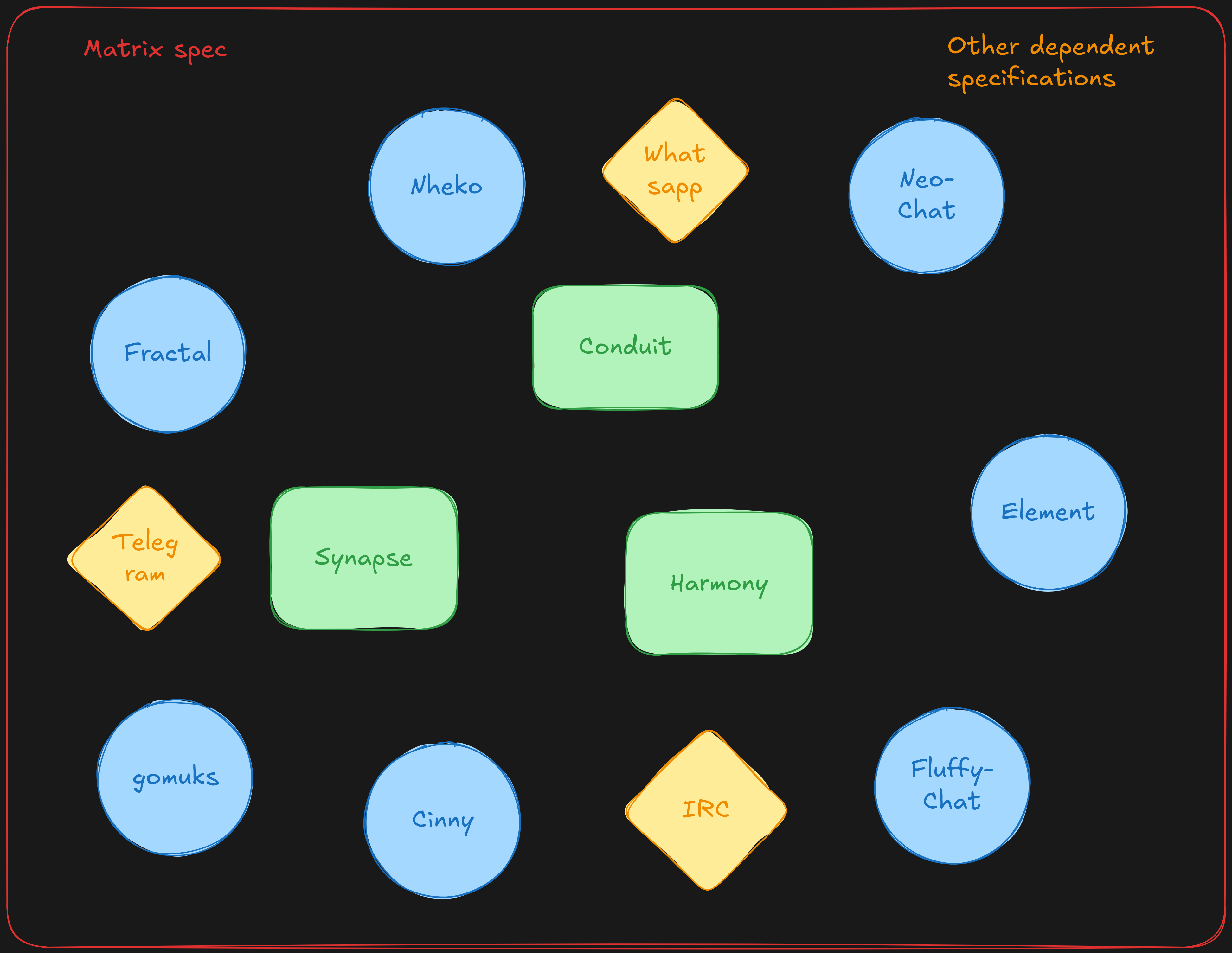
HOW TO FIX SECURITY ISSUES IN A DECENTRALIZED SYSTEM WITH MULTIPLE VENDORS

I don't bring solutions.

I don't bring blame.

LET'S ASSUME

- A security issue in the Matrix protocol
- Requires updates to all clients and servers
- May be actively abused already


Matrix spec
Other dependent specifications
Nheko
What sapp
Neo-Chat
Fractal
Conduit
Teleg ram
Synapse
Harmony
Element
gomuks
Cinny
IRC
Fluffy-Chat

HOW TO REPORT

- Don't talk about undisclosed security issues publicly
- Send an email to security@matrix.org

WHAT DOES A REPORT DO

- "We will work with you to establish a disclosure time frame for the reported vulnerability."
    - [...] aim for a fix within 90 days [...], but we may propose a longer time frame (usually 120 days) [...]
- "We will always transparently let the community know about any incident that affects them."
- "In some cases [...] we may delay publishing technical details [...] after the fix is publicly available (usually no longer than 30 days)."

SPEC FIXES NEED AN MSC

- Spec releases happen every 3 months (ish?)
  - 90 day fixes very optimistic.
- MSCs are public proposals on Github
  - You can't discuss security issues.
  - You will get questions like "why?"
- Security email adds extra corners to communication

DEPRECATION POLICY

- https://spec.matrix.org/latest/#deprecation-policy
- MSC to deprecate
- Second MSC to remove
- Usually at least 1 version in between?

SPEC VERSIONING

- Linear versioning, not semantic
- Need to support most features to claim support for a spec version (no partial feature flags in general)
- What if you don't support threads (v1.4) yet, but need to support the security fix?
- Stable flags for the win! (org.matrix.msc3916.stable for example)

SERVER UPDATES

- Server development rooms are mostly all public
- There are a lot of servers
- Anybody could leak a security issue ahead of time
- Plenty of servers don't follow a regular development schedule (i.e. university)
- Most servers don't support latest Matrix version

CLIENT UPDATES

- Client developer rooms are also mostly public
- There are event more clients!
- Even more people can blabber about stuff!
- Release schedules aren't any more regular (some clients only release once a year!)
- But most clients do support latest Matrix versions, since they carry less responsibility
- Possibly can degrade gracefully.

USER & HOSTER UPDATES

- How do you get server operators to update?
- How do you get users to update their clients?

CURRENT SOLUTION?

- Open secret about changes
  - You tell people what you are changing
  - You are secretive about the why
- Communicate a mostly clear timeline
- Little direct communication with developers and hosters

WHO IS BEHIND SECURITY@MATRIX.ORG

- Not necessarily clear, owned by foundation, operated to some extent by Element
- Whole SCT doesn't get security email?
- How can bandwidth be insured? (Improved a lot)

MY EXPERIENCE

- Reported an issue >2 years ago
- No reply (apart from auto-response) for 5 months
- Fix now in place, public disclosure pending?
- The process has improved a lot and you seem to get a timely response nowadays (possibly because of the AGPL)
- Fixing protocol issues will always be hard.

WHERE DO WE GO?

- Openwall style model?
  - A way for people to contribute security sensitive stuff to MSCs and participate in the discussion?
  - Discussion forum about security issues across implementations?
  - A way to notify packagers and hosters?
- Fix older specs?
- Security fixes for the spec outside of the spec cycle?

Feel free to discuss in #matrix-spec-discussion:neko.dev