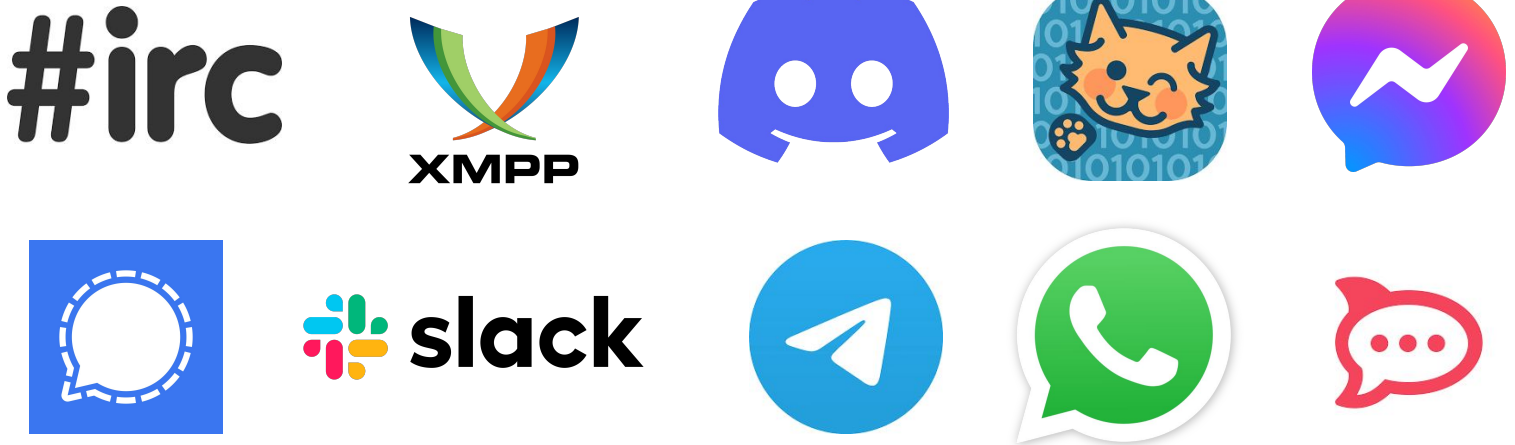
A Formal, Symbolic Analysis of Matrix

Jake Ginesin

What is Matrix?

Many Messaging Suites:



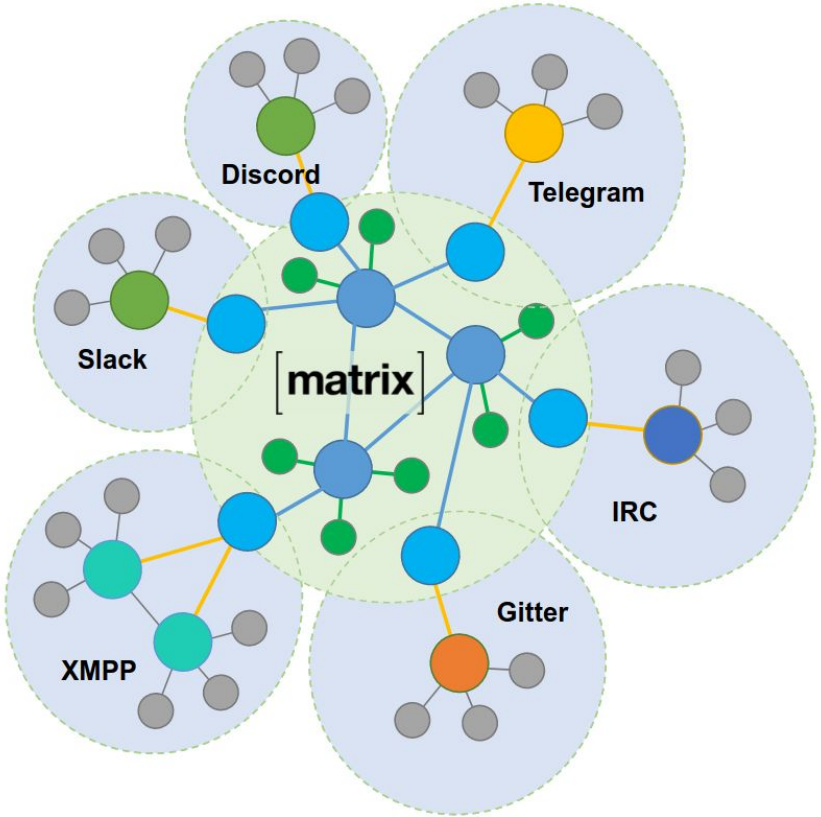
What is Matrix?

