SEPTEMBER 16 @ 1 PM ET

WHAT ZOOM GOT WRONG WITH E2EE 🙀

PRESENTED BY PATRICK WALSH,
CO-FOUNDER & CEO OF IRONCORE LABS.

@ironcorelabs

AGENDA

Less technical

1. Set a baseline
2. Recap Zoom's big 2020 fails
3. Credit where it's due
4. Aside: SaaS trust models

More technical

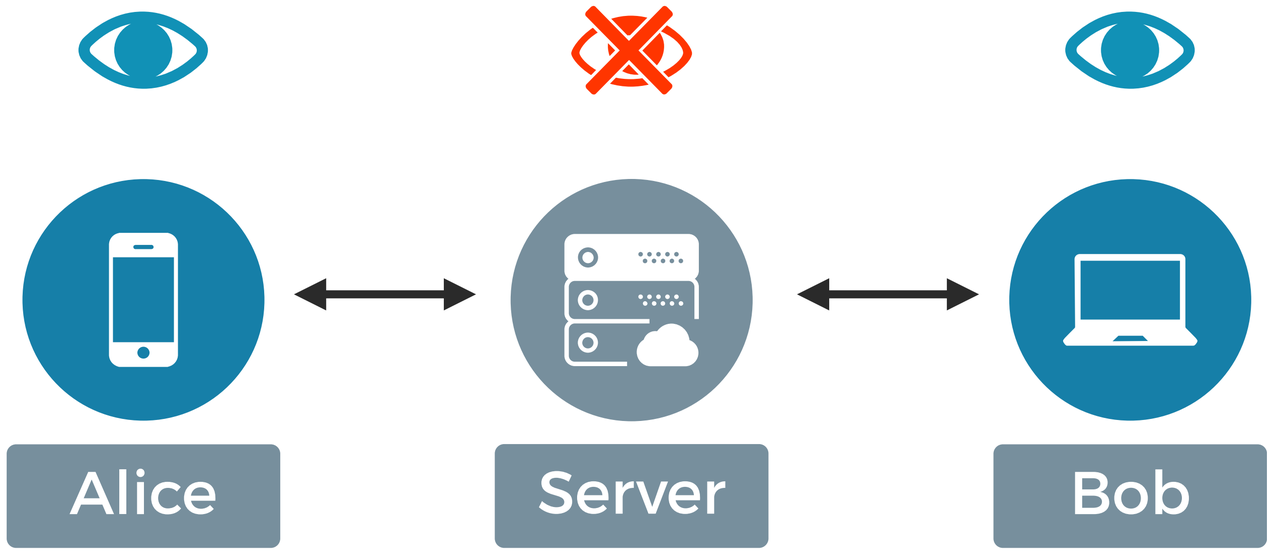
5. Zoom's E2EE architecture
6. Alternative architecture
7. Summary

E2EE: A DEFINITION

Establish a shared baseline
(And here's why...)

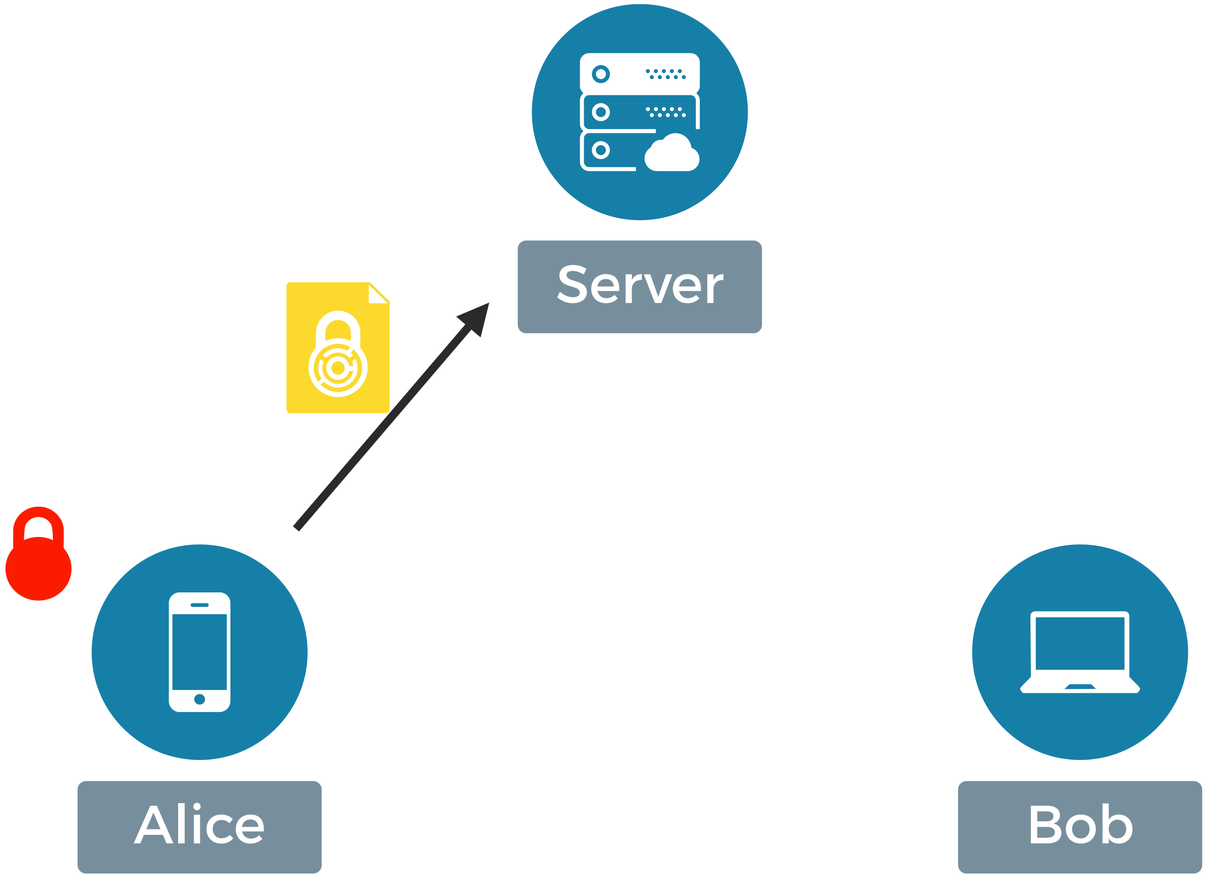
WHAT IS E2EE?

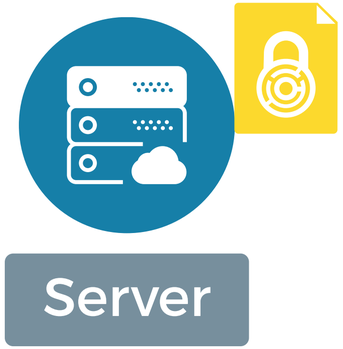
WHAT IS E2EE?



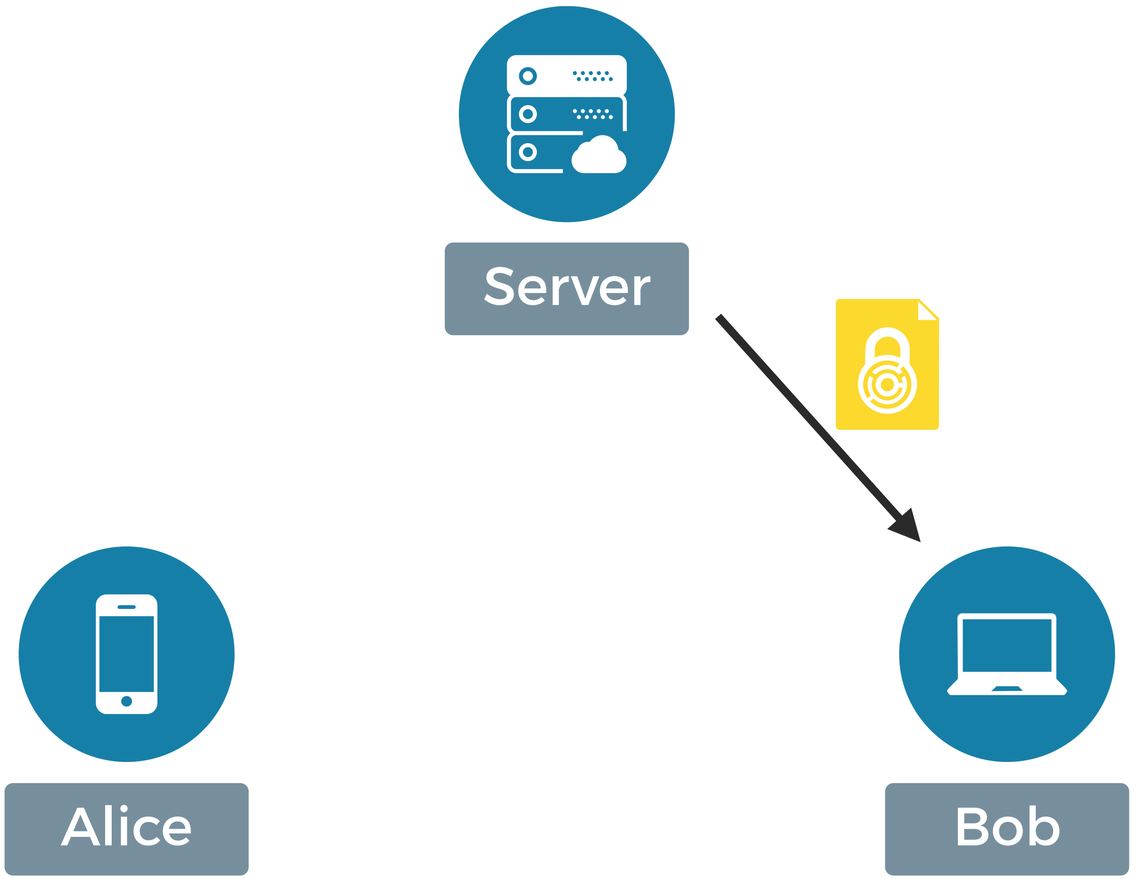
Alice talks to Bob via a server
which can’t see/hear the conversation.

Alice says, “hi bob” and encrypts that message before sending it.



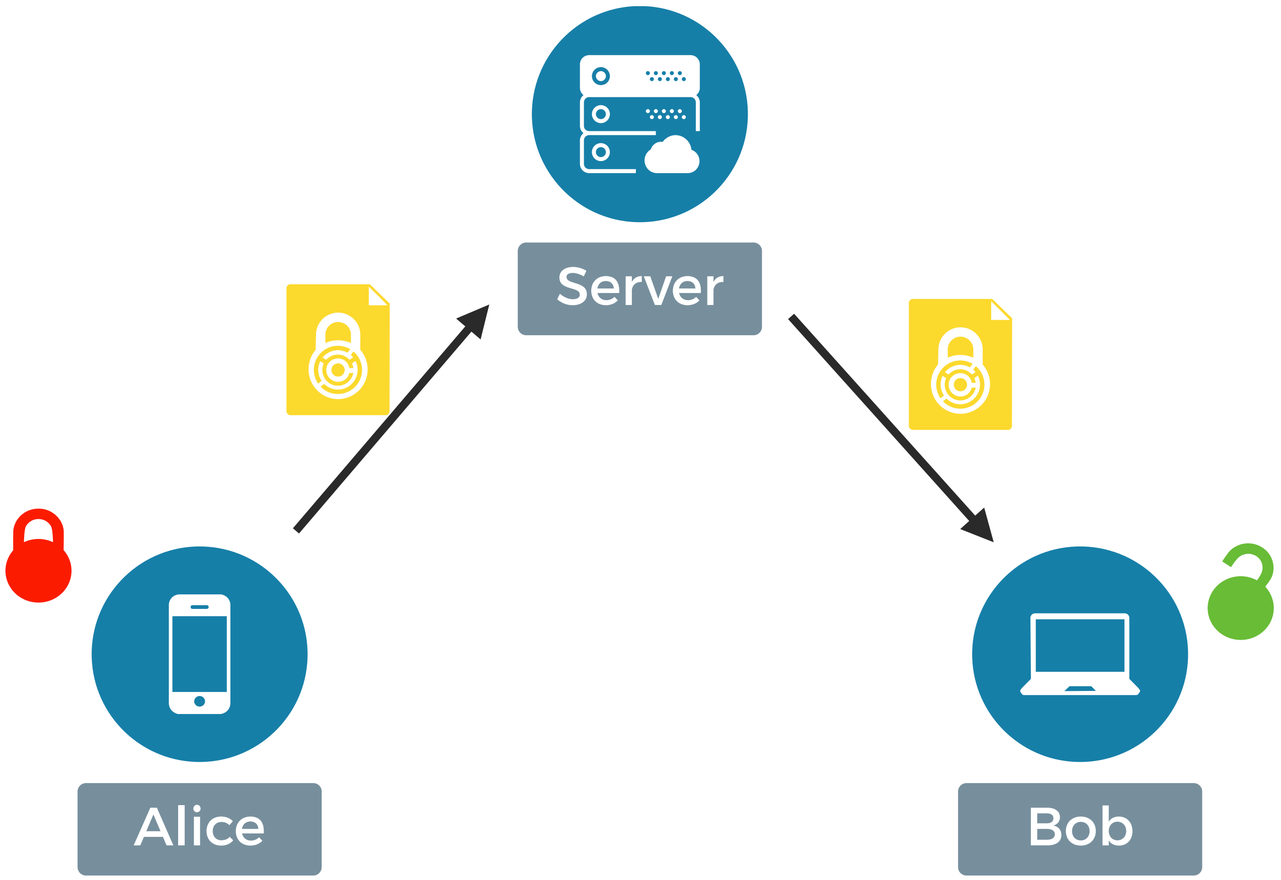


The server only sees
“AR3Z84M...”.
It never sees a key that could decrypt the data.



