I have a hard time keeping track of which contacts use which chat systems. This is one of the main reasons we created Matrix.org :)

MATRIX | OLEG FIKSEL | FrOSCon 2019
THANKS!

Special thanks for great support to:

► Matthew Hodgson - Co-Founder
  @matthew:matrix.org

► Ben Parsons - Developer Advocate
  @benpa:matrix.org
Oleg Fiksel

- DevOps Engineer
- Passionate about tech
- Like to automate everything
GOAL OF THIS TALK
GOAL OF THIS TALK

- Part 1: Provide an overview of Matrix architecture and ecosystem
GOAL OF THIS TALK

- Part 1: Provide an overview of Matrix architecture and ecosystem

- Part 2: Get hands-on experience with a Matrix demo environment (get your laptops ready)
What is Matrix?
What is Matrix?

Matrix is an open network for **secure**, **decentralised** **real-time** communication.
What is Matrix?
What is Matrix?
Why I like Matrix
Why I like Matrix

- Open source
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
Why I like Matrix

▶ Open source
▶ Distributed (no single party owns your conversations)
▶ E2E encryption as first-class citizen
▶ Encrypted voice & video calls
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications
- Integrations
Why I like Matrix

- Open source
- Distributed (no single party owns your conversations)
- E2E encryption as first-class citizen
- Encrypted voice & video calls
- Bridging in design
- Read & typing notifications
- Integrations
- Healthy and friendly community
MATRIX DISTRIBUTED ARCHITECTURE
Matrix distributed architecture

- Clients
- Home Servers
- Application Servers
- Identity Servers
E2E ENCRYPTION

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
- Without end-to-end encryption, Matrix’s replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
- Olm – a Double Ratchet implementation
- Megolm - Entirely new ratchet for group chat with shareable history
E2E encryption

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
E2E encryption

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
- Without end-to-end encryption, Matrix’s replicated conversation history is a privacy problem
E2E encryption

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
- Without end-to-end encryption, Matrix’s replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
E2E encryption

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
- Without end-to-end encryption, Matrix’s replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
- Olm – a Double Ratchet implementation
E2E encryption

- Encryption without Open Source cannot be trusted (security by obscurity doesn’t work)
- Without end-to-end encryption, Matrix’s replicated conversation history is a privacy problem
- Two years spent building decentralised E2E crypto into the heart of Matrix
- Olm – a Double Ratchet implementation
- Megolm - Entirely new ratchet for group chat with shareable history
Security Assessment

- libolm 1.3.0 assessed by NCC Group in Sept 2016
- Findings released to the public!
- Olm: 2x low risk finding, 1x informational
- Megolm: 1x high, 1x medium, 4x low risk.
- All findings fixed in libolm or the Matrix Client SDKs.
- No issues found in libolm since the audit!
Security Assessment

- libolm 1.3.0 assessed by NCC Group in Sept 2016
- Findings released to the public!
- Olm: 2x low risk finding, 1x informational
- Megolm: 1x high, 1x medium, 4x low risk.
- All findings fixed in libolm or the Matrix Client SDKs.
- No issues found in libolm since the audit!
ECOSYSTEM
Ecosystem

Matrix Open Source Ecosystem

- Synapse (1st gen Matrix Server)
- Dendrite (2nd gen Server)
- Application Services and Bridges
- Other Servers: Ruma (Rust), Jeon (Java)...
- Other Services: Bridges, Bots, Integs...
ECOSYSTEM

Matrix Open Source Ecosystem

The Matrix Specification (Client/Server API)

- Synapse (1st gen Matrix Server)
- Dendrite (2nd gen Server)
- Application Services and Bridges
- Other Servers: Ruma (Rust), Jeon (Java)...
- Other Services: Bridges, Bots, Integs...
Matrix Open Source Ecosystem

The Matrix Specification (Client/Server API)

- **Client-side**
  - Matrix Web Console
  - Matrix iOS Console
  - Matrix Android Console
  - MatrixKit (iOS)
  - matrix-android-sdk
  - matrix-ios-sdk
  - matrix-react-sdk
  - matrix-js-sdk

- **Server-side**
  - Synapse (1st gen Matrix Server)
  - Dendrite (2nd gen Server)
  - Application Services and Bridges
  - Other Servers: Ruma (Rust), Jeon (Java)...
  - Other Services: Bridges, Bots, Integs...

