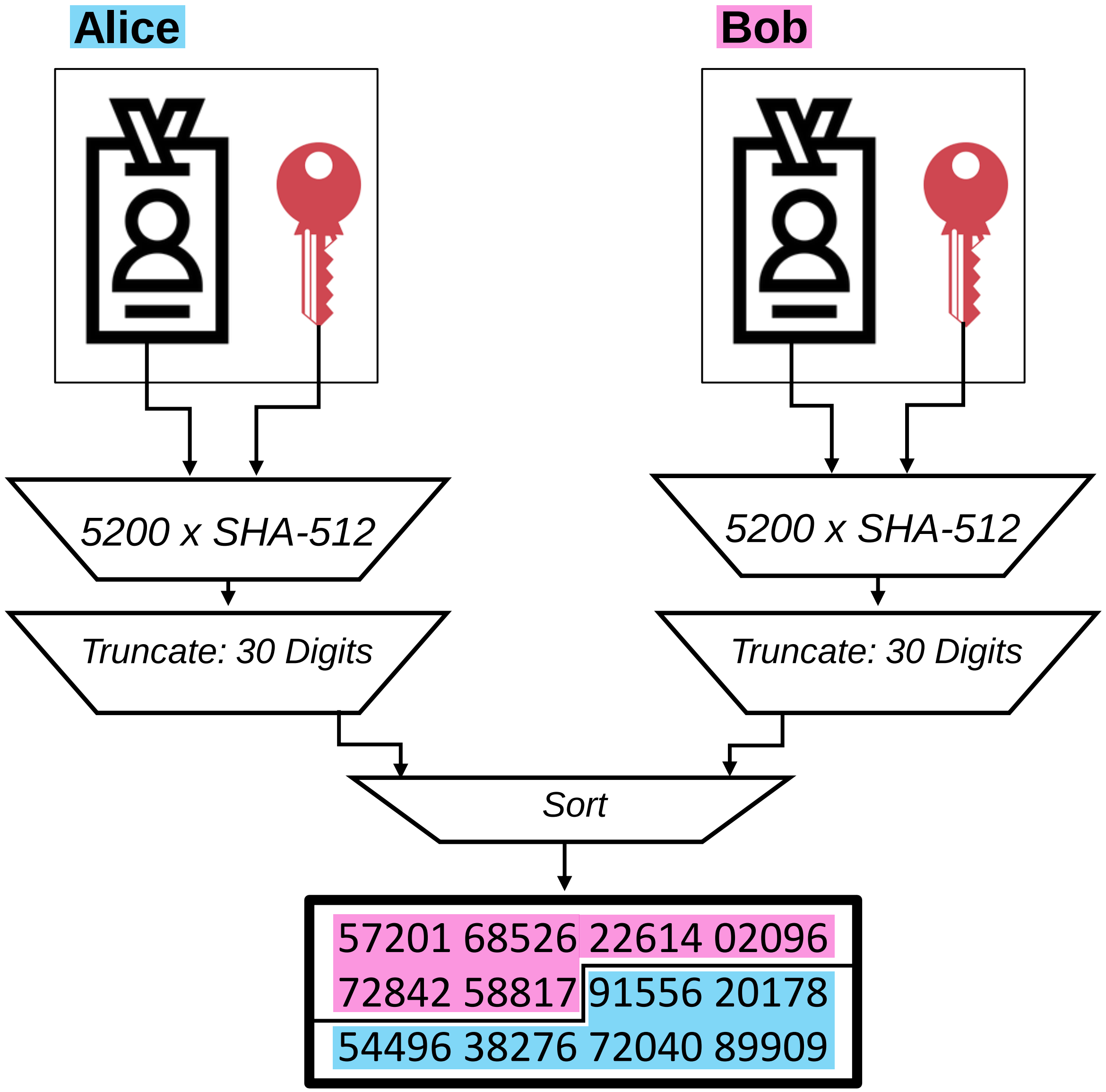
- Resist passive eavesdropping
- Perfect forward secrecy
- Repudiation
- Practical key revocations