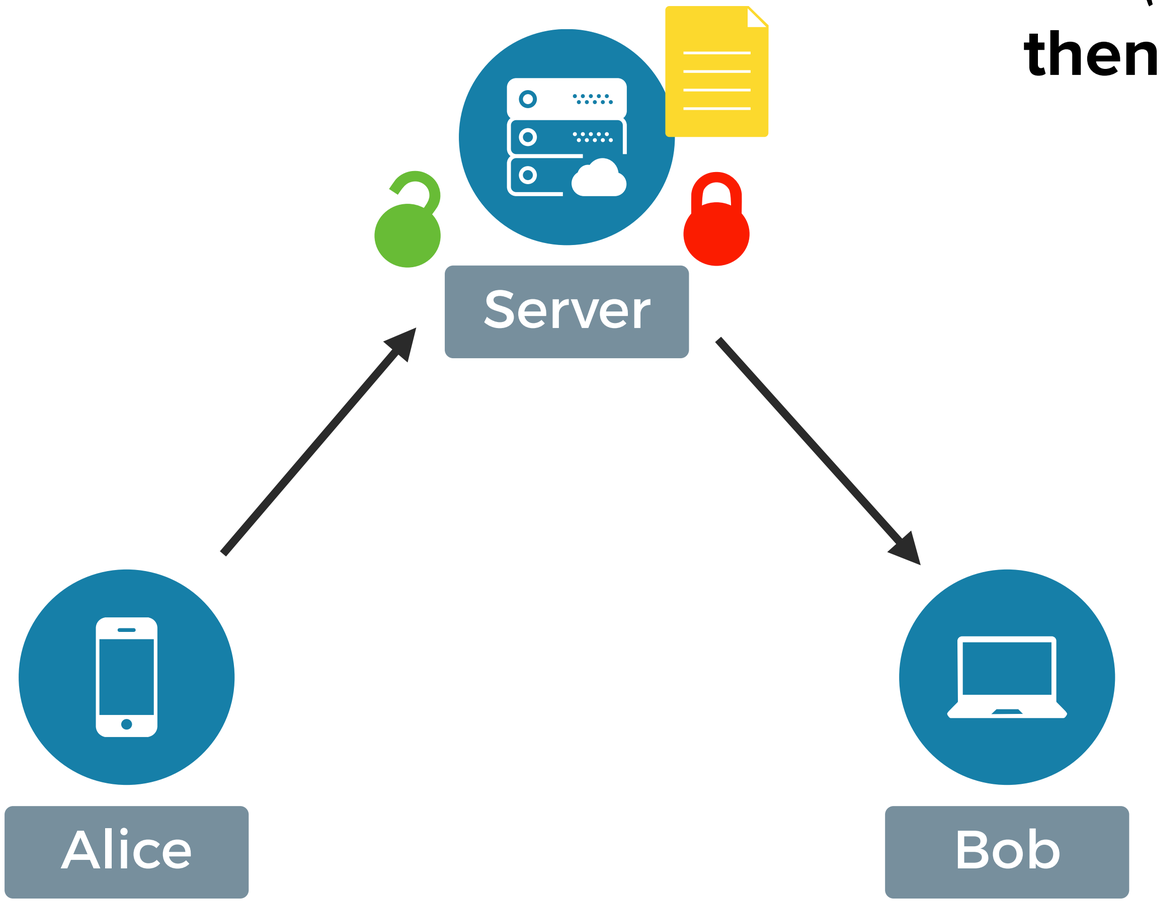
Bob decrypts the message and hears “hi bob.”

WHAT ISN'T E2EE?



Not sufficient to say Alice encrypts and Bob decrypts.

If the server decrypts it
(or could),
then it isn't E2EE.



“We protect your data with military grade encryption at rest and in transit.”

“MILITARY GRADE”

“We protect your data with military grade encryption at rest and in transit.”

–Bullshit Artist (or marketing department)

Using some AES algorithm. But: easy to screw up. No concept of who holds the keys.
This webinar is protected by “military grade encryption.”

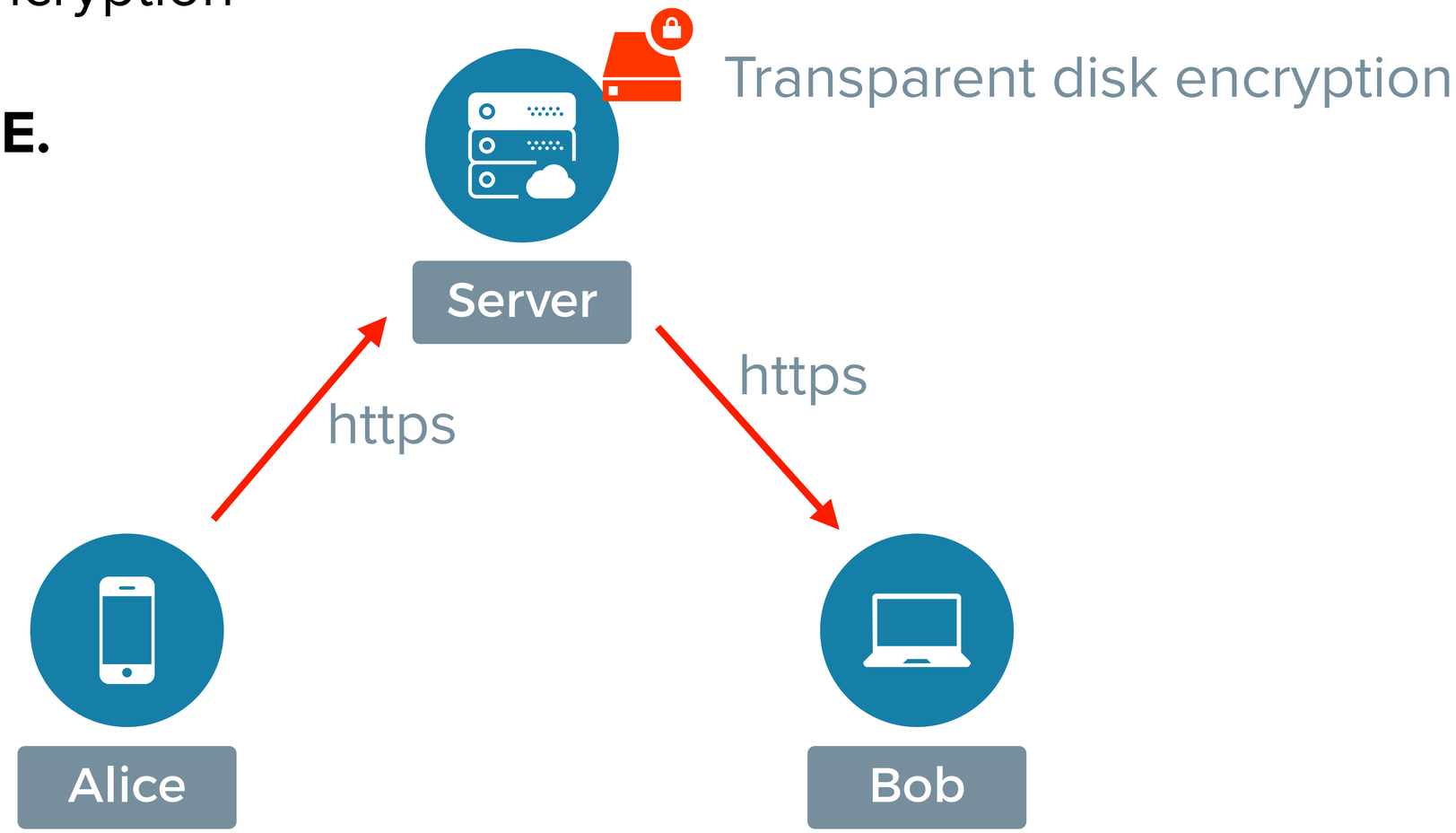
“AT REST AND IN TRANSIT”

“We protect your data with military grade encryption at rest and in transit.”

–Bullshit Artist (or marketing department)

We do the most basic thing possible: we use SSL/TLS and transparent disk encryption.

Transparent disk encryption
plus SSL
IS NOT E2EE.



The data is vulnerable to an attack against the running server.

THE ZOOM STORY: A 2020 RECAP

Yeah, we know, 2020 is maybe better forgotten...

zoom

Security Guide
Zoom Video Communications Inc.

Client Application

Role-based user security

The following pre-meeting security capabilities are available to the meeting host:

- Enable end-to-end encrypted meeting
- Secure log-in using standard username and password or SAML Single Sign On
- Start a secured meeting with password
- Schedule secured meetings with password

E2E Chat Encryption

Zoom end-to-end (E2E) chat encryption allows for a secured communication where only the intended recipient can read the secured message. Zoom use public and private key to encrypt the chat session with Advance Encryption Standard (AES256). Session keys are generated with device unique hardware ID to avoid data being read from other devices. This ensures that the session can not be eavesdropped or tampered with.

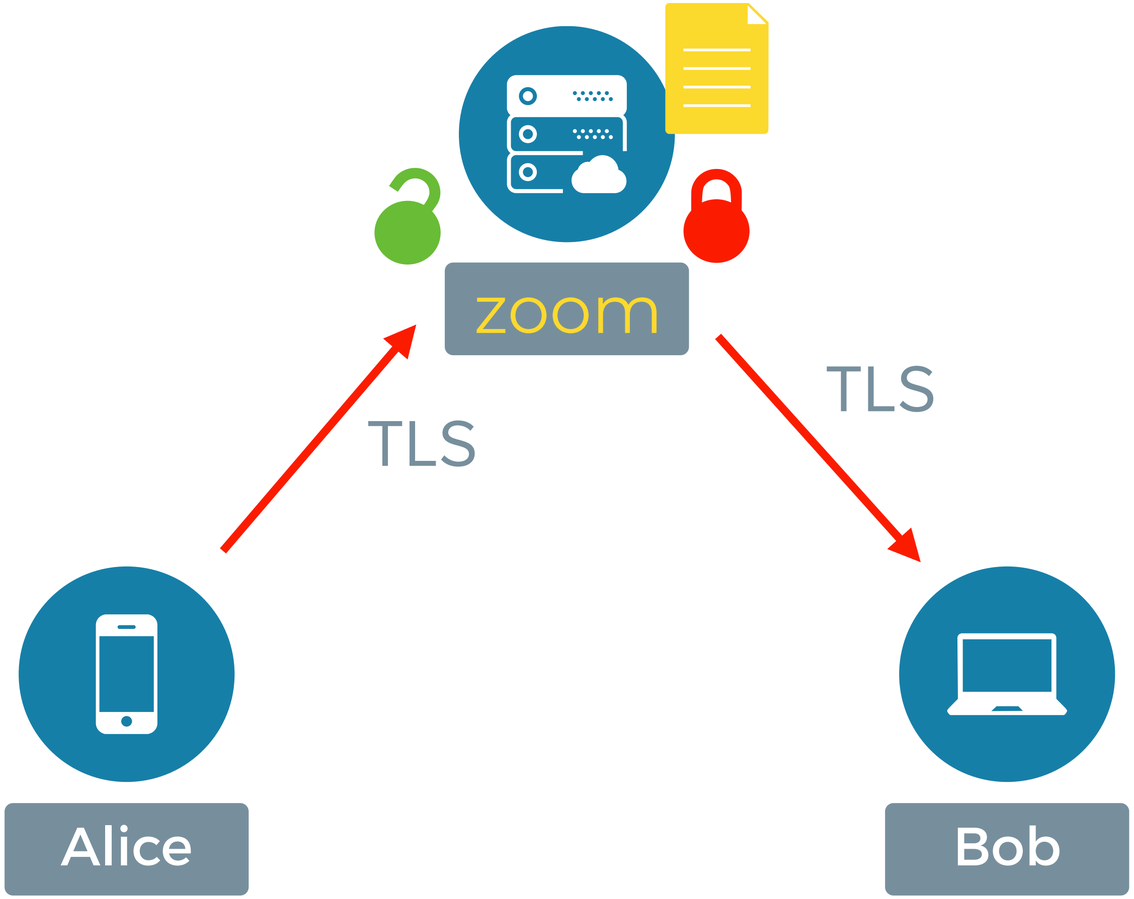
Application security: Zoom can encrypt all presentation content at the application layer using the Advanced Encryption Standard (AES) 256-bit algorithm.

