

Is Internet Secure? Expectations vs. Reality



Devashish Gosain

WhatsApp introduces new security feature to protect users from phishing scams

A lot of people fall victim to phishing scams on WhatsApp. Now, Meta takes a stand with a game-changing feature: block unknown numbers directly from your lock screen to protect users from phishing attacks.

258,000 encrypted IronChat phone messages cracked by police

They expect to cuff hundreds of criminals who used the pricey phones, which were sold with the crypto app preinstalled.

Written by
NOVEMBER 09, 2018

NAKED SECURITY DUTCH POLICE ENCRYPTED MESSAGING ENCRYPTION IRONCHAT MESSAGING NETHERLANDS

BOLLYWOOD CONTROVERSY

Sushant Rajput case: WhatsApp denies possibility of leaked chats amid NCB summons to actors

The NCB has summoned actors Deepika Padukone, Saif Ali Khan, and Shradha Kapoor reportedly on the basis of old WhatsApp chats.

CoinGate
English Portuguese Español

News Markets Crypto Guru Collection Gamble Contact HUGEwin Casino

STEP INTO THE OCTAGON OF WINS - 200% BONUS CLAIM BONUS

UFC Stake OFFICIAL BETTING PARTNER

Crypto Scams Rise in India as Another Consulting Executive Faces Fraud

A consulting executive from Gurugram, India, was allegedly scammed on Saturday under the pretext of cryptocurrency awards.

WORLD NEWS

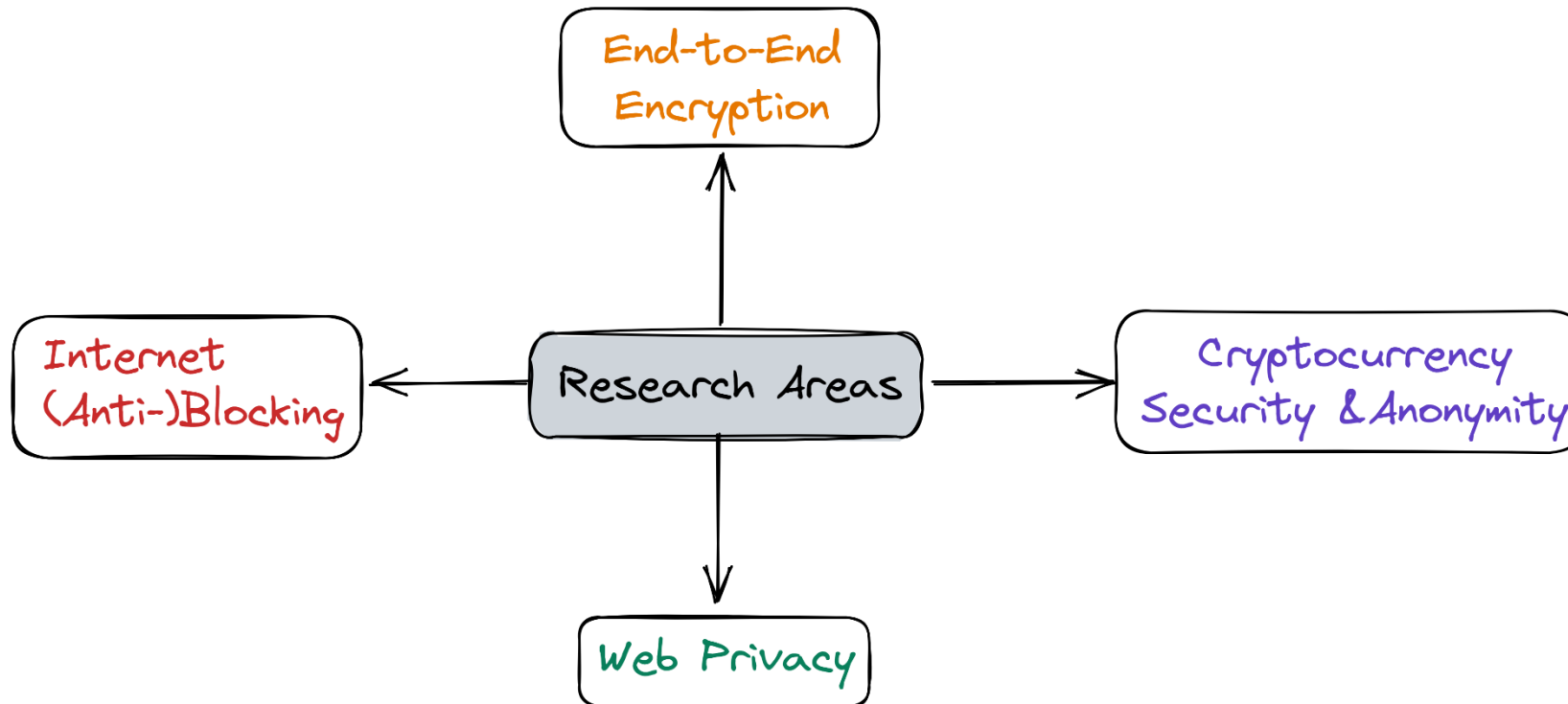
Poland's PM says authorities in the previous government widely and illegally used Pegasus spyware

Products Services Pricing Resources Partners

Luxembourg DPA issues €746 Million GDPR Fine to Amazon

30/07/2021 in Blog, GDPR

Research Directions



Research on traffic filtering (I)

Demo: Simple Deep Packet Inspection with P4

Sahil Gupta*, Devashish Gosain†, Garegin Grigoryan‡, Minseok Kwon.*, and H. B. Acharya.*

*Rochester Institute of Technology, USA † Max-Planck-Institut für Informatik, Germany ‡ Alfred University, USA
Email: *sg5414@rit.edu, * acharya@mail.rit.edu

Abstract—The P4 language allows “protocol-independent packet parsing” in network switches, and makes many operations possible in the data plane. But P4 is not built for Deep Packet Inspection – it can only “parse” well-defined packet headers, not free-form headers as seen in HTTPS etc. Thus some very important use cases, such as application-layer firewalls, are considered impossible for P4. This demonstration shows that this limitation is not strictly true: switches, that support only standard P4, are able to independently perform tasks such as blocking specific URLs (without using non-standard “extern” components, help from the SDN controller, or rerouting to a firewall). As more Internet infrastructure becomes SDN-compatible, in future, switches may perform simple application-layer firewall tasks.

I. INTRODUCTION

Modern (software-defined) networks are flexible and powerful: they have been used for load balancing [1], [2], detecting network attacks (notably denial-of-service [3], port scans [4]), and simple (network-layer) firewalls [5]). It is natural to

ICNP 21

(a) optional fields, (b) variable field ordering, and (c) variable-length fields. So our research question is, “is it possible (in all practically significant cases) to detect URLs of (malicious)

DeeP4R: Deep Packet Inspection in P4 using Packet Recirculation

Sahil Gupta
Rochester Institute of Technology
Rochester, NY, USA
sg5414@rit.edu

Minseok Kwon
Rochester Institute of Technology
Rochester, NY, USA
jmk@cs.rit.edu

Abstract—Software-defined networks are useful for multiple tasks, including firewalling, telemetry, and flow analysis. In particular, the P4 language makes it possible to carry out some simple packet processing tasks in the data plane, *i.e.*, on the switch itself (without real-time support from the SDN controller or a server). However, owing to the limitations of packet parsing in P4, these tasks involve only the packet headers. In this paper, we present a novel approach that allows Deep Packet Inspection (DPI) – *i.e.*, inspection of the packet payload – in the data plane, using P4 alone. We make use of the fact that in P4, a switch can clone and recirculate packets. One copy (clone) can be recirculated, slicing off a byte in each round, and using a finite-state machine to check if a target string has yet been seen. If the target string is found, the other copy (original packet) is discarded; if not, it is passed through. Our approach allows us to build the first application-layer firewall (URL filter) in the data plane, and to achieve essentially line-rate performance while filtering thousands of URLs, on a commodity programmable switch. It may in future also be used for other DPI tasks.

Index Terms—Software-Defined Networks (SDN), Programmable Dataplane, Application-Layer Firewall

than to trust the manufacturer for strong security guarantees (*i.e.*, that the firewall is not itself malicious [7]), does not violate user privacy, *etc.*). Further, such middleboxes are usually on-path rather than in-path [8], and may only inspect a sample of traffic so as not to become a bottleneck. A comprehensive line-rate filtering solution is very expensive, and even modest firewalls may be out of the reach of small businesses. Such lack of access was one of the original motivations for developing Software-Defined Networks [9]. It is, therefore, natural to ask why DPI tasks, such as URL filtering, are not performed using programmable switches, which are friendly to the network administrators and usually provide high performance for data-plane tasks.

We find that DPI-in-SDN is challenging because, in general, the payload is large and unpredictable in structure compared to packet headers. For example, one payload item – the HTTP application-layer header – has 47 possible fields, and these fields can occur out-of-order, have variable lengths, or can be

Predictable Internet Clients and In-Switch Deep Packet Inspection

Sahil Gupta
Rochester Institute of Technology
Rochester, NY, USA
sg5414@rit.edu

Devashish Gosain
Max Planck Institute for Informatics
Saarbrücken, Germany
dgosain@mpi-inf.mpg.de

Hrishikesh B Acharya
Rochester Institute of Technology
Rochester, NY, USA
acharya@mail.rit.edu

for net-
: black-
admin-
standard
tandard
to parse
) – thus
boxes.
: First,
dictable
up for

give a programmable switch the ability to parse these headers². If a switch can (extract and) filter traffic by application-layer headers, *e.g.* site URL or file type, it becomes an application layer firewall, *i.e.* performs DPI. The question immediately arises why such solutions do not replace black-box firewalls.

Indeed, such ideas have been proposed – for example, Sekar’s CoMB architecture [7] built on the Click modular router [8]. But *current SDN platforms are not intended for Deep Packet Inspection*. The P4₁₆ standard makes this ex-

ICCCN 23

INFOCOM 23

Research involving cryptocurrency (III)

On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies

Piyush Kumar Sharma
imec-COSIC, KU Leuven
pkumar@esat.kuleuven.be

Devashish Gosain
Max Planck Institute for Informatics
dgosain@mpi-inf.mpg.de

Claudia Diaz
imec-COSIC, KU Leuven
Nym Technologies SA
cdiaz@nymsa.com

Abstract—Cryptocurrency systems can be subject to deanonymization attacks by exploiting the network-level communication on their peer-to-peer network. Adversaries who control a set of colluding node(s) within the peer-to-peer network can observe transactions being exchanged and infer the parties involved. Thus, various network anonymity schemes have been proposed to mitigate this problem, with some solutions providing theoretical anonymity guarantees.

