Can Johnny build a protocol?

Co-ordinating developer and user intentions for privacy-enhanced secure messaging protocols

Ksenia Ermoshina
(CNRS)
Harry Halpin
(INRIA)
Francesca Musiani
(CNRS)

RESEARCH CONTEXT

NEXTLEAP.EU

- Horizon 2020 project: NeXt generation Techno-social and Legal Encryption Access and Privacy
- https://nextleap.eu
- Study, validate, and deploy core protocols to form the foundation for a secure, trust-worthy, and privacy-respecting Internet

RESEARCH CONTEXT

- Proliferation of secure messaging protocols (Ermoshina, Musiani, Halpin 2016) →
- Developers are in a state of flux about security and privacy properties flux of these protocols;
- Interoperability problem;

Aim of this study

- Do user beliefs and understanding align with the reality of the protocol and its implementation?
- Do different types of users have different needs regarding S&P?
  - ➔ Study **interaction** effects and "translation" between users and developers
  - ➔ Take into account **'intermediaries'** (e.g. infosec trainers), understood as 'knowledge brokers' / interactional experts

METHODOLOGY

QUALITATIVE METHODS; STS

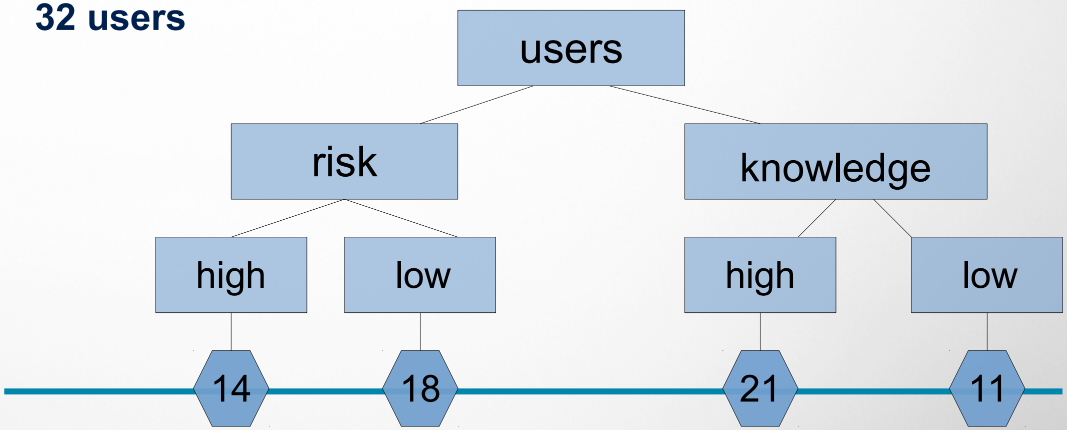
How?

Semi-structured Interviews (1 to 3 hours), ehtnography, web-ethnography;

How many?

52 interviews between October 2016 and March 2017 (48 on time of paper submission);

- **17 developers**
- **3 NGO** experts (EFF, CAPS project)
- **32 users**



DESIGN QUESTIONS FOR PROTOCOLS

Do users and developers care of...

- Security Properties (forward secrecy, repudiation…)
- Group Support
- Privacy Properties (metadata protection)
- Decentralization
- Standardization
- Licensing

THESES

#1 “Developer-User Disconnect”

Properties of protocols are not understood by users, and needs of users not systematically gathered by developers prior to design.

#2 “High-Risk User Problem”

High-risk users have different needs and behavior than low-risk users, yet are less studied.

#3 “Security Trainings Differ by Risk”

Trainers from high-risk countries will suggest different practices and tools than their colleagues from low-risk countries.

FINDINGS

Security Properties:

- No one except developers care about deniability;
- High-risk use ephemeral messages and one time secrets to acquire deniability;
- High-risk users want to “see encryption” happening;
- High-risk users confound initial fingerprint verification and key verification if key material changes;
- But use “voice calls” and social context to check for errors if key material changes;
- People trust security due to reputation of developer and jurisdiction of app (exemple : Pavel Durov – Telegram - leaving Russia).

FINDINGS

Group Support

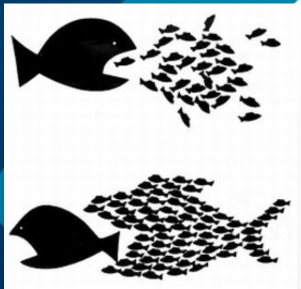
- “important usability feature and a scientific problem”
- but Telegram and OTR goes to cleartext in groups
- Telegram stays most popular in Iran and Russia;
- Inertia and ‘network factor’ - prevent from ‘migration’ to more secure tools;
- Non-security properties matter: **stickers**, broadcasting functions;

FINDINGS

As they say, the devil's in the details...
NOTHING TO WORRY ABOUT. IT'S JUST METADATA.
NSA
©2013 Jeff Parker FLORIDA TODAY
CAGLECARTOONS.COM

Privacy properties:

- Developers confuse possible metadata collection by third parties with their own logging of user data;
- Metadata and centralization problem – related for devs, not for users;
- Privacy is a “first world problem” for high-risk activists (Iran, Ukraine);



Decentralization:

- Technical challenge/social experiment;
- Important to developers and low-risk users, not high-risk users
- High-risk users aspire at social decentralization, but can not trust existing tools;
- High-risk trainers do not focus on decentralization