No out-of-the-box *resistance against active attacks*

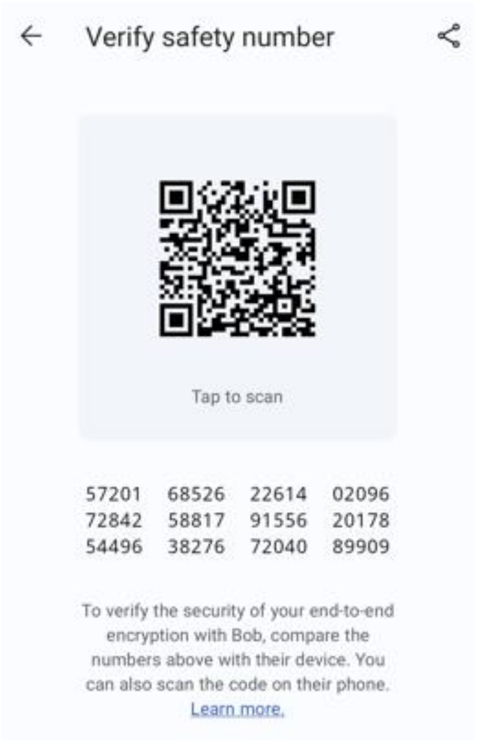
- Impersonation attacks
- Man in the middle attacks

► User must mitigate through out-of-band verification of per-conversation *safety number*

The Safety Number

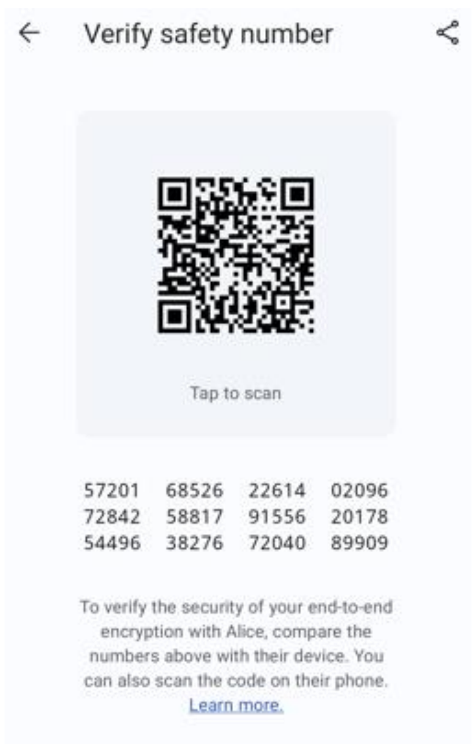


57201 68526 22614 02096
72842 58817 91556 20178
54496 38276 72040 89909



57201 68526 22614 02096
72842 58817 91556 20178
54496 38276 72040 89909

To verify the security of your end-to-end encryption with Bob, compare the numbers above with their device. You can also scan the code on their phone. Learn more.