Other Clients:
- Quaternion (Qt/C++)
- Nheko! (Qt/C++)
- Fractal (GTK+/Rust)
- Seaglass (macOS)
- Thunderbird
- gomuks

...and many many more
<table>
<thead>
<tr>
<th>INTRODUCTION</th>
<th>Architecture</th>
<th>Ecosystem</th>
<th>Clients</th>
<th>Bridges</th>
<th>Integrations</th>
<th>API</th>
<th>Roadmap</th>
<th>Summary</th>
<th>Hands-on</th>
<th>End</th>
</tr>
</thead>
</table>

## Clients

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
- Fractal (GTK)
- Gomuks (TUI)
Clients

- Riot (Web)
Clients

- Riot (Web)
- Nheko (Qt)
CLIENTS

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
Clients

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
CLIENTS

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
- Fractal (GTK)
Clients

- Riot (Web)
- Nheko (Qt)
- Quaternion (Qt)
- Seaglass (MacOS)
- Fractal (GTK)
- Gomuks (TUI)
Clients - RIOT
Clients - Nheko

Matrix HQ
The Official Matrix HQ - please come chat here! | To support Matrix.org development: https://patreon.co...
CLIENTS - QUATERNION

Accounts    View    Room
Rooms (8)    Settings    Help

People (3 rooms)
ChanServ (PM on chan...)
Denis
freenode-connect (P...)
Ungrouped rooms (4...)
@appservice-irc:matri...

Debian
Unofficial Debian room

Advice on new server install:
I have a debian server at home (still on jessie 32 bit) that is running off a RAID5 (3Ware 9000 series card). I want to upgrade the whole system by changing all the disks (they are 5 years old now and I don't want to risk it failing plus I'm running out of space) and setting up RAID10 which is far more reliable.

I want to also install LUKS dm-crypt to encrypt content. My thought was to install a small SSD where I would install the root partition (/) but unencrypted. I would then install /var, /home and /mnt on the RAID10. Reason why I want /var on the RAID10 is that I have MySQL databases that I want to keep encrypted too.

Any thoughts on weaknesses of this approach?

anonymou53 joined the room

Tekka joined the room

grin

mylux: sounds plausible. maybe you would worry about your /etc

Send a message (over HTTPS) or enter a command...
CLIENTS - SEAGLASS
**CLIENTS - Fractal**

Fractal

(Those grey unread counters make me anxious, I don't know how you can cope with them)

**Tobias Bernard**
we need some way to inject mock content for screenshots :D
how do I disable devel styling?

**biLelmoussaoui**
Tobias Bernard open Inspector and remove the devel class from the headerbar

**Tobias Bernard**
biLelmoussaoui: ah lol didn't think of that

**Alexandre Franke**
Tobias Bernard, I wish we had an easy way to mock every time I see your designs, so we could compare them to the implementation.

**Tobias Bernard**

![Fractal Matrix messaging app](https://www.freedesktop.org/software/fractal)
CLIENTS - GOMUKS

| 11:41:49 | scvnc | Mautrix-Telegram Bridge
| 11:51:39 | Zouppen-irc (IRC) | Smartass (IRC)
| 11:48:03 | Zouppen (IRC) | M9L76
| 11:51:39 | Zouppen-irc (IRC) | Andrew Manning
| 11:51:39 | Zouppen-irc (IRC) | rxcmm
| 11:51:39 | Zouppen-irc (IRC) | Guest 229767
| 11:51:39 | Zouppen-irc (IRC) | Guest 237848

