Building E2EE and User Identity

Merry Ember Mou
Zoom Video Communications
Enigma 2021
Former Twitter Employees Charged With Spying for Saudi Arabia

The Justice Department’s charges raised questions about the security of technology companies.

Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People

This morning, WhatsApp made the scope of the Apple-FBI encryption battle look kinda small.

SMS TO RCS —

Google is testing end-to-end encryption in Android Messages

End-to-end encryption is growing in popularity. Google is getting on board.

DAN GOODIN - 11/19/2020, 12:33 PM
Agenda

• Integrating E2EE into Zoom
• Building user identity in subsequent phases
Moving Key Generation to the Client
Zoom Meetings

Alice (Leader) -> Server -> Bob

Meeting data flow:
- Alice sends data to the server.
- Server processes the data.
- Server sends data to Bob.

© 2021 Zoom Video Communications, Inc.
Server-Managed Meeting Key

Leader

Alice

Server-Managed Meeting Key

Server

Bob

mk
E2EE Implementation Goals

- Minimize changes to existing code
- Reduce introducing complexity
- Maintain meeting quality and performance
E2EE Design

Alice - Leader

Bob

Carol

Server

mk
E2EE Design: Device Key
E2EE Design: Ephemeral Key
E2EE Design: Sharing Meeting Key

Leader Alice

Server

Device mk1

Ephemeral

device

Bob

device ephemeral

Carol

device ephemeral

E2EE Design: Sharing Meeting Key
E2EE Design: Key Rotation

- **Alice** (Leader)
- **Bob**
- **Carol**
- **Dave**

The diagram illustrates a leader, Alice, with ephemeral and device keys. The server acts as a hub, connecting Alice, Bob, Carol, and Dave through ephemeral and device keys. The key rotation process involves the leader generating ephemeral keys for each participant and sending them securely through the server.
E2EE Design: Leader Participant List

Participants (9)

In the Meeting (9)

- MM: Merry Mou (Co-host, me)
- JW: (Host)
- MZ: (Host)
- AM: (Co-host)
- BC: (Co-host)
- JB: (Co-host)
- MS: (Co-host)
E2EE Design: Participant List

Alice, Bob, Carol

Alice, Bob, Carol
E2EE Design: Participant List

- Alice
- Bob
- Carol

Alice, Bob, Carol
ephemeral
ephemeral
ephemeral

Leader

Server

Bob
ephemeral
device

Carol
device
ephemeral
Leader change notification
Leader change notification

Meeting leader security code, to detect Meddlers-In-The-Middle (MITMs)
Delivering E2EE
Performance: Meeting Keys

- Joining a meeting must be easy
Performance: Meeting Keys

- Joining a meeting must be easy
- Participants must get meeting keys
Performance: Meeting Keys

• Joining a meeting must be easy
• Participants must get meeting keys
• Throttling rekeys
Performance: Participant List Heartbeats

- UI update frequency
Performance: Participant List Heartbeats

- UI update frequency
- Network traffic
Performance: Participant List Heartbeats

- UI update frequency
- Network traffic
- Noticing notifications
Deploying E2EE

- Client library interface
Deploying E2EE

- Client library interface
- Stand-alone keyservers
Deploying E2EE

• Client library interface
• Stand-alone keyservers
• Backwards compatibility
From Device Key to User Identity
Today one of my 4th grade students renamed himself "reconecting ..." on our Zoom call and pretended that he was having internet issues to avoid participating in our lesson.

imgur.com/k9p0AJ...
Building User Identity
Building User Identity

device

Alice

“Alice Foo” really!
A User is

device

device

Alice
A User is

(Display Name: “Alice Foo”)
Email Address: alice@company.com
Account Domain Name (ADN): company.com
Auditable User Identity

Link 1: Add Laptop
Link 2: Change Email
Link 3: Add Phone
Link 4: Remove Phone

User Sigchain
Auditable User Identity

User Sigchain Links

Merkle Root
User Identity In a Meeting
Sharing Sigchains

Leader

Alice

device
ephemeral

device
ephemeral

Bob

device
ephemeral

Server

Carol

device
ephemeral

("Bob Bar")
bob@company.com
company.com

("Carol Baz")
("Guest" mode)

("Alice Foo")
alice@company.com
company.com
Do I trust the email and ADN are associated with this user?
Do I trust the email and ADN are associated with this user?

Have I seen this user and/or this device before?
Do I trust the email and ADN are associated with this user?

Have I seen this user and/or this device before?

Does this user have an attestation of their sigchain from their IdP? (if applicable)
• E2EE security depends on knowing who’s at the “ends.”
Takeaways

- E2EE security depends on knowing who’s at the “ends.”

- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.
Takeaways

- E2EE security depends on knowing who’s at the “ends.”

- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.

- “Is it secure?” is not a yes/no question.
Takeaways

- E2EE security depends on knowing who’s at the “ends.”

- Building E2EE into an existing product requires balancing implementation complexity, performance, and UI/UX.

- “Is it secure?” is not a yes/no question.

@zoom_us
@merry
merry.mou@zoom.us
github.com/zoom/zoom-e2e-whitepaper