CISPA
HELMHOLTZ CENTER FOR
INFORMATION SECURITY

Who am I?

Me

- *Masters in Computer Engineering from TU Wien*
- *Doctoral researcher at CISPA Helmholtz Center in Saarbrücken*

- *Usable Security and Privacy Research*
  - **E2EE Messaging**
  - **Secure Experience Design**
  - **Social Cybersecurity**

Saarbrücken, Germany

Traineeship in the European Commission: Cybercrime Policy

- CSAM regulation ‘*Chatkontrolle*’
- Data retention
- Anonymization, VPNs, Private Relay
- Law enforcement access to encrypted data
- Online Fraud

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

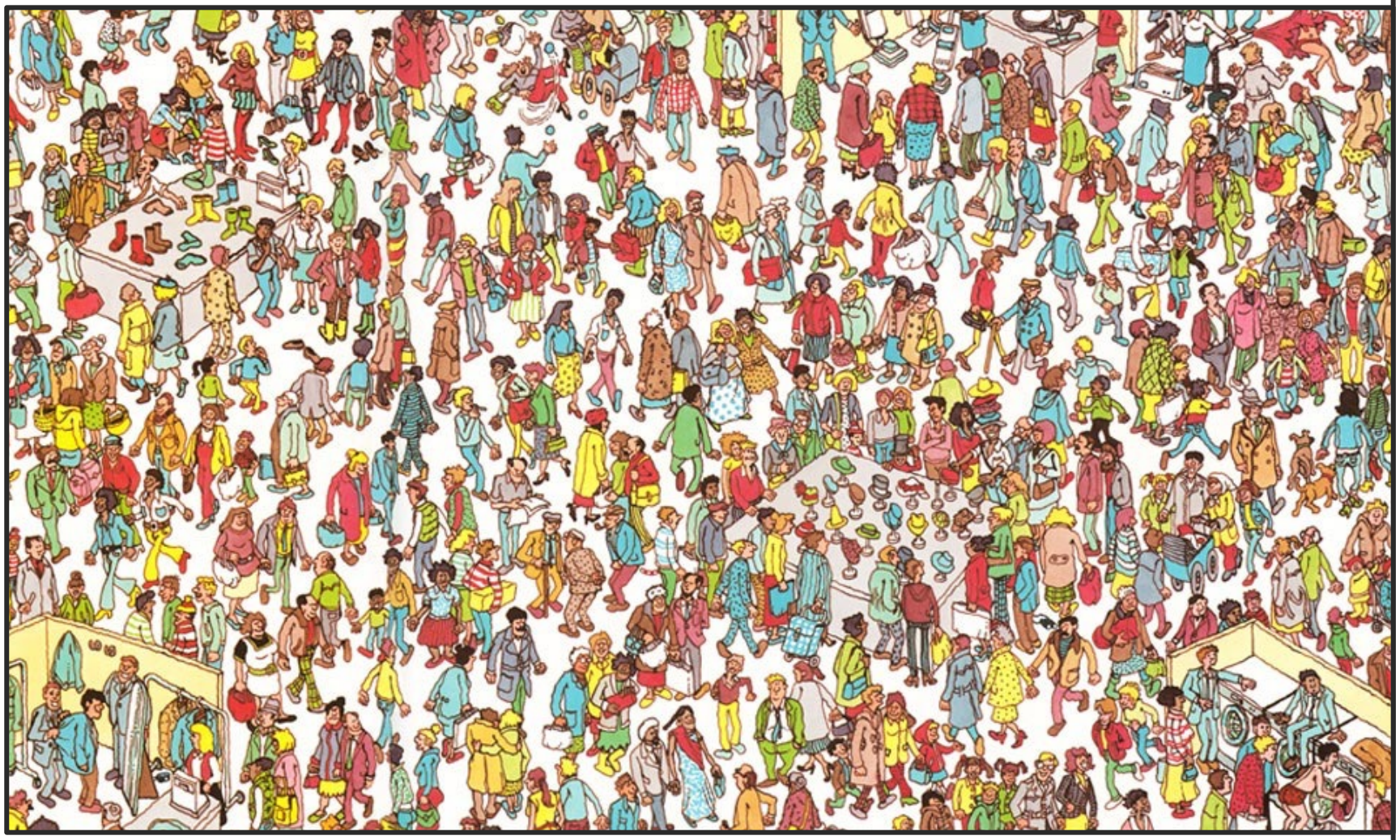
The Tor over VPN Phenomenon

A Case Study

Matthias Fassl
Alexander Ponticello
Adrian Dabrowski
Katharina Krombholz

Low-Latency Anonymity Network

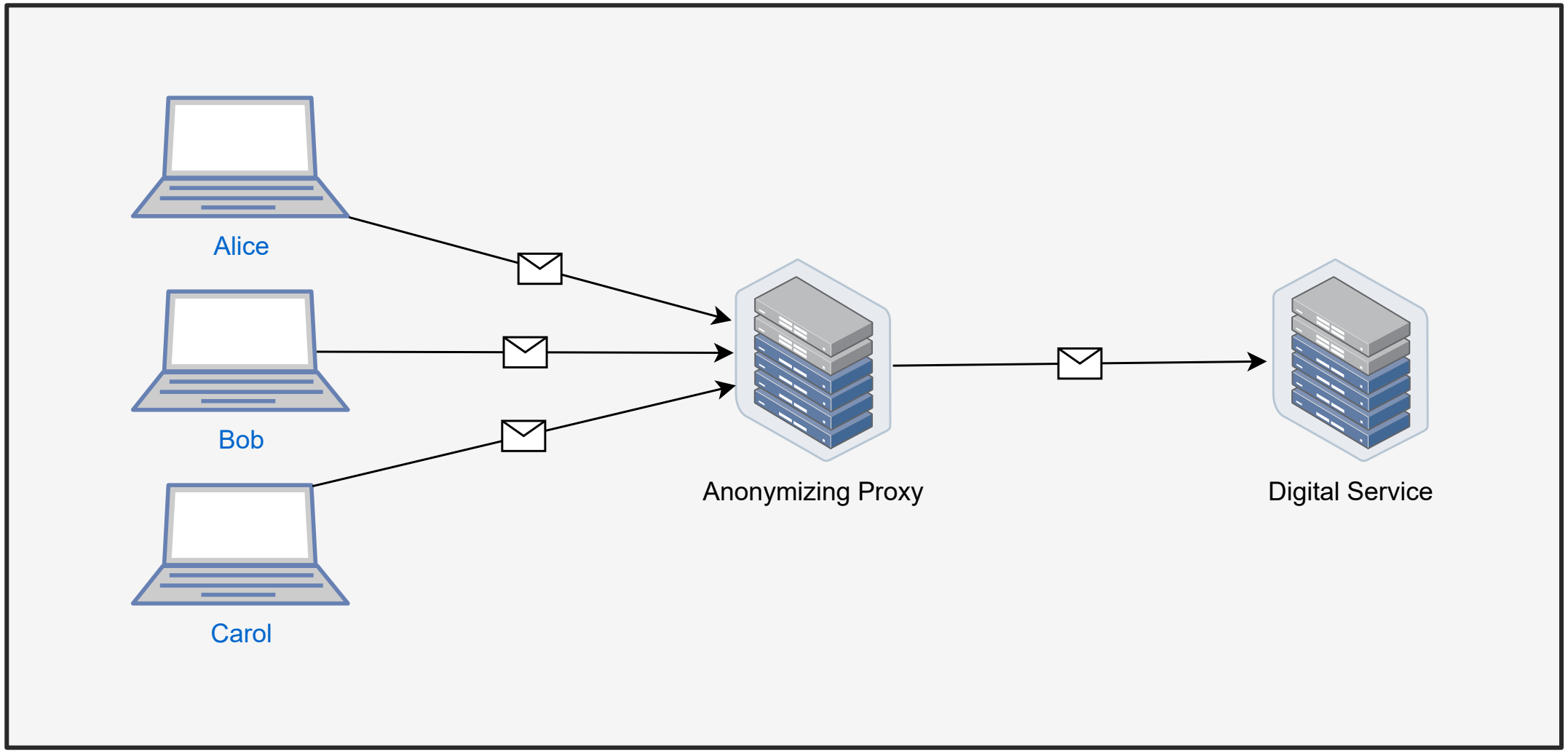
Anonymity Loves Company



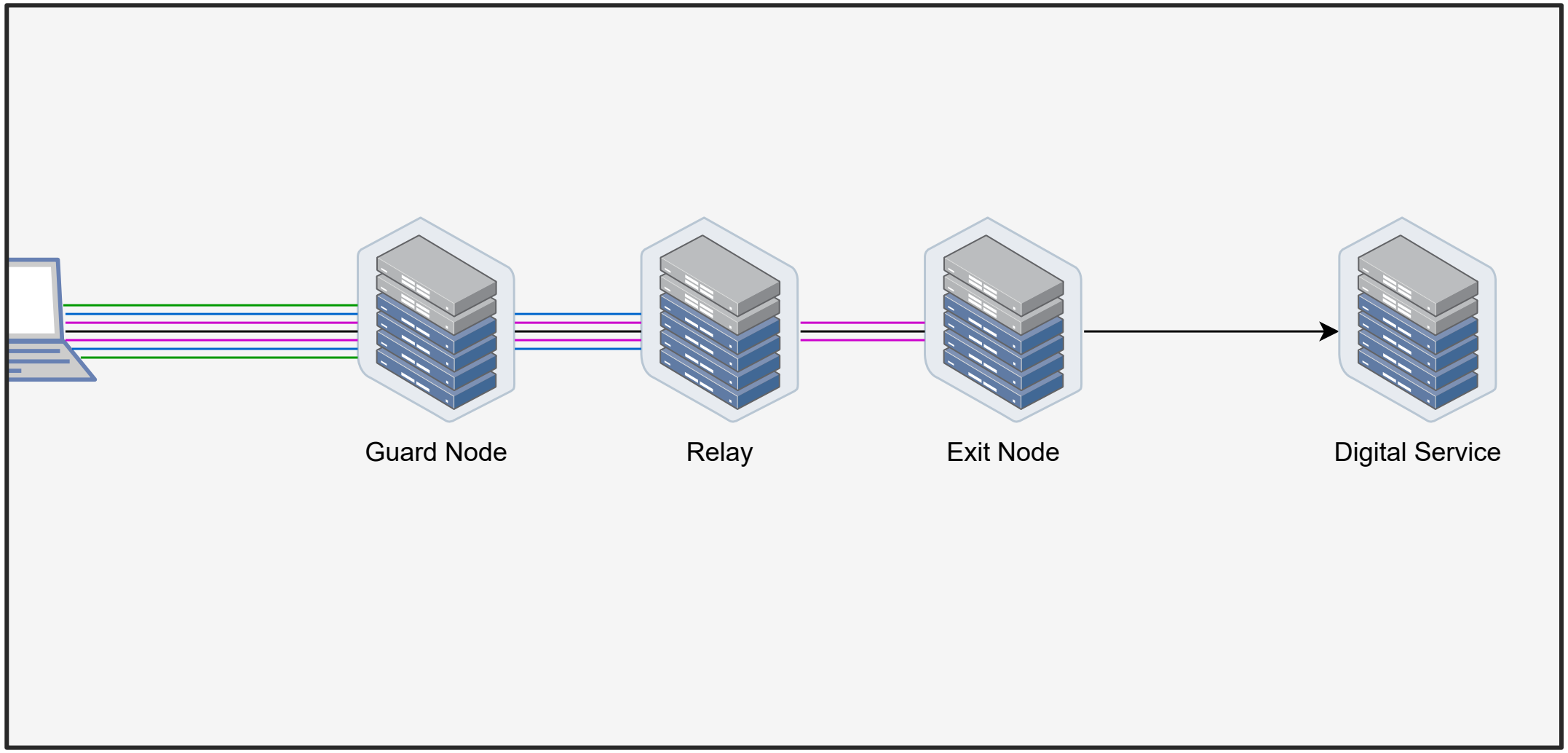
Hiding in a large *anonymity set*

requires that everyone appears and behaves in the same way

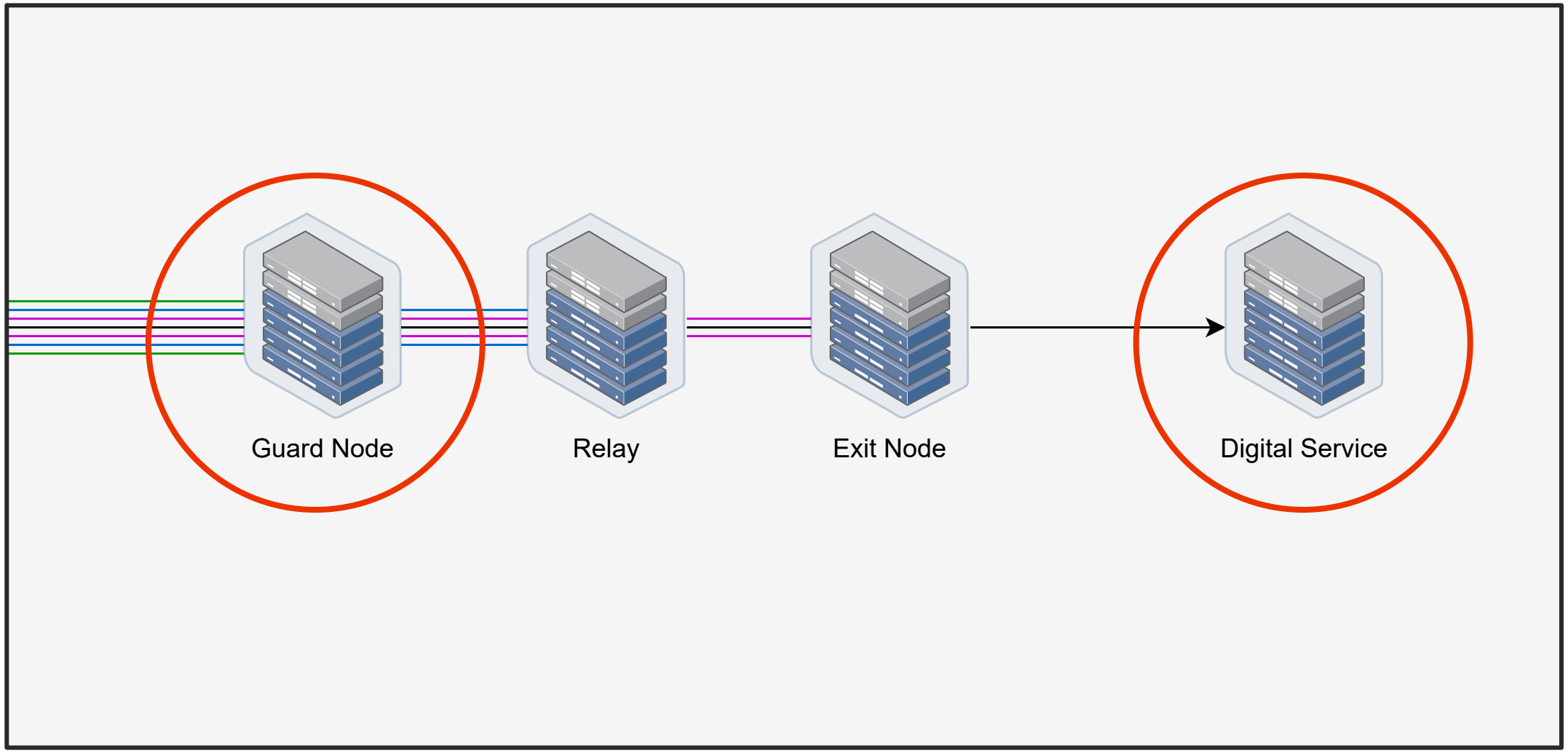
Anonymizing Proxy