In this work, we model such peer-to-peer network anonymity solutions and evaluate their anonymity guarantees. To do so, we propose a novel framework that uses Bayesian inference to obtain the probability distributions linking transactions to their possible originators. We characterize transaction anonymity with those distributions, using entropy as metric of adversarial uncertainty on the originator's identity. In particular, we model

underlying technologies. The de aspects of blockchains have rec and are by now well understood other hand, understanding the systems presents additional comp requires protection both on-chain to-peer network used to transport transaction is considered private third parties to identify its source analyzing blockchain data, nor data available to peers. The default actions in the Bitcoin network h: prone to network-level deanonym where the public identifier of a

Poster: Hades: Practical Partitioning Attack on Cryptocurrencies

Vinay Shetty
Saarland University
s8vishet@stud.uni-saarland.de

Piyush Kumar Sharma
imec-COSIC, KU Leuven
pkumar@esat.kuleuven.be

Devashish Gosain
imec-COSIC, KU Leuven
Max Planck Institute for Informatics
dgosain@esat.kuleuven.be

Abstract—Bitcoin is unarguably one of the most widely used cryptocurrency systems and is an excellent realization of blockchain technology. However, Bitcoin is shown to be vulnerable to partitioning attacks. These attacks aim at isolating a Bitcoin node from the rest of the Bitcoin network such that the attacker controls the victim(s) view of the blockchain.

The latest attack, Erebus, however, requires cooperation from AS-level adversaries (e.g., tier-1 AS), which makes the attack practically daunting. In this work, we demonstrate a new practical partitioning attack, *Hades*, that does not need the cooperation of ASes; instead, it just requires control of a few hundred cloud hosts. We exploit the capability of instantiating

it practically controls thousands of Bitcoin instances without the cooperation of an AS-level adversary. This scale of nodes helps the attacker to perform the partitioning attack following the approach described in the original Erebus paper.

Through simulations, we demonstrate the feasibility of Hades. Our initial results show that it is certainly beneficial for the adversary to consider onion addresses as an attack vector for the partitioning attack. Hades can have severe implications with respect to partitioning attacks as even a normal user with control of a few hundred cloud hosts can successfully launch this attack. This significantly reduces the required resources

NDSS 2023

NDSS 2023

Research on end-to-end encryption (II)



Automatic Detection of Fake Key Attacks in Secure Messaging

Tarun Kumar Yadav
Brigham Young University
tarun141@byu.edu

Devashish Gosain
Max Planck Institute for Informatics
dgosain@mpi-inf.mpg.de

Amir Herzberg
University of Connecticut
amir.herzberg@gmail.com

Daniel Zappala
Brigham Young University
zappala@cs.byu.edu

Kent Seamons
Brigham Young University
seamons@cs.byu.edu

ABSTRACT

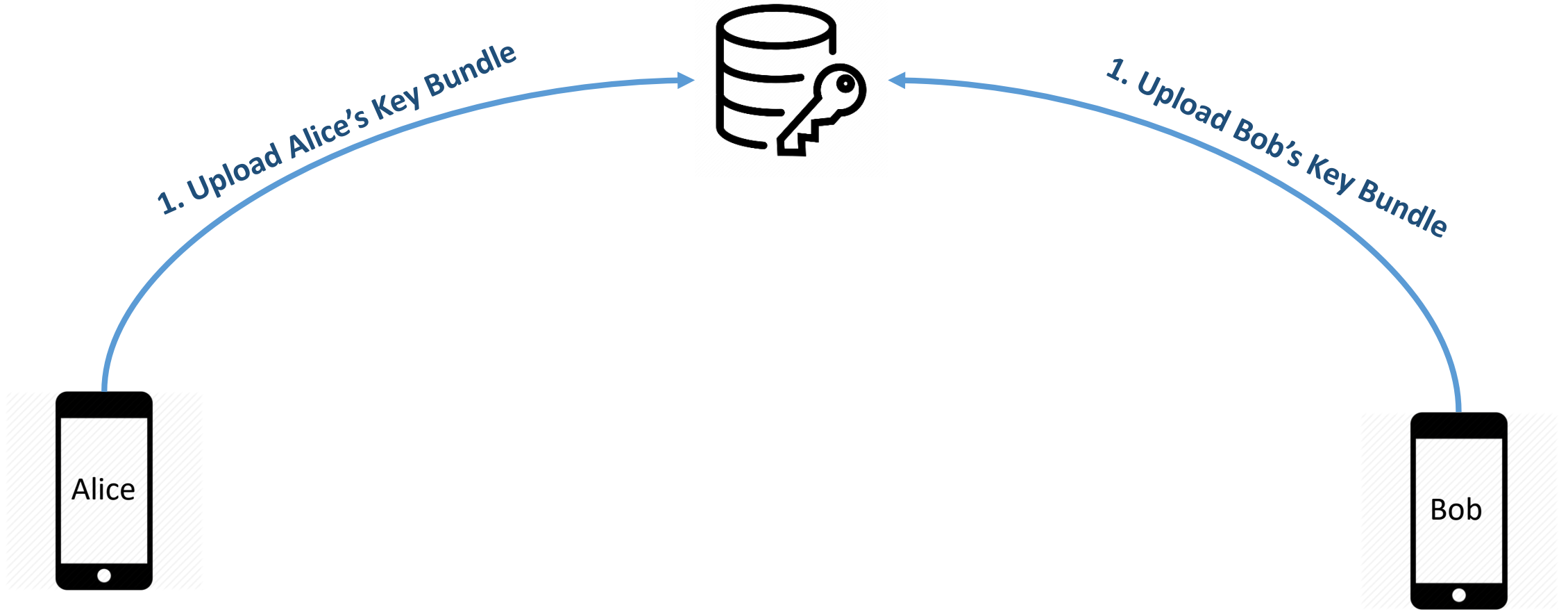
Popular instant messaging applications such as WhatsApp and Signal provide end-to-end encryption for billions of users. They rely on a centralized, application-specific server to distribute public keys and relay encrypted messages between the users. Therefore, they prevent passive attacks but are vulnerable to some active attacks. A malicious or hacked server can distribute fake keys to users to perform man-in-the-middle or impersonation attacks. While typical secure messaging applications provide a manual method for users to detect these attacks, this burdens users, and studies show it is ineffective in practice. This paper presents KTACA, a completely automated approach for key verification that is oblivious to users and easy to deploy. We motivate KTACA by designing two approaches to automatic key verification. One approach uses client auditing (KTCA) and the second uses anonymous key monitoring (AKM). Both have relatively inferior security properties, leading to

1 INTRODUCTION

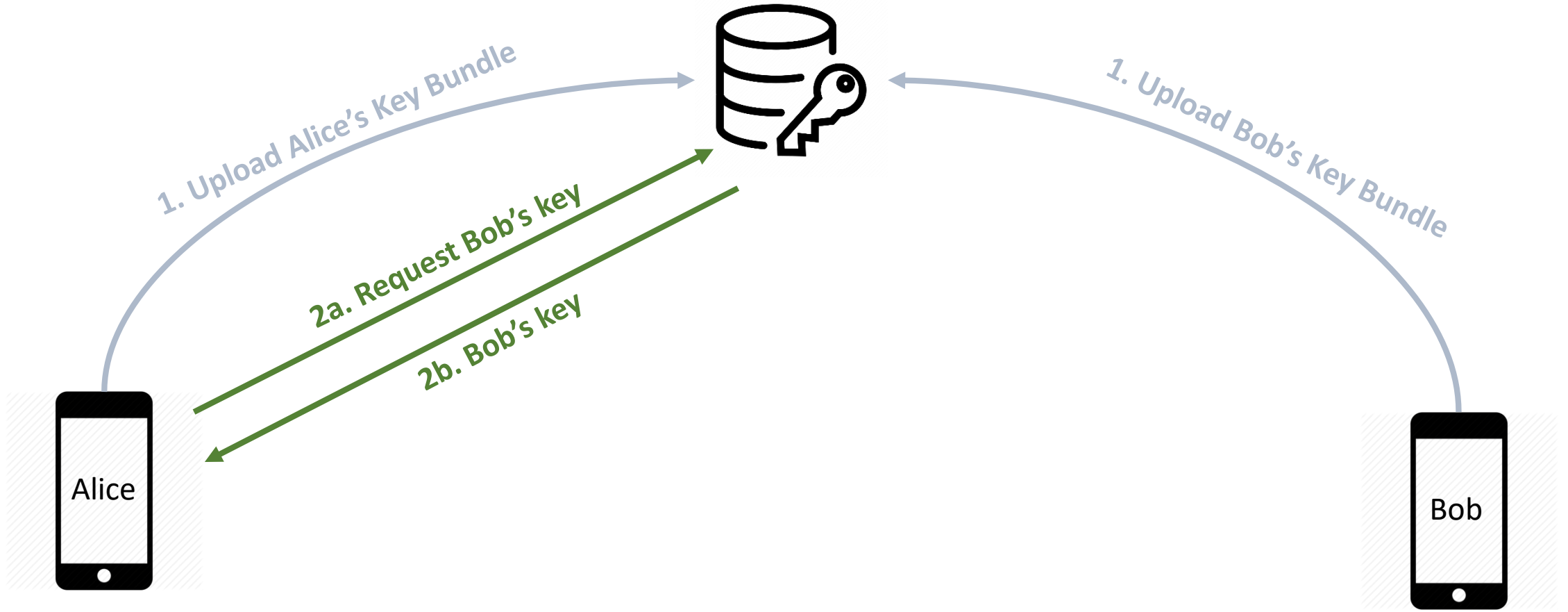
Secure messaging applications provide billions of users with end-to-end encryption to ensure message privacy. A long list of applications provides this service, including WhatsApp, iMessage, Facebook Messenger, Skype, Signal, Threema, Wire, Wickr, Viber, and Riot. The application's underlying encryption protocols vary, though many use the Signal protocol or some derivation.

All the secure messaging applications listed above use a centralized server to exchange public keys and relay messages among users. The end-to-end encryption (E2EE) protocols assume the honest-but-curious model. When Alice wishes to communicate with Bob, she requests Bob's key from the server (and vice-versa). A malicious or compromised server can launch a man-in-the-middle (MITM) attack against Alice and Bob by providing them with fake keys. The server then has access to the plaintext as it decrypts and re-encrypts each message that it relays between them.

