September 8, 2016

cyber

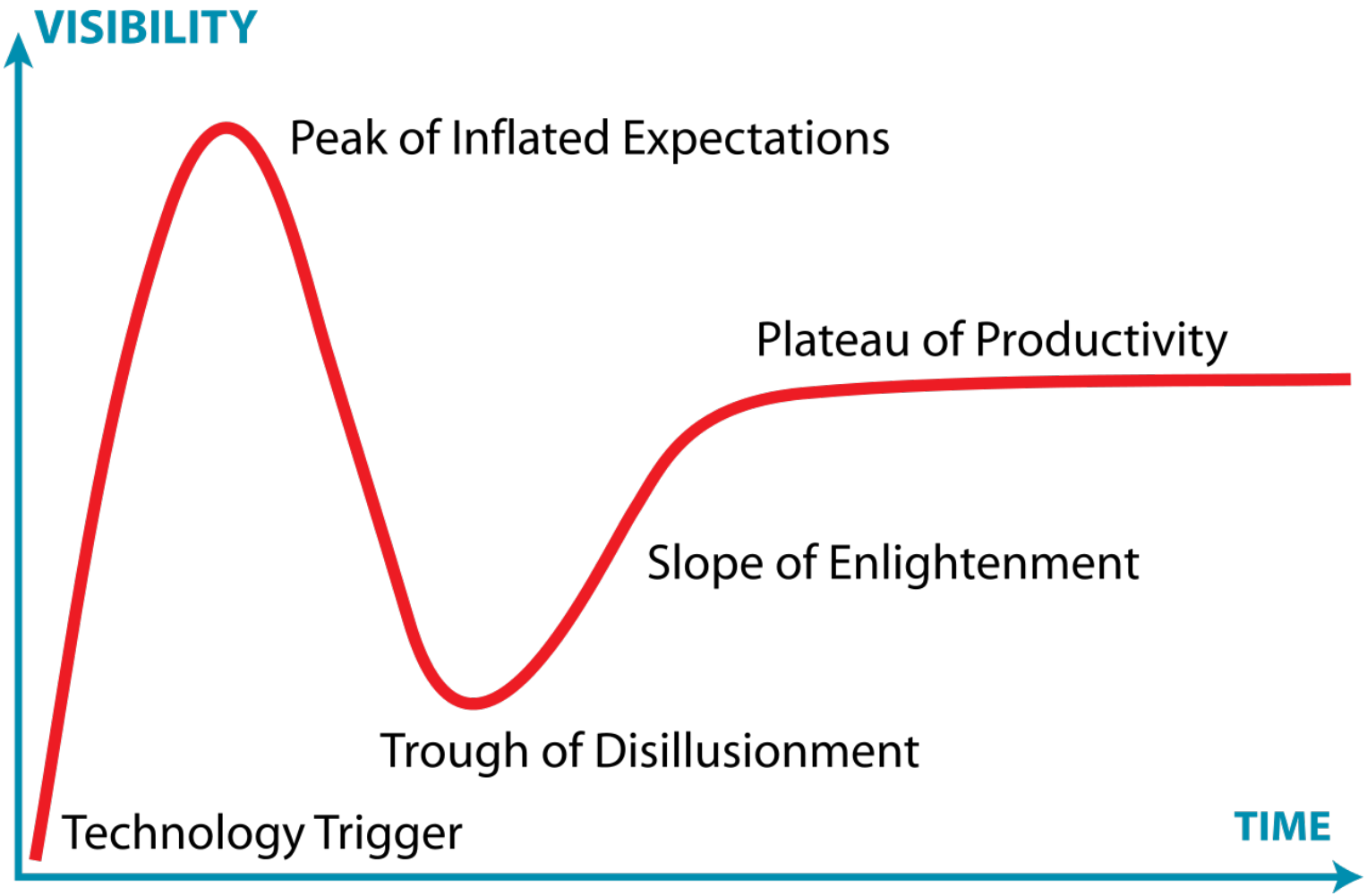
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber
cybercybercyber cybercybercyber cybercybercyber cybercybercyber

