Secure Messaging - open challenges and its relevance for a Paralelní Polis

Frank Braun

October 11, 2014

the history of cryptoanarchy

- Paralelní Polis, Václav Benda, **1977** ($\rightarrow$ parallel institutions)
- New Libertarian Manifesto, Samuel Edward Konkin III, **1980** ($\rightarrow$ agorism)
- Alongside Night, J. Neil Schulman, **1979** (agorism novel)
- The Crypto Anarchist Manifesto, Timothy C. May, **1988** ($\rightarrow$ cryptoanarchy)
- T.A.Z.: The Temporary Autonomous Zone, Hakim Bey, **1991** ($\rightarrow$ TAZ)
- A Lodging of Wayfaring Men, Paul Rosenberg, **2007** (cryptoanarchy novel)
- The Second Realm - Book on Strategy, Smuggler, **2010** ($\rightarrow$ cryptoanarchy + TAZ)

cryptoanarchy - a paralelní polis

what we stand for:

- non-aggression principle (NAP)
- freedom of transaction for consenting adults
- zero-tolerance for uninvited bullies

what won't work:

- convincing the masses (try it, if you don't believe me)
- revolution (contradicts the NAP)

what will work:

> *"A cryptographically secured virtual space which allows us to transact freely without the intervention from violent third parties." (+ TAZ)*

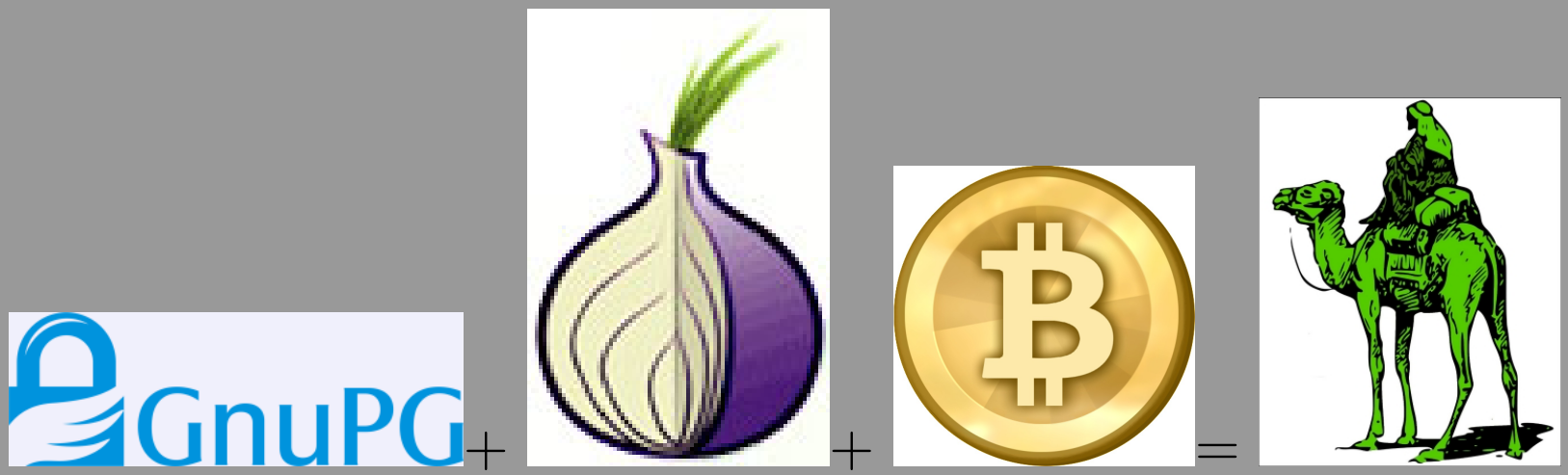
requirements for cryptoanarchy

fundamental building blocks:

- provable pseudonyms ($\rightarrow$ reputation)
- secure messaging
  - confidentiality: encryption of the data (what is said?)
  - deniability: anonymization of the meta-data (who talks to whom?)
- digital cash ($$$)

$\Rightarrow$ virtual black markets

state of the art: silk road recipe



state of the art: overview

	dominant	alternatives
identities	PGP	—
encryption	PGP	OTR[1]
anonymization	TOR	I2P[2]
digital cash	BTC	DGC[3]

[1] off-the-record messaging
[2] invisible internet project
[3] digital gold currency

PGP

Phil Zimmermann released the first version of PGP in **1991**
Version 1.0 of GnuPG was released in **1999**

- outdated
- no perfect forward secrecy
- authenticated messages have no plausible deniability
- RSA might get broken soon
- better available alternatives (e.g., ECDSA) are not used

off-the-record messaging

Nikita Borisov, Ian Goldberg, Eric Brewer (**2004-10-28**).
"Off-the-Record Communication, or, Why Not To Use PGP".
Workshop on Privacy in the Electronic Society.