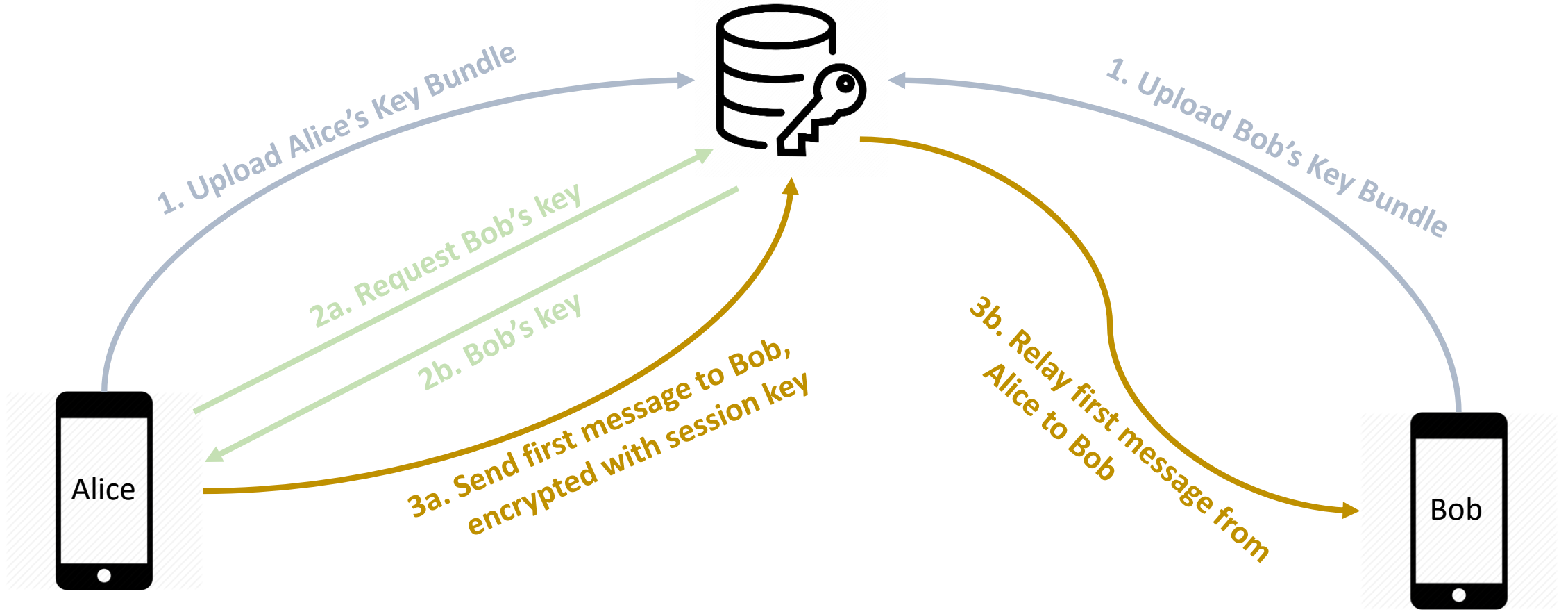
Key distribution



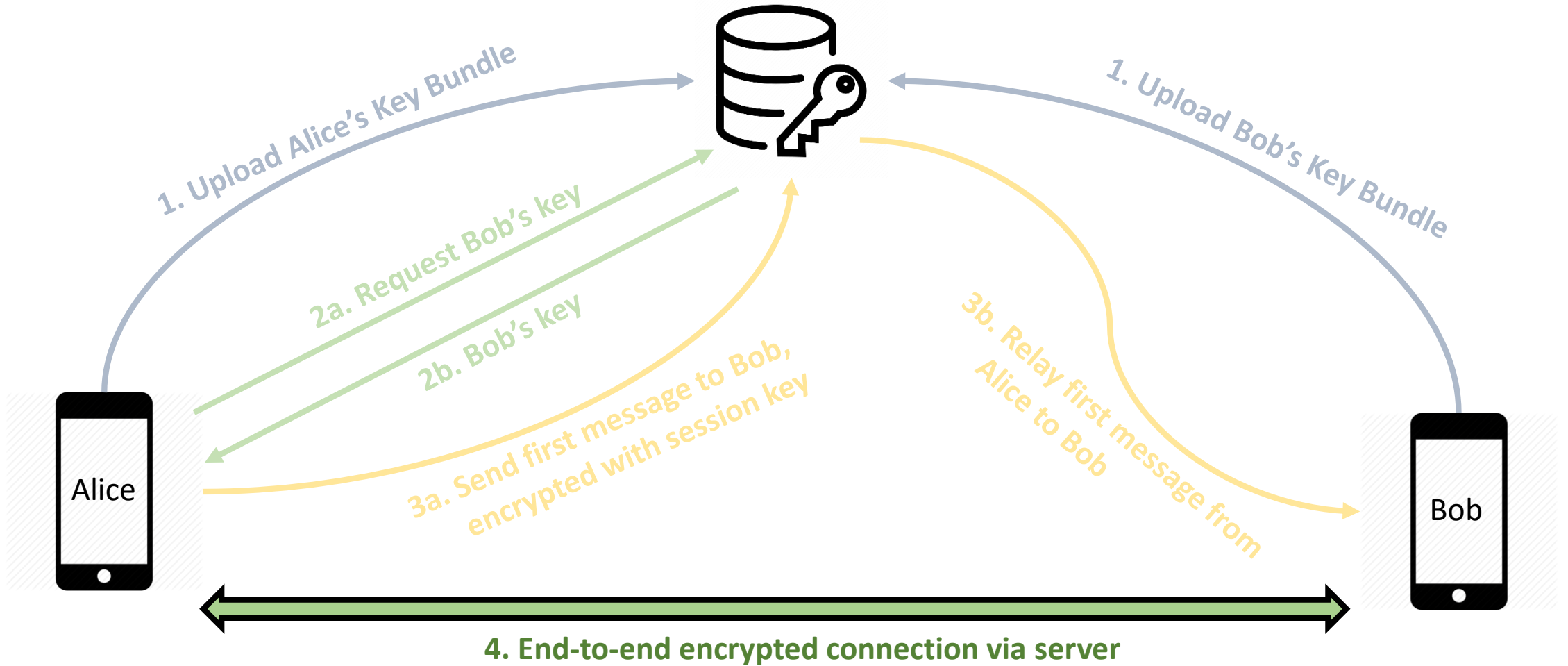
Key distribution



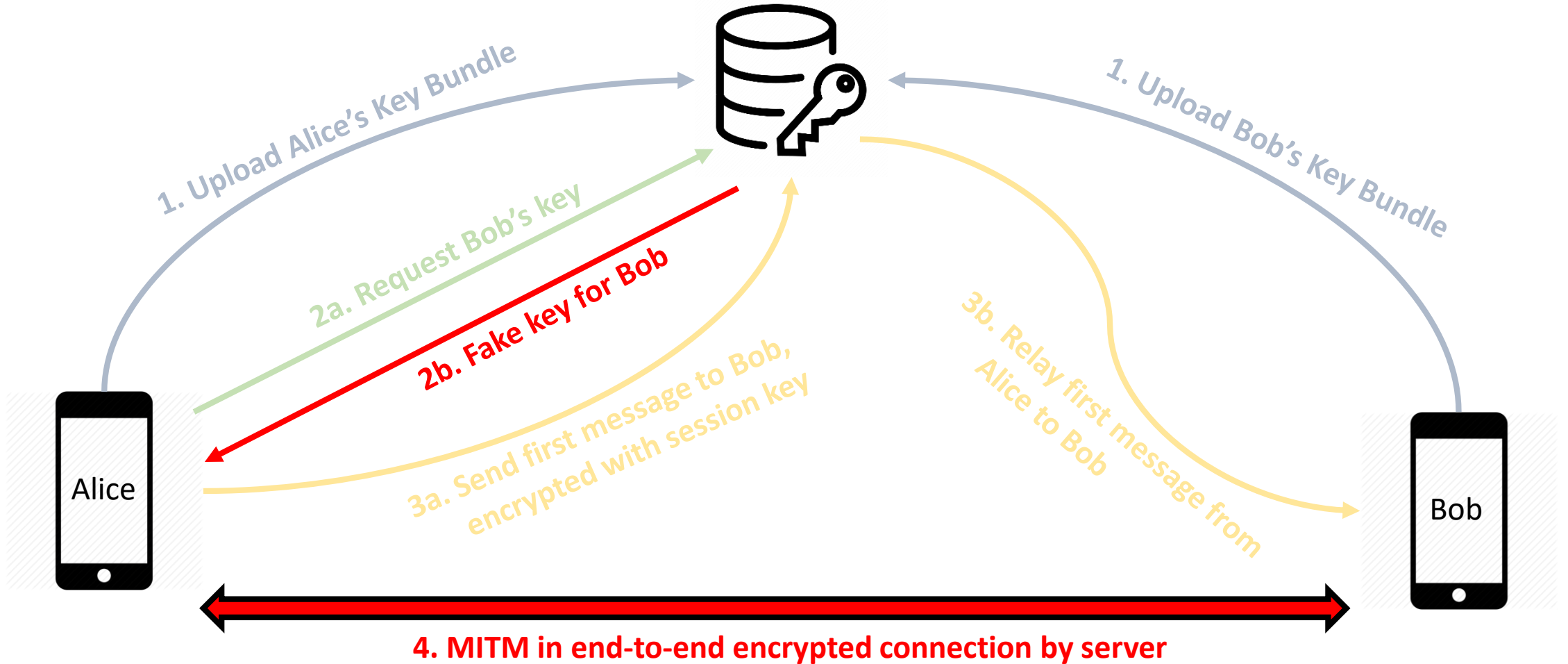
Key distribution



Key distribution



Fake Key attack on new connection



March 8, 2019, 3:24 PM MST

By David Ingram

Every six minutes, on average, Facebook gets a request from a U.S. government agency for information about gangs, drug trafficking or other suspected crimes, and the social network generally cooperates, turning over at least some data 86 percent of the time, according to the company's most recent report on the [topic](#).

WhatsApp is at risk in India. So are free speech and encryption.

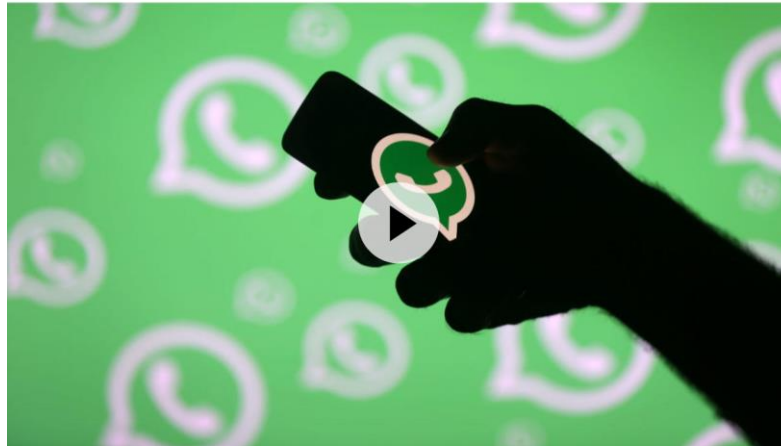
India is proposing new content laws that could be a "sledgehammer" for free speech.

By Kurt Wagner | Feb 19, 2019, 6:00am EST

Whatsapp confirms 'targeted' cyber surveillance attack



Issued on: 14/05/2019 - 09:26 Modified: 14/05/2019 - 18:32



Dado Ruvic, Reuters | A man poses with a smartphone in front of a displayed Whatsapp logo in this illustration.

Text by: FRANCE 24 [Follow](#)

Video by: Erin Ogunkeye

Spyware crafted by an "advanced cyber actor" infected multiple targeted mobile phones through the popular WhatsApp communications program without any user intervention through in-app voice calls, the company said.