this talk

- who said why pgp is broken
- how others do it (nothings perfect)

myself

- free software since '95,
- 10 years telco security/development,
- worked with tactical tech, digiges, lqdn, bits of freedom, others
- founder of budapest and coach for bratislava and prague hackerspaces
- can do break some crypto - placed top 10 in CHES'15 challenge
- building my own crypto /o\ - e.g. native smime support for mutt back in the days
- playing a lot with pgp


VISIBILITY
Peak of Inflated Expectations
Plateau of Productivity
Slope of Enlightenment
Trough of Disillusionment
Technology Trigger
TIME

"experts" agree

- Taking a PGP break. Encrypted communications via Signal/WhatsApp/Jabber/Ricochet instead please. - C. Soghoian (twitter profile)
- I have recently come to the conclusion that e-mail is fundamentally unsecurable. The things we want out of e-mail, and an e-mail system, are not readily compatible with encryption. I advise people who want communications security to not use e-mail, but instead use an encrypted message client like OTR or Signal. - Bruce Schneier (2015)

secushare

1. Downgrade Attack: The risk of using it wrong.
2. The OpenPGP Format: You might aswell run around the city naked.
3. Transaction Data: Mallory knows who you are talking to.
4. No Forward Secrecy: It makes sense to collect it all.
5. Cryptogeddon: Time to upgrade cryptography itse
6. Federation: Get off the inter-server super-highway.
7. Discovery: A Web of Trust you can't trust.
8. PGP conflates non-repudiation and authentication.
9. Statistical Analysis: Guessing on the size of messages.
10. Workflow: Group messaging with PGP is impractical.
11. Complexity: Storing a draft in clear text on the server
12. Overhead: DNS and X.509 require so much work.
13. Targeted attacks against PGP key ids are possible
14. TL;DR: I don't care. I've got nothing to hide.
15. The Bootstrap Fallacy: But my friends already have e-mail!

matt green (2014)

"It's time for PGP to die "

- PGP keys suck
- PGP key management sucks
- No forward secrecy
- The OpenPGP format and defaults suck

`http://blog.cryptographyengineering.com/2014/08/whats-matter-with-pgp.html`

saltpack

1. PGP encryption doesn't authenticate the sender.
2. GnuPG will output data that doesn't verify.
3. Anonymous recipients aren't fully anonymous.
4. PGP ASCII armor isn't friendly to modern apps and phones.
5. Lack of Constraints Can Be Dangerous

`https://saltpack.org/pgp-message-format-problems`

leap

- Public key problem (discovery,validation,availability,revocation): nicknym, nyms
- Availability problem (multi-device data-at-rest): soledad
- Update problem: tuf
- Meta-data problem: tls
- Asynchronous problem: triple DH, axolotl
- Group problem: proxy re-encryption, ring signatures
- Resource problem: ?

SoK: Secure Messaging paper

- [..] this approach [..] causes a loss of all forms of repudiation.
- [..] Without destination validation, surreptitious forwarding attacks are possible. Without participant consistency, identity misbinding attacks might be possible.
- Defenses against replay attacks should also be included.
- A second issue with naive asymmetric cryptography is the lack of forward or backward secrecy.