Mautrix-Telegram Bridge
Gomuk
Mauuin Gitlab Bot
Quick Sync Room

Riot
Mastodon, Social Net & Mi
Telegram
Freenode NickServ

Favorites 6

Mautrix-Telegram Bridge
Gomuk
Mauuin Gitlab Bot
Quick Sync Room

People 93

Rooms 78

telethon off-topic
#test:matrix.org
Mauuni Test Room (11)

Matrix HQ

Zouppen-irc (IRC): I mean there's "Zouppen (IRC)" and "Zouppen-irc (IRC)" in this room

their IDs are @freenode_Zouppen:matrix.org and @freenode_Zouppen-irc:matrix.org

vurpo: Zouppen-irc is a native IRC connection via irssi and Zouppen is Matrix connection which I'm unable to throw out from here

Hail_Spalecake (IRC) joined the room.
Hail_Spalecake (IRC) left the room.

at least managed to reclaim the nick although not managed to throw that bastard out of irc

buff-Ebel#1796 changed their display name to Halfy (Discord).

---

the leave event so it's just the irc bridge lagging

tulir: it allows showing the entire user list and then control+F:
P
shirish: are you thinking about IRCv3?
tulir: I 'think so' do you have a link I can look into it.

found https://ircv3.net/, reading.
tulir: Michael (t3chguv): have posted https://github.com/matrix-
org/matrix-appservice-irc/issues/583, maybe most of these 'commands' are already implemented and just the documentation is missing, don't know.

dead wj

IRC is dead.

And I have killed it.### LONG LIVE IRC

shirish: have you checked /help in the bridge status room? Riot

only autocompletes Riot commands

tulir: thank you, was thinking it would be /help but that didn't

work. /help does give some info. but not much.

shirish: look at /command

tulir: Michael (t3chguv): http://paste.debian.net/1026078/

jason s)

--> noctul joined the room.

Zouppen-irc (IRC): I mean there's "Zouppen (IRC)" and "Zouppen-irc (IRC)" in this room

their IDs are @freenode_Zouppen:matrix.org and @freenode_Zouppen-irc:matrix.org

vurpo: Zouppen-irc is a native IRC connection via irssi and Zouppen is Matrix connection which I'm unable to throw out from here

Hail_Spalecake (IRC) joined the room.
Hail_Spalecake (IRC) left the room.

at least managed to reclaim the nick although not managed to throw that bastard out of irc

buff-Ebel#1796 changed their display name to Halfy (Discord).
BRIDGES
BRIDGES

3rd party Clients

3rd party Server

Bridge

matrix
BRIDGES

IRC clients

ircd (e.g. Freenode)

matrix-appservice-irc

matrix
Bridges

- matrix-appservice-irc
- matrix-appservice-slack
- matrix-appservice-purple
- matrix-appservice-bridge
- matrix-appservice-node
- matrix-js-sdk
- Node JS
INTEGRATIONS
INTEGRATIONS

- Etherpad
INTEGRATIONS

► Etherpad
► RSS
INTEGRATIONS

- Etherpad
- RSS
- Grafana
INTEGRATIONS

▶ Etherpad
▶ RSS
▶ Grafana
▶ Jitsi
INTEGRATIONS

- Etherpad
- RSS
- Grafana
- Jitsi
- Custom
**INTEGRATIONS - ETHERPAD**

This pad text is synchronized as you type, so that everyone viewing this room sees the same text. This allows you to collaborate seamlessly on documents, while chatting in Riot!

Hello Oleg!

Hello FrOSCon

---

Oleg changed the power level of @benpa:matrix.org from Default (0) to Moderator (50).

benpa

oh, somehow I don't have permission ;)

Now you can.

@dejikseLinfo changed the pinned messages for the room.

@dejikseLinfo changed the power level of @matthew:matrix.org from Default (0) to Moderator (50).