Secured Communications

Zoom can secure all session content by encrypting the communications channel between the Zoom client and the multimedia router using a 256-bit Transport Layer Security (TLS) encryption tunnel.

- 👍 In their marketing, their app, and their Security Guide, Zoom **advertised End to End Encryption**.
- 😩 But their multimedia router decrypted all of the audio and video content that passed through it.

THAT'S NOT E2EE



The Intercept_

ZOOM MEETINGS AREN'T END-TO-END ENCRYPTED, DESPITE MISLEADING MARKETING

The video conferencing service can access conversations on its platform.

Micah Lee, Yael Grauer

March 31 2020, 2:00 a.m.

HELL HATH NO FURY LIKE SECURITY RESEARCHERS MISLEAD

Privacy advocates and lawyers are pissed, too...

Feedback in chat

WHAT WAS YOUR REACTION TO THIS NEWS?

WHY DOES IT MATTER?

Can’t we just trust Zoom?

Seems unlikely they’re listening in to millions of calls.

WHO IS ZOOM?

Many people, partners, and governments

- **Zoom's employees** — at least the Operations group and probably also Engineering.
  - **Global workforce** — including in countries that actively conduct industrial espionage.
- **Zoom's operating countries** — Zoom is subject to the laws of the countries they operate in.
- **Zoom's security practices** — how well are they really protecting that data?

LOWLIGHTS FROM THE WORST TWO MONTHS

MOTHERBOARD
TECH BY VICE

Zoom iOS App Sends Data to Facebook Even if You Don't Have a Facebook Account

Zoom's privacy policy isn't explicit about the data transfer to Facebook at all.

By Joseph Cox

March 26, 2020, 6:00am Share Tweet Snap

Ex-NSA hacker drops new zero-day doom for Zoom

Zack Whittaker @zackwhittaker / 7:00 am MST • April 1, 2020 Comment

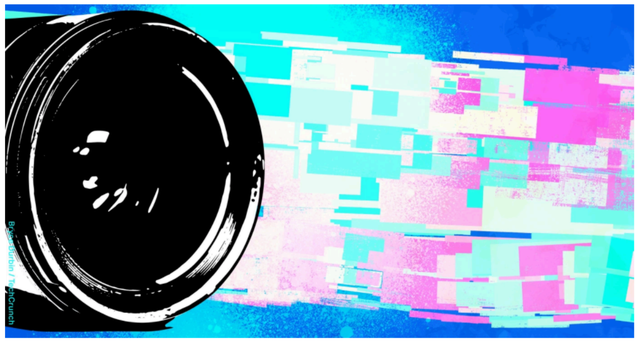


Image Credits: Bryce Durbin/TechCrunch

Mashable TECH SCIENCE SOCIAL GOOD AMPLIFY MORE

Tech FOLLOW MASHABLE >

Zoom is a work-from-home privacy disaster waiting to happen

2020

MAR

Doc Searls Weblog

Home About Me2B People vs. Adtech

‹ We haven't seen this movie before • More on Zoom and privacy ›

Zoom needs to clean up its privacy act

March 27, 2020 in adtech, advertising, Business, conferencing, privacy, problems | 5 comments

[21 April 2020—Hundreds of people are arriving here from this tweet, which calls me a "Harvard researcher" and suggests that this post and the three that follow are about "the full list of the issues, exploits, oversights, and dubious choices Zoom has made." So, two things. First, while I run a project at Harvard's Berkman Klein Center, and run a blog that's hosted by Harvard, I am not a Harvard employee, and would not call myself a "Harvard researcher." Second,

The New York Times

The Coronavirus Outbreak › LIVE Latest Updates Maps and Cases Vaccine Tracker F.D.A. Regul

New York Attorney General Looks Into Zoom's Privacy Practices

As the videoconferencing platform's popularity has surged, Zoom has scrambled to address a series of data privacy and security problems.

The New York Times

The Coronavirus Outbreak › LIVE Latest Updates Maps and Cases Vaccine Tracker Limited Valu

'Zoombombing' Becomes a Dangerous Organized Effort

Zoom, the videoconferencing app, has become a target for harassment and abuse coordinated in private off-platform chats.

The 'S' in Zoom, Stands for Security

uncovering (local) security flaws in Zoom's latest macOS client

by: Patrick Wardle / March 30, 2020

HOME › TECH

Zoom is being sued for allegedly handing over data to Facebook

Bustle

Life

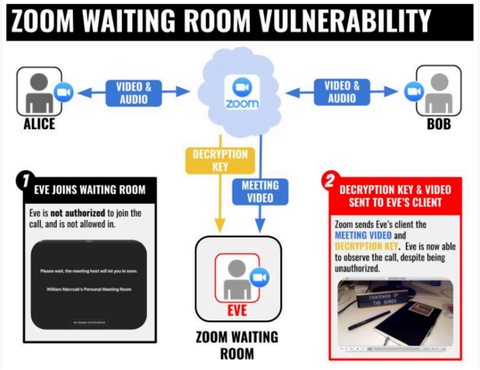
This Hidden Zoom Feature Tells Your Boss When You're In Other Tabs During A Meeting

'Zoombombing' Attacks Disrupt Classes

Online Zoom classes were disrupted by individuals spewing racist, misogynistic or vulgar content. Experts say professors using Zoom should familiarize themselves with the program's settings.

By Elizabeth Redden // March 26, 2020

Zoom's privacy policy: "**Does Zoom sell Personal Data? Depends what you mean by 'sell.'**"



A Feature on Zoom Secretly Displayed Data From People's LinkedIn Profiles

After an inquiry from Times reporters, Zoom said it would disable a data-mining feature that could be used to snoop on participants during meetings without their knowledge.

TC

INTERNATIONAL • ONLINE SECURITY

Zoom backlash intensifies as companies from Daimler to BofA institute bans and curbs over security concerns

BY DEBBY WU, VLAD SAVOV, LANANH NGUYEN, AND BLOOMBERG

April 23, 2020 3:15 AM MST

2020

APR

MOTHERBOARD
TECH BY VICE

Zoom is Leaking Peoples' Email Addresses and Photos to Strangers

For at least a few thousand people, Zoom has treated their personal email addresses as if they all belong to the same company, letting them video call each other.

Zoom admits some calls were routed through China by mistake

Zack Whittaker

@zackwhittaker / 6:12 pm MDT • April 3, 2020

Save Comment

Image: TechRepublic/Brandon Vigliarolo

LEADERSHIP & MANAGEMENT NEW YORK CITY DEPARTMENT OF EDUCATION

NYC forbids schools from using Zoom for remote learning due to privacy and security concerns

ADVERTISING/SPEA

Posts Tagged: zWarDial

A Little Sunshine / The Coming Storm / Time to Patch — 77 Comments

2 'War Dialing' Tool Exposes Zoom's Password Problems

APR 20

As the Coronavirus pandemic continues to force people to work from home, countless companies are now holding daily meetings using videoconferencing services from **Zoom**. But without the protection of a password, there's a decent

Advertisement

EDITORS' PICK | 42,358 views | Apr 1, 2020, 12:45pm EDT

Zoom Users Beware: Here's How A Flaw Allows Attackers To Take Over Your Mac Microphone And Webcam

Kate O'Flaherty Senior Contributor

Cybersecurity

I'm a cybersecurity journalist.

ars TECHNICA SUBSCRIBE SIGN IN

UNPATCHED BUG —

Attackers can use Zoom to steal users' Windows credentials with no warning

Zoom for Windows converts network locations into clickable links. What could go wrong?

DAN GOODIN - 4/1/2020, 10:38 AM

Your Zoom videos could live on in the cloud even after you delete them

Yet another Zoom issue found.

The Intercept_

ZOOM'S ENCRYPTION IS "NOT SUITED FOR SECRETS" AND HAS SURPRISING LINKS TO CHINA, RESEARCHERS DISCOVER

Zoom rolled out its own encryption system and included an algorithm with known serious issues, say University of Toronto researchers.

Micah Lee

April 3 2020, 4:00 a.m.

@ironcorelabs

WHY PICK ON ZOOM?

Aren't they following best practices?

(Bear with us: we'll balance out all the negatives in a minute.)

1. ZOOM IS THE LEADER

zoom	skype	Cisco webex
64% market share	26% market share	10% market share

Video conferencing market share

Per Bessemer's 2020 State of the Cloud

Or by daily active users:

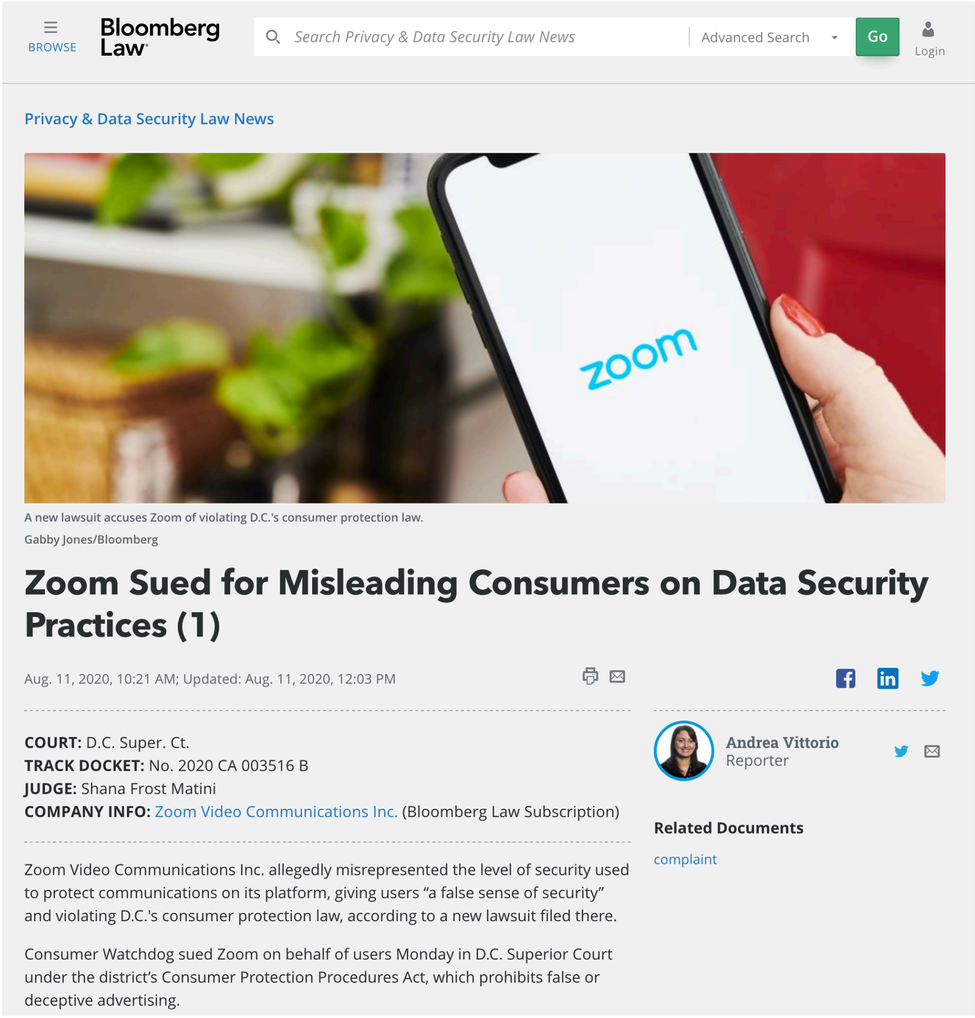
Zoom: 300m, Meet: 100m, Teams: 75m [as of June 2020]

Zoom is still the leader.

2. ZOOM LIED

And got caught

(eventually)



BROWSE

Bloomberg Law

Search Privacy & Data Security Law News

Advanced Search

Go

Login

Privacy & Data Security Law News

A new lawsuit accuses Zoom of violating D.C.'s consumer protection law.

Gabby Jones/Bloomberg

Zoom Sued for Misleading Consumers on Data Security Practices (1)

Aug. 11, 2020, 10:21 AM; Updated: Aug. 11, 2020, 12:03 PM

COURT: D.C. Super. Ct.
TRACK DOCKET: No. 2020 CA 003516 B
JUDGE: Shana Frost Matini
COMPANY INFO: Zoom Video Communications Inc. (Bloomberg Law Subscription)

Zoom Video Communications Inc. allegedly misrepresented the level of security used to protect communications on its platform, giving users “a false sense of security” and violating D.C.'s consumer protection law, according to a new lawsuit filed there.