SoK: Secure Messaging

N. Unger, S. Dechand, J. Bonneau, S. Fahl, H. Perl, I. Goldberg, M. Smith

- key-exchange: security, usability, adoption
- conversation: security, deniability, usability
- group conversations
- transport: privacy, usability, adoption

`https://www.computer.org/csdl/proceedings/sp/2015/6949/00/6949a232.pdf`

key-exchange

Scheme	Example	Security Features						Usability									Adoption						
		Network MitM Prevented	Operator MitM Prevented	Operator MitM Detected	Operator Accountability	Key Revocation Possible	Privacy Preserving	Automatic Key Initialization	Low Key Maintenance	Easy Key Discovery	Easy Key Recovery	In-Band No Shared Secrets	Alert-less Key Renewal	Immediate Enrollment	Inattentive User Resistant	Multiple Key Support	No Service Provider	No Auditing Required	No Name Squatting	Asynchronous	Scalable
Opportunistic Encryption†*	TCPCrypt	-	-	-	-	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
+TOFU (Strict)†	-	◐	◐	◐	◐	-	●	●	●	●	-	●	●	-	●	●	-	●	●	●	●	●	●
+TOFU†*	TextSecure	◐	◐	◐	◐	-	●	●	●	●	●	●	●	-	●	-	-	●	●	●	●	●	●
Key Fingerprint Verification†*	Threema	●	●	●	●	◐	●	-	-	-	-	-	●	-	-	-	-	●	●	●	●	●	●
+Short Auth Strings (Out-of-Band)†*	SilentText	●	●	●	●	◐	●	-	-	-	-	-	●	-	-	-	-	-	●	●	-	●	●
+Short Auth Strings (In-Band/Voice/Video)†*	ZRTP	●	●	●	●	◐	●	-	-	-	-	◐	●	-	-	-	-	●	●	●	-	●	●
+Socialist Millionaire (SMP)†*	OTR	●	●	●	●	◐	●	-	-	-	-	●	-	-	-	-	-	●	●	●	-	●	●
+Mandatory Verification†*	SafeSlinger	●	●	●	●	◐	●	-	-	-	-	●	-	-	●	●	-	●	●	●	-	●	●
Key Directory†*	iMessage	●	-	-	-	●	-	●	●	●	●	●	●	●	●	●	-	●	●	◐	●	●	●
+Certificate Authority†*	S/MIME	●	-	-	-	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
+Transparency Log	-	●	-	◐	◐	-	-	●	●	●	●	●	●	◐	●	●	●	-	●	●	●	●	●
+Extended Transparency Log†	-	●	-	◐	●	●	-	●	●	●	●	●	●	◐	●	●	●	-	●	●	●	●	●
+Self-Auditable Log†	CONIKS	●	-	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	◐	●	●	●	●	●
Web-of-Trust†*	PGP	●	●	●	◐	◐	-	-	-	◐	◐	-	-	-	-	●	●	●	●	●	●	●	●
+Trust Delegation†*	GnuNS	●	●	●	◐	◐	●	-	-	◐	◐	-	-	-	-	●	●	●	●	●	●	●	●
+Tracking*	Keybase	●	◐	◐	-	◐	-	◐	◐	◐	◐	-	-	-	●	-	●	-	◐	●	●	●	●
Pure IBC†	SIM-IBC-KMS	●	-	-	-	-	●	●	●	●	●	●	●	●	●	●	-	-	●	-	●	●	●
+Revocable IBC†	-	●	-	-	-	◐	●	●	●	●	●	●	●	●	●	●	-	-	●	-	●	●	●
Blockchains*	Namecoin	●	●	●	●	-	●	●	◐	●	●	●	●	-	●	●	●	-	-	-	●	-	●
Key Directory+TOFU+Optional Verification†*	TextSecure	◐	◐	◐	◐	●	-	●	●	●	●	●	-	●	-	◐	-	●	●	●	●	●	●
Opportunistic Encryption+SMP†*	OTR	◐	◐	◐	◐	●	●	-	●	-	-	◐	◐	-	●	-	●	●	●	●	●	-	●