Etherpad widget added by @benpa:matrix.org
INTEGRATIONS - RSS
INTEGRATIONS - JITSI
## Integrations - Custom

- **Ping Room**
  - Room for ping testing.
  - Set up your own maubot: [GitHub](https://github.com/maubot/maubot).

### Ping Stats

<table>
<thead>
<tr>
<th>#</th>
<th>Ping server</th>
<th>Median</th>
<th>Geom. mean</th>
<th>Mean</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>matrix.tetradon.nl</td>
<td>248 ms</td>
<td>314.0 ms</td>
<td>364.8 ms</td>
<td>2 176.5 ms²</td>
</tr>
<tr>
<td>2</td>
<td>poddery.com</td>
<td>363.0 ms</td>
<td>1344.2 ms</td>
<td>44.3 seconds</td>
<td>5 48.9 seconds</td>
</tr>
<tr>
<td>3</td>
<td>smnk.nl</td>
<td>384 ms</td>
<td>616.7 ms</td>
<td>1696.2</td>
<td>1 327.0 ms</td>
</tr>
</tbody>
</table>

**User Activity:**
- bobfett: Pong! (ping) took 405 ms to arrive
- bobfett: Pong! (ping) took 435 ms to arrive
- bobfett: Pong! (ping) took 416 ms to arrive
- Echo Bot: Pong! (ping) took 401 ms to arrive
- PongBob (casavant): Pong! (ping) took 497 ms to arrive
- Oleg joined the room.
**Client-Server API**

```bash
1  curl -XPOST -d '{"msgtype":"m.text", "body":"Wake up Neo..."}'
   https://matrix.org/_matrix/client/r0/rooms/#matrix:matrix.org/send/m.room.message?access_token=ACCESS_TOKEN
2  {
3    "event_id": "YUwRidLecu"
4  }
```
Server-Server API

- Synchronises messages and room state between servers, in real-time
- Can retrieve historic messages from each other
- Query profile and presence information about users on each other's servers
Server-Server API

- Synchronises messages and room state between servers, in real-time
Server-Server API

- Synchronises messages and room state between servers, in real-time
- Can retrieve historic messages from each other
**Server-Server API**

- Synchronises messages and room state between servers, in real-time
- Can retrieve historic messages from each other
- Query profile and presence information about users on each other’s servers
APPLICATION SERVICES API

- Have privileged access to the server
- Can subscribe to server traffic to provide custom application logic
- Can masquerade as 'virtual users'
APPLICATION SERVICES API

- Have privileged access to the server
APPLICATION SERVICES API

- Have privileged access to the server
- Can subscribe to server traffic to provide custom application logic
APPLICATION SERVICES API

- Have privileged access to the server
- Can subscribe to server traffic to provide custom application logic
- Can masquerade as 'virtual users'
Latest features & Roadmap
Latest features
### Matrix 1.0 release

<table>
<thead>
<tr>
<th>MATRTEX 1.0 RELEASE</th>
</tr>
</thead>
<tbody>
<tr>
<td>First stable release of the protocol standard</td>
</tr>
<tr>
<td>Official SSL certificates for S2S needed</td>
</tr>
<tr>
<td>Using .well-known URIs to discover servers</td>
</tr>
<tr>
<td>Switching to room version 4 for new rooms (fixes the Hotel California bug)</td>
</tr>
</tbody>
</table>
Matrix 1.0 release

- First stable release of the protocol standard
Matrix 1.0 release

- First stable release of the protocol standard
- Official SSL certificates for S2S needed
Matrix 1.0 release

- First stable release of the protocol standard
- Official SSL certificates for S2S needed
- Using .well-known URIs to discover servers
Matrix 1.0 release

- First stable release of the protocol standard
- Official SSL certificates for S2S needed
- Using .well-known URIs to discover servers
- Switching to room version 4 for new rooms (fixes the Hotel California bug)
Edits & Reactions
Edits & Reactions
NEW KEY BACKUP (1/5)
NEW KEY BACKUP (1/5)

Never lose encrypted messages

Messages in this room are secured with end-to-end encryption. Only you and the recipient(s) have the keys to read these messages.