- innovation (yeay!)
- perfect forward secrecy
- plausible deniability of message content

but: OTR is a synchronous, instant messaging solution

low-latency, high-bandwidth anonymity is dead

- low-latency: $<$ 1 second
- high-latency: $>$ 1 minute
- low-bandwidth: chat
- high-bandwidth: large emails, pictures, websites

anonymity	low-bandwidth	high-bandwidth
low-latency	✓[4]	✗[5]
high-latency	✓[6]	✓[7]

[4] consent-based networks; dining cryptographers
[5] TOR (on life support)
[6] not important
[7] the future of secure asynchronous messaging

the problem with TOR

there are two approaches for anonymity that work

- mixing and relaying (works only for high-latency)
- consent-based networks (only practical for low-bandwidth)

TOR is a low-latency, high-bandwidth solution with problems

- many nodes are compromised
- statistical analysis of the network flows reveals identities

$\Rightarrow$ there is no possible solution for the low-latency, high-bandwidth scenario under current threat model (global view of the network)

$\Rightarrow$ we need a paradigm shift to high-latency systems!

- **not** just for messaging, but for hidden sites, too!
- back to (local) bulleting board systems (BBS)?
- store and forward systems FidoNet style?

the sad state of mix networks

- around forever: David Chaum, Untracable electronic mail, return addresses, and digital pseudonyms, *Comm. ACM*, 24, 2 (**Feb. 1981**); 84-90
- evolution of remailers:
  - type I: cypherpunk remailers
  - type II: mixmaster remailers
  - type III: mixminion remailers
- **but**: mostly forgotten
- shift to TOR (and I2P)
- **but**: we will loose them (or already have)

$\Rightarrow$ we have to go back to the cypherpunk roots of remailers!

pitfalls of “free” infrastructure

in TOR:

- many nodes are operated by intelligence agencies
- no monetary incentives to run a TOR node

in email:

- spam
- move to centralized, web-based mail makes you the product

in Bitcoin:

- costs of running a full Bitcoin node go up
- no monetary incentives to do so

$\Rightarrow$ solution: service-backed digital currencies

- monetary incentive to run independent nodes
- digital cash of relatively stable value

identity-key binding is broken

how to go safely from identity (e.g., “John Doe”) to public key?

approaches:

- public key infrastructure (PKI) (used in SSL)

→ FAIL

- manual fingerprint comparison (used for PGP)
- web of trust (also used for PGP)

→ really?!?
→ FAIL

⇒ we need a solution to the identity-key binding problem which is easy to use and safe against man-in-the-middle (MITM) attacks!

post-quantum cryptography

we need encryption that is secure for the coming **decades**

- long statutes of limitations (maximum time after an event to start legal proceedings)
- some stuff needs to be safe for as long as we live (and we live longer!)

problems:

- long-term storage of encrypted messages is a reality
- increasing computing power (Moore's law)
- better algorithms to break cryptographic algorithms
- quantum computers

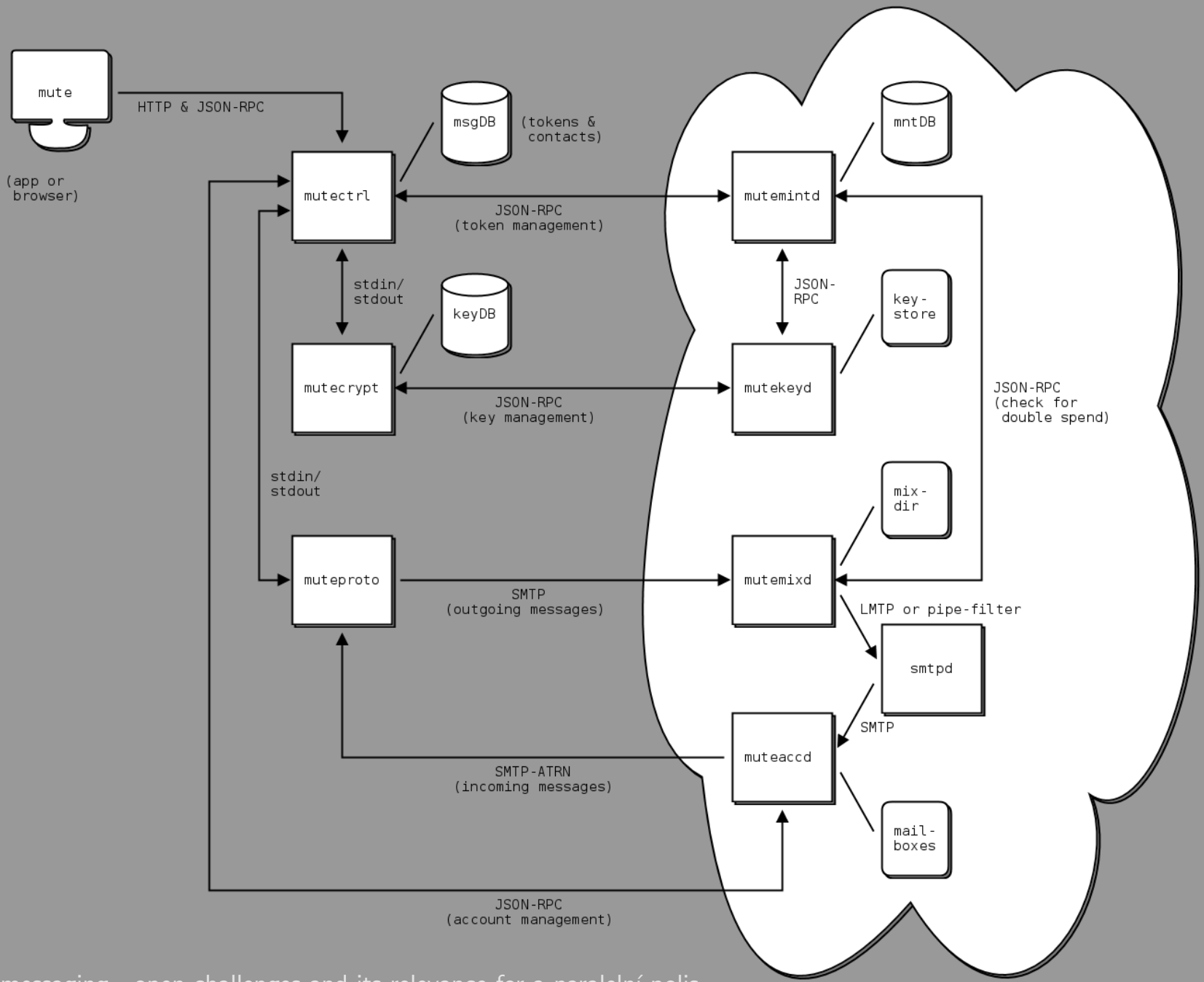
$\Rightarrow$ we need post-quantum cryptography for secure messaging!