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

key-exchange security

- Network MitM Prevention (hkps, fingerprints)
- Operator MitM Prevention (direct key exchanges)
- Operator MitM Detection (fingerprints)
- Operator Accountability (?, better logging)
- Key Revocation Possible (yay)
- Privacy Preserving (not true)

key-exchange usability

- Automatic Key Initialization (no)
- Low Key Maintenance (no)
- Easy Key Discovery (depends)
- Easy Key Recovery (no)
- In-band (no)
- No Shared Secrets (yes)
- Alert-less Key Renewal (no)
- Immediate Enrollment (no)
- Inattentive User Resistant (no)

key-exchange adoption

- Multiple Key Support (no)
- No Service Provider Required (depends)
- No Auditing Required (yes)
- No Name Squatting (yes)
- Asynchronous (no)
- Scalable (depends)

conversations

Scheme	Example	Security and Privacy														Adoption					Group Chat				
		Confidentiality	Integrity	Authentication	Participant Consistency	Destination Validation	Forward Secrecy	Backward Secrecy	Anonymity Preserving	Speaker Consistency	Causality Preserving	Global Transcript	Message Unlinkability	Message Repudiation	Particip. Repudiation	Out-of-Order Resilient	Dropped Message Resilient	Asynchronicity	Multi-Device Support	No Additional Service	Computational Equality	Trust Equality	Subgroup Messaging	Contractable	Expandable
TLS+Trusted Server†*	Skype	-	-	-	-	-	-	-	-	-	-	●	●	●		●	●	●	●	-	●	●	●	◐	◐
Static Asymmetric Crypto†*	OpenPGP, S/MIME	●	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	●					
+IBE†	Wang et al.	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	-					
+Short Lifetime Keys	OpenPGP Draft	●	●	●	-	-	◐	◐	●	-	-	-	-	-	-	●	●	●	●	-					
+Non-Interactive IBE†	Canetti et al.	●	●	●	-	-	●	-	●	-	-	-	-	-	-	◐	●	●	●	●					
+Puncturable Encryption†	Green and Miers	●	●	●	-	-	●	-	●	-	-	-	-	-	-	●	●	●	●	●					
Key Directory+Short Lifetime Keys†	IMKE	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	●	●	●	-	-	-					
+Long-Term Keys†	SIMPP	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	-	●	●	-	-	-					
Authenticated DH†*	TLS-EDH-MA	●	●	●	●	●	◐	◐	●	-	-	-	●	●	◐	●	●	-	-	●					
+Naïve KDF Ratchet*	SCIMP	●	●	●	●	●	●	◐	●	◐	-	-	●	●	◐	◐	◐	-	-	●					
+DH Ratchet†*	OTR	●	●	●	●	●	◐	●	●	◐	◐	-	●	●	◐	◐	◐	-	-	●					
+Double Ratchet†*	Axolotl	●	●	●	●	●	●	●	●	◐	◐	-	●	●	◐	●	◐	-	-	●					
+Double Ratchet+3DH AKE†*	-	●	●	●	●	●	●	●	◐	◐	◐	-	●	●	◐	●	◐	-	-	●					
+Double Ratchet+3DH AKE+Prekeys†*	TextSecure	●	●	●	●	●	●	●	-	◐	●	-	●	●	●	◐	◐	●	-	-					
Key Directory+Static DH+Key Transport†	Kikuchi et al.	●	●	-	-	●	◐	◐	-	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
+Authenticated EDH+Group MAC†	GROK	●	●	◐	-	●	◐	◐	●	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
GKA+Signed Messages+Parent IDs†	OldBlue	●	●	●	●	●	◐	◐	●	●	-	-	-	-	-	●	●	◐	-	●	●	●	-	-	-
Authenticated MP DH+Causal Blocks†*	KleeQ	●	●	◐	◐	◐	●	●	●	◐	◐	●	-	●	●	●	●	◐	-	●	●	●	-	-	●
OTR Network+Star Topology†	GOTR (2007)	●	●	-	-	-	◐	●	-	-	-	-	●	●	●	◐	●	◐	-	●	-	-	-	●	●
+Pairwise Topology†		●	●	●	●	●	◐	●	●	-	-	-	●	●	●	◐	●	◐	-	●	●	●	●	●	●
+Pairwise Axolotl+Multicast Encryption*	TextSecure	●	●	●	-	●	●	●	-	●	●	-	●	●	●	●	●	●	-	-	●	●	●	●	●
DGKE+Shutdown Consistency Check†	mpOTR	●	●	●	●	●	◐	◐	●	◐	-	-	-	●	●	●	●	-	-	●	●	●	-	-	-
Circle Keys+Message Consistency Check†	GOTR (2013)	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	-	-	-	◐	●	●	-	●	●