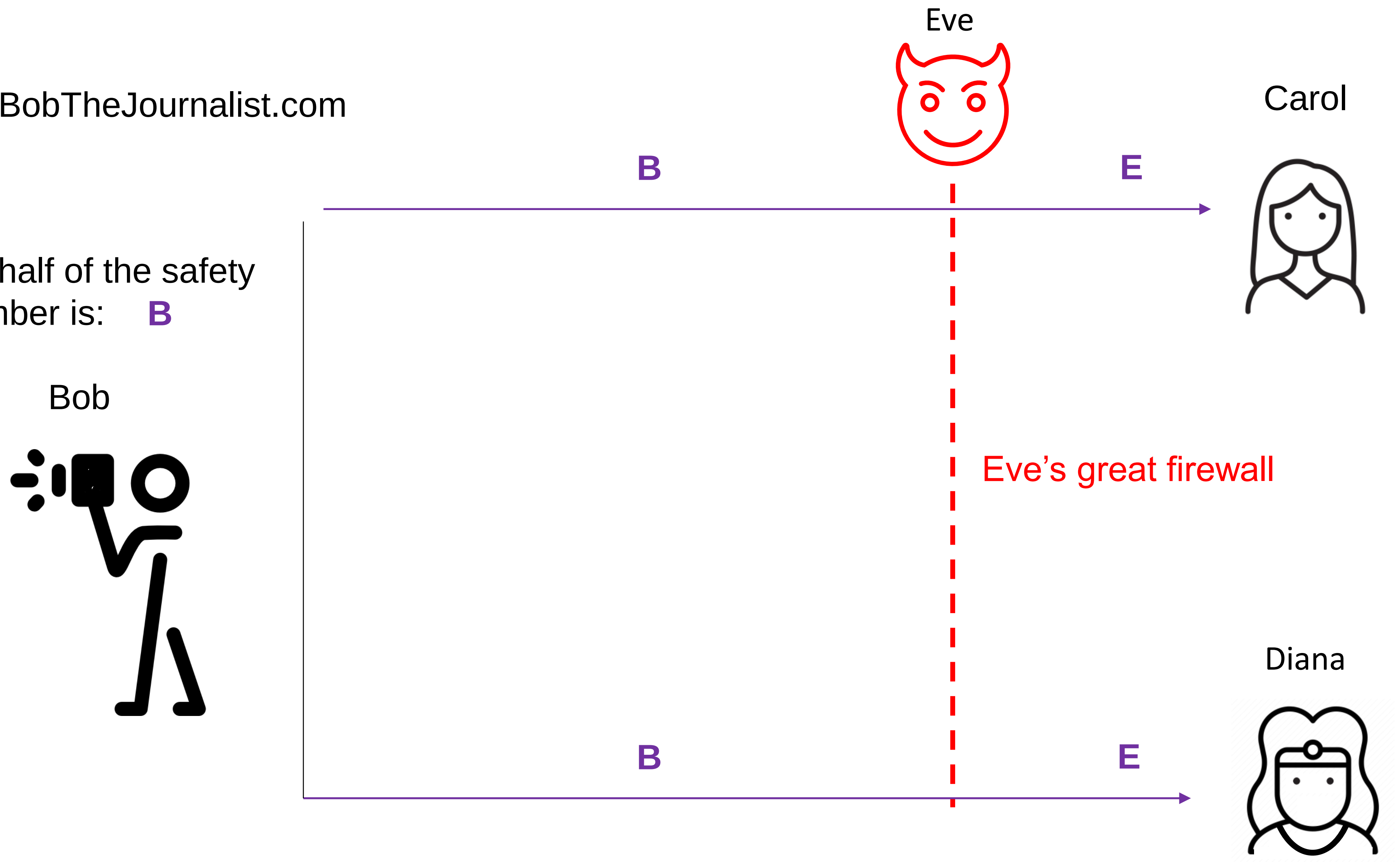
57201 68526 22614 02096
72842 58817 91556 20178
54496 38276 72040 89909

To verify the security of your end-to-end encryption with Alice, compare the numbers above with their device. You can also scan the code on their phone. Learn more.