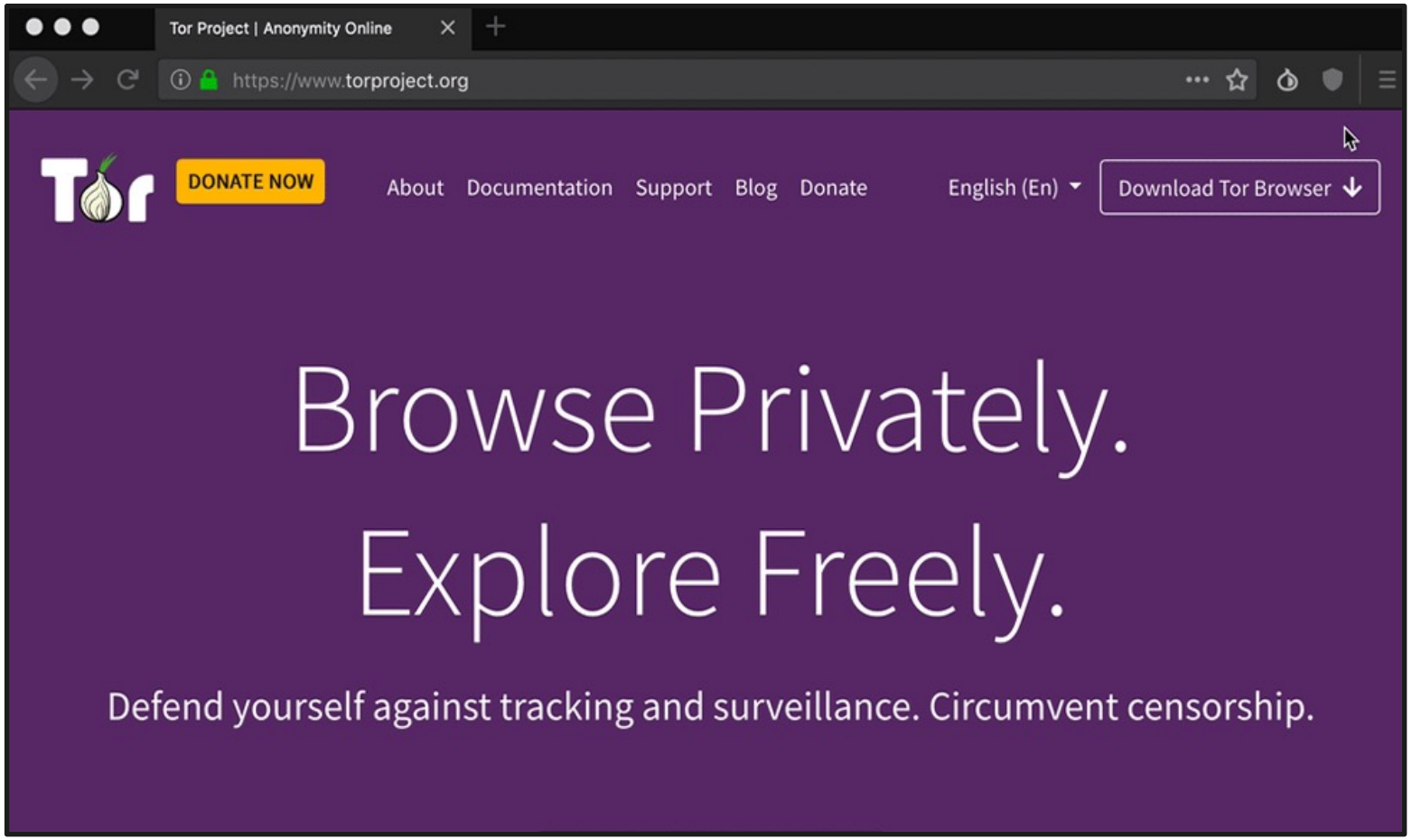
Onion Routing



Timing Attacks

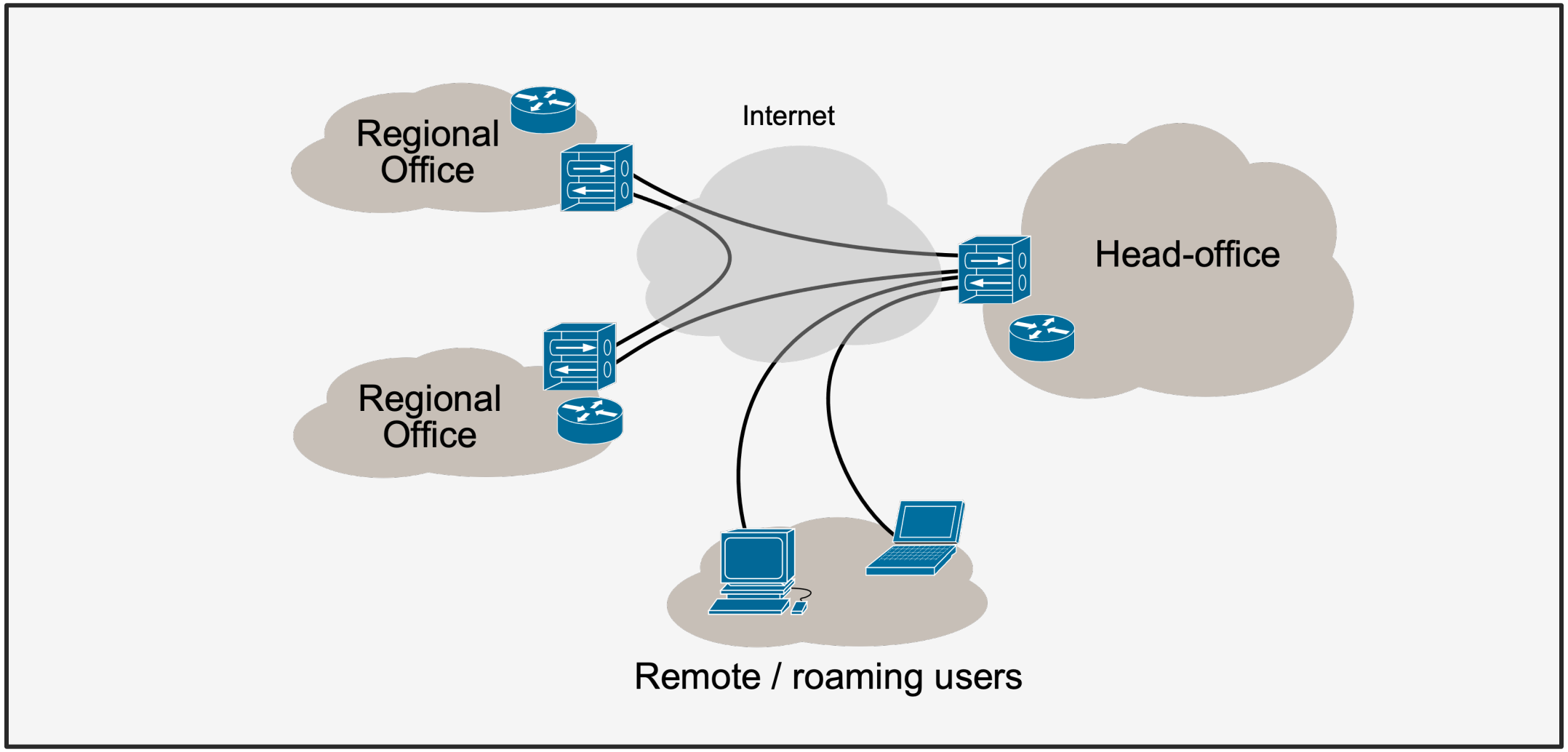


Fingerprinting



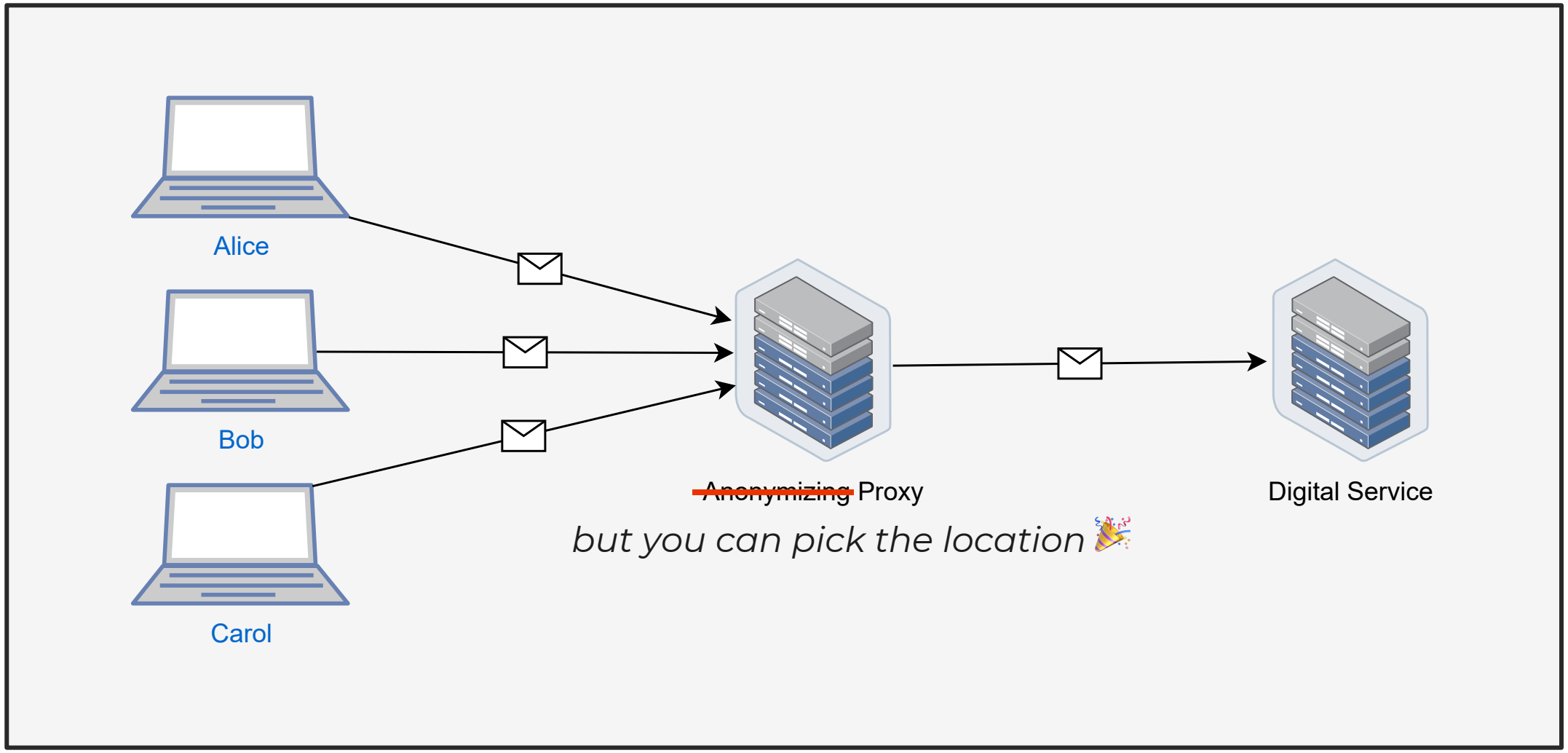
Virtual Private Network

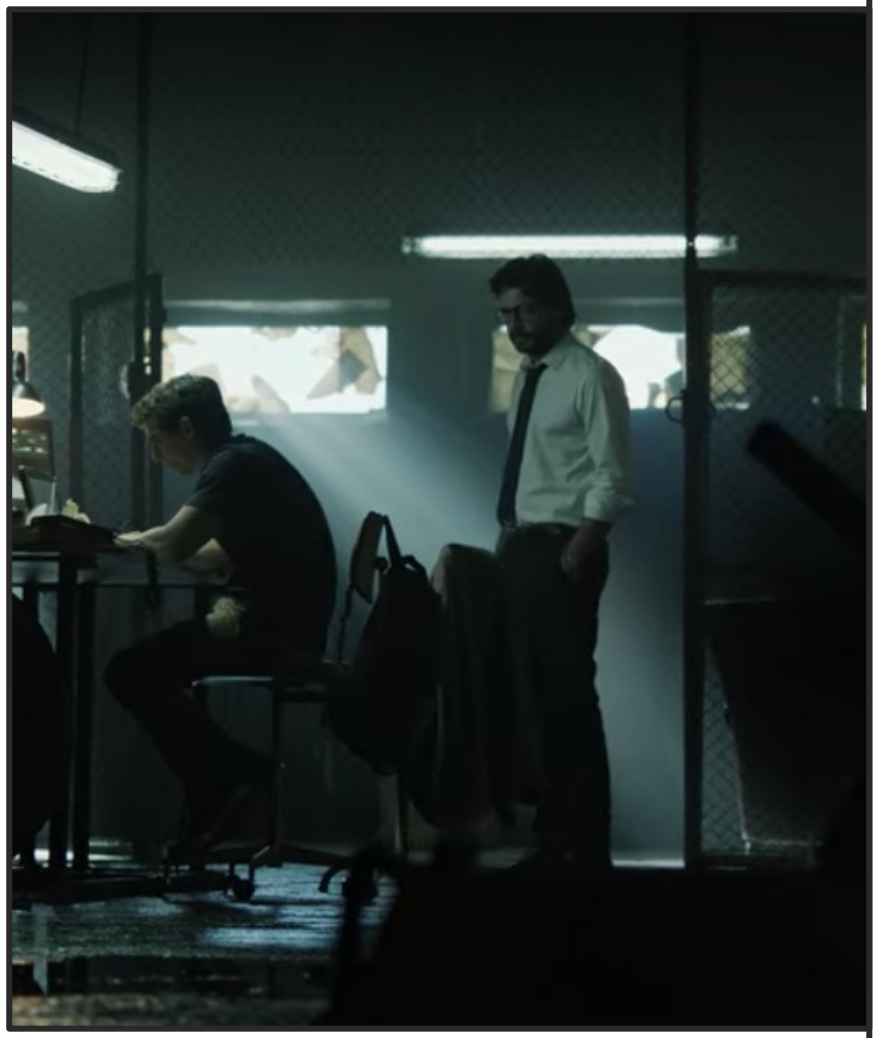
Traditional Idea of VPNs



Commercial Consumer VPNs

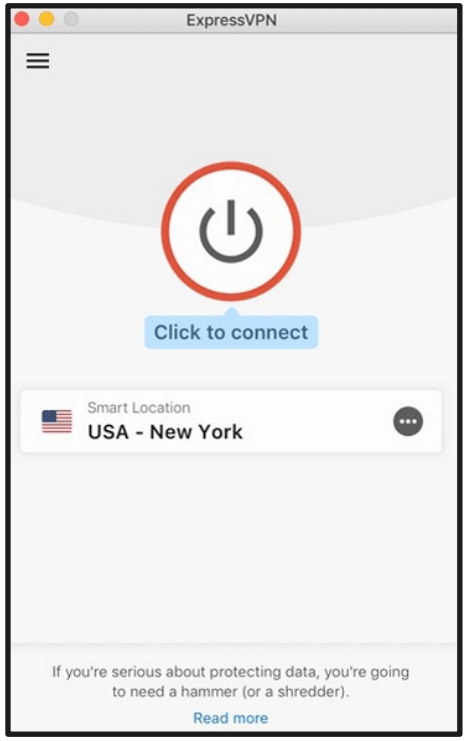
Consumer VPNs



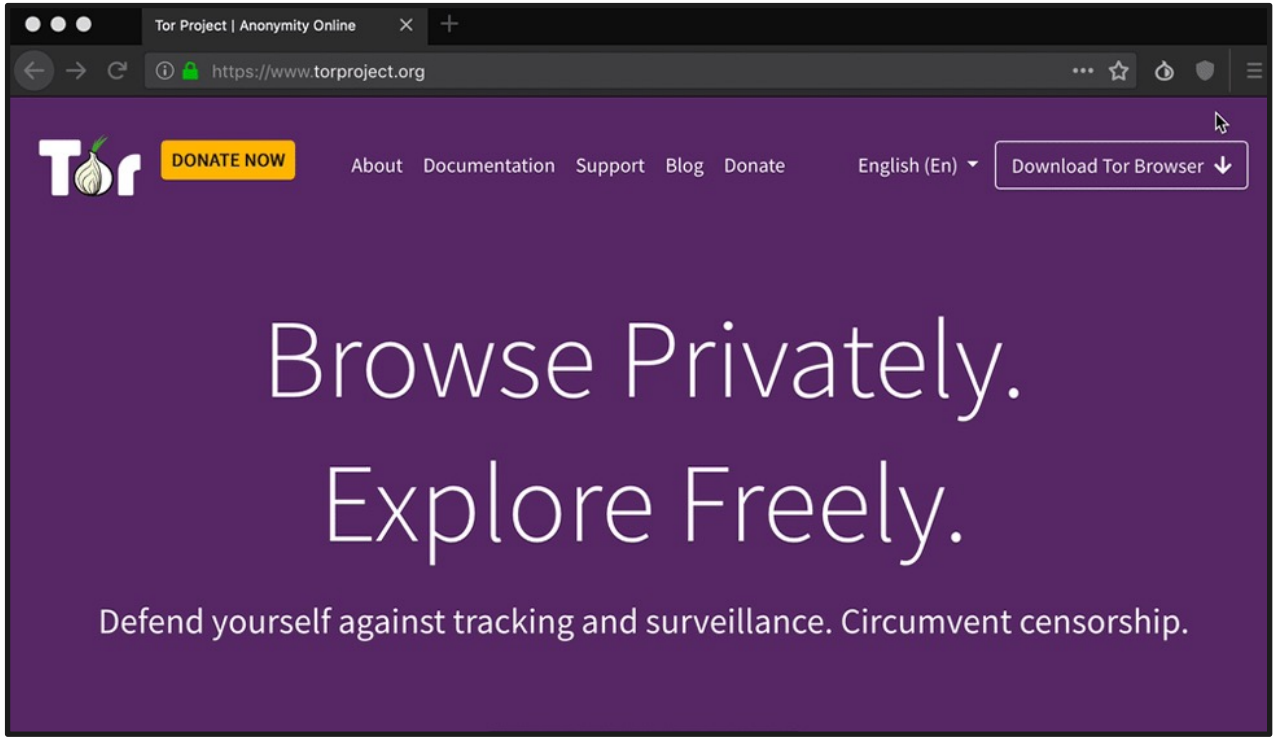


Tor over VPN

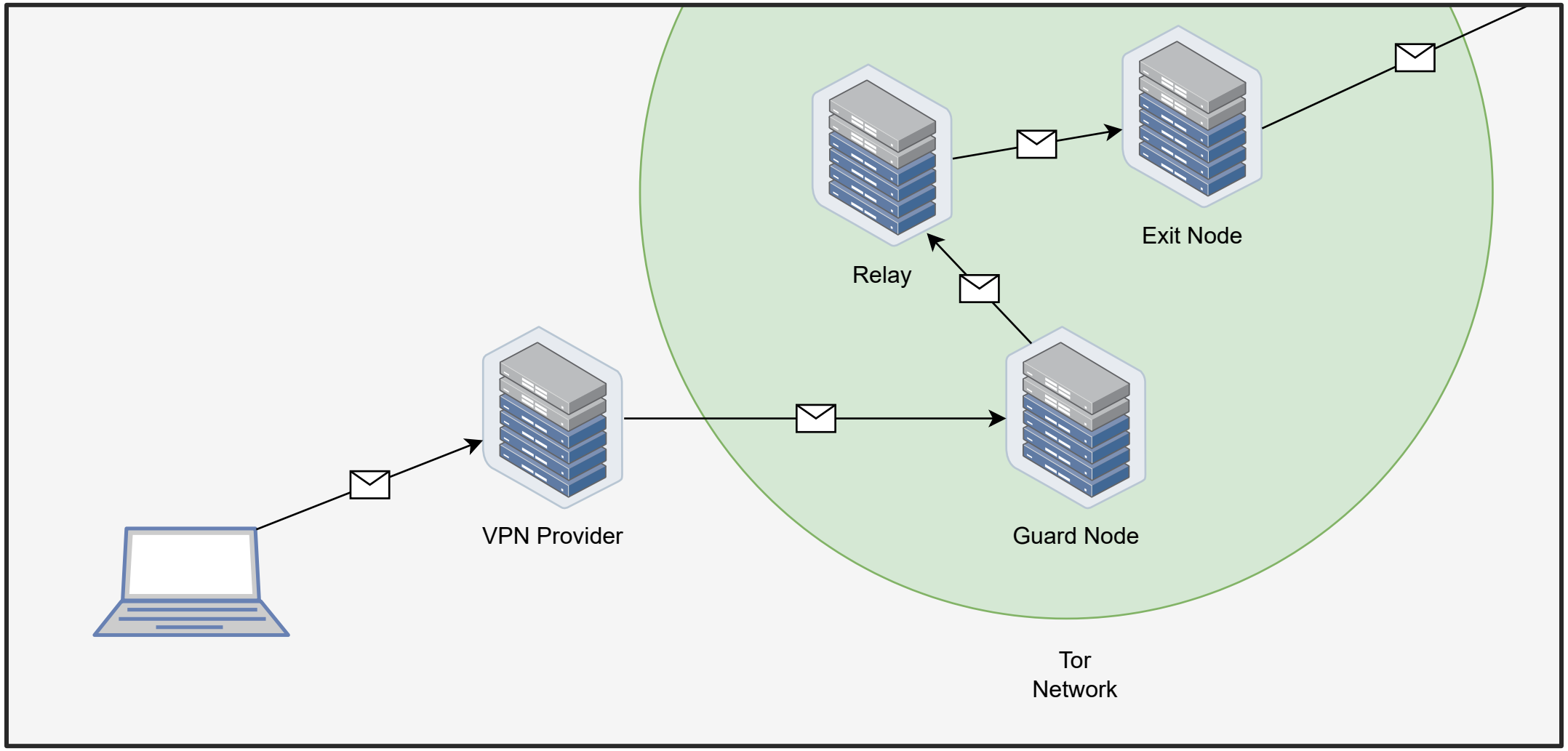
Tor over VPN


ExpressVPN
Click to connect
Smart Location
USA - New York