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

conversation security

- Confidentiality (yes)
- Integrity (yes)
- Authentication (yes)
- Participant Consistency (no)
- Destination Validation (no)
- Forward Secrecy (no)
- Backward Secrecy (no)
- Anonymity Preserving (no)
- Speaker Consistency (no)
- Causality Preserving (no)
- Global Transcript (no)

consersation deniability

- Message Unlinkability (depends)
- Message Repudiation (no)
- Participation Repudiation (no)

group converstions

none supported.

- Computational Equality (no)
- Trust Equality (no)
- Subgroup messaging (no)
- Contractible Membership (no)
- Expandable Membership (no)

conversation Usability

- Out-of-Order Resilient (yes)
- Dropped Message Resilient (yes)
- Asynchronous (yes)
- Multi-Device Support (yes)
- No Additional Service (no)

transport

Scheme	Example	Privacy					Usability					Adoption									
		Sender Anonymity	Recipient Anonymity	Particip. Anonymity	Unlinkability	Global Adv. Resistant	Contact Discovery	No Message Delays	No Message Drops	Easy Initialization	No Fees Required	Topology Independent	No Additional Service	Spam/Flood Resistant	Low Storage	Low Bandwidth	Low Computation	Asynchronous	Scalable		
Store-and-Forward[†*]	Email/XMPP	-	-	-	-	-	●	◐	●	●	●	●	-	-	●	●	●	●	●		
+DHT Lookup[†*]	Kademlia	◐	◐	-	-	-	●	◐	●	●	●	●	●	◐	●	◐	●	●	●		
Onion Routing+Message Padding[†*]	Tor	●	-	●	●	-	-	◐	●	●	●	●	◐	-	●	●	●	-	●		
+Hidden Services[*]	Ricochet	●	●	●	◐	-	-	◐	●	●	●	●	◐	-	●	●	●	-	●		
+Inbox Servers[†]	-	●	-	●	●	-	-	◐	●	●	●	●	-	-	●	●	●	●	●		
+Random Delays[†*]	Mixminion	●	-	●	●	◐	-	-	●	●	●	●	-	-	◐	●	●	●	●		
+Hidden Services+Delays+Inboxes+ZKGP[*]	Pond	●	-	●	●	◐	-	-	●	●	●	●	-	●	◐	●	●	●	●		
DC-Nets[†*]	-	●	●	-	-	●	-	-	●	●	●	-	●	-	●	●	●	-	-		
+Silent Rounds[†]	Anonycaster	●	●	-	-	●	-	-	●	●	●	-	●	◐	●	●	●	-	-		
+Shuffle-Based DC-Net+Leader[†]	Dissent	●	●	-	-	●	-	-	●	●	●	-	●	●	●	●	●	-	-		
+Shuffle-Based DC-Net+Anytrust Servers[†]	Verdict	●	●	-	-	●	-	-	●	●	●	-	-	●	●	●	●	-	◐		
Message Broadcast[†]	-	-	●	●	●	●	●	●	●	●	●	●	●	-	-	-	◐	-	-		
+Blockchain	-	◐	●	●	●	●	●	-	-	●	-	●	◐	●	-	-	-	●	-		
PIR[*]	Pynchon Gate	-	●	●	●	●	●	-	●	◐	●	●	-	-	-	◐	◐	●	◐		

transport privacy

- Sender Anonymity (yes)
- Recipient Anonymity (no)
- Participation Anonymity (no)
- Unlinkability (maybe)
- Global Adversary Resistant (no)

transport usability

- Contact Discovery (yes*)
- No Message Delays (yes*)
- No Message Drops (yes*)
- Easy Initialization (no)
- No Fees Required (yes)

transport adoption properties

- Topology Independent (yes)
- No Additional Service (no)
- Spam/Flood Resistant (no)
- Low Storage Consumption (yes)
- Low Bandwidth (yes)
- Low Computation (yes)
- Asynchronous (yes)
- Scalable (yes)

diversity!!!5!