How to securely initiate contact? **Safety numbers**

https://BobTheJournalist.com

My half of the safety number is: **B**

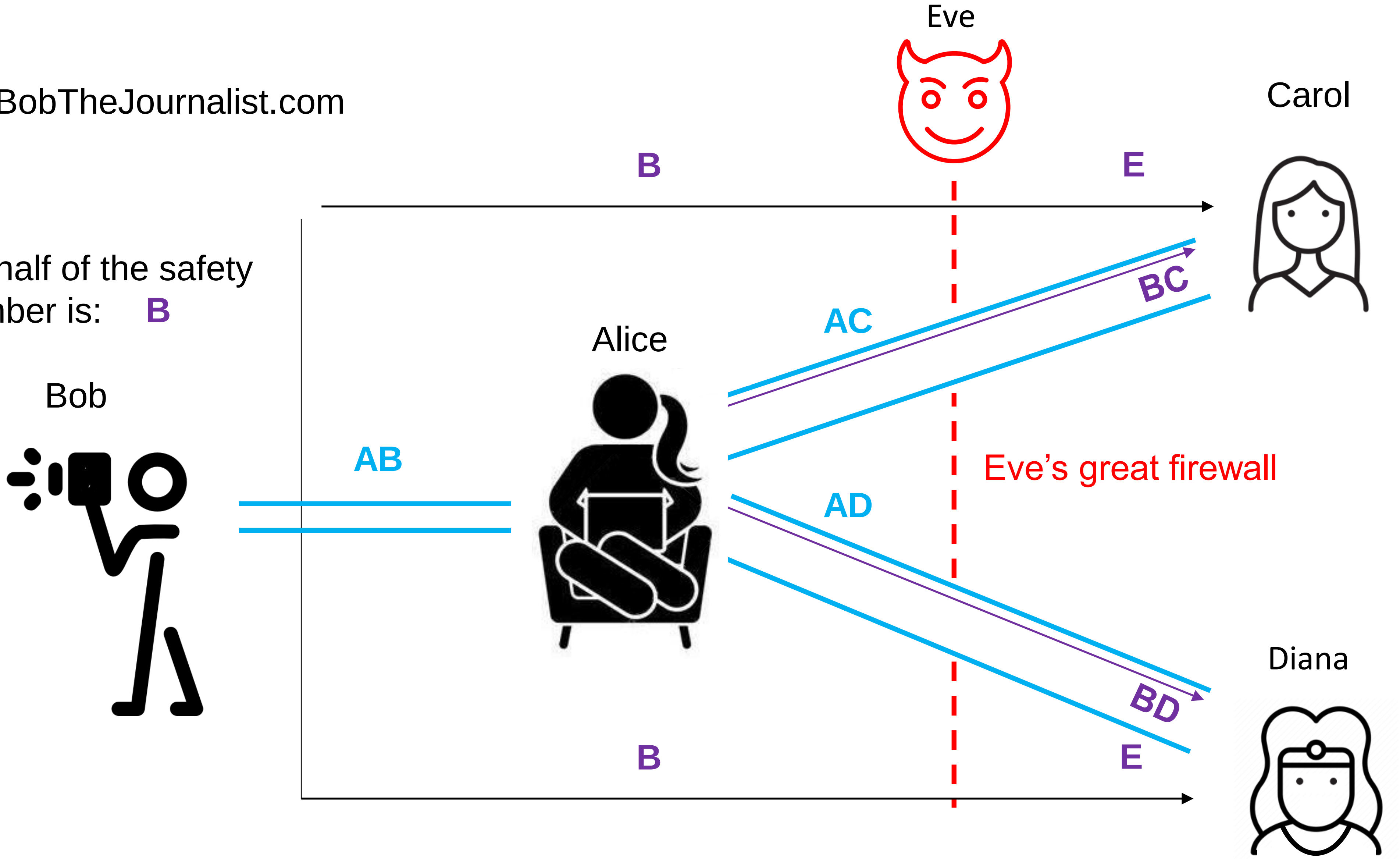


How to securely initiate contact?

Safety numbers

https://BobTheJournalist.com

My half of the safety number is: **B**



A Trusted Introduction

Demo!

A Trusted Introduction

Properties:

- *Relative* &
- *Ephemeral* trust
- Introducer information may be purged (*anonymous introduction*)
- On key change: user can query list of *named introductions* and request a refresh
- *User controls* sharing of information

► Process mirrors **real-world human interactions**

► Trustworthiness of introduction is anchored in *preexisting trust-relationship* with the *introducer*

Open Questions

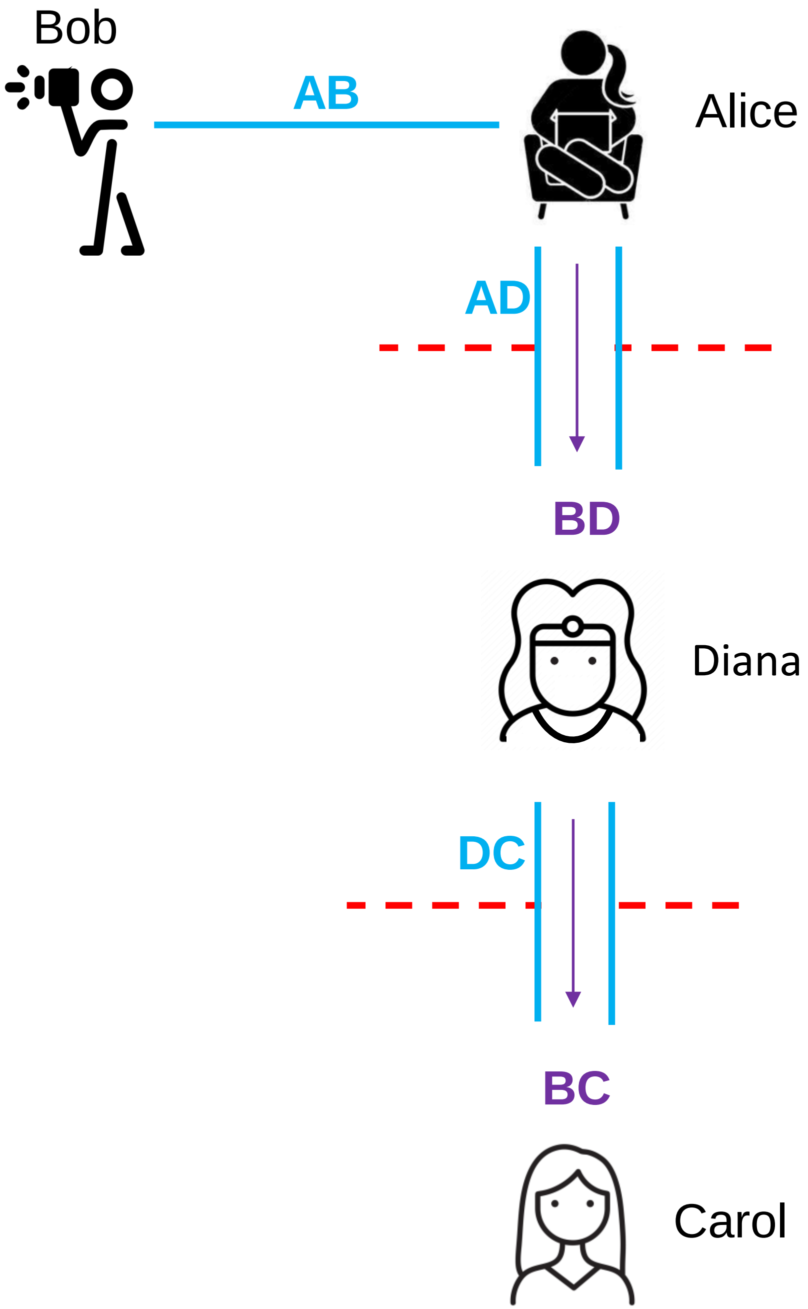
1. Introduction Chains?

