Matrix: An open network for secure, decentralized communication

Sumner Evans

August 31, 2021

Beeper

A bit about me

- I graduated in 2018 with my bachelor's in CS from Mines.
- I graduated in 2019 with my master's in CS, also from Mines.
- I worked at The Trade Desk for two years right after graduating.
- I currently am teaching *CSCI 400 Principles of Programming Languages* and I have previously taught *CSCI 406 Algorithms* and *CSCI 564 Advanced Computer Architecture*.
- I started at Beeper in July.

A bit about you

I'd like to get to know everyone a bit more and get a feel for everyone's experience levels.

- How many of you have taken Algorithms?
- How many of you have taken Data Structures?
- How many of you have taken Intro to Computer Science?
- How many of you are in the ACM Matrix chat?

A bit about you

I'd like to get to know everyone a bit more and get a feel for everyone's experience levels.

- How many of you have taken Algorithms?
- How many of you have taken Data Structures?
- How many of you have taken Intro to Computer Science?
- How many of you are in the ACM Matrix chat?

A bit about you

I'd like to get to know everyone a bit more and get a feel for everyone's experience levels.

- How many of you have taken Algorithms?
- How many of you have taken Data Structures?
- How many of you have taken Intro to Computer Science?
- How many of you are in the ACM Matrix chat?

A bit about you

I'd like to get to know everyone a bit more and get a feel for everyone's experience levels.

- How many of you have taken Algorithms?
- How many of you have taken Data Structures?
- How many of you have taken Intro to Computer Science?
- How many of you are in the ACM Matrix chat?

A bit about you

I'd like to get to know everyone a bit more and get a feel for everyone's experience levels.

- How many of you have taken Algorithms?
- How many of you have taken Data Structures?
- How many of you have taken Intro to Computer Science?
- How many of you are in the ACM Matrix chat?

Overview

1. Why Matrix?
2. What does Matrix provide?
3. How does it work?

Why Matrix?

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let’s talk about chat platforms…

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Let's talk about chat platforms...

Which of the following chat networks do you use/have you used?

- SMS/MMS
- iMessage
- LinkedIn
- Snapchat
- WhatsApp
- Instagram
- Discord
- Facebook Messenger
- Hangouts
- Slack
- Microsoft Teams
- Signal
- Telegram
- Wire

What do all of these chat networks have in common?

They are **non-interoperable, and many are closed source and/or unencrypted**.

Why is this a problem?

The **closed source** platforms are problematic because you can never be sure *how your data is being used*.

The **unencrypted** platforms are problematic because your messages are not private.

And, because none of them are interoperable, you have to have a ton of chat apps on your phone.

Why is this a problem?

The **closed source** platforms are problematic because you can never be sure *how your data is being used*.

The **unencrypted** platforms are problematic because your messages are not private.

And, because none of them are interoperable, you have to have a ton of chat apps on your phone.

Why is this a problem?

The **closed source** platforms are problematic because you can never be sure *how your data is being used*.

The **unencrypted** platforms are problematic because your messages are not private.

And, because none of them are interoperable, you have to have a ton of chat apps on your phone.

What does Matrix provide?

Matrix solves all your problems

Matrix is an **open** specification for **encrypted**, **decentralized** communication.

It is also designed in such a way that it makes it easy to break down walled garden communication platforms via **bridging**.

Matrix solves all your problems

Matrix is an **open** specification for **encrypted**, **decentralized** communication.

It is also designed in such a way that it makes it easy to break down walled garden communication platforms via **bridging**.

A side note

I first became interested in Matrix when I was the incoming Chair of ACM. Robby (VC) and I tried out most of the open source chat platforms and ended up landing on Matrix because it had all of these characteristics.

Matrix is an *open specification*

Open specifications and standards are all around you. They just make sense™.

Examples:

- Power plugs
- USB
- Wi-Fi
- Every crypto algorithm that's any good

Open protocols allow for *open development* and *clean-room implementations*, they *encourage competition*, and are *externally auditable*.

Matrix is an *open specification*

Open specifications and standards are all around you. They just make sense™.

Examples:

- Power plugs
- USB
- Wi-Fi
- Every crypto algorithm that's any good

Open protocols allow for *open development* and *clean-room implementations*, they *encourage competition*, and are *externally auditable*.

Matrix is an *open specification*

Open specifications and standards are all around you. They just make sense™.

Examples:

- Power plugs
- USB
- Wi-Fi
- Every crypto algorithm that's any good

Open protocols allow for *open development* and *clean-room implementations*, they *encourage competition*, and are *externally auditable*.

Matrix is an *open specification*

Open specifications and standards are all around you. They just make sense™.

Examples:

- Power plugs
- USB
- Wi-Fi
- Every crypto algorithm that's any good

Open protocols allow for *open development* and *clean-room implementations*, they *encourage competition*, and are *externally auditable*.

Matrix is *encrypted* by default*

Matrix has encryption built-in. It is implemented using Olm, which is a clone of the Signal protocol

Matrix is *decentralized*

Anyone can host a *homeserver*, and communicate with any other homeserver in the federation.

Think of it like email. You can email somebody using Outlook from Gmail.

Every server in the federation gets a copy of a room, so no one entity controls the network.

This also means that the network is resilient to individual server outages, or even wider internet outages.

Matrix is *decentralized*

Anyone can host a *homeserver*, and communicate with any other homeserver in the federation.

Think of it like email. You can email somebody using Outlook from Gmail.

Every server in the federation gets a copy of a room, so no one entity controls the network.

This also means that the network is resilient to individual server outages, or even wider internet outages.

Matrix is *decentralized*

Anyone can host a *homeserver*, and communicate with any other homeserver in the federation.

Think of it like email. You can email somebody using Outlook from Gmail.

Every server in the federation gets a copy of a room, so no one entity controls the network.

This also means that the network is resilient to individual server outages, or even wider internet outages.

Matrix is *decentralized*

Anyone can host a *homeserver*, and communicate with any other homeserver in the federation.

Think of it like email. You can email somebody using Outlook from Gmail.

Every server in the federation gets a copy of a room, so no one entity controls the network.

This also means that the network is resilient to individual server outages, or even wider internet outages.

Matrix allows for *bridges* and *bots*

Bridges bring external chat networks into Matrix. More on this later.

Bots allow for automated interactions and notifications.

Matrix allows for *bridges* and *bots*

Bridges bring external chat networks into Matrix. More on this later.

Bots allow for automated interactions and notifications.

How does it work?

Architecture

eventual consistency

Client-Server API

Federation (Server-Server) API

A bit of graph theory

DAG

A bit of software engineering

Git

The event DAG

State events