strong selectors (fingerprinting)

- pgp stealth (2003)[1]
- tls
- nacl-based: nonce + ephemeral pubkey + ciphertext + mac

[1] http://www.cypherspace.org/adam/stealth/

nacl-based

- https://github.com/stef/pbp (python)
- https://github.com/jedisct1/minisign (c)
- https://github.com/wbl/cpgb (c)
- https://github.com/Spark-Innovations/SC4 (js)
- https://github.com/davidlazar/flycrypt (go)
- https://github.com/carlos8f/salty (js)
- https://saltpack.org/encryption-format (keybase)

lack of pfs

- compartments: smartcards, gnuk, sc4-hsm
- axolotl
- PITCHFORK

PFS: axolotl

confidentiality, integrity, authentication, participant consistency, destination validation, forward secrecy, backward secrecy (aka future secrecy), causality preservation, message unlinkability, message repudiation, participation repudiation, and asynchronicity. It does not provide anonymity preservation, and requires servers for the relaying of messages and storing of public key material.
pros:

- can do multiple devices

cons:

- tracks state
- data in motion
- adds extra headers for additional devices

libsodium based axolotl implementations:

- `https://github.com/1984not-GmbH/molch`
- `https://github.com/stef/libsaxolotl`

PITCHFORK+pbp

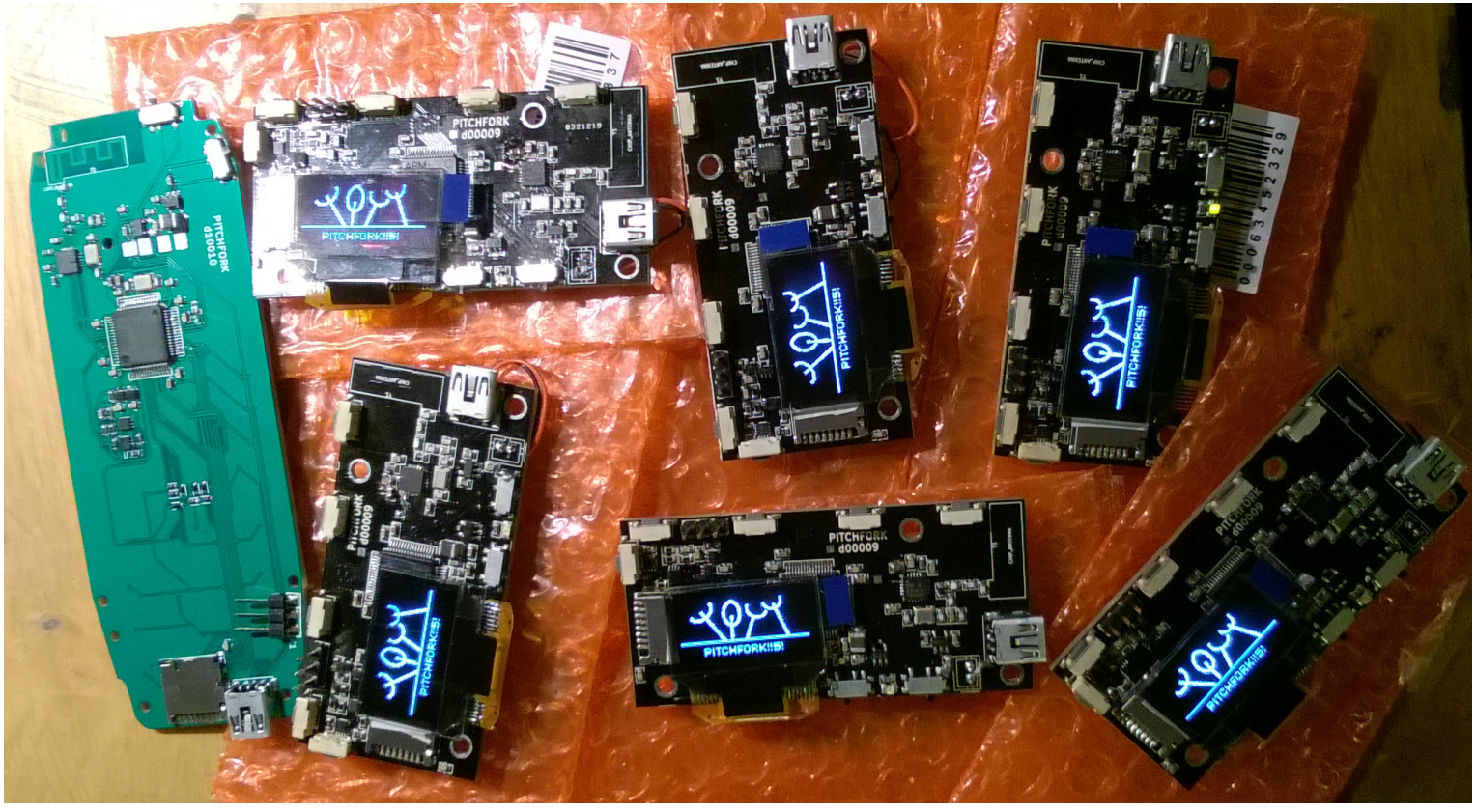
- experimental PFS[2]
- no fingerprints
- HW support
- multi-device support!