   Safety & sound reasoning ↔ accessibility

2. How much can/should we automate?

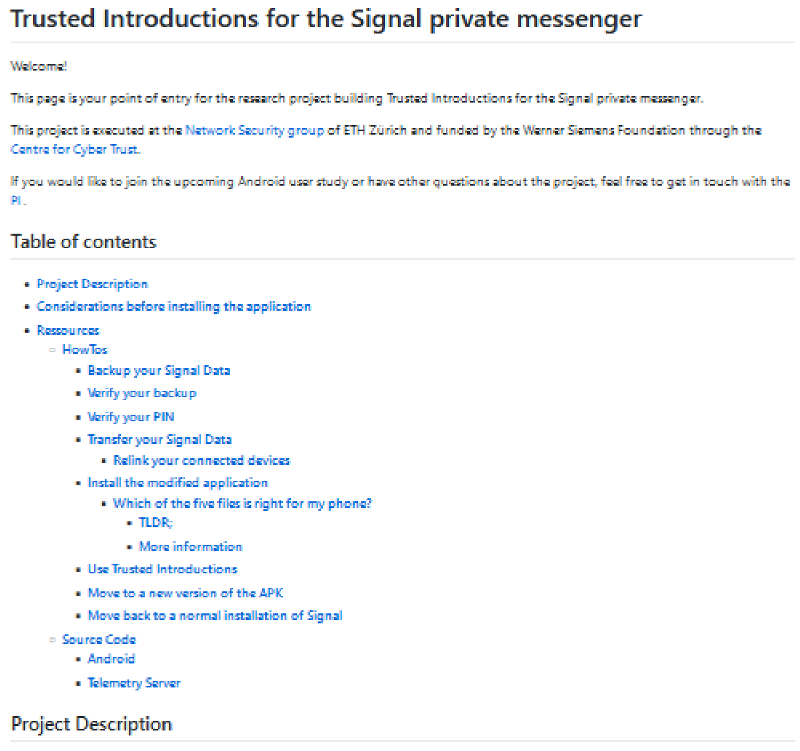
3. How to approach threat communication?

4. Could gamification help speed up adoption?



Join the fun!

https://trusted-introductions.github.io/



Trusted Introductions for the Signal private messenger

Welcome!