If you're serious about protecting data, you're going to need a hammer (or a shredder).
Read more

+


Tor Project | Anonymity Online
https://www.torproject.org
DONATE NOW
About
Documentation
Support
Blog
Donate
English (En)
Download Tor Browser
Browse Privately.
Explore Freely.
Defend yourself against tracking and surveillance. Circumvent censorship.

Effect of Tor over VPN



Is Tor over VPN useful?

Censorship

Hide Tor Use

Malicious Guard Node

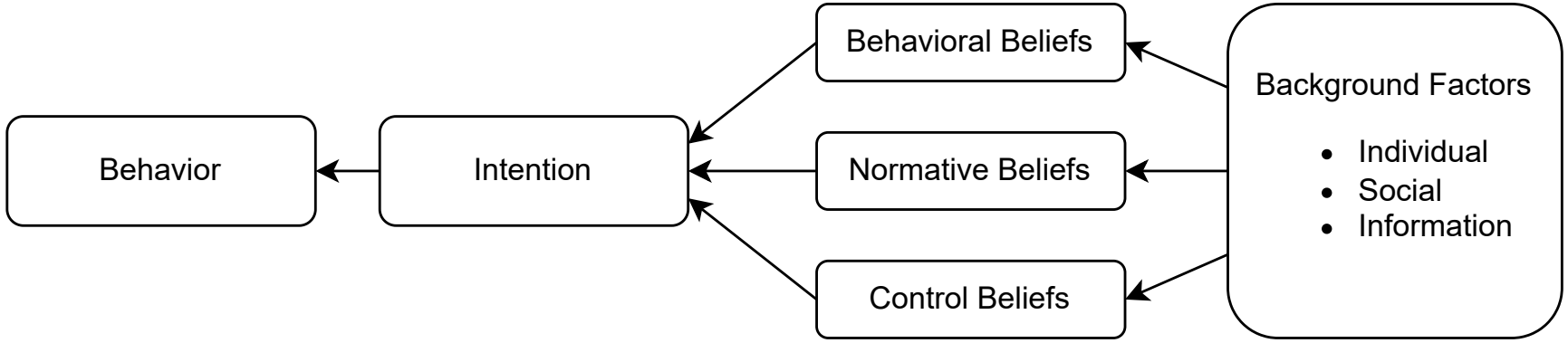
Is Tor over VPN useful?