US, UK and Australia urge Facebook to create backdoor access to encrypted messages

Facebook says it opposes calls for backdoors that would 'undermine the privacy and security of people everywhere'

Julia Carrie Wong in San Francisco
@juliacarriew
Thu 3 Oct 2019 19:37 EDT
540



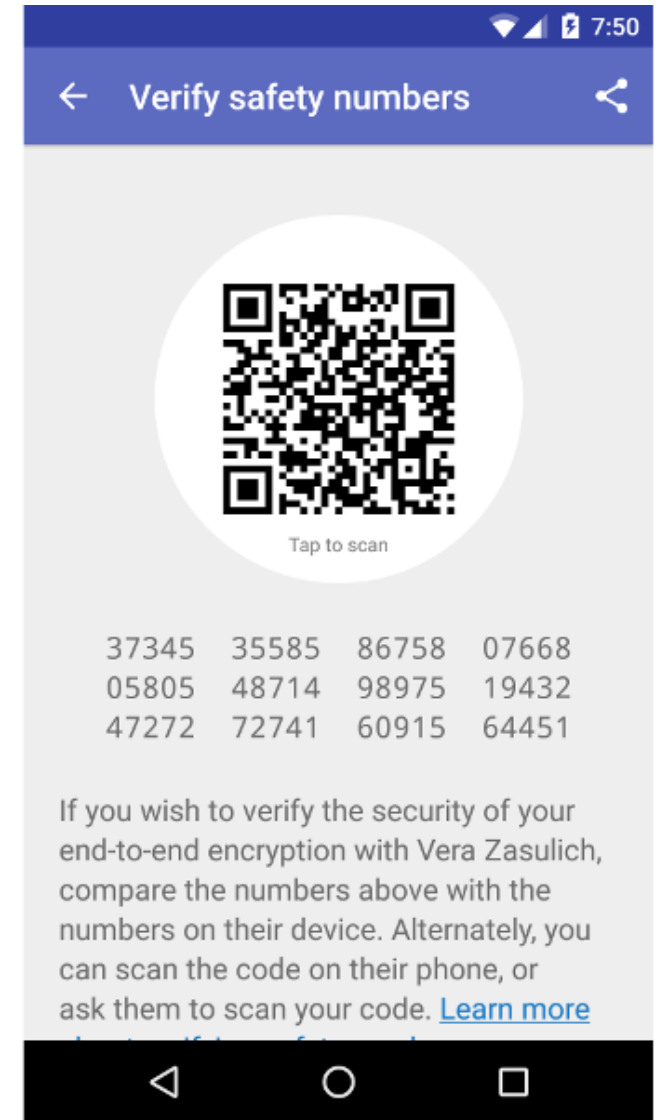
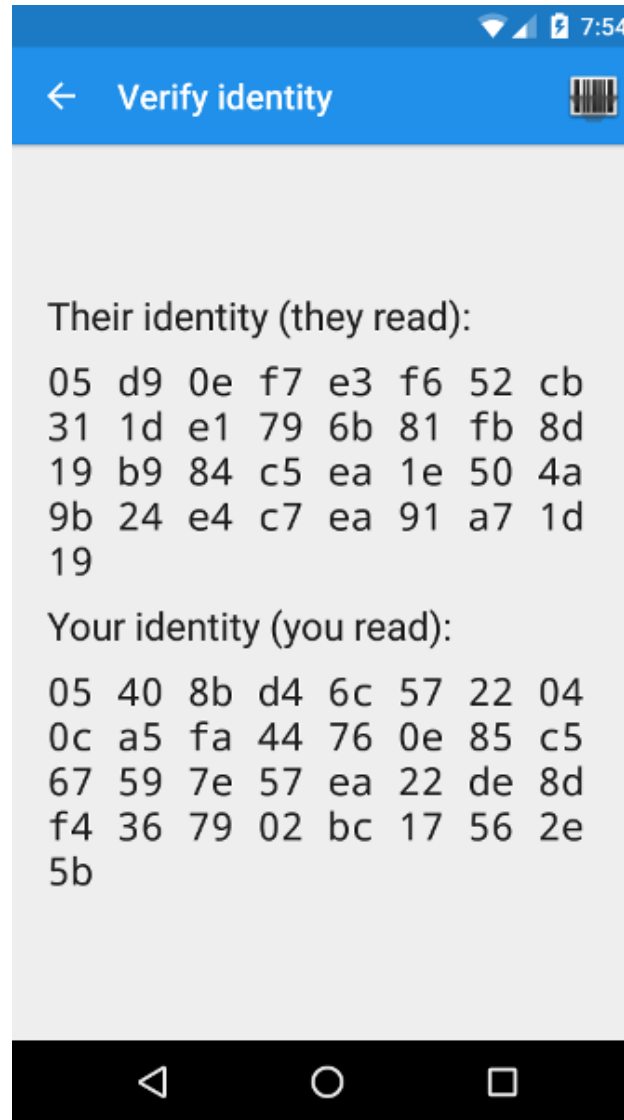
Australia to become first country in the world to force WhatsApp and other apps to include spyware to allow Big Brother spies to read your messages

- Government could be spying on your messages as part of new security laws
- Labor and government came to an in-principle agreement on key parts of the bill
- Bill is yet to be signed off by parliament's intelligence and security committee
- Powers are limited to 'serious offences' such as terrorism and organised crime

By SAHAR MOURAD FOR DAILY MAIL AUSTRALIA and AUSTRALIAN ASSOCIATED PRESS
PUBLISHED: 08:16 EST, 4 December 2018 | UPDATED: 01:41 EST, 6 December 2018

Current authentication process

- not usable
- almost no one does it



Current authentication process

- not usable
- almost no one does it

Can Johnny Finally Encrypt? Evaluating E2E-Encryption in Popular IM Applications

Amir Herzberg
Dept. of Computer Science
Bar-Ilan University, Israel
amir.herzberg@gmail.com

Hemi Leibowitz
Dept. of Computer Science
Bar-Ilan University, Israel
leibo.hemi@gmail.com

When SIGNAL hits the Fan: On the Usability and Security of State-of-the-Art Secure Mobile Messaging

Svenja Schröder
University of Vienna
Email: svenja.schroeder@univie.ac.at

Markus Huber, David Wind, Christoph Rottermann
St. Pölten University of Applied Sciences
Email: {markus.huber, is121030, is121023}@fhstp.ac.at

Is that you, Alice? A Usability Study of the Authentication Ceremony of Secure Messaging Applications

Authors:

Elham Vaziripour, Justin Wu, Mark O'Neill, Ray Clinton, Jordan Whitehead, Scott Heidbrink, Kent Seamons, and Daniel Zappala, *Brigham Young University*

Usable authentication process

- lack of awareness
- continuous manual effort
- rare attack

Action Needed! Helping Users Find and Complete the Authentication Ceremony in Signal

Authors:

Elham Vaziripour, Justin Wu, Mark O'Neill, Daniel Metro, Josh Cockrell, Timothy Moffett, Jordan Whitehead, Nick Bonner, Kent Seamons, and Daniel Zappala, *Brigham Young University*

"Something isn't secure, but I'm not sure how that translates into a problem": Promoting autonomy by designing for understanding in Signal

Authors:

Justin Wu, Cyrus Gattrell, Devon Howard, and Jake Tyler, *Brigham Young University*; Elham Vaziripour, *Utah Valley University*; Kent Seamons and Daniel Zappala, *Brigham Young University*

Can we automate the detection of
fake key attacks?



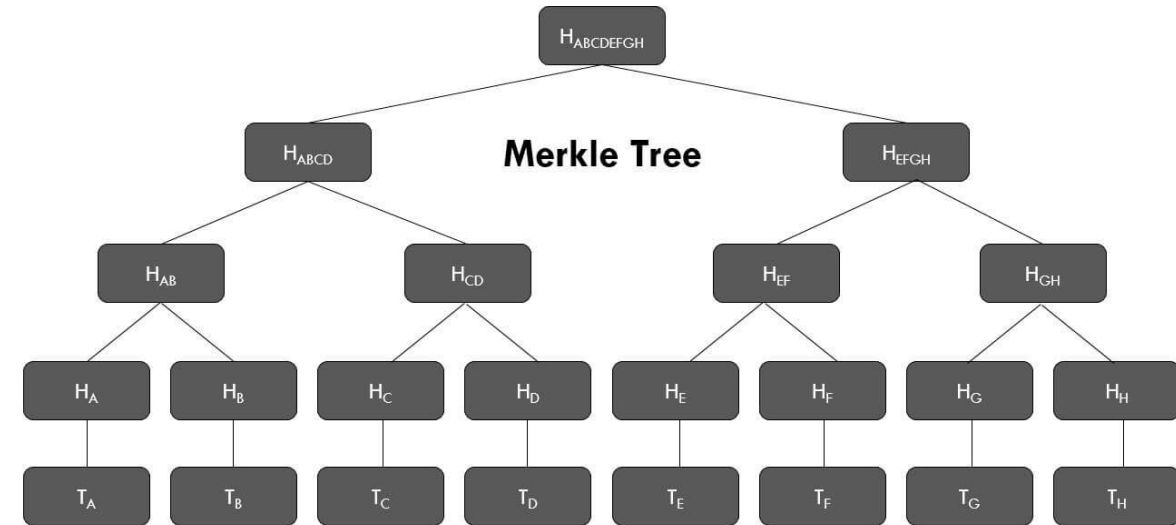
Our defenses

1. Key Transparency with Client Auditors
2. Anonymous Key Monitoring
3. Key Transparency with Anonymous Client Auditors

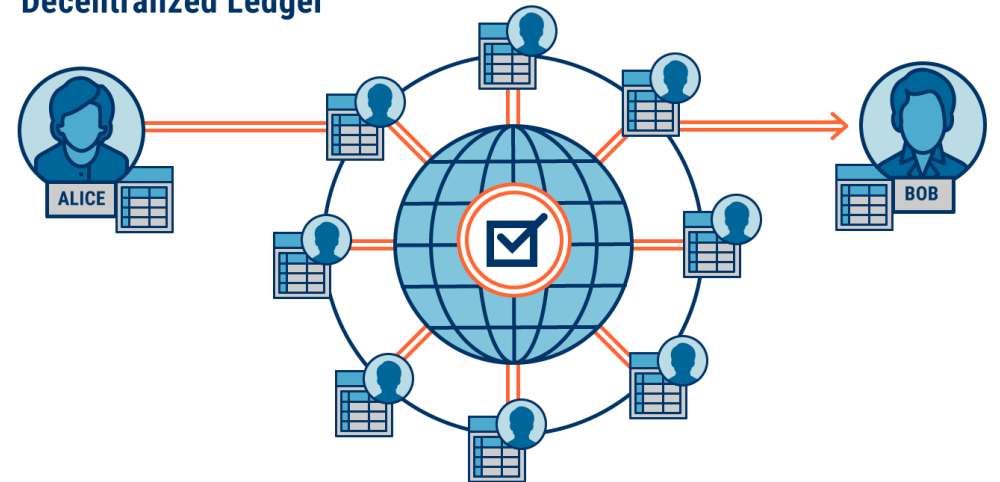
Fake key attack detection

1. Key Transparency with Client Auditors

- Clients monitor their own key
- Clients verify their contact's keys
- Clients audit STRs to detect equivocation