summary of open challenges

- perfect forward secrecy
- anonymous messaging
- service-backed digital currency
- identity-key binding
- post-quantum cryptography

next-step in secure messaging: mute - an overview

- mute is a privacy enhancing communication system
- asynchronous secure messaging based on SMTP
- full client, not just encryption and key management
- end-to-end encryption with open-source client (written in Go)
- mobile (Android, iOS) and desktop (Linux, Mac, Windows)
- payment by the user to finance the system and to limit spam
- mute solves **many** of the open challenges
- perfect forward secrecy (with first message!)
- plausible deniability of message content
- better-than-nothing anonymity: mixing/delaying of messages
- multi-nym support with strong separation
- closed beta: early 2015
- public release: mid 2015


mute
HTTP & JSON-RPC
(app or browser)
msgDB
(tokens & contacts)
mutectrl
JSON-RPC (token management)
mutemintd
mntDB
stdin/ stdout
keyDB
mutecrypt
JSON-RPC (key management)
mutekeyd
JSON- RPC
key- store
JSON-RPC (check for double spend)
stdin/ stdout
mix- dir
muteproto
SMTP (outgoing messages)
mutemixd
LMTP or pipe-filter
smtpd
SMTP
muteaccd
SMTP-ATRN (incoming messages)
mail- boxes
JSON-RPC (account management)

mute: identity-key binding without MITM attack

mute features a key server which provides

- human-friendly identities (e.g., `john.doe`)
- authenticity of the identity-key relationship
- MITM attack (by third parties or key server) is impossible!

cliffhanger: we will publish

- key server design
- key server protocol
- client source code

ASAP, please check `http://mute.berlin` for updates!

secure messaging roadmap

	state of the art[8]	mute	future
end-to-end encryption	✓	✓	✓
asynchronous communication	✓	✓	✓
secure identity-key binding	(✓[9])	✓	✓
human-friendly identities	✗	✓	✓
service-backed digital cash	✗	✓	✓
perfect forward secrecy	✗	✓	✓
plausible deniability	✗	(✓[10])	✓
anonymous messaging	✗	(✓[11])	✓
post-quantum cryptography	✗	✗[12]	✓

[8] shown for PGP; OTR has PFS, but is synchronous

[9] manual fingerprint comparison or web-of-trust

[10] for message content; only some deniability of communication relationship

[11] stop-and-forward mix

[12] possible in later versions

conclusion

low-latency, high-bandwidth anonymity is dead

⇒ we need a paradigm shift to high-latency systems!

⇒ asynchronous messaging rules!

take away:

> *"widely deployed anonymous secure messaging is absolutely fundamental for a paralelní polis."*

acknowledgments: smuggler (mute's chief architect)

contacts:

- `frank@cryptogroup.net` (please use PGP, key on key server)
- `94CC ADA6 E814 FFD5 89D0 48D7 35AF 2AC2 CEC0 0E94`
- `#agora` IRC channel / community: `https://anarplex.net/`

register for mute news and beta invitation: `http://mute.berlin`