Censorship

Hide Tor Use

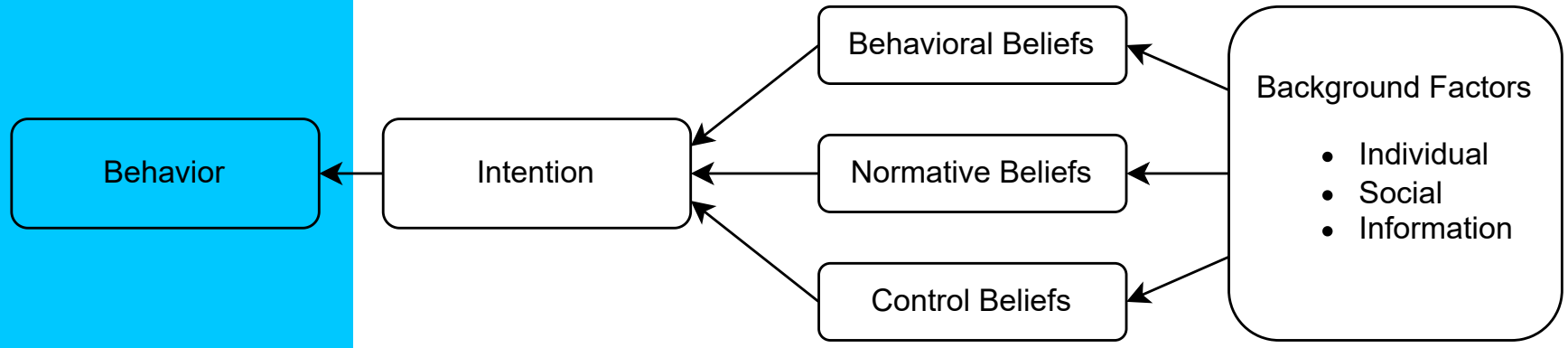
Malicious Guard Node

Theory of Reasoned Action



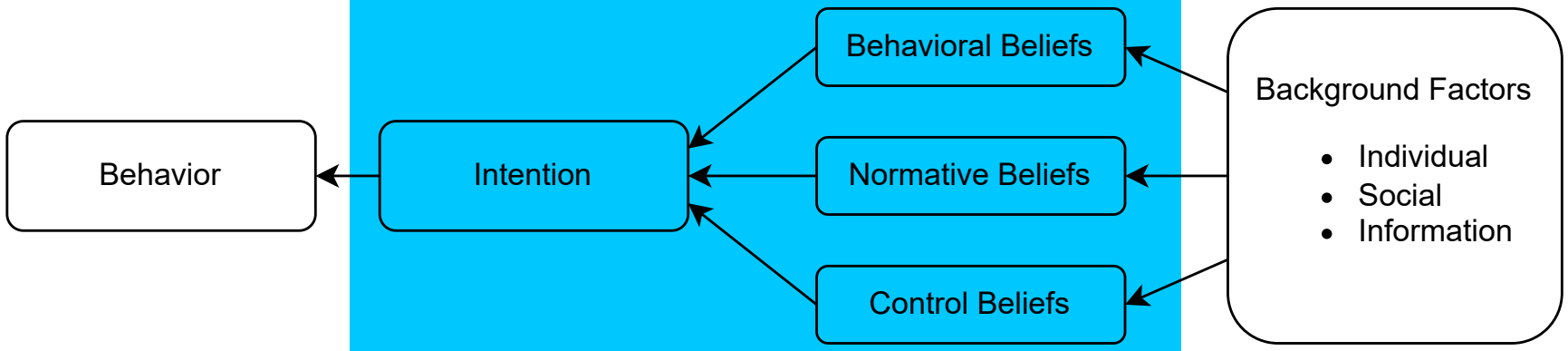
MEASUREMENT

Theory of Reasoned Action



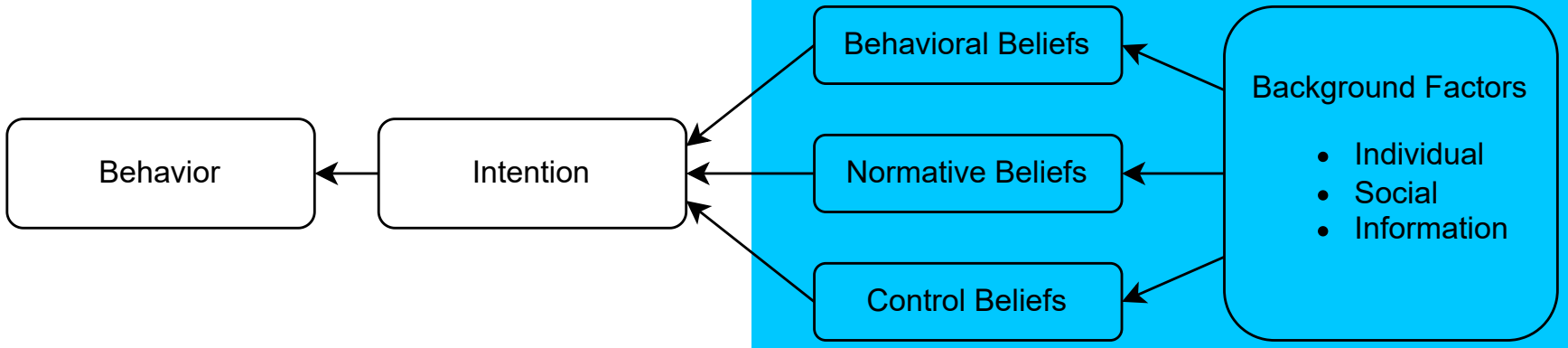
USER SURVEY

Theory of Reasoned Action



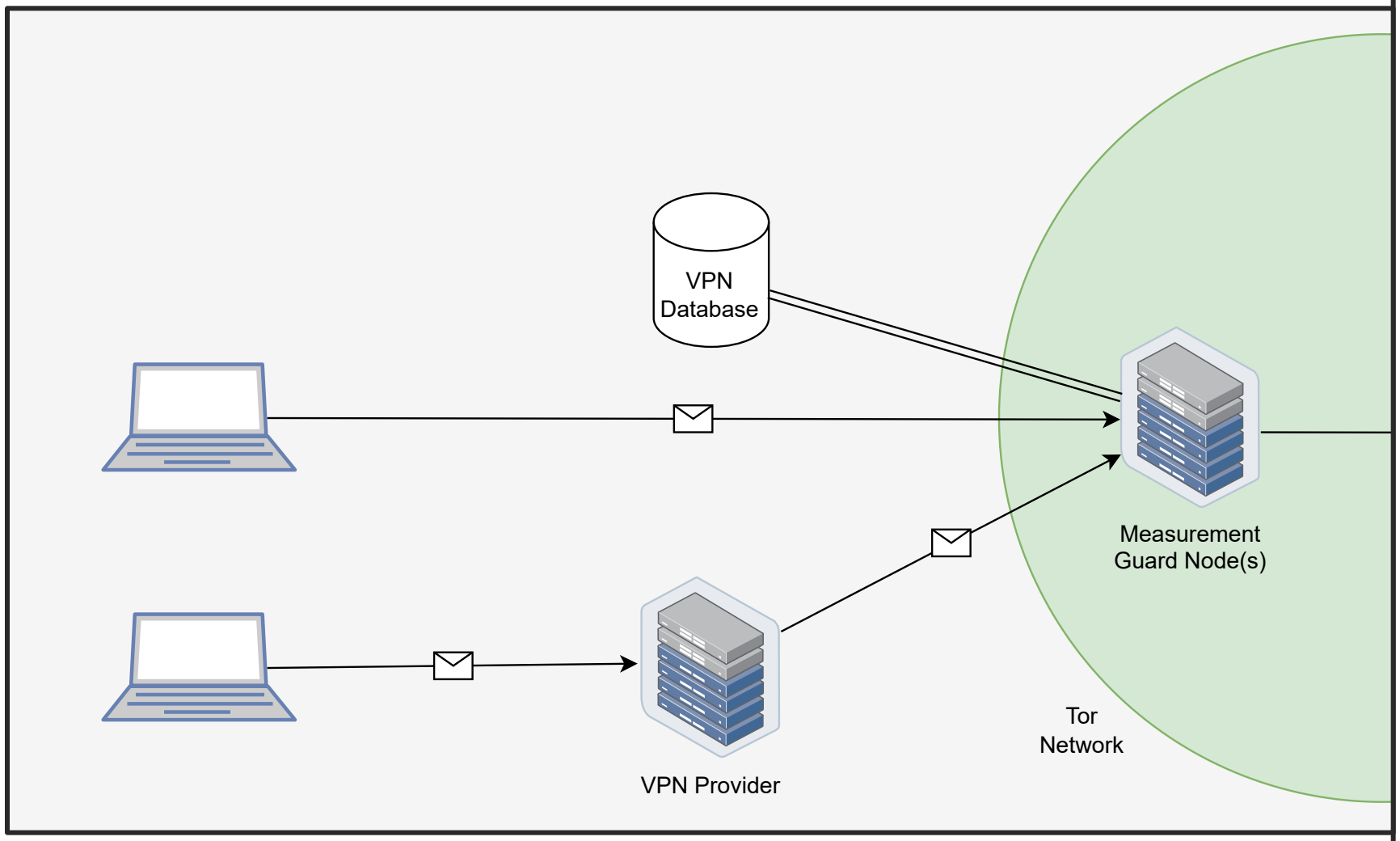
DOCUMENT ANALYSIS

Theory of Reasoned Action



MEASUREMENT

Behavior Measurement



1% of Tor's entire guard bandwidth

5 - 6% of connections to the Tor network come from VPN servers

USER SURVEY

Users' Intention

$\frac{2}{3}$	$\frac{1}{3}$
Used VPN specifically to access Tor *intentional*	Always used a VPN *unintentional*

Users' Beliefs

Normative Beliefs	Behavioral Beliefs