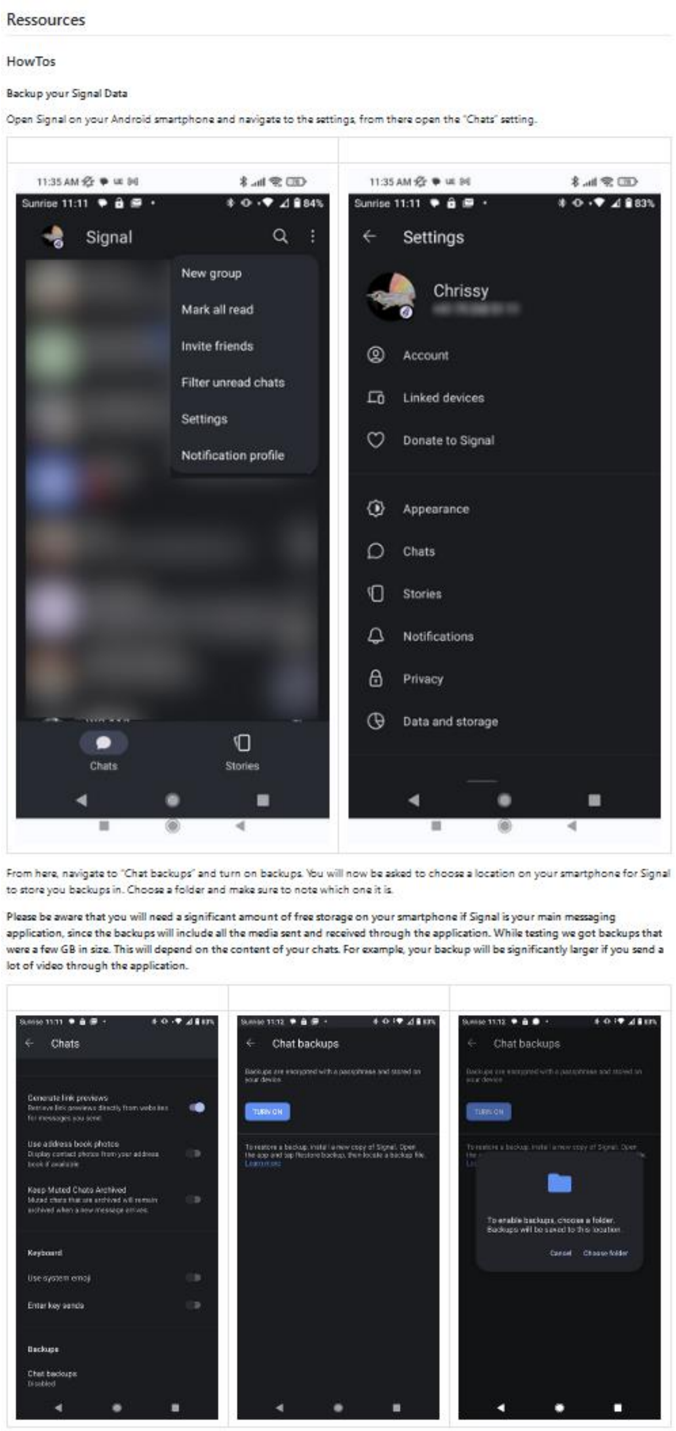
This page is your point of entry for the research project building Trusted Introductions for the Signal private messenger.

This project is executed at the Network Security group of ETH Zürich and funded by the Werner Siemens Foundation through the Centre for Cyber Trust.

If you would like to join the upcoming Android user study or have other questions about the project, feel free to get in touch with the PI .