[2] https://github.com/stef/pbp/blob/master/doc/chaining-dh.txt

PITCHFORK I

- open [hfs]w, modern (post-quantum) algos
- has a threat model
- no more key-signing parties
- 2.4GHz radio, sd-card reader, display, buttons.

PITCHFORK II



key discovery/validation

- 32B nacl pubkeys in tweets
- minilock
- safeslinger
- coniks
- PITCHFORK
- keybase

minilock

pros:

- no stored state or key

cons:

- key is always derived from kdf(password,userid) and calculated on the fly

`https://github.com/kaepora/miniLock/blob/`

opmsg

`https://github.com/stealth/opmsg`

- bitcoin as a WoT
- gpg-chameleon

keybase

tracking:
`https://keybase.io/docs/server_security/tracking`

coniks

supports all key exchange properties, except:

- no: Operator MitM Prevention
- maybe: Operator MitM Detection, No name-squatting
- no specification like signal :/

Authenticated DH (sigma, ratchets, etc)

- repudiation or authenticity
- surreptitious forwarding attacks
- identity misbinding attacks

salted&iterated keys - time/memory hardness

- argon2i

privacy

- pond (solves spam)
- percy++ (PIR)
- dissent
- pynchon gate (PIR)
- hkps hidden service
- parcimonie

postquantum!

- codecrypt `https://github.com/exaexa/codecrypt`
  - McEliece cryptosystem (compact QC-MDPC variant) for encryption
  - Hash-based Merkle tree algorithm (FMTSeq variant) for digital signatures
- cr3 `https://github.com/stef/cr3`
  - sphincs+keccak

conclusions

- <3 diversity!
- write a pluggable chameleon dispatcher
- build and break more PITCHFORKS!!!5!
- crowdsupply pre-order campaign.

Questions

- twitter: : @pitchf___ (3 underscores)
- irony pgp key: 0x970DEB6694D50988 - s@ctrlc.hu
- pbp(nacl encryption/base85)

```
LLBXh0ge}M]vNOz1<PX&^U[hIINAL{e/qqblajJe
```