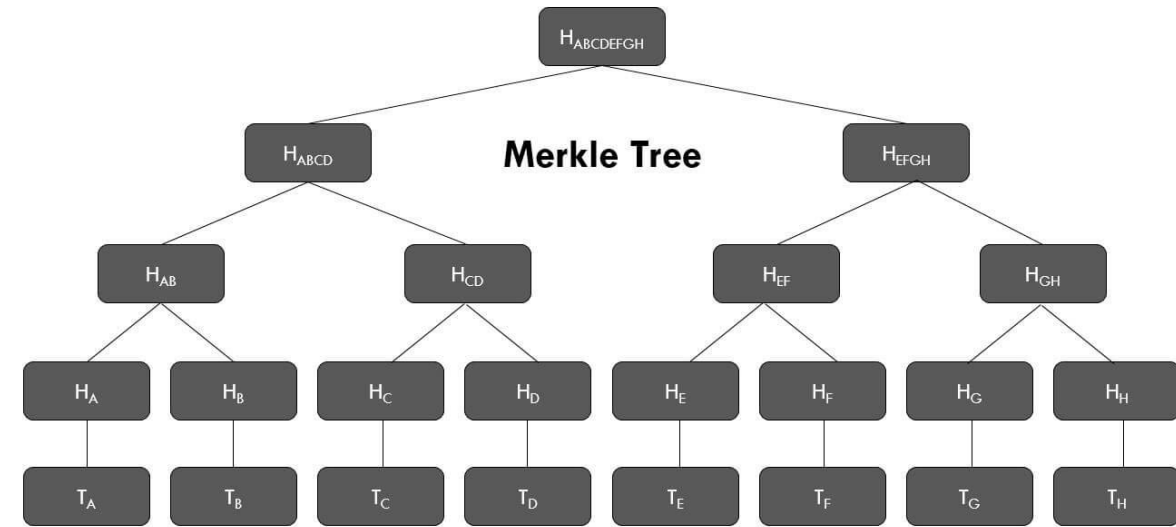
Decentralized Ledger



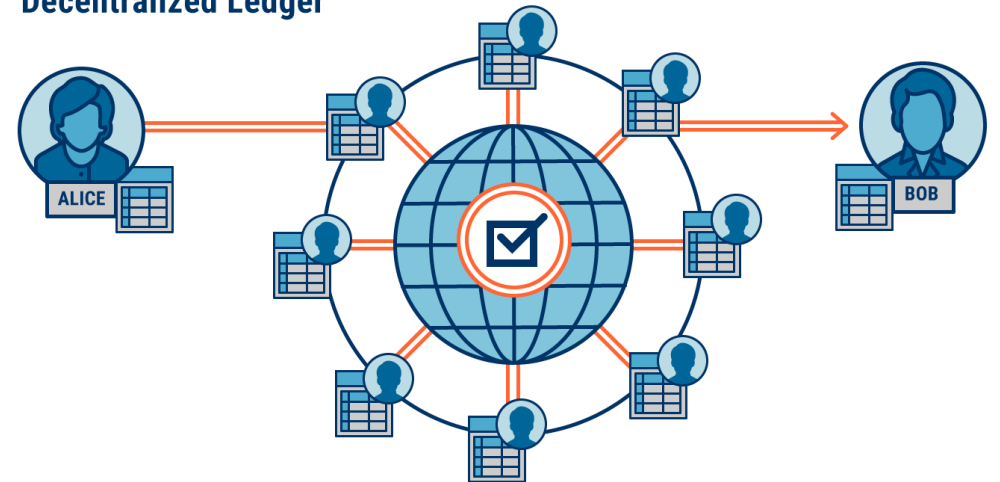
Fake key attack detection

1. Key Transparency with Client Auditors

- **assumes connected graph**

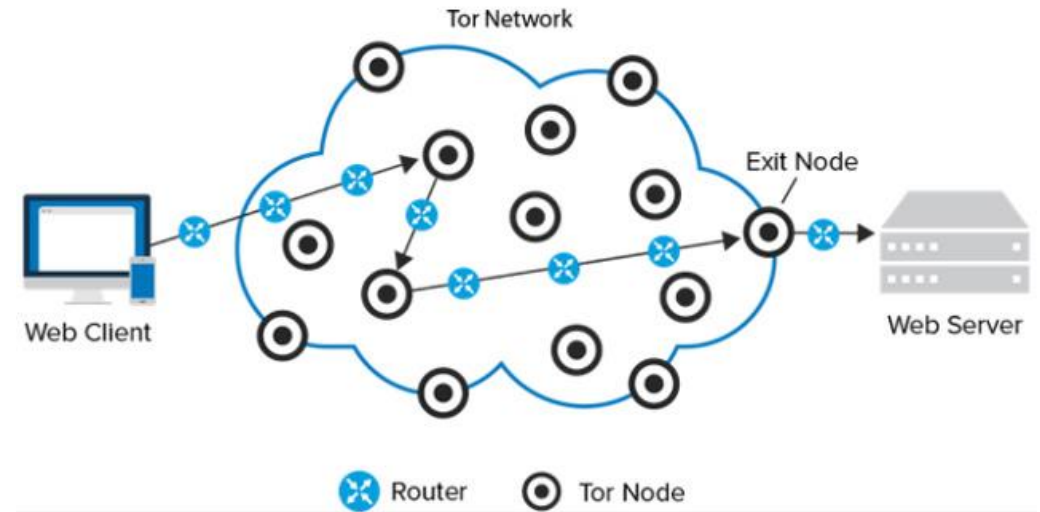


Decentralized Ledger



Fake key attack detection

1. Key Transparency with Client Auditors
2. Anonymous Key Monitoring
 - Clients monitor their own keys
 - Clients monitor their contact's key for a few epochs



Contribution

Designed three automated key verification solutions

Used threat analysis to compare how well they detect fake key attacks

Implemented attacks and defenses to demonstrate their feasibility

Provides detection without burdening users

Detection capability may deter attacks

Network Privacy

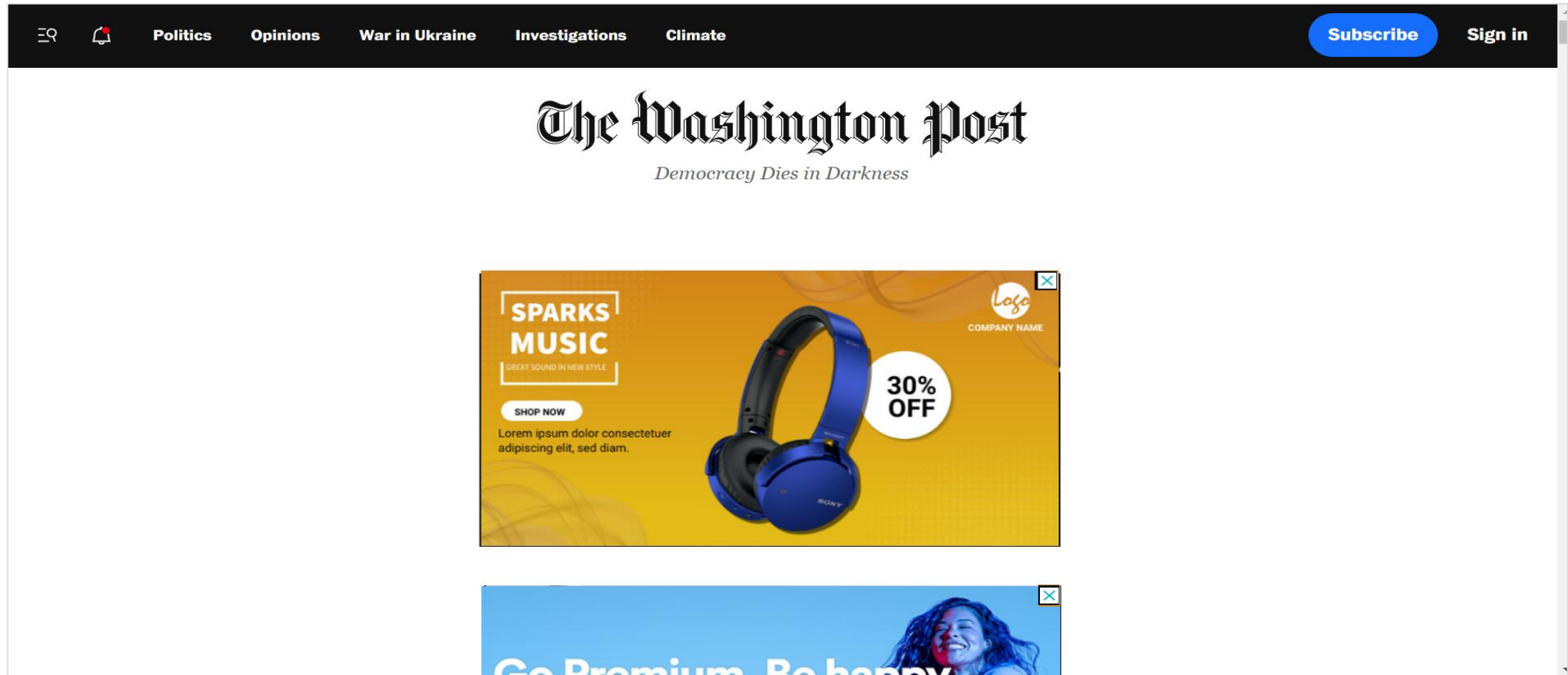
How web cookies influence user's privacy?



Cookies---Threat to Privacy?

The image shows a screenshot of the Spotify website interface. At the top left is the Spotify logo. The top right contains links for Premium, Support, Download, Sign up, and a Log in button. A left sidebar lists navigation options: Home, Search, Your Library, Create Playlist, and Liked Songs. The main content area is divided into two sections: 'Focus' and 'Spotify Playlists'. The 'Focus' section features seven playlists: Peaceful Piano, Deep Focus, Instrumental Study, Jazz Vibes, Focus Flow, Workday Lounge, and Beats to think to. The 'Spotify Playlists' section features seven playlists: Today's Top Hits, RapCaviar, All Out 2010s, Rock Classics, Chill Hits, Viva Latino, and Mega Hit Mix. At the bottom, a purple banner reads 'PREVIEW OF SPOTIFY Sign up to get unlimited songs and podcasts with occasional ads. No credit card needed.' and includes a 'Sign up free' button.

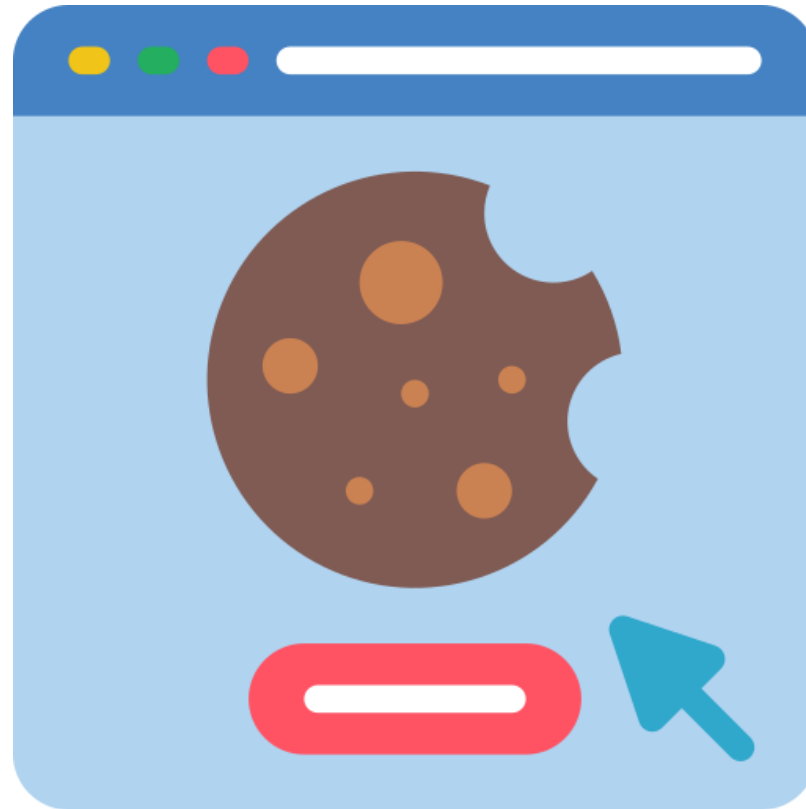
Cookies---Threat to Privacy?