Consumer Watchdog sued Zoom on behalf of users Monday in D.C. Superior Court under the district’s Consumer Protection Procedures Act, which prohibits false or deceptive advertising.

Andrea Vittorio
Reporter

Related Documents

complaint

Who has banned Zoom? Google, NASA, and more

by **Brandon Vigliarolo** in **Security**
on April 9, 2020, 11:34 AM PST

Companies that have banned Zoom

- **Google** has banned Zoom from company-owned computers; administrators will disable it this week, and Google employees have been directed to use Duo instead.
- **SpaceX** has forbidden employees from using Zoom, citing security and privacy concerns.
- **Smart Communications**, a Philippines-based ISP, has banned Zoom for internal use.

Governments and government agencies that have banned Zoom

This list of countries where Zoom won't function is based on the US government's list of sanctions; countries on that list are not included here.

- **Taiwan** has banned Zoom for use by all government agencies.
- **NASA** has banned all employees from using Zoom.
- The **German Foreign Ministry** has restricted Zoom use to personal computers in emergency situations only, as reported by Reuters.
- The **United States Senate** has urged its members to choose platforms other than Zoom due to security concerns, but has not issued an outright ban.
- The **Australian Defense Force** banned its members from using Zoom after an Australian comedian Zoom bombed one of its meetings.

Educational institutions that have banned Zoom

- **New York City's Department of Education** has banned teachers from using Zoom and encourages them to switch to Microsoft Teams.
- **Clark County Public Schools** in Nevada has disabled Zoom on all school computers.

3. ZOOM DUG A DEEP HOLE

Enterprise customers got spooked

4. THEY'RE DIGGING OUT

(And so should everyone.)

Zoom freezes feature development to fix security and privacy issues

Romain Dillet @romaindillet / 3:34 am MDT • April 2, 2020

Comment

Zoom has been widely criticized over the past couple of weeks for terrible security, a poorly designed screensharing feature, misleading dark patterns, fake end-to-end-encryption claims and an incomplete privacy policy. Despite

👍 CREDIT TO ZOOM

#1 POWER + USABILITY

USA TODAY

TECH

If Zoom's out, what about WebEx, Google Meet or Skype? We tried them all, here's what we found

Jefferson Graham USA TODAY

Published 7:00 a.m. ET Aug. 27, 2020 | Updated 3:39 p.m. ET Aug. 28, 2020

View Comments

Product	USA Today Rating
Google Meet	★★½☆☆
Webex	★★★½☆
Skype	★★★☆☆
Microsoft Teams	★★★☆☆
Facebook Messenger Rooms	★★☆☆☆

* We know this misses many other video conferencing options which may have fared better.

- Other options disappointing by comparison.
  - Teachers on Microsoft Teams and Google Meet can't even control who can or can't mute.
  - Host moderation controls are almost non-existent in most platforms where a business setting is assumed.
- None of these companies has end-to-end encryption either (yet).

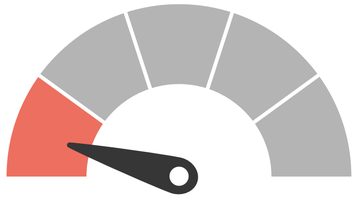
SERIOUS STEPS TOWARD SECURITY

- Apologized and fixed instead of denying and defending
- Dedicated the company to the improvement effort
- Hired top security and cryptography consultants and employees
- Promised end-to-end encryption and sought comment on the detailed plans
- Weekly CEO calls on security/ privacy updates
- Bought an encryption company
- Removed anti-privacy “features”
- Added policy controls governing access across countries
- Updated privacy policy
- Much more…

ASIDE: TRUST MODELS

SAAS TRUST MODELS

(For Confidentiality)

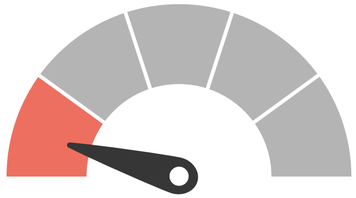


Full Trust

Most SaaS companies require customers to fully trust them, their partners, their employees, and the governments where they do business.

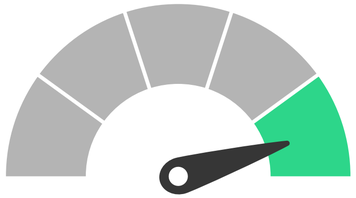
SAAS TRUST MODELS

(For Confidentiality)



Full Trust

Most SaaS companies require customers to fully trust them, their partners, their employees, and the governments where they do business.

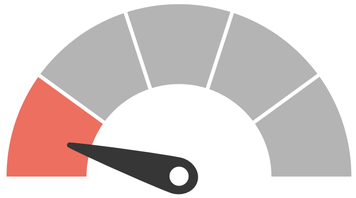


Zero Trust

This is the gold standard where a SaaS provider is never in a position to see customer data. All data is end-to-end encrypted and only clients can decrypt.

SAAS TRUST MODELS

(For Confidentiality)

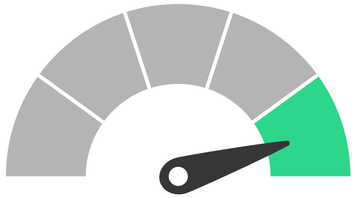


Full Trust

Most SaaS companies require customers to fully trust them, their partners, their employees, and the governments where they do business.

Ephemeral

Companies are granted full access to data and promise to drop the keys needed to access the data if that access isn't renewed. There is not a granular audit trail.

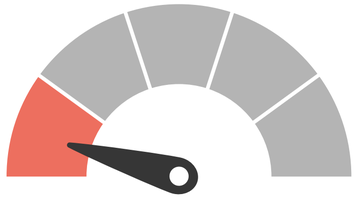


Zero Trust

This is the gold standard where a SaaS provider is never in a position to see customer data. All data is end-to-end encrypted and only clients can decrypt.

SAAS TRUST MODELS

(For Confidentiality)



Full Trust

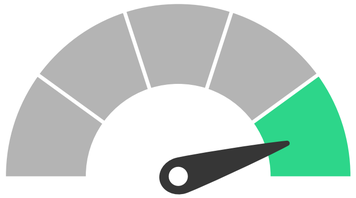
Most SaaS companies require customers to fully trust them, their partners, their employees, and the governments where they do business.

Ephemeral

Companies are granted full access to data and promise to drop the keys needed to access the data if that access isn't renewed. There is not a granular audit trail.

Trust-but-Verify

This security model allows a SaaS company to see and use data, but with no way to bypass cryptographic gates controlled by the customer. This brings transparency of access and rich audit trails.

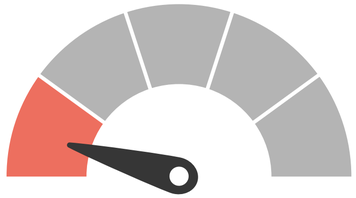


Zero Trust

This is the gold standard where a SaaS provider is never in a position to see customer data. All data is end-to-end encrypted and only clients can decrypt.

SAAS TRUST MODELS

(For Confidentiality)



Full Trust

Most SaaS companies require customers to fully trust them, their partners, their employees, and the governments where they do business.

Ephemeral

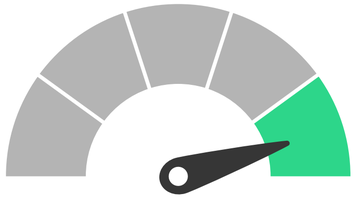
Companies are granted full access to data and promise to drop the keys needed to access the data if that access isn't renewed. There is not a granular audit trail.

Trust-but-Verify

This security model allows a SaaS company to see and use data, but with no way to bypass cryptographic gates controlled by the customer. This brings transparency of access and rich audit trails.

Split Trust

Used when data or ability to access it requires two or more parties to collude. For example, if one company holds the keys and another holds the data and the two come together in the client.

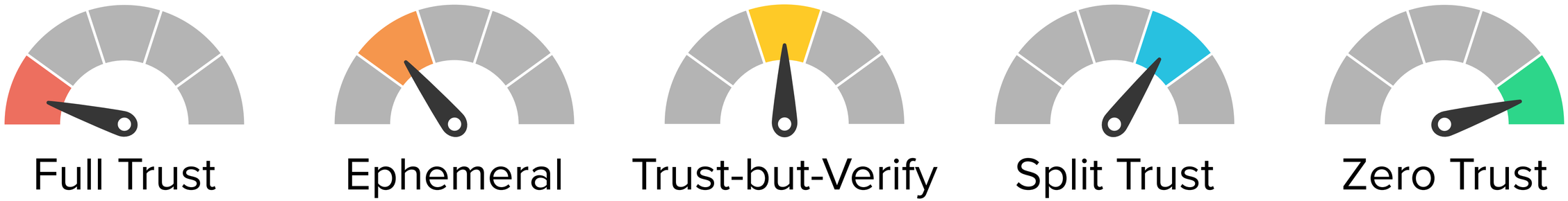


Zero Trust

This is the gold standard where a SaaS provider is never in a position to see customer data. All data is end-to-end encrypted and only clients can decrypt.

SAAS TRUST MODELS

(For Confidentiality)



- **These models can be mixed depending on the data.**
  - As we'll see in a minute, Zoom's E2EE plans don't include things like cloud recordings, which will remain Full Trust.
- **Regarding confidentiality**
  - SaaS still trusted for availability and integrity and maybe for some operations such as revocation of access.

Discussion

DO YOU THINK THE “FULL TRUST” MODEL IS A PROBLEM?

Let us know in the chat if you’re willing to discuss live on video at the end.

ZOOM'S E2EE APPROACH

zoom / zoom-e2e-whitepaper

Watch 35

Code | Issues 9 | Pull requests | Actions | Security | Insights

master | 1 branch | 0 tags | Go to file | Add file | Code

maxtaco rearrange PDFs 3de4dd8 on Jun 17 12 commits

archive	rearrange PDFs	3 months ago
doc	small fix: un-reverse sender and receiver keys in B...	3 months ago
CHANGELOG.md	typo fix in changelog	3 months ago
LICENSE.md	Initial commit	4 months ago
README.md	rearrange PDFs	3 months ago
zoom_e2e.pdf	small fix: un-reverse sender and receiver keys in B...	3 months ago

README.md

Zoom End-to-End Encryption Whitepaper

This is the home of the whitepaper documenting Zoom's planned end-to-end encryption system. The latest released PDF will always be available here. This repository will be updated as we implement and iterate our cryptographic design.

Timeline

- **17 June 2020**: Version 2 was published. See the changelog for a summary of what changed. We still value feedback, recommendation and corrections. Please continue to post them under Issues.
- **22 May 2020 - 5 June 2020**: A comment period on the initial design
- **22 May 2020**: Version 1 was published.

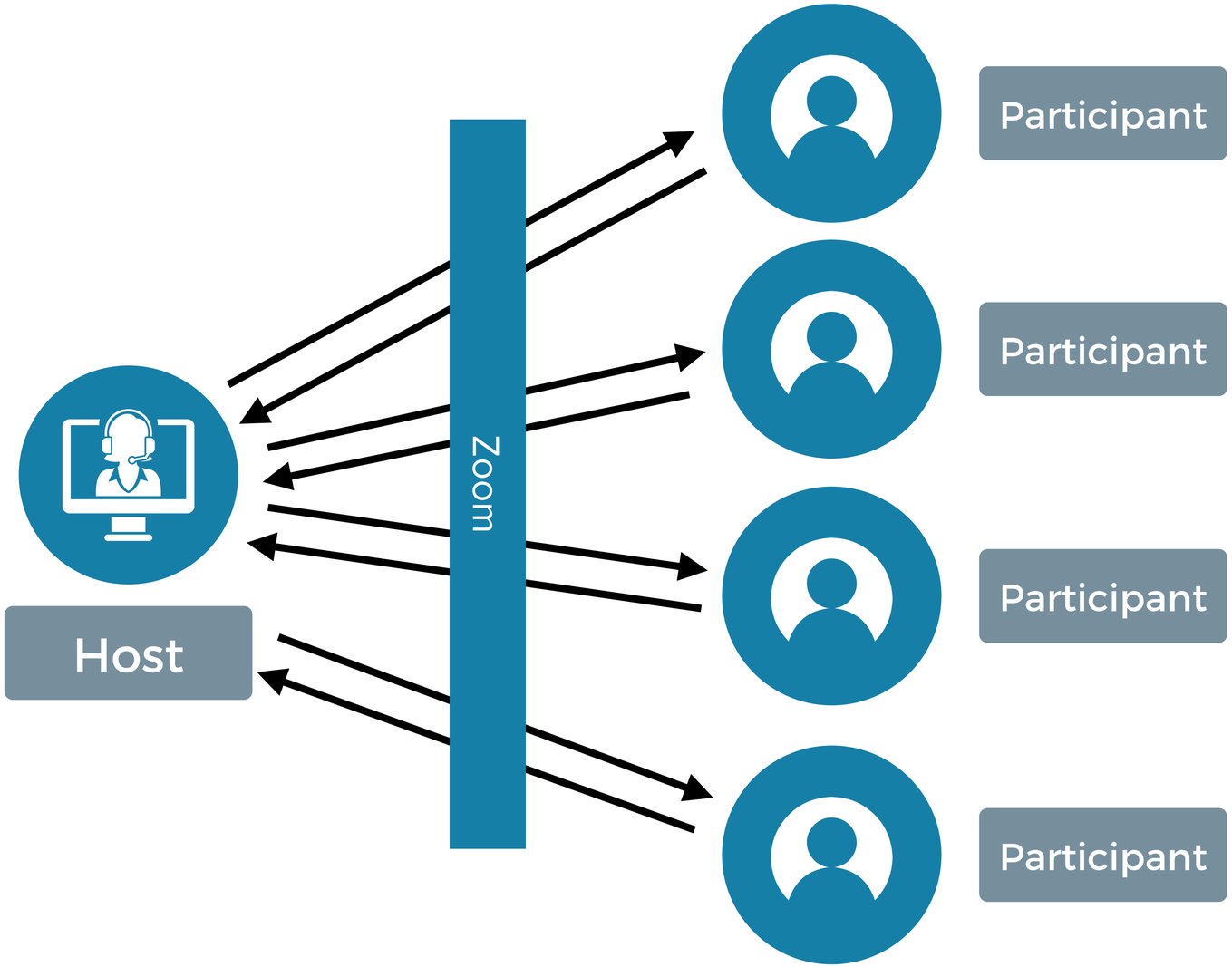
PROLOGUE

- This is a thorough plan and they put it out for public comment.
  - Great move by Zoom.
- There are some very smart people who contributed to this that we admire.