"After conducting some research, I found it improves your privacy and security" (P74)	*Protection from "unsavory characters" (P102) on the Tor network*
	Control Beliefs
	"I might as well set up as many safeguards as I can" (P73)

DOCUMENT ANALYSIS

Information Sources

Online newspapers
16 most read in US
and Germany

Social Media
Reddit, Twitter,
StackExchange

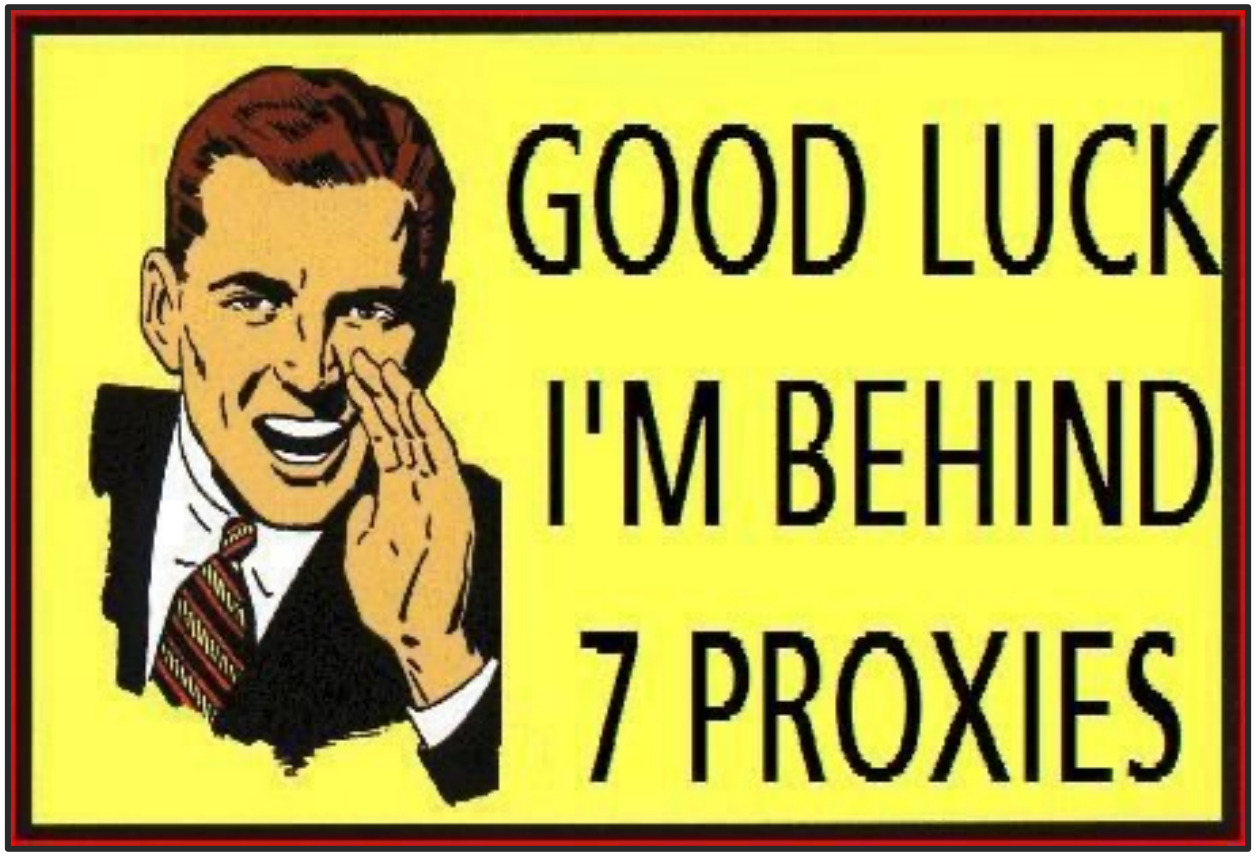
VPN Providers
20 most popular

Doing everything in a list of security practices	Tor Browser is “just” a privacy-preserving browser
“many Russians were skilled at using it [Tor] and VPNs [for evading censorship]” (News932:2)	*“Get a VPN, download tor or DuckDuckGo [Privacy Browser]” (Twitter1000:33)*