FINDINGS

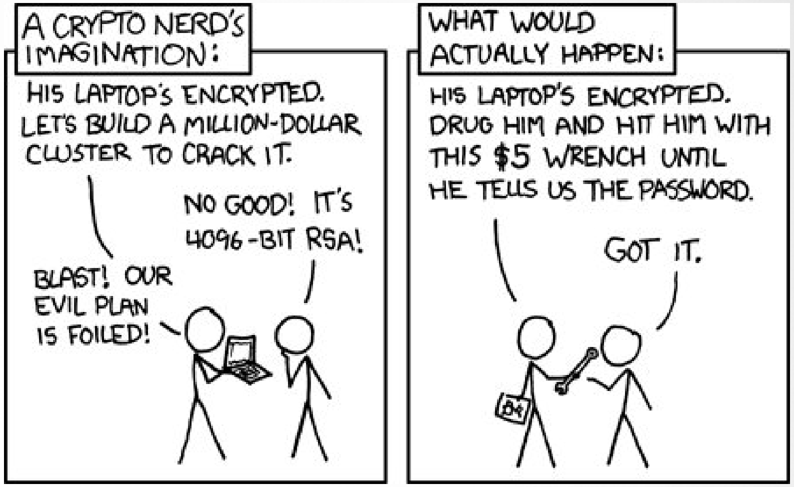
Standardization

- Not of interest to users, important to developers, but discontent with existing bodies (IETF, XMPPF, W3C);
- 'Quasi-standards' by 'running code' like Signal Protocol.
- Standards as business model

Licensing

- Preference for open-source ;
- GPL is a 'lifestyle choice' ;
- More happy to pay for 'not being the product' (Threema) ;
- High-risk trainers – do not spend time on licensing (may recommend closed source - WhatsApp)

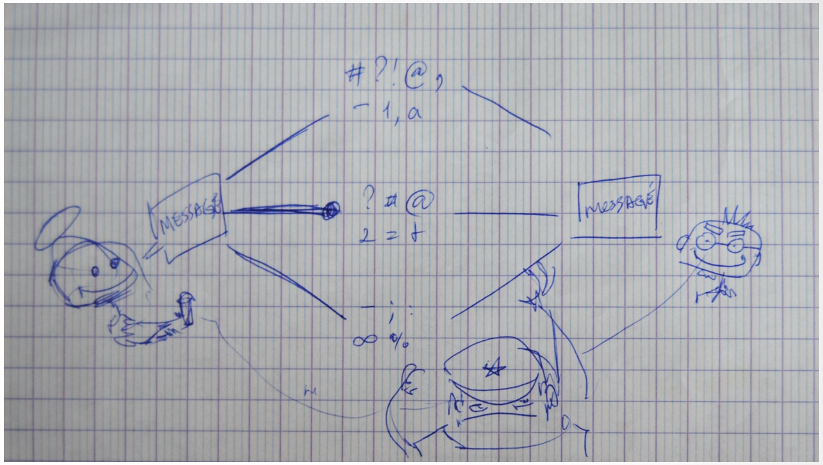
CONCLUSIONS


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Developers aim at high-risk users but...

- Concerned with cryptographic details of protocol like repudiation, and not more holistic threats such as device seizures ;
- Ephemeral messaging only recently added ;

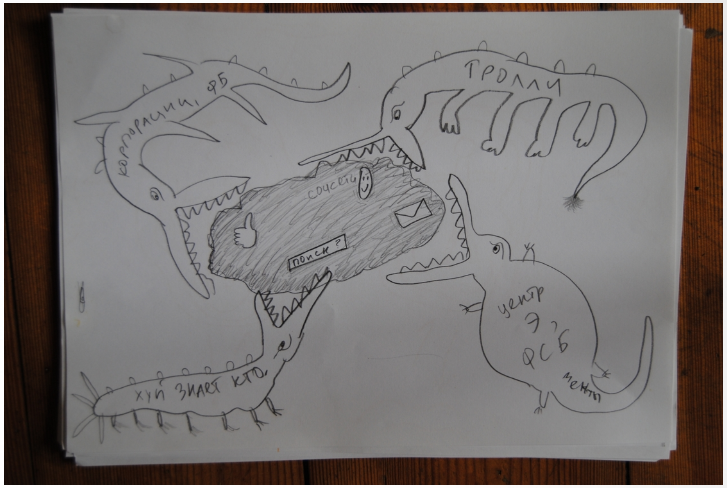
CONCLUSIONS



Users have different threat models by risk

- **High-risk users** concerned about physical device compromise and <u>active attacks</u> by <u>local active adversary</u> (e.g. their government) ;
- **Low-risk** users concerned about passive <u>monitoring</u> and attacks such as server-seizures ;

CONCLUSIONS



Trainers customize training based on risk

- High-risk - focus on hard-drive encryption, legal aspects, operational security; build recommendations on users previous knowledge; recommend what's easier and quicker to adopt ;
- Low-risk – may spend more time on explaining cryptographic concepts ; on PGP ; on FLOSS alternatives to GAFAM ;

FUTURE WORK

- Further interviews of **high-risk users** in Middle East;
- **More interviews** of every category, in order to get statistical significance (at least 20 needed of each group) and balance in interviews;
- **User studies** to determine how properties (geolocation via IP, deniability, forward secrecy) lead users to react in different situations ;
- Gathering **user drawings** and designing a study with UCL PhD students in usability ;

THANK YOU !

Ksenia.ermoshina@cnrs.fr

Harry.halpin@inria.fr

Francesca.musiani@cnrs.fr