THE MEETING KEY

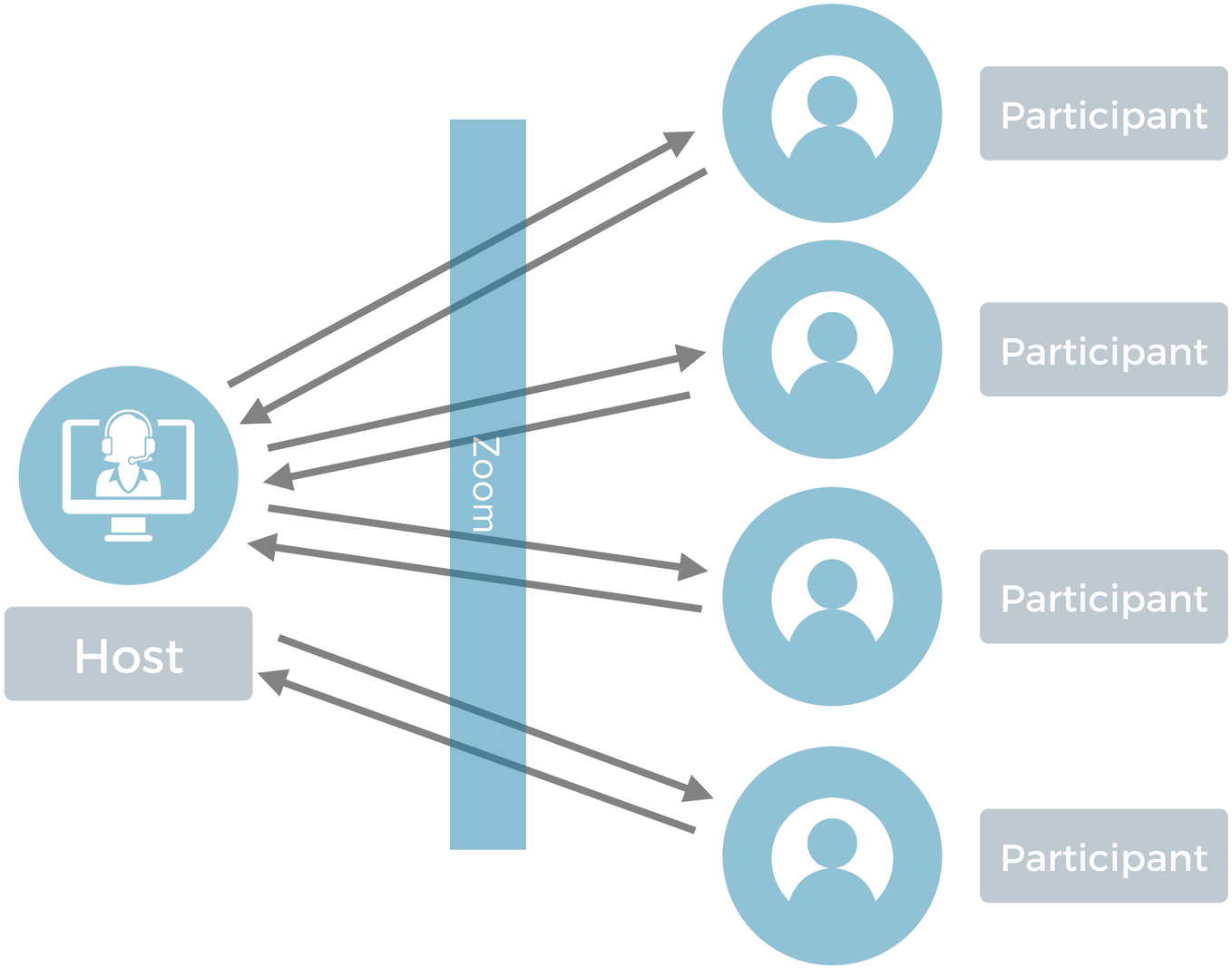
- Meeting contents are symmetrically encrypted with AES using a shared key.
- The key changes through the meeting.
- Most of the protocol is about sharing that key securely so Zoom can't see it and only authorized users can.

BASIC APPROACH



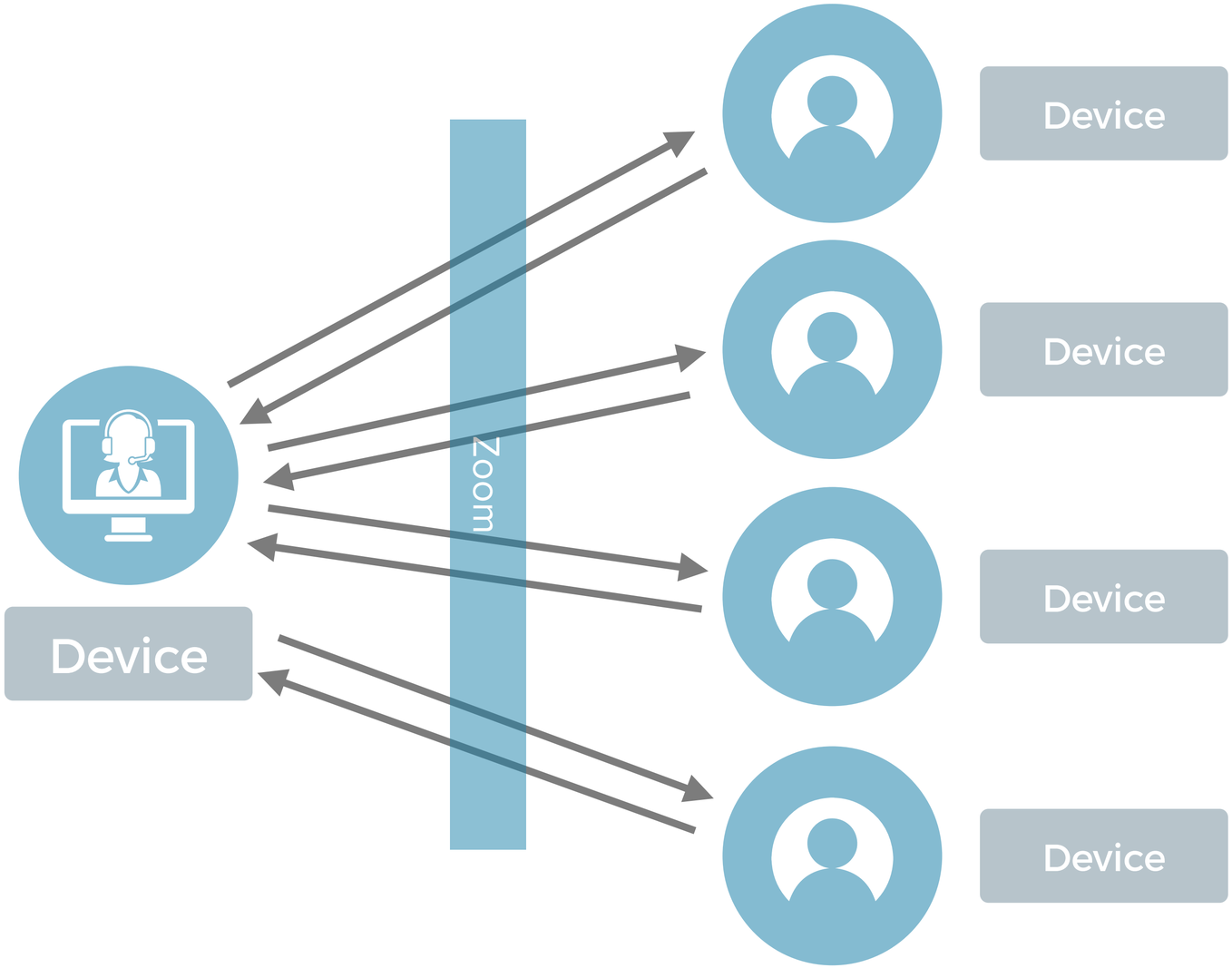
- One-to-one encrypted channels (through Zoom)
- Pairwise negotiation and key distribution
- Device level: per-device signing keys bootstrap the handshake.

BASIC APPROACH 👍



- **Pro's**
  - Well understood.
  - Uses common algorithms and protocols.
  - Point-to-point encryption is something we're reasonably good at (eg, TLS, Noise).

BASIC APPROACH 👎



- **Con's**
  - Everyone has to do lots of accounting on everyone else's devices.
    - Key pinning won't be effective.
  - Not suitable for large meetings
    - Zoom allows up to 1,000 people; 10,000 for webinars.
    - Could brick the host's device (esp. if mobile).
  - Only works for the streaming audio/video, not assets.

MEETING LEADER SECURITY CODE

*"The leader reads out the **meeting leader security code**, and everyone in the meeting in turn does the same thing.*

If the code does not match, the participant should speak up in the meeting, and the leader should rotate the meeting key by kicking them out."

MEETING LEADER SECURITY CODE

- Required to prevent Monkey-in-the-Middle (MitM) attacks.
- Zoom recommends people check the security codes out-of-band (via email or some such).
- Zoom recommends everyone re-read the code every time someone joins.

MEETING LEADER SECURITY CODE

- Unusable in small ones.
- Essentially impossible in a large meeting.
- No one will do this.
- → No real MitM protection.

IDENTITY

- Zoom is the root of trust for identity (Phase 1).
- They envision a future where companies, via a mechanism like SSO, will provide keys for their users.
  - 👍 intra-company meetings, 👎 inter-company meetings.
  - Zoom expects customers to build this.
  - Unlikely in the short-term and risky in the long term.
- **If Zoom's identity servers are subverted, everything else is undermined. Not zero-trust.**

MISSING FUNCTIONALITY

"We will not support Web browsers, PSTN dial-in, and other legacy devices. There also will be no support for "Join Before Host", Cloud Recording, and some other Zoom features."

MISSING FUNCTIONALITY

- You have to start somewhere so I don't want to dwell on this too much.
  - Also legacy devices are just plain impossible to support.
- Disappointing that E2EE meetings will be second-class to "regular" meetings in a number of ways.
- I wish they had set a goal to make E2EE the system-wide default and aimed to have little or no trade off in features and functionality.