Perceived Social Norms

The cool kids are already using Tor over VPN *For people who are "very serious about browsing anonymity" (VPN43:2)* *"is popular among computer-savy circles" (News913:2)*	**Assumed general practice** *"Pretty sure most Tor users do [use both at the same time]" (Redddit708:6)* **Recommendation without justification** *"Tor + VPN is a good combo" (Reddit708:5)*

Security-Related Meme References



SUMMARY

Summary

- Users expect general security and privacy benefits
- Misconceptions of technology shape behavior
- Normative beliefs contribute to spread
- Giving effective security and privacy advice is hard

Check our blog post

https://medium.com/acm-cscw/4d2db91bfecc

Matthias Fassl
@n0gat

Alexander Ponticello
@alip0nti

Adrian Dabrowski
@atrox_at

Katharina Krombholz
@cathykxx

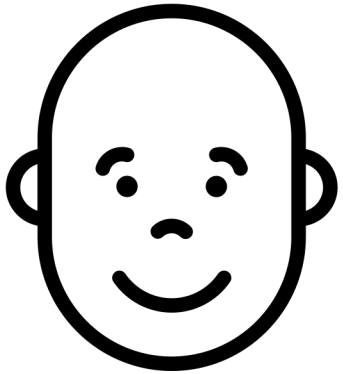
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

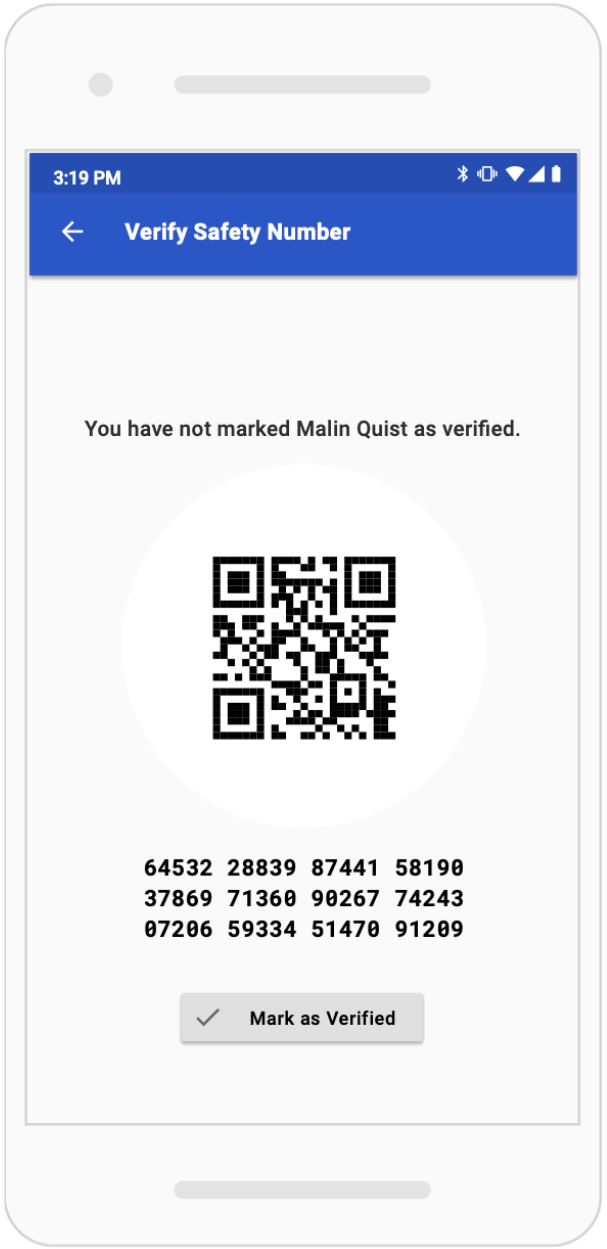
Why ~~Johnny~~ I Can't Authenticate

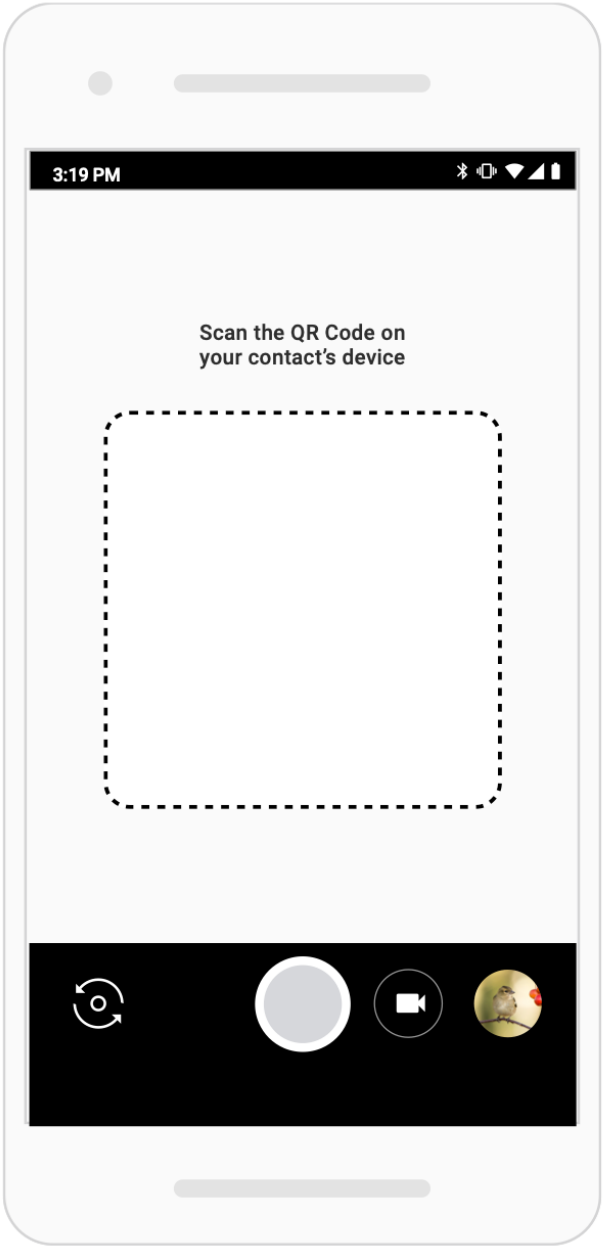
Understanding the Low Adoption of Authentication Ceremonies with Autoethnography

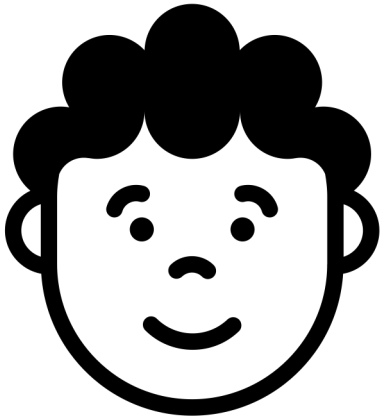
Matthias Fassl
Katharina Krombholz

What are Authentication Ceremonies in E2EE Messengers?

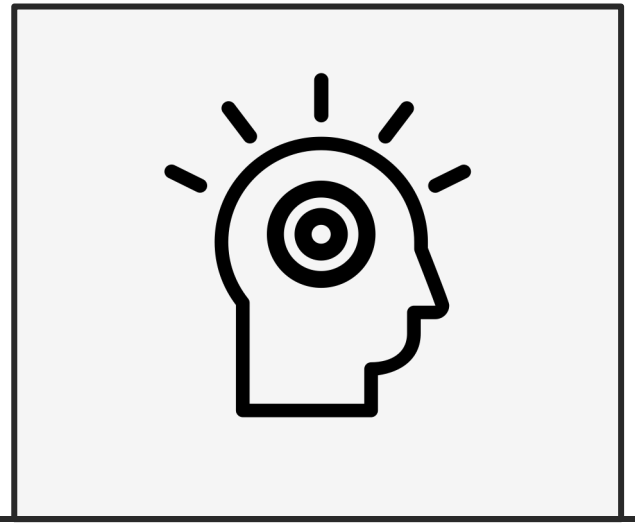




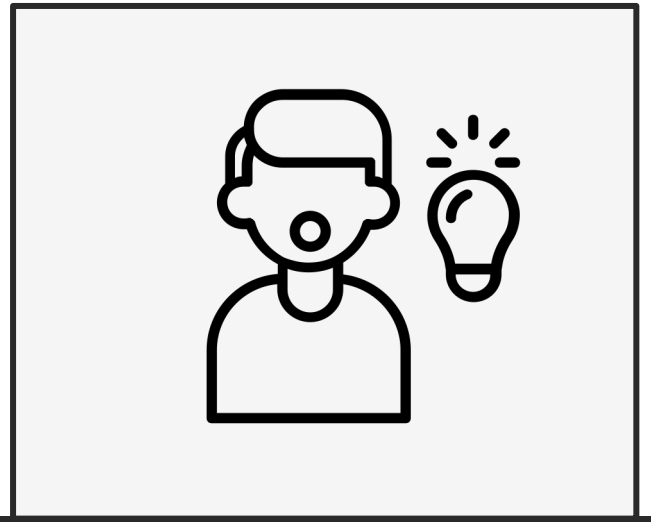




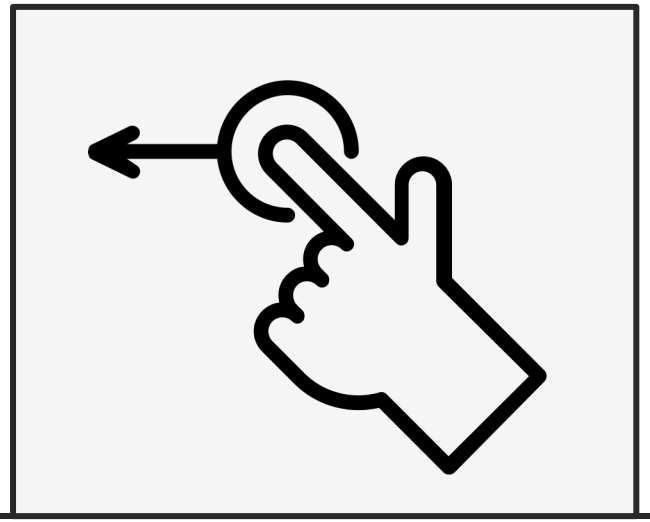
Known Issues with Authentication Ceremonies



