

MatrixRTC

The key sharing problem

td
td@technodisaster.com

Disclaimer

- If you see a security vulnerability, please come to me after the talk.

How do other providers do it?

- Jitsi: uses olm sessions, participants limited to 20

How do other providers do it?

- Jitsi: uses olm sessions, participants limited to 20
- Zoom: own weird protocol where they elect a leader which creates a shared key with all the participants

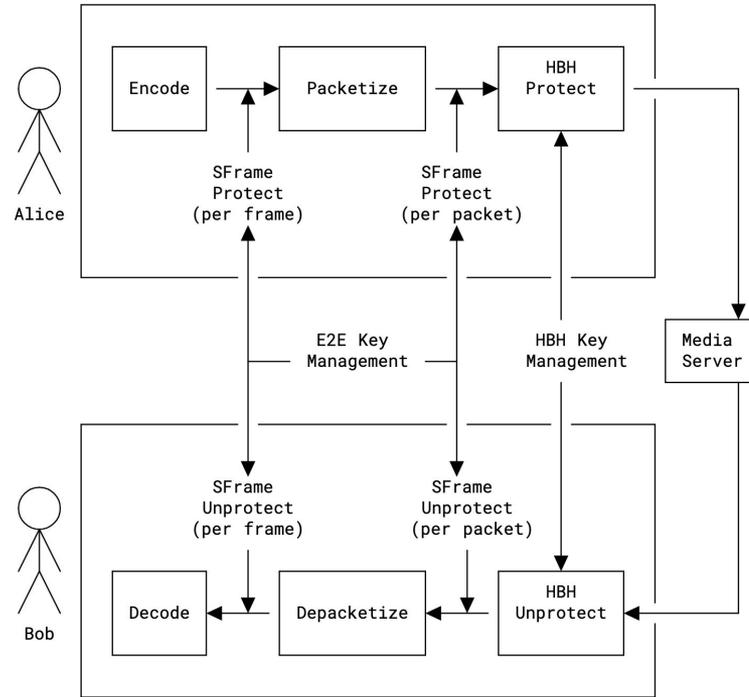
How do other providers do it?

- Jitsi: uses olm sessions, participants limited to 20
- Zoom: own weird protocol where they elect a leader which creates a shared key with all the participants
- Webex, Discord, Cloudflare, Wire - MLS

How do other providers do it?

- Jitsi: uses olm sessions, participants limited to 20
- Zoom: own weird protocol where they elect a leader which creates a shared key with all the participants
- Webex, Discord, Cloudflare, Wire - MLS
- Google meet and Microsoft teams both have a limit of 20–50 participants in true e2ee mode

Current state of MatrixRTC E2EE



Key sharing

Key sharing

- Should be done via a secure channel.

Key sharing

- Should be done via a secure channel.
- Current state, use shared keys or per participant keys.

Key sharing

- Should be done via a secure channel.
- Current state, use shared keys or per participant keys.
- Rotate keys on every leave and join. Creates a burst.

Key sharing

- Should be done via a secure channel.
- Current state, use shared keys or per participant keys.
- Rotate keys on every leave and join. Creates a burst.
- Can be sent via room events or to-device events.

Optimizations in key sharing

Optimizations in key sharing

- Debounce on leave .

Optimizations in key sharing

- Debounce on leave .
- Throttle on join.

Optimizations in key sharing

- Debounce on leave .
- Throttle on join.
- Use ratcheting on join.

Optimizations in key sharing

- Debounce on leave .
- Throttle on join.
- Use ratcheting on join.
- Pre-share key on onboarding screen.

Optimizations in key sharing

- Debounce on leave .
- Throttle on join.
- Use ratcheting on join.
- Pre-share key on onboarding screen.
- Retry mechanism, but also rate limit it.

Famedly Call

- Standalone app and integrated in the Famedly messenger
- Used by 2 of the largest university clinics (which specialize in early born)
- 40–50 participants with 720p video turned on for everyone
- Work is being done to combine MLS and Matrix.
- DEMO!

		chtefsdytpen	swkpbxrqldrf	epyvggliupzi	qpixclpzecky	yqkojbugkfew	toqwgmbfwbz
xabkootoebmq	cjzxebczmzkg	mqlevdcfvepv	rsjlshrrfojv	setvutqocjfi	ztsjeottufsa	sudgxsdfcowa	qalpskhlehqa
jwlqlacizdww	vdxwnhvkwcwi	jctnjmevhpql	jwwoshchmtbw	arsngrwdcnlh	cijbyrbikmp	htshbjcwkkbq	efkxwptngpfh
oobrxrktfoez	rkzhpijzydjp	reqrcyjhksv	gnqwxaqivfrg	ebgbhvfrlos	dloegtvsesvw	ivoskmbjwngo	ibqhkcmtaoxk
ithbksakclq	hseljdsqvjay	kzhtrwfmzbju	xuuhfvivfnoo	ezbrullgfixe	folehhckohqe	hkdcujcpmkdr	xdicevxlscsq
waitodcdpzb	mhgzriyaoyzh	jxmqshomufwg	ykhvjvpaftzs	lxfsmlnhfdn	aruavvhjalq		dbkkmvbyfvcj
imqurmzbgvnj	YA	YR	WA				

Thank you!

Questions?

td

matrix: @td:technodisaster.com

email, fedi: td@technodisaster.com