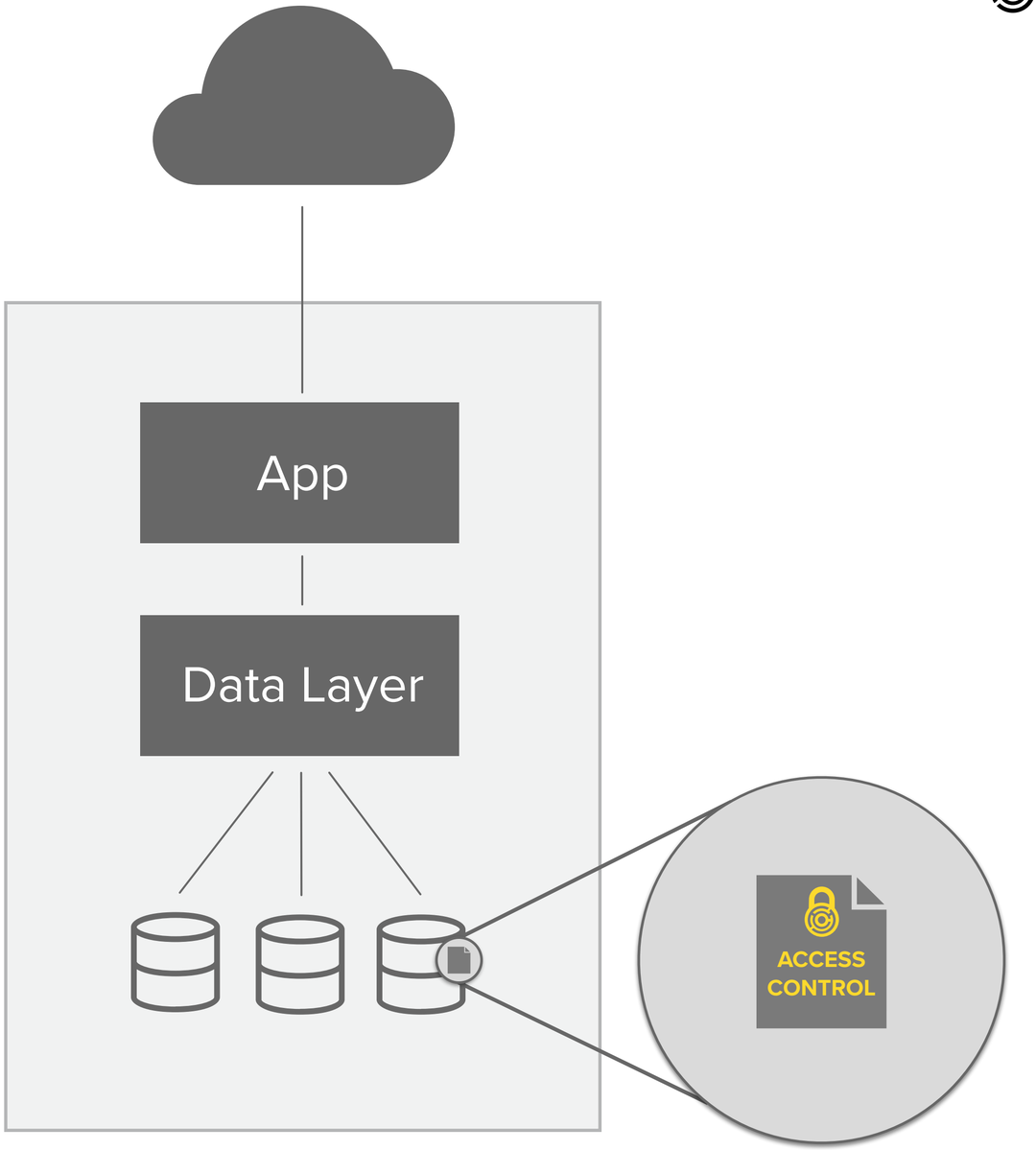
WE CAN DO BETTER

TECHNICAL BACKGROUND

IRONCORE LABS

DATA CONTROL PLATFORM

Enables **zero-trust** and minimal-trust architectures with **cryptographic orthogonal access controls**.

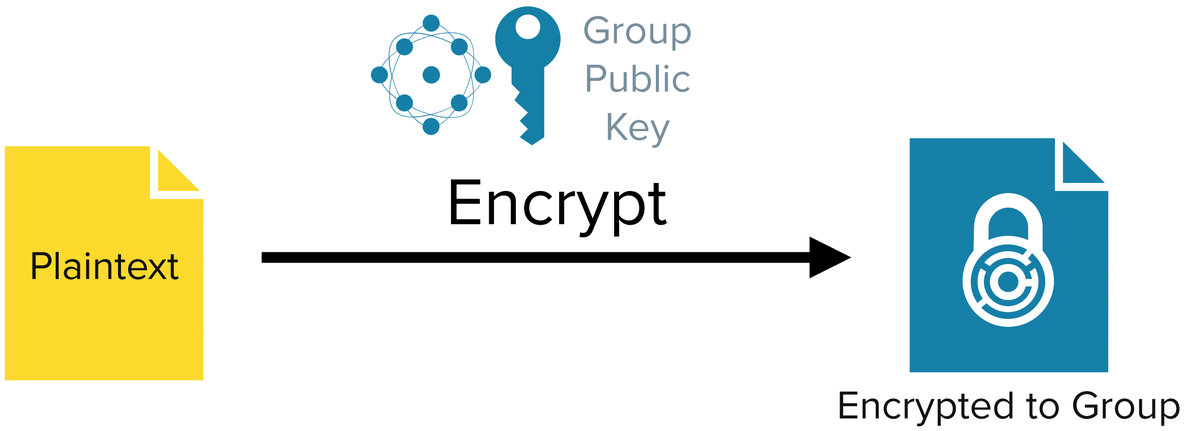


DATA CONTROL PLATFORM

Initially created for stored data, but can be **applied to other domains,** including **video conferences**.

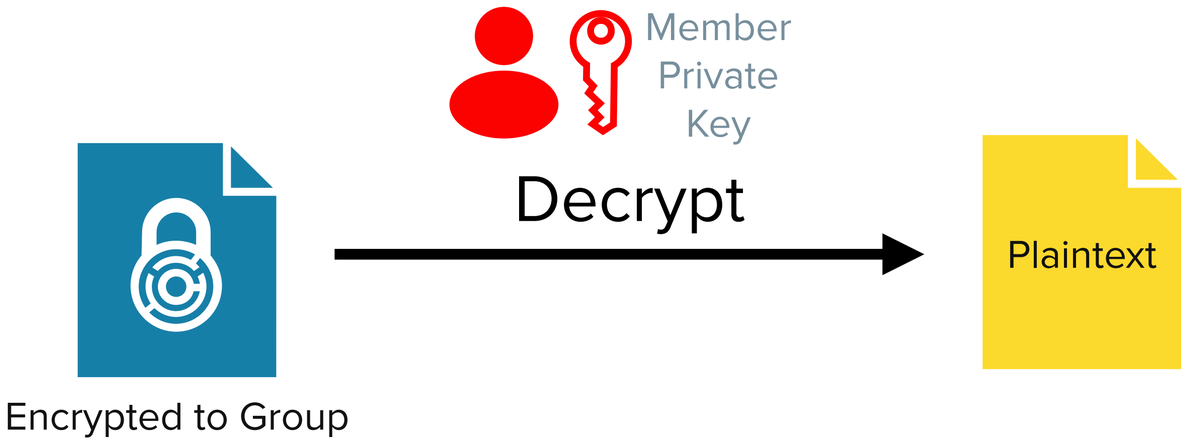
PUBLIC KEY CRYPTOGRAPHY

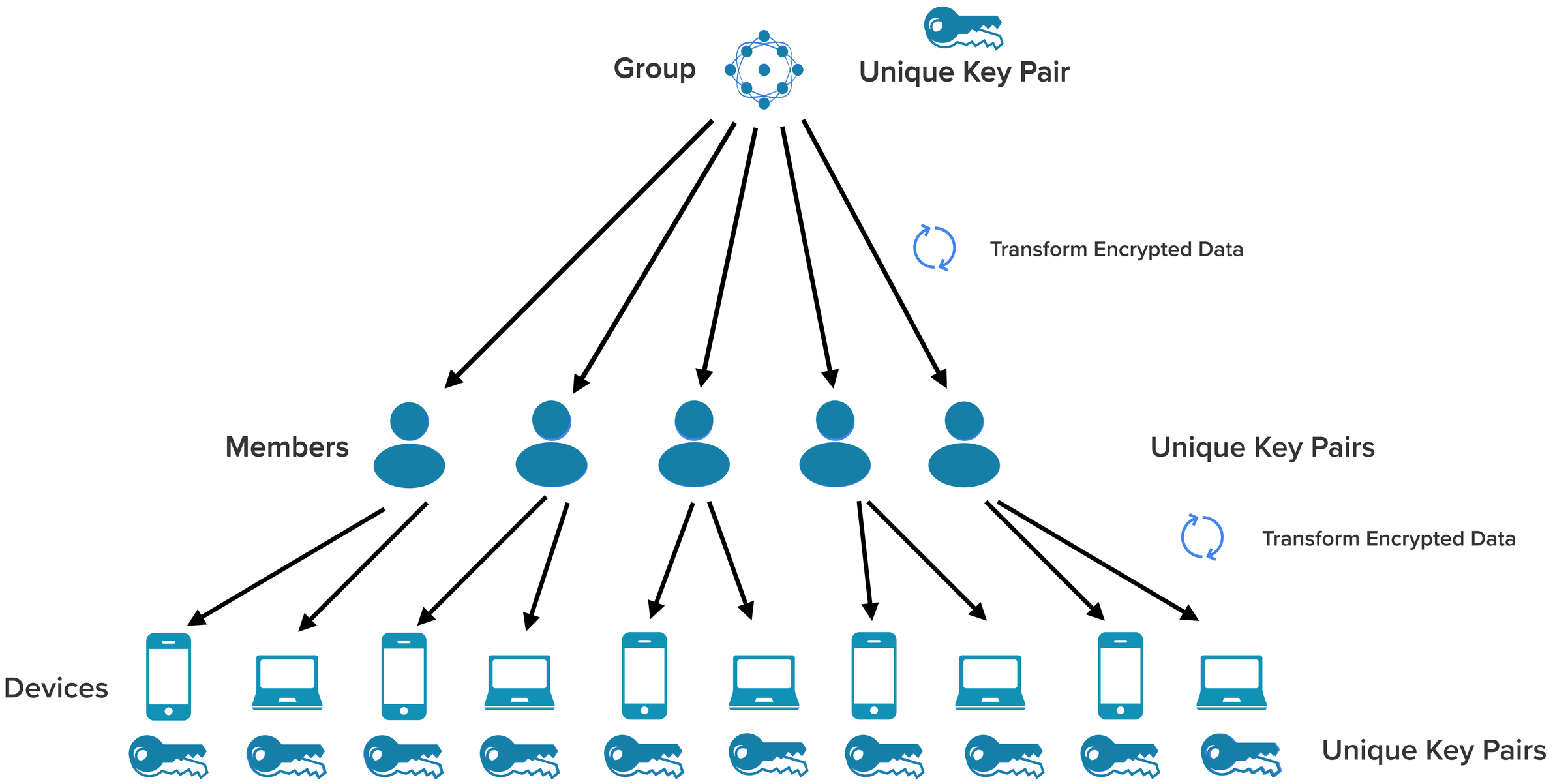
WITH GROUPS

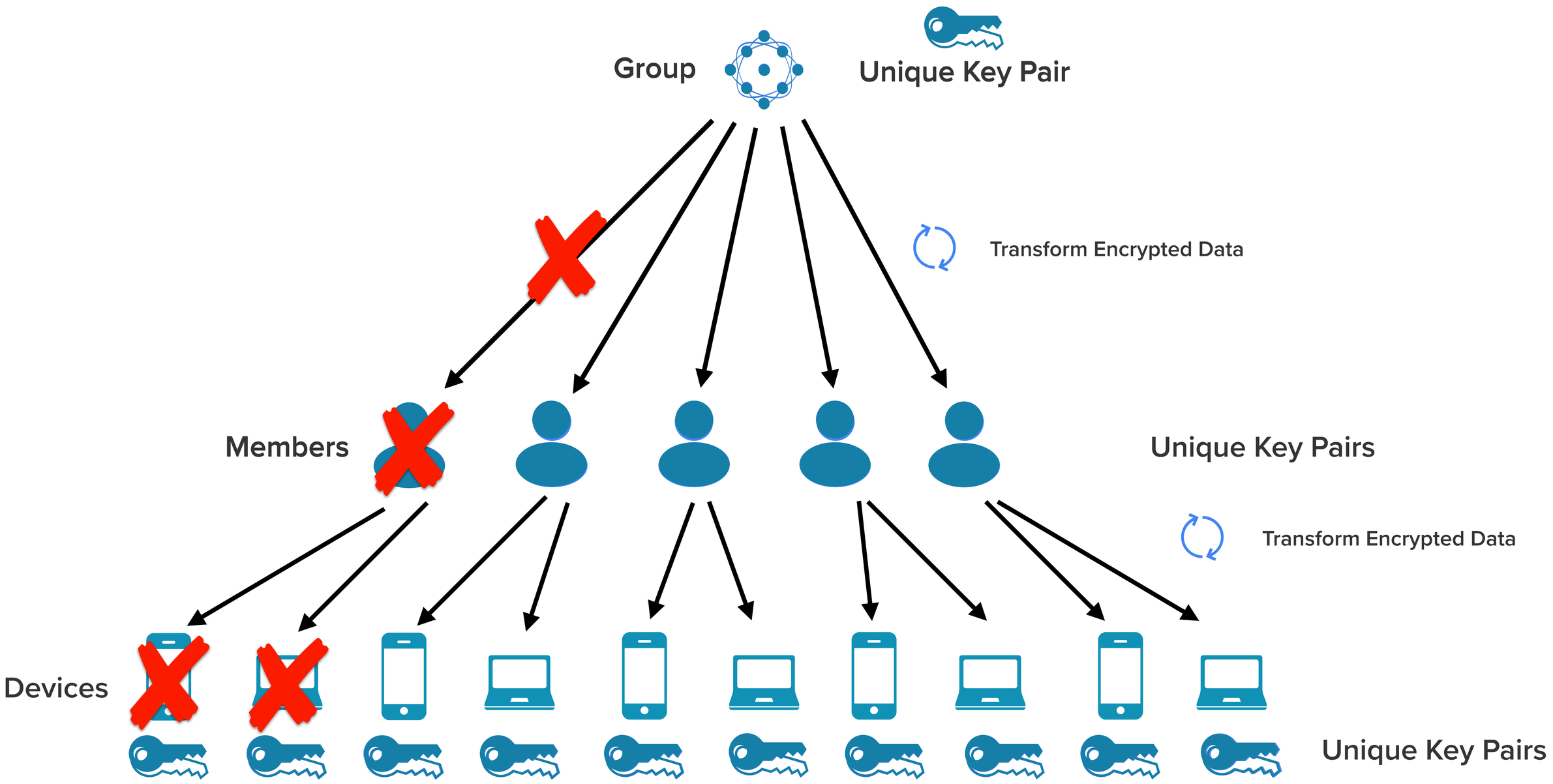


PUBLIC KEY CRYPTOGRAPHY

WITH GROUPS




Group
Unique Key Pair
Transform Encrypted Data
Members
Unique Key Pairs
Transform Encrypted Data
Devices
Unique Key Pairs