Cookies---Threat to Privacy?

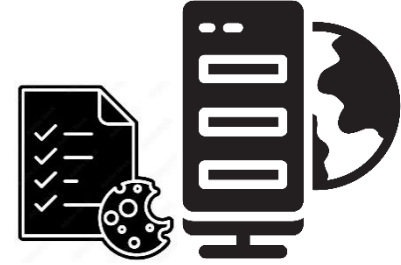
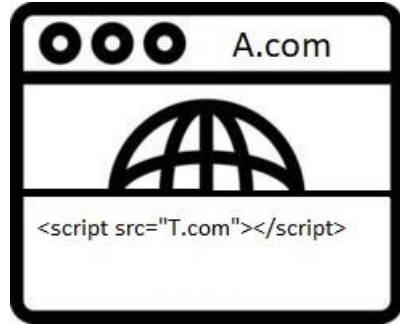
The screenshot shows a news website interface. At the top is a dark navigation bar with a search icon, a notification bell, and menu items: Politics, Opinions, War in Ukraine, Investigations, and Climate. On the right side of the navigation bar are buttons for 'Subscribe' and 'Sign in'. Below the navigation bar, there is a yellow placeholder advertisement with the text 'Lorem ipsum dolor consectetur adipiscing elit, sed diam.' and an image of blue Sony headphones. Below that is a blue Spotify Premium advertisement featuring a woman dancing, with the text 'Go Premium. Be happy.' and 'Premium sounds amazing. Enjoy ad-free music on all your devices.*'. A green button at the bottom of the ad says 'GET SPOTIFY PREMIUM'. Below the ads, there are two article headlines: 'Washington's bank rescue fails to erase all doubts' and 'Bank failures since 2007'. The second headline includes a sub-headline 'Washington Mutual \$307B' and a small graphic of a bank building. In the bottom right corner, the text 'Signature Bank' is visible.

Cookies---Threat to Privacy?

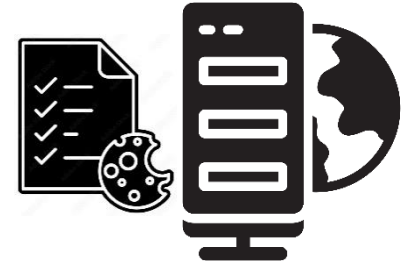


T.com
(jh234)

A.Com
(lkcv4)



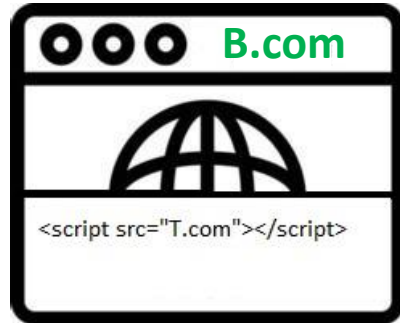
T.com



A.com

T.com
(jh234)

B.Com
(fg56a)

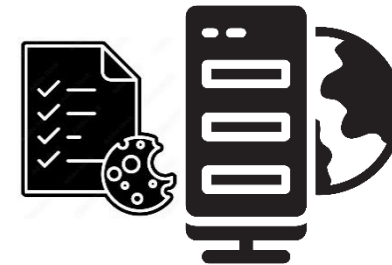


jh234



T.com

A.com
B.com



B.com

Privacy Laws

- General Data Protection Regulation (GDPR)
 - EU law
 - May 25, 2018
 - Enhance individuals' control and rights over their personal data
- California Consumer Privacy Act (CCPA)
 - California State law
 - January 1, 2020

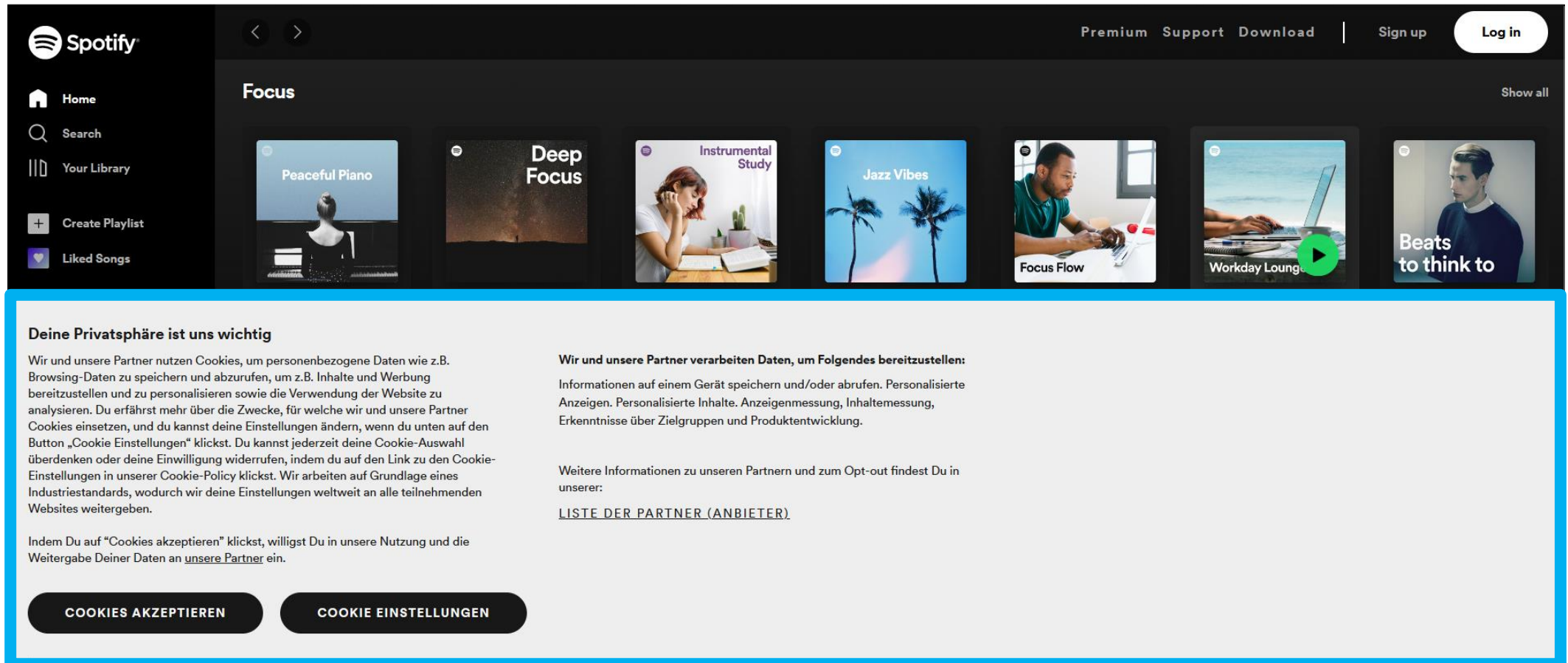


GDPR violations (examples)

- Amazon -
 - It was not notified before
- Meta – €4
 - Instagram 13 and
 - It violated email ac
- WhatsApp
 - WhatsApp data pro notice



Cookie Banners (notices)



The image shows a screenshot of the Spotify website interface. At the top, the Spotify logo is on the left, and navigation links for Premium, Support, Download, Sign up, and Log in are on the right. The main content area is titled 'Focus' and displays several playlist thumbnails: 'Peaceful Piano', 'Deep Focus', 'Instrumental Study', 'Jazz Vibes', 'Focus Flow', 'Workday Lounge', and 'Beats to think to'. A blue-bordered cookie banner is overlaid on the bottom half of the page. The banner contains the following text:

Deine Privatsphäre ist uns wichtig

Wir und unsere Partner nutzen Cookies, um personenbezogene Daten wie z.B. Browsing-Daten zu speichern und abzurufen, um z.B. Inhalte und Werbung bereitzustellen und zu personalisieren sowie die Verwendung der Website zu analysieren. Du erfährst mehr über die Zwecke, für welche wir und unsere Partner Cookies einsetzen, und du kannst deine Einstellungen ändern, wenn du unten auf den Button „Cookie Einstellungen“ klickst. Du kannst jederzeit deine Cookie-Auswahl überdenken oder deine Einwilligung widerrufen, indem du auf den Link zu den Cookie-Einstellungen in unserer Cookie-Policy klickst. Wir arbeiten auf Grundlage eines Industriestandards, wodurch wir deine Einstellungen weltweit an alle teilnehmenden Websites weitergeben.

Indem Du auf „Cookies akzeptieren“ klickst, willigst Du in unsere Nutzung und die Weitergabe Deiner Daten an [unsere Partner](#) ein.

Wir und unsere Partner verarbeiten Daten, um Folgendes bereitzustellen:

Informationen auf einem Gerät speichern und/oder abrufen. Personalisierte Anzeigen. Personalisierte Inhalte. Anzeigenmessung, Inhaltmessung, Erkenntnisse über Zielgruppen und Produktentwicklung.

Weitere Informationen zu unseren Partnern und zum Opt-out findest Du in unserer:

[LISTE DER PARTNER \(ANBIETER\)](#)

At the bottom of the banner are two buttons: 'COOKIES AKZEPTIEREN' and 'COOKIE EINSTELLUNGEN'.