Users are not aware of them



Users do not understand purpose



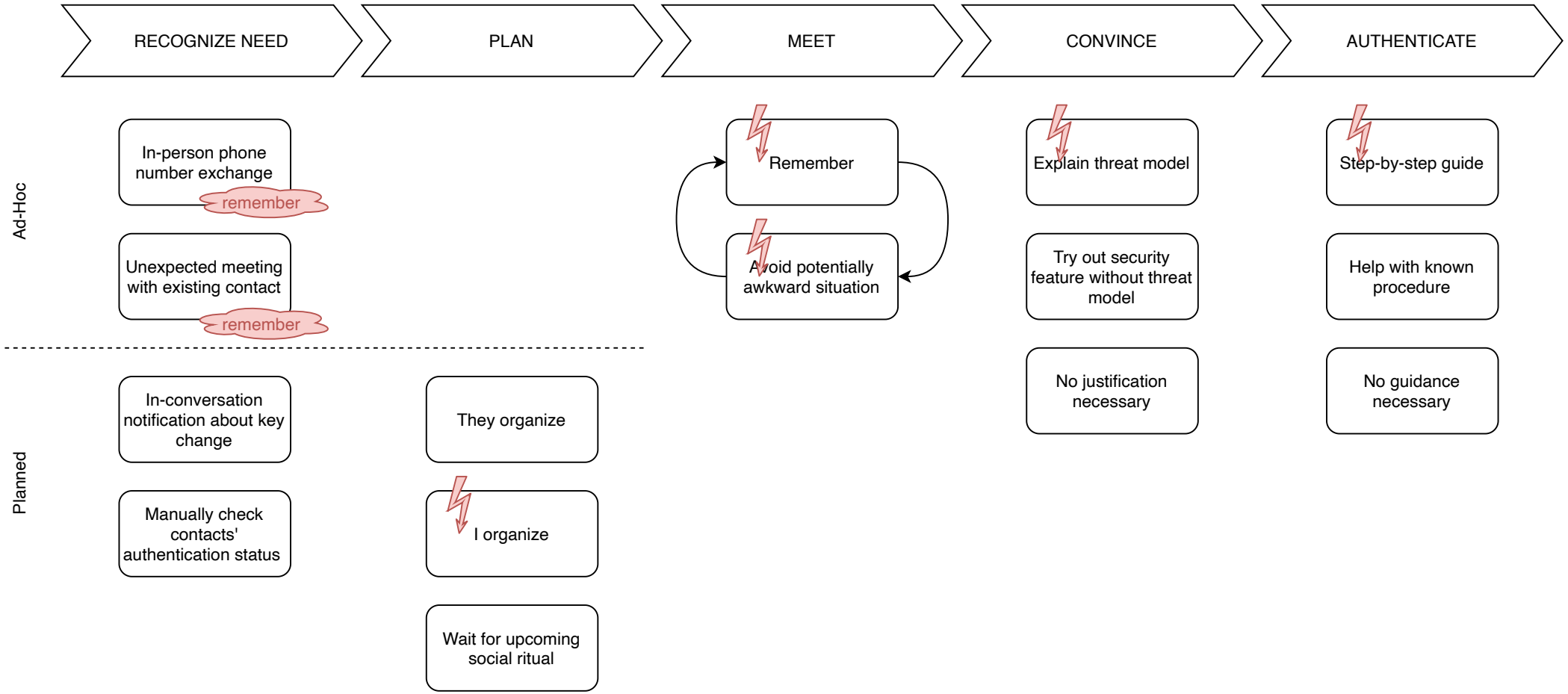
They are hard to use

Method

- 5-month diary study
  - Trigger-based entries
  - Meta entries
  - Periodic reminder for entries
- Open Coding procedure for analysis
  - Elements of planning and conducting authentication procedure
  - My feelings
  - The sociocultural context of interactions

Total diary entries	69
Successful authentication ceremonies	17
Countries	Austria, Germany, and Japan

Phase Model of Secure Messenger Authentication



Emotions

- Overwhelmed by mental load
- Worried about possible reactions

Sociocultural Aspects

Authentication ceremonies are embedded in social rituals

- Social rules and norms apply
- Can make authentication easier

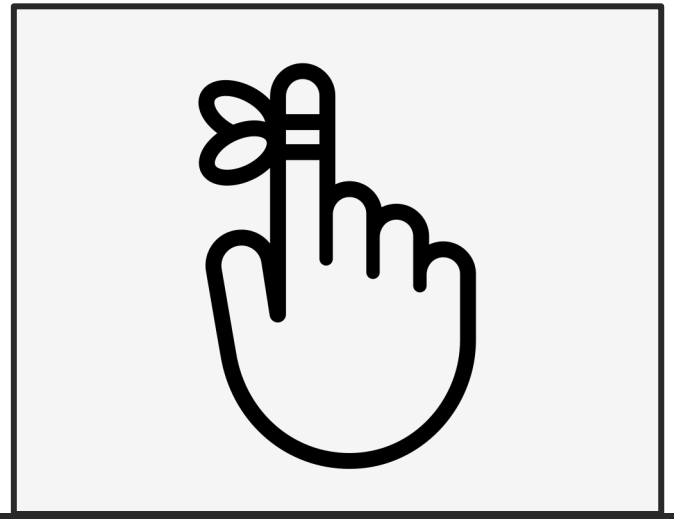
Using Autoethnography to Research Authentication Ceremonies

(1) **Long-Term Insights into everyday behavior**

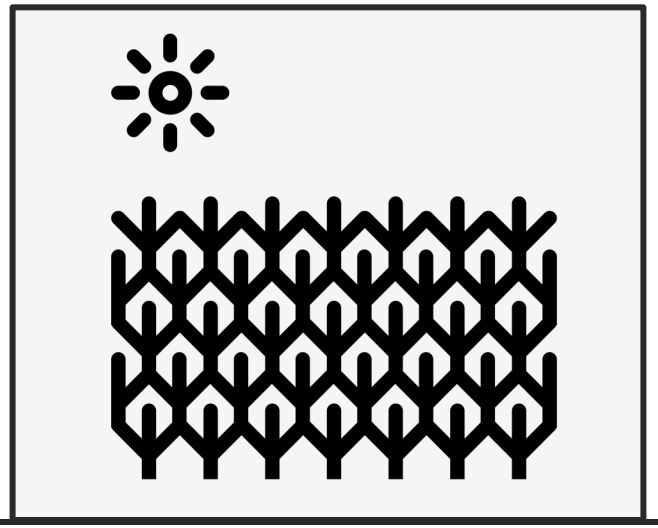
(2) **Planning and organizing**
- **Remote**
- **In Person**

(3) **User-to-User interaction specific to social context, e.g.,**
- **Friends & family**
- **Business partners**

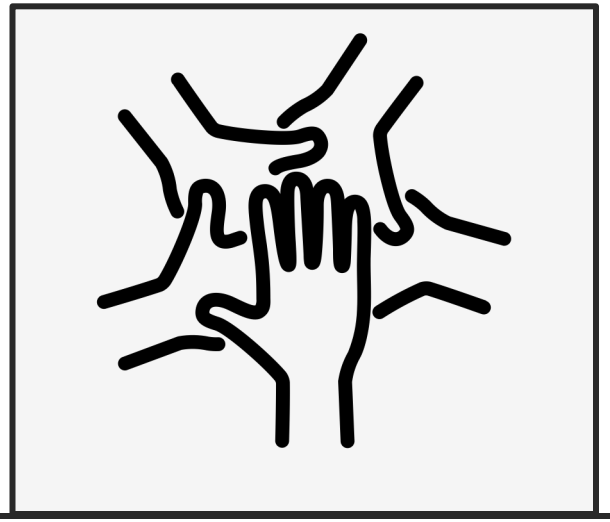
Summary and Implications



Commitment and reminder mechanisms



Emphasize field research on Authentication Ceremonies



Methods for designing cooperative security mechanisms

Matthias Fassl

matthias.fassl@cispa.de