Group
Unique Key Pair
Transform Encrypted Data
Members
Unique Key Pairs
Transform Encrypted Data
Devices
Unique Key Pairs

TRANSFORM CRYPTOGRAPHY

Proxy re-encryption with these properties:

- Unidirectional — A → B
- Multi-hop — A → B → C
- Non-interactive — Offline

WHO'S HEARD OF PROXY RE-ENCRYPTION?

It's okay if you haven't...

PROXY RE-ENCRYPTION (PRE)

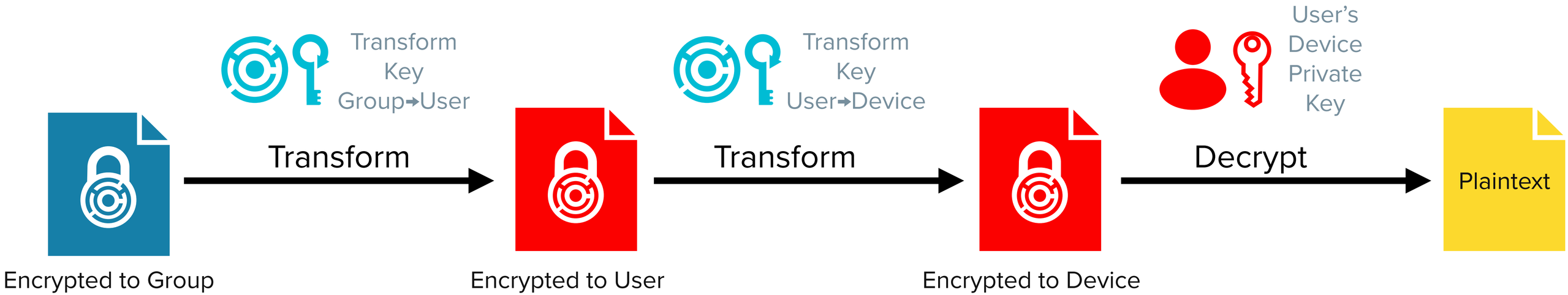
Basic Concept

$C_a \rightarrow \boxed{\text{proxy}} \rightarrow C_b$

A ciphertext for **Alice** can be transformed into a ciphertext for **Bob** with the help of one or more **semi-trusted proxies** without the proxies learning any information about the message or the private keys of the other parties.

TRANSFORM CRYPTOGRAPHY

Basic Example

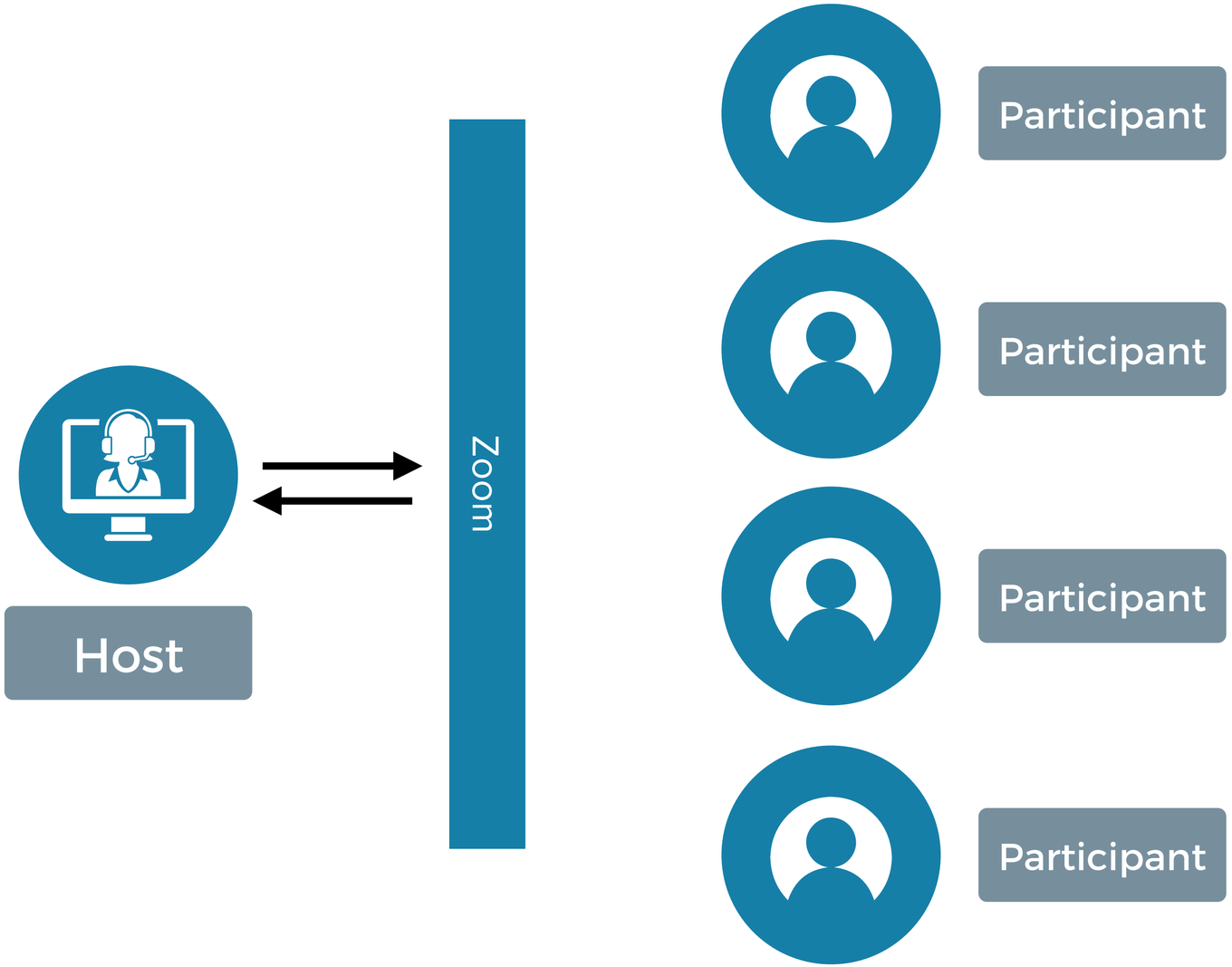


USING TRANSFORM CRYPTO WITH VIDEO CONFERENCING

THE MEETING KEY

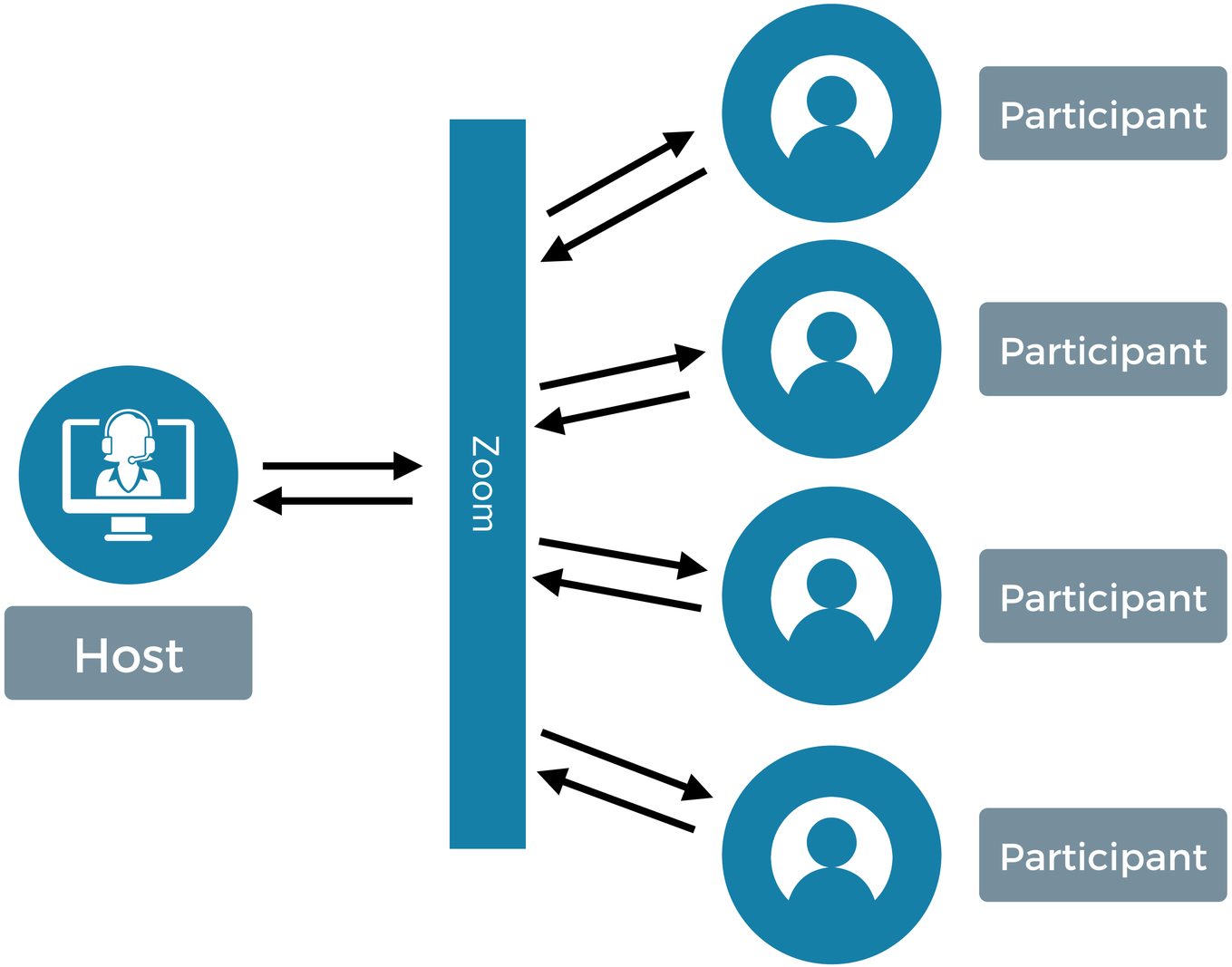
- Same goal here: generate a meeting key and share it just with approved participants.
- Rotate as needed.

HOST STARTS MEETING



1. Host creates ephemeral cryptographic group for the duration of the meeting.
2. Host adds each invited user to the group.
3. Host generates a random meeting key.
4. Host encrypts the meeting key to the group.