Matrix (From their marketing):

“An open network for secure, decentralised real-time communication”

Manifesto: matrix.org/about

What is Matrix good at?



What is Matrix good at?

- Open Standard & Governance
- Fully Encrypted
- Authentication*
- Federated
- Persistent
- Pub-sub

Is Matrix Important?

Approx. 130 Million Users, including:

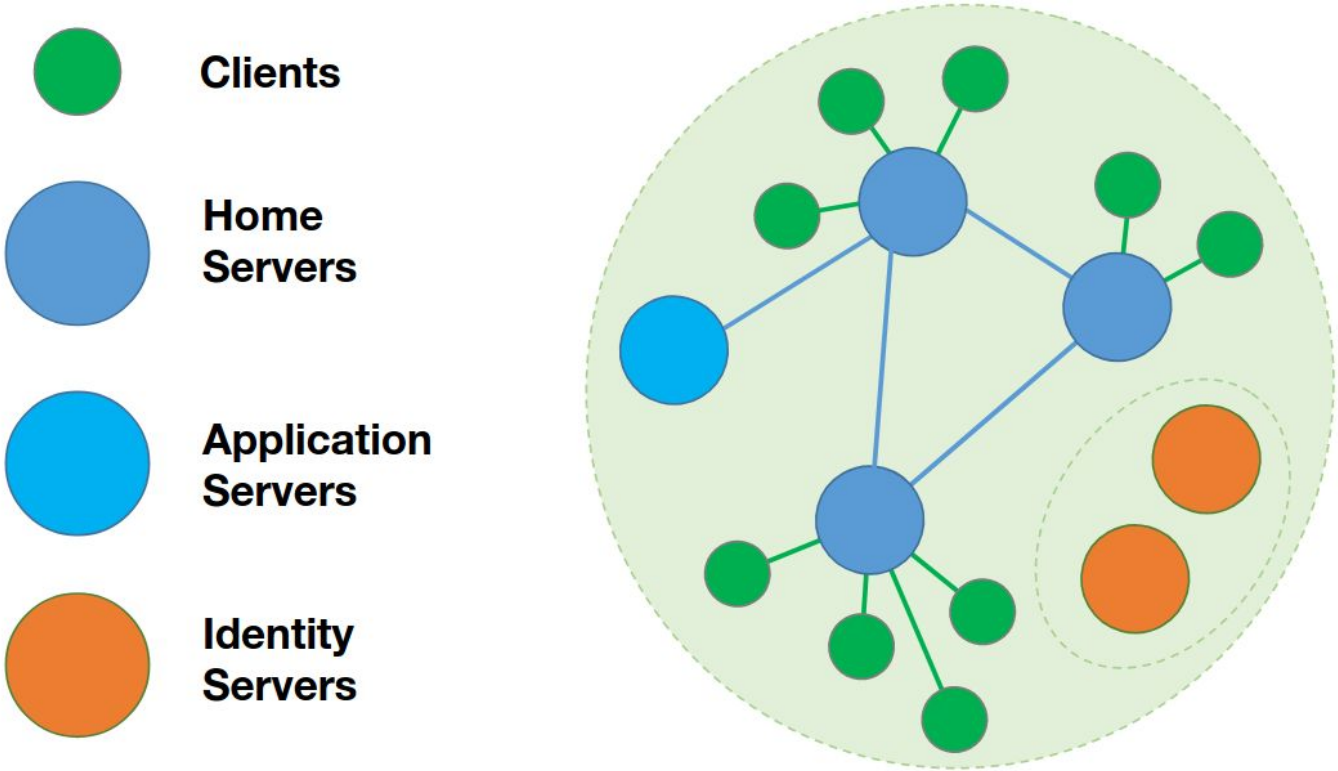
Federal Ministry of Defence

Federal Ministry of Health

moz://a

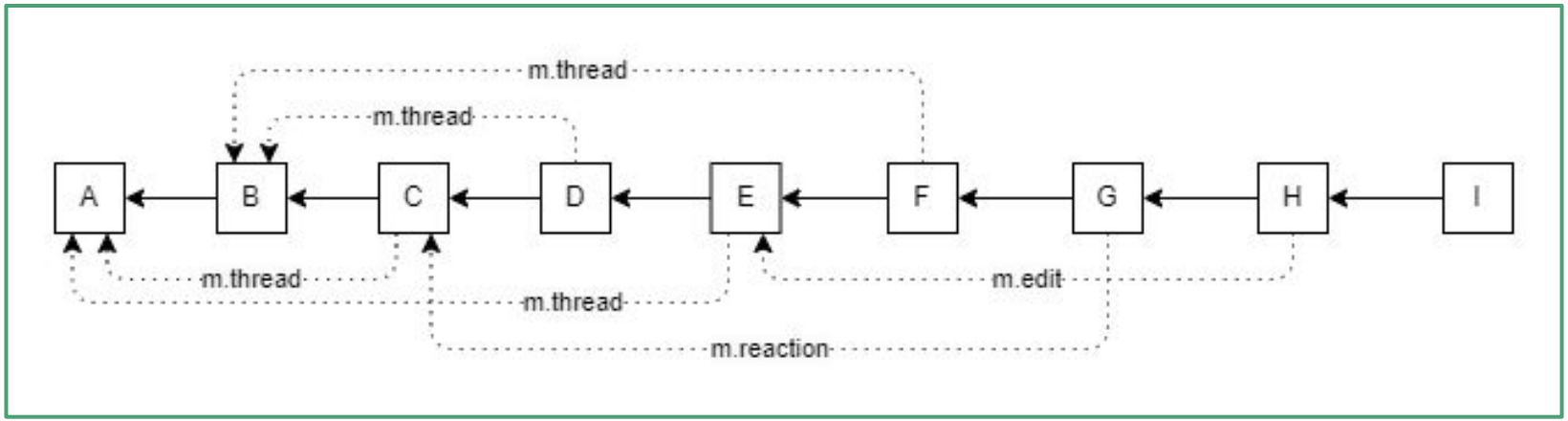
Försäkringskassan

Matrix Architecture: High Level



Matrix Architecture: Rooms

Everything is a room, and rooms are just DAGs



Matrix’s Crypto

- Olm: Secure Peer to Peer
- Megolm: Secure Peer to Multi-Peer

Olms are cute!! ->

Matrix's Crypto: Olm

- Olm: modified Signal. X3DH, Double-Ratchet.

Protocol	Olm	OMEMO (Signal)
IdentityKey	Curve25519	X25519
FingerprintKey[1]	Ed25519	none
PreKeys	Curve25519	X25519
SignedPreKeys[2]	none	X25519
Key Exchange Algorithm[3]	Triple Diffie-Hellman (3DH)	Extended Triple Diffie-Hellman (X3DH)
Ratcheting Algoritm	Double Ratchet	Double Ratchet

Matrix’s Crypto: Megolm

- Users have a signing key and a ratchet key
- When a peer sends a msg, all ratchets advance
- Ratchet key is shared to new peers via Olm

$$New\_Key = HKDF(HMAC(Old\_Key))$$

Matrix’s Crypto: Megolm caveats

- Informally, Megolm is not elegant!
- No transcript agreement
- No backward secrecy