Research Questions

- How many websites do show the banners?
 - Does the banner give users the options to explicitly agree or decline?
- Do they respect the users preferences?
- Do websites exhibit different behavior?
 - Geographic location (EU vs. non-EU)
 - User agent (mobile vs. desktop)

Goals

Analysis of cookie landscape from different perspectives in a automated way

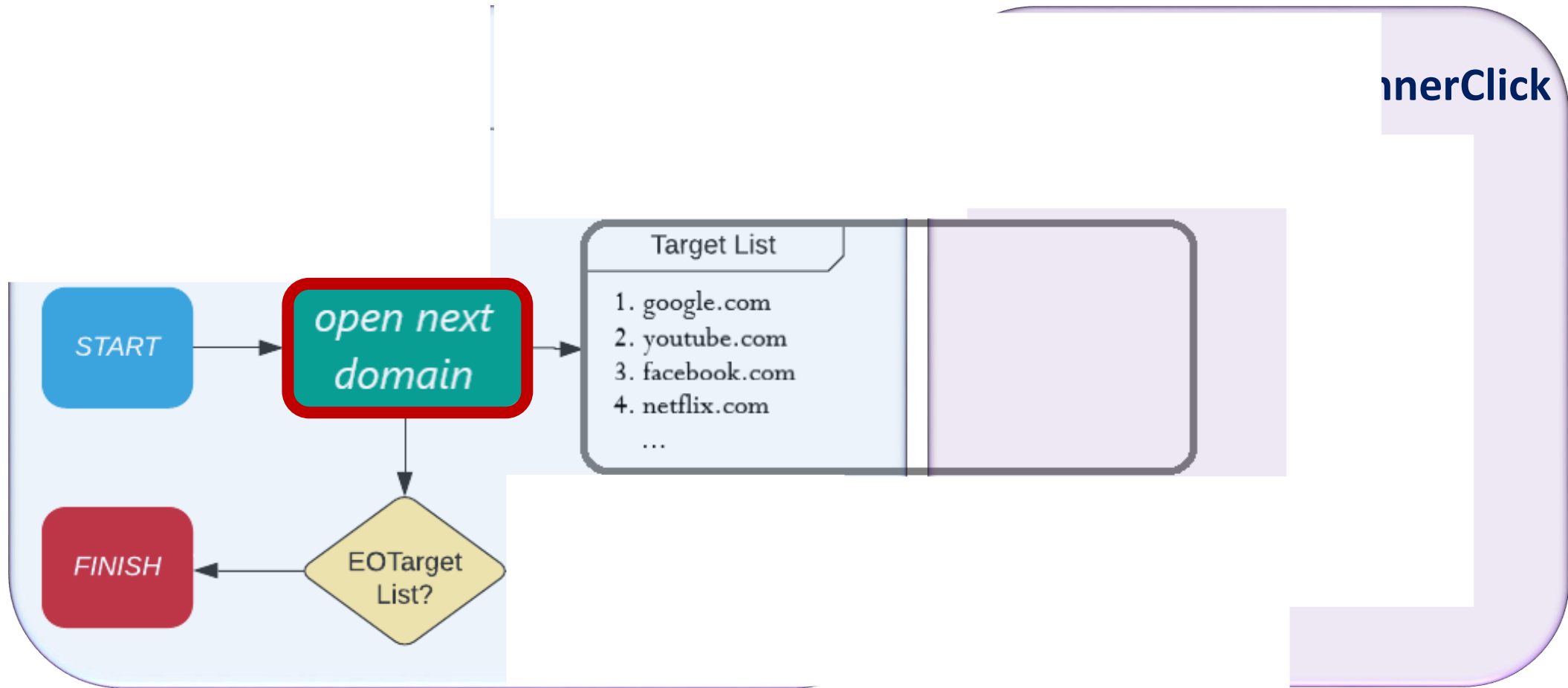
- Detection of cookie banners
- Interaction with cookie banners
- Impact of geographic locations
- Consistency of websites
- Cookie differences between
 - landing and inner pages
 - Mobile and desktop
- Impact of CCPA

Goals

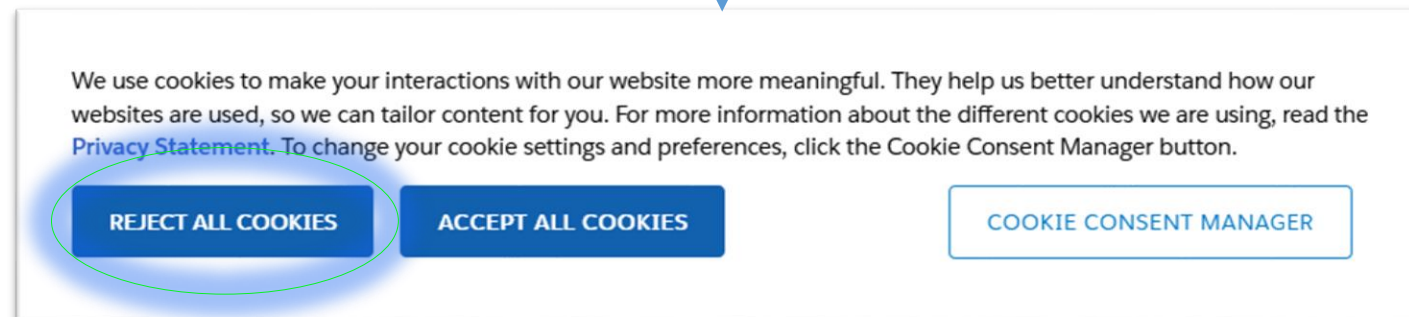
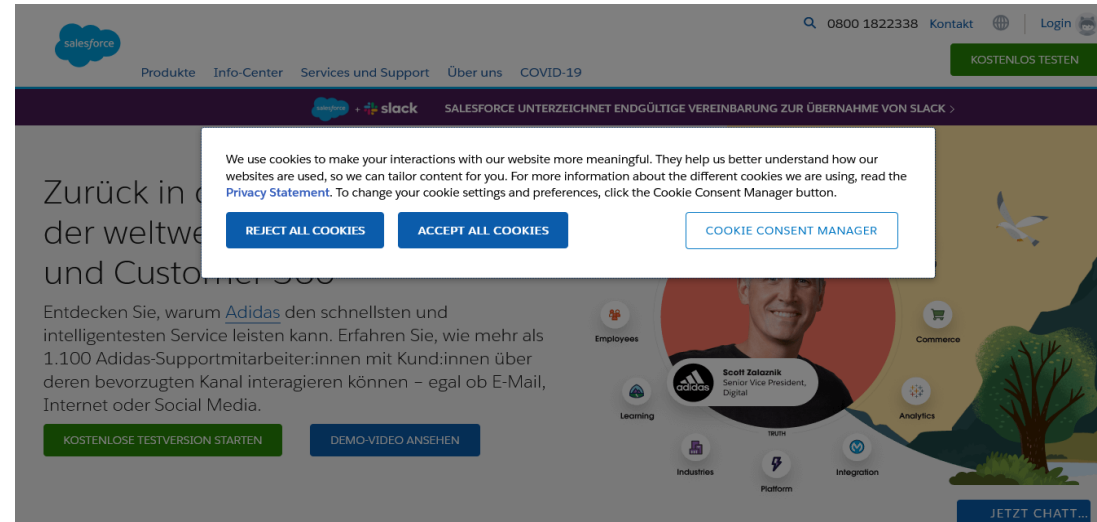
Analysis of cookie landscape from different perspectives in a automated way

- Detection of cookie banners
- Interaction with cookie banners
- Impact of geographic locations
- Consistency of websites
- Cookie differences between
 - landing and inner pages
 - Mobile and desktop
- Impact of CCPA

