Minority Report on Brian’s Nostr-diverted travelogue

Bill Ricker

2023-03-15

- Notes (live)
  - Nostr Relay
  - secp256k1
  - Censorship-resistant
  - “Mastodon is like BBS” FUD
- Cryptographic Libraries
- DB Node safety; web service security
- **Crypto bros**

Notes (live)

Nostr Relay

- so this is a protocol and relay platform for social media, independant of apps ?
    - (how is that different from BlueSky and AT ? Jack is competing with himself?)
- some craptobro thing?
    - Yes. BTC-centric community.
    - ("Fiat" in name is a clue.)
- Identity is important.
    - Ability to work anonymously is also important.
    - At least if one favors resisting autocracy.
- Big Corp federated identity is a privacy problem.
    -    (Deplatforming is yes also a problem)
    - An identity solution created by the BTC community is not reassuring.
- "private keys are easy to mismanage",sigh.
    - they recreated the PGP private key sharing failure case? Progress needs to be progress.
    - it's not even as good as PGP, since PGP allowed for some keyrolling/revocation use-cases ??
- "protocol" "relay" ? Yeah, UseNet (where PGP grew up) had that.
- "for benefit of relays, not users" ooof.
- "they want to do this right" - lots of trust there !

secp256k1

- is a BTC specific elliptic curve.
- ED25519 is a good curve.
- NIST's curve isn't.
- I can't take a BTC endorsed curve seriously, even less so than the NSA-tainted NIST curve.

Censorship-resistant

```
- people generaly want something censored, they just disagree on who
should decide and what
-
```

“Mastodon is like BBS” FUD

```
- More like UseNet. Your current identity was user@node, but we followed
them to user@newnode when they changed jobs or got a new BSD VAX with a
new name.
- "pull rug out" - you can move nodes easily in Mastodon, unlike BBS;
requirement to give notice before pulling plug. Recent demonstration
that this works!
- Unsurprising that people with BTC groupthink have problem with a
community with play-nice requirement.
```

Cryptographic Libraries

(more regarding Tink than Nostr; does Nostr use Tink or just BTC libraries?)

- why low level “extensional” crypto libs are dangerous
    - programer who has to choreograph low level crypto primitives needs to be a cryptologic professional
- build-your-own-lib worse,
    - programer who builds low level cryptologic primitives or choreographic libraries needs to be a cryptologic professional
- hi level intentional (choreographic/use-case-centered) libraries are good,
    - competing intentional libs e.g. SaltStack LibNaCl (https://nacl.cr.yp.to/) wikipedia (https://en.wikipedia.org/wiki/NaCl_(software))

    - https://en.wikipedia.org/wiki/Comparison_of_cryptography_libraries
    - of concern, Tink doesn't even make the comparison list.
    - one good news on Tink (https://github.com/google/tink/blob/master/docs/FIPS.md) is it works with validated modules and can be built to FIPS-only to only use those in a Federal enfironment.

- the special dangers of Dunning-Krueger confidence with Cryptography), "Most any man can create a cipher that he himself can't solve without the key." This mirage has deluded many of the otherwise brightest minds including Thomas Jefferson.

- and perhaps the impossibility of one size fits all implementation and/or different solutions for different threat models. (see PGP rant in recent September talks (http://blu.org/cgi-bin/calendar/speakers/b-ricker1))

- reminder of the engineering ethics of not working outside your professional competence.
  From my history, theory, and maths readings, I know enough to know how much more of
  the detailed practicalities in modern cryptologic coding I do NOT know.

Tracking is a dangerous word. Activism requires anonymous commenting for the protection of the disadvantaged. (The real problem comes when the advantaged use anonymity to punch down, although the advantaged will complain about their victims punching up.)

DB Node safety; web service security

Never expose the DB to unnecessary connections.

Open ports will disclose PG's existence.

PG has default port numbers that are well known.

If you must for some [reason] (WHYYY????) expose PG to “all interfaces, from any IP,” changing the port number **and** requiring a certificate on the connection are good mitigations.

Even if you use a really strong password, their running rainbow table bruteforce against your DB node could be a DoS or DO runs up the CPU-Hours charges incident, so not only don’t rely on password, don’t even allow one.

(SSH Port Tunneling is your friend.)

- Don’t be too cavalier in Alpha/Beta

If [they] can plant a backdoor now, you may never get rid of them, and never see them.

If one burns an expendable Alpha instance down, saving no data, rebuilding from recipe elsewhere, any backdoors *should* not follow.

But there’s always the temptation to push the prototype from alpha to beta, (and then beta users (reasonably) expect their data to roll into production). Any backdoors made sticky via SQL injection (or creating extra privileged users) will promote with the data from Alpha to Beta to Production. Oops.

Crypto bros

I really resent the debasement of terminology. Crypto means Cryptology or Crytozoology !

CraptoCoyns are a debasement of Cryptology.

My general impression is if they’re (competent AND NOT greedy), they avoided the CraptoCoyn space entirely and stayed with either real cryptology or other software.

Competent software coders (who might be greedy or not) and are involved with CraptoCoyns are generally not real cryptologists and so shouldn’t be trusted building secure services, they’re sniffing the D-K glue.

They may be useful for general coding but they’re tainted by association for building trusted infrastructure.

(Remember how they said BTC was anonymous? See how BTC users were getting convicted despite anonymity? D-K School of InSecure Assurances at your service!)

One does wonder who “satoshi nakamoto” really was.

He (if indeed it was a single person) had some real math chops, but oversold the anonymity property, so probably wasn’t a serious INFOSEC person.

Unless that was intentional malicious indirection.