Table of contents

Project Description



Ressources

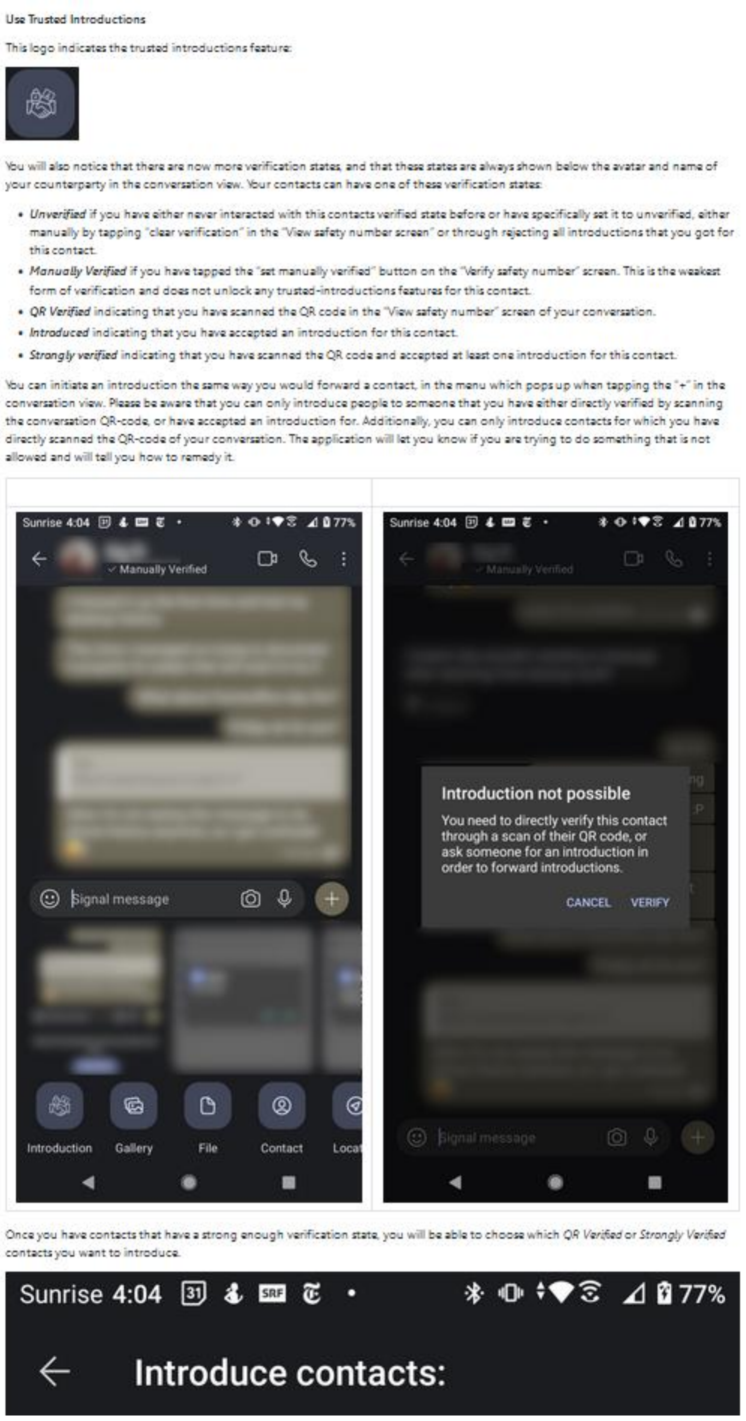
HowTos

Backup your Signal Data

Open Signal on your Android smartphone and navigate to the settings, from there open the "Chats" setting.

From here, navigate to "Chat backups" and turn on backups. You will now be asked to choose a location on your smartphone for Signal to store you backups in. Choose a folder and make sure to note which one it is.

Please be aware that you will need a significant amount of free storage on your smartphone if Signal is your main messaging application, since the backups will include all the media sent and received through the application. While testing we got backups that were a few GB in size. This will depend on the content of your chats. For example, your backup will be significantly larger if you send a lot of video through the application.



Use Trusted Introductions

This logo indicates the trusted introductions feature:

You will also notice that there are now more verification states, and that these states are always shown below the avatar and name of your counterparty in the conversation view. Your contacts can have one of these verification states:

- *Unverified* if you have either never interacted with this contacts verified state before or have specifically set it to unverified, either manually by tapping "clear verification" in the "View safety number screen" or through rejecting all introductions that you got for this contact.
- *Manually Verified* if you have tapped the "set manually verified" button on the "Verify safety number" screen. This is the weakest form of verification and does not unlock any trusted-introductions features for this contact.
- *QR Verified* indicating that you have scanned the QR code in the "View safety number" screen of your conversation.
- *Introduced* indicating that you have accepted an introduction for this contact.
- *Strongly verified* indicating that you have scanned the QR code and accepted at least one introduction for this contact.

You can initiate an introduction the same way you would forward a contact, in the menu which pops up when tapping the "+" in the conversation view. Please be aware that you can only introduce people to someone that you have either directly verified by scanning the conversation QR-code, or have accepted an introduction for. Additionally, you can only introduce contacts for which you have directly scanned the QR-code of your conversation. The application will let you know if you are trying to do something that is not allowed and will tell you how to remedy it.

Sunrise 4:04
77%
Manually Verified
Signal message
Introduction
Gallery
File
Contact
Loca
Introduction not possible
You need to directly verify this contact through a scan of their QR code, or ask someone for an introduction in order to forward introductions.
CANCEL
VERIFY

Once you have contacts that have a strong enough verification state, you will be able to choose which *QR Verified* or *Strongly Verified* contacts you want to introduce.

Thank you!

Christelle Gloor
CAB F81
Universitätstrasse 6
8092 Zürich
christelle.gloor@inf.ethz.ch

Adrian Perrig
CAB F85.1
Universitätstrasse 6
8092 Zürich
adrian.perrig@inf.ethz.ch