Methodology



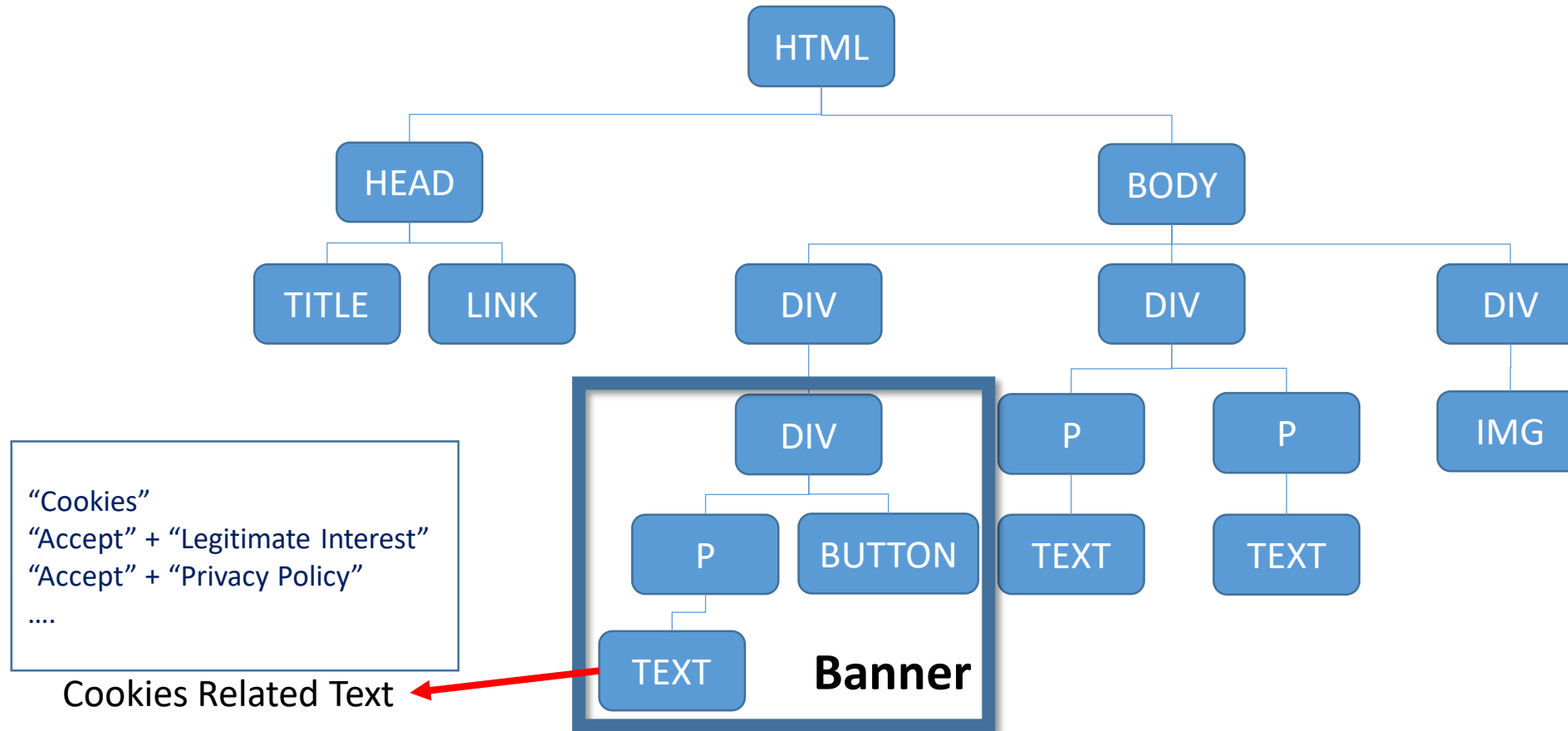
BannerClick



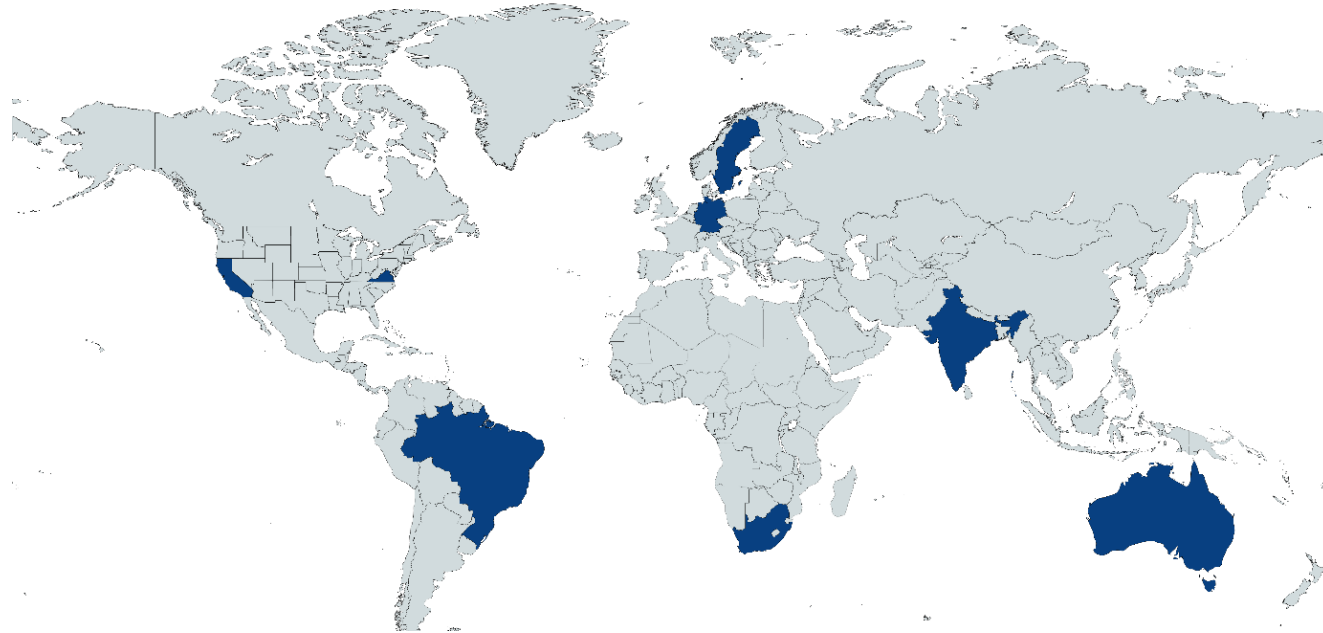
Research Challenges

- There is no standardization of banners; they differ in:
 - Shape & size
 - Location (top, bottom, middle etc.)
 - Content
 - Language
- Websites with Consent Management Platform (CMPs)
 - CMP are dedicated contractors just to manage banners
 - They use different APIs to show banner
- Banners adhere to different privacy laws differently
 - Banners respecting GDPR show “accept” and “reject” options
 - Banners respecting CCPA contains “DNMPI” link

BannerClick – Detection

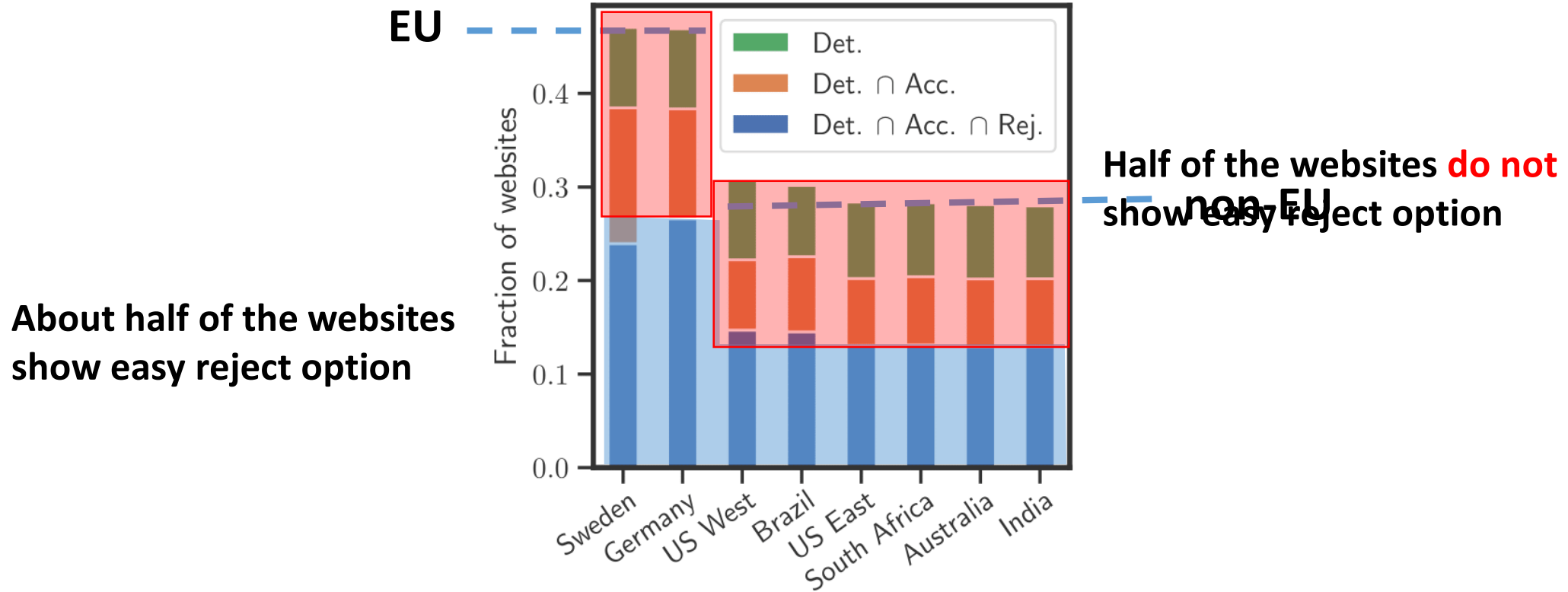


Measurement Setup



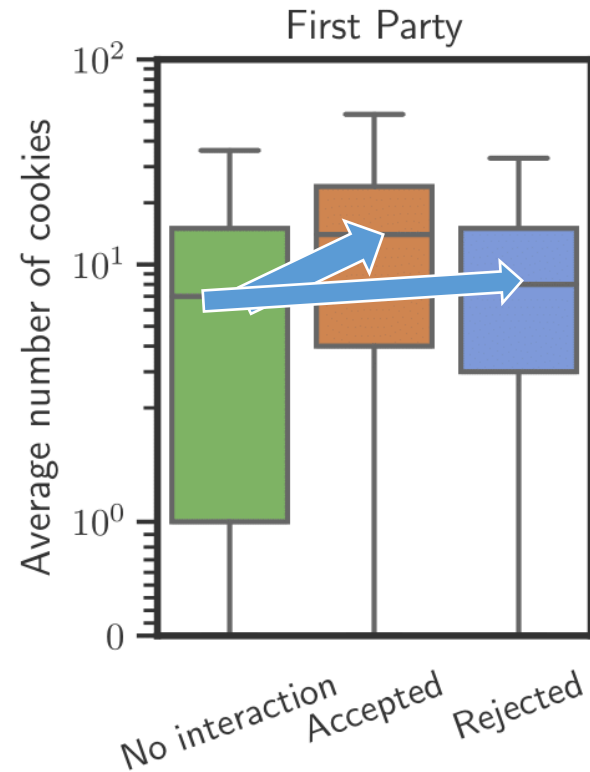
- **8 vantage points:** Germany, Sweden, US West, US East, India, Brazil, South Africa, Australia
- **Target list:** Tranco Top 10k domains

Banners Detected, Accepted, Rejected



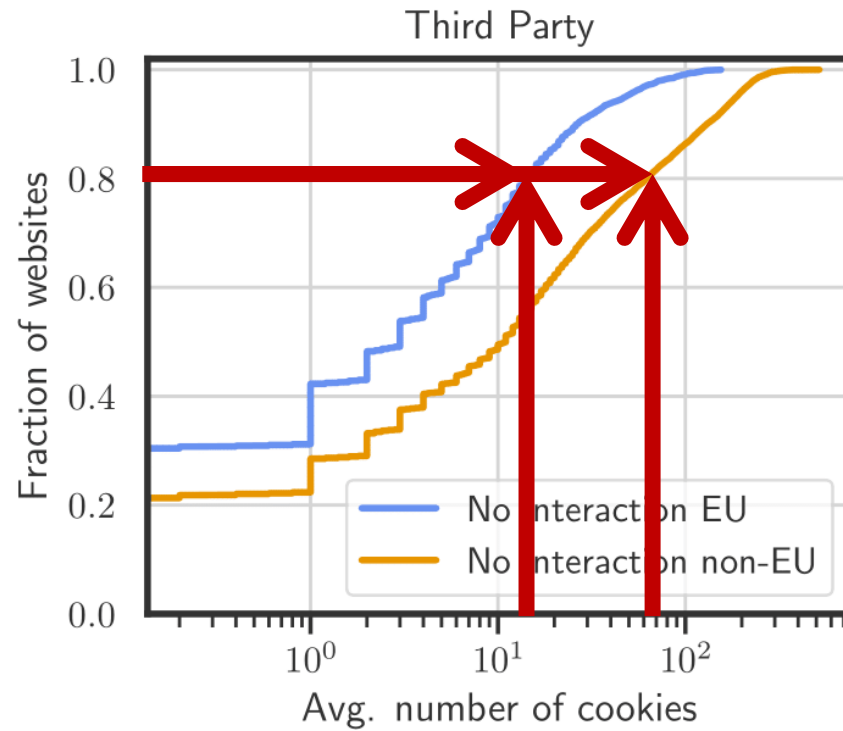
More banners in EU compared to non-EU countries

Cookies Differences After Interaction



Interacting with banners impacts cookie distribution

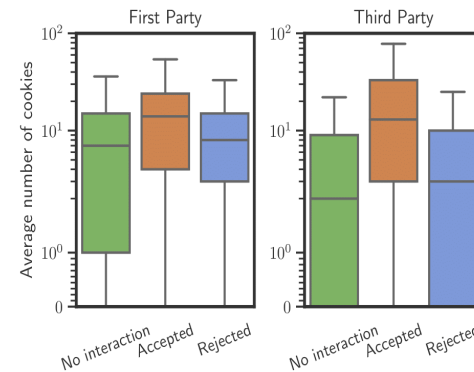
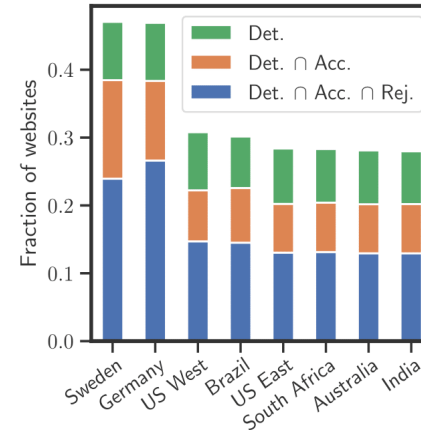
Cookies – EU vs. non-EU



Fewer cookies in EU compared to non-EU

Conclusion

- Impact of
 - Geographical location of users
 - Interaction with banner
- Check out the paper
 - CCPA impact
 - Landing vs. Inner pages
 - Mobile vs. Desktop
 - Consistency analysis
- Source code available
 - BannerClick
 - Analysis data for reproducibility



[bannerclick.github.io](https://github.com/bannerclick)

Prospective Students

- We target top-tier security/networks venues
 - CCS, Usenix Security, NDSS, PETS, IMC, IEEE S&P, AsiaCCS
- On average requires 2 years to publish a paper
- You have knack for systems and networks
 - Apply!
- Keen in Network Security
 - Apply!
- Want to see tangible security impact on society
 - Apply!

Future Research

- On Privacy Laws
 - India recently passed data privacy bill; studying the cookie landscape, data retention etc.
- Network Structure
 - Analyzing the topological properties of Bitcoin
- Studying threat landscape of recently deployed anonymous mix network (NYM)
- Internet traffic filtering
 - How VoIP calls are filtered in the middle east
- Studying the impact of Deniability offered by E2E protocols like Signal