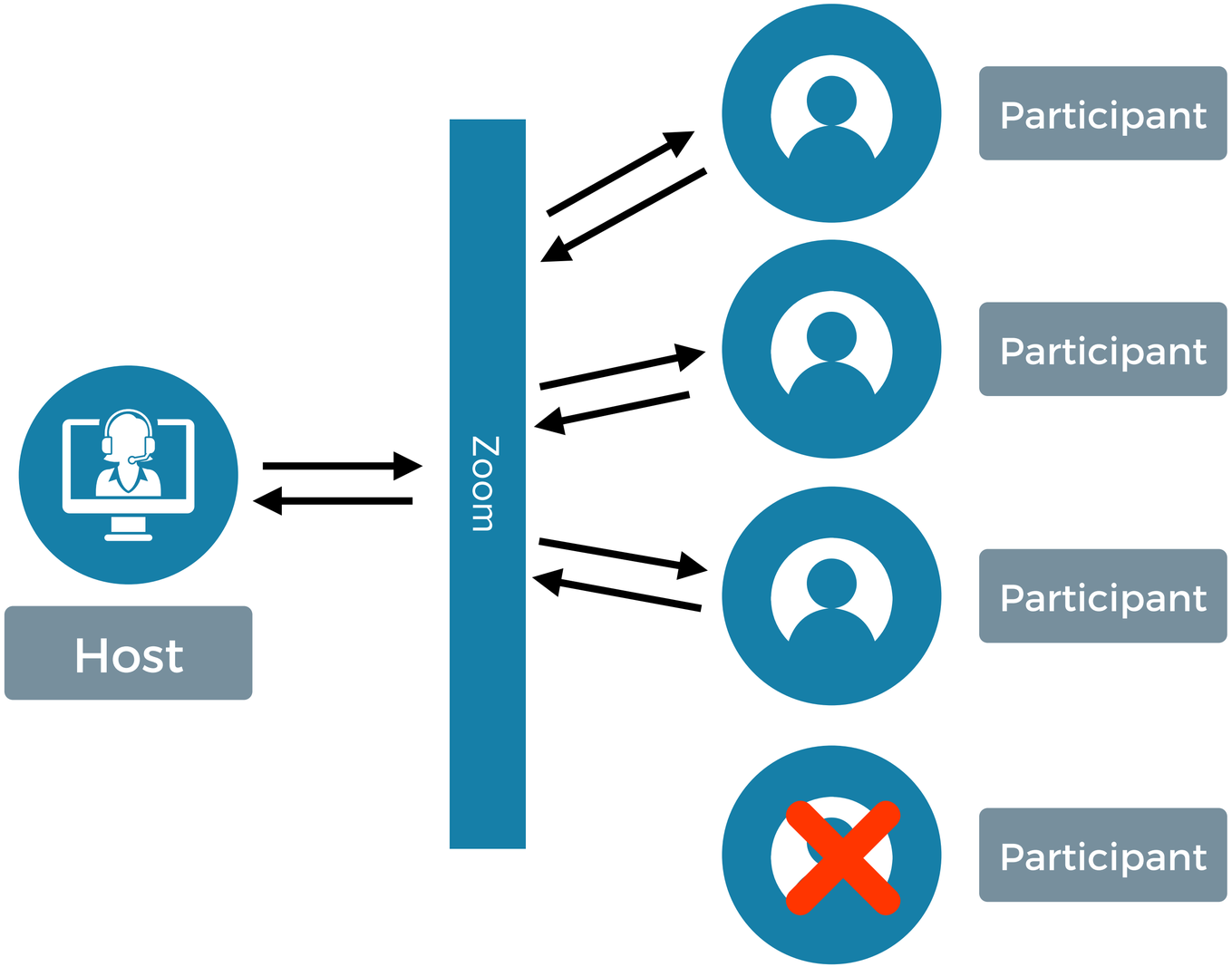
PARTICIPANT JOINS



1. Host adds the user to the group (if not already).
2. Participant fetches the encrypted meeting key and decrypts it with their local device key.

Note: host adds at the user level, user decrypts at the device level.

PARTICIPANT LEAVES



1. The host removes them from the group.

   They can no longer decrypt new meeting keys.

2. The host generates a new meeting key.

3. Host sends new meeting key to the remaining participants.

7 ADVANTAGES OVER ZOOM'S APPROACH

1. READY TO USE

No need to buy a cryptography company and hire teams of cryptographers. It’s ready to integrate today.

2. PERFORMANCE

- Host's work is the same regardless of the size of the meeting.
- The system scales horizontally by adding zero-trust servers.
- Participants all decrypt simultaneously.
- Supports 10,000+ participants.

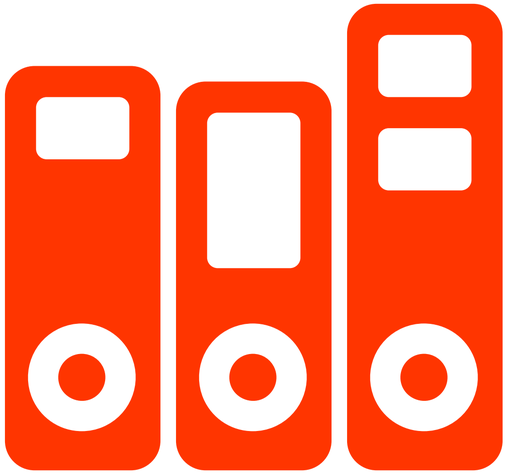
3. REVOCATION

- Device and user revocation is instant.
- Zoom uses revocation lists 🤮.

4. MEANINGFUL PINNING

- Users can pin the user public keys of other participants to detect future imposter attacks.
- These pinned keys are independent of the device used by the user.

5. ENCRYPT MORE THINGS



- Hosts can utilize durable cryptographic groups to end-to-end encrypt meeting assets.
  - Agenda
  - Chat transcripts
  - Shared presentations
  - Meeting summaries
  - Meeting recordings
  - Transcripts, etc.
- (Less functionality lost, more future possibilities, and less risk of a breach of toxic data).

6. KEY LIFETIMES

- Zoom does not plan to ever rotate device signing keys.
- IronCore allows rotation of keys at every level on any schedule.
- For Forward Secrecy, participants' can rotate device keys at the end of every meeting.

7. IDENTITY LINKS

Zoom has complicated identity linking.

We link identities and users keys and support standard SSO mechanisms.

CLICK DOWN A LEVEL

You can get the link in the Q&A session.
You will be the first to get it.

VALIDATED

PEER REVIEWED AND PUBLISHED

Published & Presented: ACM Security in Cloud Computing

2018-acm-scc-Cryptographically-Enforced-Orthogonal-Access-Control.pdf (page 1 of 9)

Cryptographically Enforced Orthogonal Access Control at Scale

Bob Wall
IronCore Labs, Inc.
Bozeman, Montana
bob.wall@ironcorelabs.com

Patrick Walsh
IronCore Labs, Inc.
Boulder, Colorado
patrick.walsh@ironcorelabs.com

ABSTRACT

We propose a new approach to cryptographically enforced data access controls that uses public key cryptography to secure large numbers of documents with arbitrarily large numbers of authorized users. Our approach uses a *proxy re-encryption (PRE)* scheme to handle the problems typical of public key cryptography including key management, rotation, and revocation, in a highly scalable way, while providing end-to-end encryption and provable access.

In this paper we describe a system based on this approach. We call it an *orthogonal access control* system, because it allows the decision about the groups to which to encrypt a piece of data to be made independently and asynchronously from the decision about who belongs to a group and can therefore decrypt the data. We define specific requirements for a PRE scheme needed to support the system, and we provide a specific instance that meets these requirements. We detail the algorithms that make up the scheme, and we present an enhancement that provides better revocability of keys.

CCS CONCEPTS

• **Security and privacy** → **Access control**; **Key management**; **Public key encryption**;

more reliable security and access control in a world of distributed data. In particular, *end-to-end encryption* is seeing more wide-spread adoption. However, current end-to-end encryption tools are mostly restricted to person-to-person communication applications like messaging and email.

Practical systems that manage access to data by groups of users typically resort to a model using an access control server that manages symmetric keys and hands them to requesting users based on policy. While public key-based systems have a better security model, they suffer from scalability and complexity problems. Consider, for example, using PGP to secure data. A user can securely encrypt a file to a set of other users, given their public keys. However, there is a linear increase in the time and space required to encrypt the file to each user. When access to an encrypted file must be granted to a new user, someone with access to the file must decrypt it, then re-encrypt it to the entire list, plus the new recipient. If files are encrypted to teams of people and a person leaves the team, every file shared with the team must be found, decrypted, and re-encrypted to the list minus the departing user. The same process must be followed if a user's keys are compromised. This solution does not scale to large groups of users.

We propose a system that is built to embed in applications to pro-

@ironcorelabs

SECURITY PROOF

PRE-IND-CCA2 Proof

2018-IronCore-CCA-proof-draft.pdf (page 1 of 9)

SECURITY OF PROXY RE-ENCRYPTION

IRONCORE LABS

Introduction

The purpose of this document is to provide a detailed sketch of the proof of security of Ironcore Labs' Proxy Re-Encryption algorithm against chosen ciphertext attacks. The underlying hard problem upon which security is based is the most common hard problem used to prove security for pairing-based cryptography.

Definition 0.1. The *Decisional Bilinear Diffie-Hellman* Problem (DBDH) is the problem, given $\mathbf{g}, \mathbf{g}_1, a\mathbf{g}, b\mathbf{g}$, to distinguish $\epsilon(\mathbf{g}, \mathbf{g}_1)^{ab}$ from a random element of G_T.

Our goal is to prove indistinguishability under adaptive chosen-ciphertext attacks (IND-CCA2), which is the strongest notion of security defined in the literature for proxy re-encryption, and the industry standard. It is defined in a paper of Canetti-Hohenberger. Proofs of CCA2 security have been claimed for our underlying protocol, but have not appeared in print in detail.

This document has two parts. The first is a proof of IND-CCA2 for the underlying encryption with authentication hash. It contains some of the principal ideas of the full proof. The second part contains the full proof.

IND-CCA2 for basic encryption/decryption

OPEN SOURCED

94% Test Coverage + Auto-fuzz Testing

GitHub, Inc. github.com/ironcorelabs/recrypt

build.sbt	Remove checkinit from JS build (#2)	2 months ago
icla.pdf	Initial open source release	2 months ago
ocla.pdf	Initial open source release	2 months ago
scalastyle-config.xml	Initial open source release	2 months ago
version.sbt	Setting version to 1.3.2-SNAPSHOT	2 months ago

README.md

Recrypt

build passing | codecov 94% | scaladoc 1.3.1 | npm package 1.3.1

This is a library that implements a set of cryptographic primitives that are needed for a *multi-hop proxy re-encryption* scheme.

The library is implemented in Scala, and the build produces a `.jar` you can use with Java applications. It also cross-compiles to Javascript, so you can use the library in web applications to add end-to-end encryption.

Proxy Re-Encryption

A proxy re-encryption (PRE) scheme is a public-key encryption scheme, meaning that each participant has a pair of related keys, one public and one private. If Alice wants to encrypt a message so that only Bob can read it, she obtains Bob's public key and uses the public key encryption algorithm to secure the message. When Bob receives the encrypted

GitHub

@ironcorelabs

AUDITS

Premier Cryptography Reviewers

nccgroup-IronCoreLabs_Cryptography_Assessment_Customer_Facing_Document-5-2-18.pdf (page 1 of 2)

nccgroup

NCC Group
123 Mission Street, Suite 900
San Francisco, CA 94105
415.268.9300
https://nccgroup.trust/us

IronCore Labs

1750 30th Street. Suite 500.
Boulder CO 80301

April 30, 2018

Introduction

Between the days of February 26th and March 20th, 2018, one (1) consultant from NCC Group's Cryptography Service practice expended three (3) person-weeks of effort on a review of IronCore's proxy re-encryption protocol and implementation. The review aimed in particular at validating the specific choice of the pairing-friendly elliptic curve in the protocol, and verifying that the Scala implementation is a secure incarnation of that protocol.

The review covered IronCore's recrypt library implementation (version 7.0.2-SNAPSHOT, then 8.0.1-SNAPSHOT), and the protocol description in two articles (called orig_algo.pdf and icl_impl.pdf). A one-day retest was performed in April 2018 on version 11.0.0-SNAPSHOT.

Two specific questions were the focus during this review:

1. Are the chosen pairing and elliptic curve (optimal Ate pairing on the Naehrig-Niederhagen-Schwabe curve) cryptographically sound and secure?
2. Is the Scala implementation a faithful and correct incarnation of the protocol?

SUMMARY

- We're fans of Zoom's E2EE initiative.
  - They're pushing the market forward. Any E2EE is better than the current state for video conferencing. **And we'll use it when it's available if Zoom competitors don't offer alternatives.**
- Zoom's approach can be improved.
  - Without sacrificing any security, Zoom could solve more problems at greater scale with a more modern approach.
- Privacy matters and privacy sells.
  - Especially to Enterprise customers. They are willing to pay for premium security.
  - We all want control over who can see/hear/read our conversations and our data.

STAY TUNED

- At IronCore, we're releasing new features all the time.
- Recent examples:
  - Policy-based data controls
  - Encrypted search
  - Expanded language and platform support
  - Private key rotation mechanisms
- Coming soon:
  - Near real-time security event log push to SaaS customers.

Poll

SIGN UP FOR OUR MONTHLY NEWSLETTER?

IRONCORE LABS

LOCK YOUR DATA.

UNLOCK YOUR SALES.

@ironcorelabs

Q&A

(Also please indicate if you're willing to come on camera.)