- Dependency on a secure key exchange channel (Olm)
- Authentication is *hard*

Matrix's Crypto: Previous Analysis

- "Practically-exploitable Cryptographic Vulnerabilities in Matrix" [Albrecht et al. IEEE S&P 2023]
- "Device-Oriented Group Messaging: A Formal (Computational) Cryptographic Analysis of Matrix' Core" [Albrecht et al. IEEE S&P 2024]

No symbolic analysis? :(

Why Symbolic Analysis?

Symbolic Model

- Primitives are perfect black boxes
- No Algebraic or numeric values
- Can be fully automated
- Produces verification of no contradictions (theorem assures no missed attacks)

Computational Model

- Primitives are nuanced (IND-CPA, IND-CCA, etc)
- Security bounds (2^128, etc)
- Human-assisted
- Produces game-based proofs, similar technique to hand proofs

Our Contributions

Symbolic cryptographic analysis of Olm & Megolm analysis in Verifpal

Megolm & room logic analysis in Spin (in progress)

Verifpal Models Developed & Verified

- Diffie-Hellman (auth & no auth)
- Triple Diffie-Hellman (3DH & X3DH)
- Single & Double Ratchet (DH, 3DH, X3DH)
- Olm (auth & no auth)
  - 6h & 111GB RAM
- Megolm without Olm
  - 2h & 56GB RAM
- Megolm with Olm
  - 23h and 840GB of RAM...

Reproduced limitations
& known attacks

Spin Models Developed & Verified

- Olm handshake
- Megolm limitations: lack of consistency, message replays, untrustworthy peers (in progress)

Any Questions? :D