Securely back up your keys to avoid losing them.

Start using Key Backup

Not now

Don't ask me again
NEW KEY BACKUP (2/5)

Secure your backup with a passphrase

**Warning**: you should only set up key backup from a trusted computer.

We'll store an encrypted copy of your keys on our server. Protect your backup with a passphrase to keep it secure.

For maximum security, this should be different from your account password.

Enter a passphrase...

▼ Advanced

Set up with a Recovery Key
New key backup (3/5)

Recovery key

Your recovery key is a safety net - you can use it to restore access to your encrypted messages if you forget your passphrase.

Keep your recovery key somewhere very secure, like a password manager (or a safe)

As a safety net, you can use it to restore your encrypted message history if you forget your Recovery Passphrase.

Your Recovery Key

Copy to clipboard  Download
NEW KEY BACKUP (4/5)

Keep it safe

Your Recovery Key has been **copied to your clipboard**, paste it to:

- Print it and store it somewhere safe
- Save it on a USB key or backup drive
- Copy it to your personal cloud storage

[Back] [OK]
New key backup (5/5)

Success!

Your keys are being backed up (the first backup could take a few minutes).
Roadmap
**ROADMAP**

- Better Synapse scalability (Workers, UID Loadbalancing)
- Improve Synapse’s minimal footprint to run on smaller hardware.
- New device trust (cross signing devices) - key step to enable E2EE by default.
ROADMAP

- Better Synapse scalability (Workers, UID Loadbalancing)
ROADMAP

► Better Synapse scalability (Workers, UID Loadbalancing)

► Improve Synapse’s minimal footprint
   To run on smaller hardware.
ROADMAP

- Better Synapse scalability (Workers, UID Loadbalancing)
- Improve Synapse’s minimal footprint
  To run on smaller hardware.
- New device trust (cross signing devices)
  Key step to enable E2EE by default.
SUMMARY

The number of messaging platforms is growing every day. Matrix solves the problem of uniting those platforms in a way you want it. The community is rapidly evolving. The community is great! Get involved!
SUMMARY

▶ The number of messaging platforms is growing every day
The number of messaging platforms is growing every day

Matrix solves the problem of uniting those platforms in a way YOU want it
SUMMARY

▶ The number of messaging platforms is growing every day

▶ Matrix solves the problem of uniting those platforms in a way YOU want it

▶ Matrix community is rapidly evolving
SUMMARY

- The number of messaging platforms is growing every day
- Matrix solves the problem of uniting those platforms in a way YOU want it
- Matrix community is rapidly evolving
- The community is great! Get involved!
GENTLEMEN, START YOUR ENGINES LAPTOPS
GENTLEMEN, START YOUR ENGINES LAPTOPS

▶ Browse to (use Chrome or Firefox):
https://riot.froscon2019.fiksel.info
GENTLEMEN, START YOUR ENGINES LAPTOPS

- Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info
- Create an account
GENTLEMEN, START YOUR ENGINES LAPTOPS

▶ Browse to (use Chrome or Firefox):
https://riot.froscon2019.fiksel.info

▶ Create an account

▶ Join the channel #FrOSCon2019:froscon2019.fiksel.info
Gentlemen, start your engines laptops

▶ Browse to (use Chrome or Firefox): https://riot.froscon2019.fiksel.info
▶ Create an account
▶ Join the channel #FrOSCon2019:froscon2019.fiksel.info
▶ Have fun!
Thanks!

Oleg Fiksel

Email: oleg@fiksel.info
Matrix: @oleg:fiksel.info

Oleg Fiksel
Email: oleg@fiksel.info
Matrix: @oleg:fiksel.info
LINKS

- Matrix 1.0 release notes
- Message Editing & Reactions
- Deploy Matrix stack with Ansible
- Proposals for device trust