Subject: A few thesis regarding privacy and security
From: "Andreas Kuckartz" <a.kuckartz@ping.de>
Date: 01/20/2014 10:46 PM
To: group-strint-submission@w3.org

A few thesis regarding privacy and security for W3C/IAB workshop on Strengthening the Internet Against Pervasive Monitoring (STRINT), 28 February – 1 March 2014, London

Andreas Kuckartz, a.kuckartz@ping.de
W3C Federated Social Web Community Group
http://www.w3.org/community/fedsocweb/

Low hanging fruit: Weak encryption is better than no encryption.

Enforced encryption is better than opportunistic encryption. Due to network effects it is difficult to deploy enforced encryption to existing networks (SMTP, XMPP [1] are examples). New standardization efforts need to learn from that.

"Meta" information is most important: Who is communicating with whom. The social graph needs to be protected. That is difficult. Support projects like Tor and GNUnet. Create and use standards for anonymous communication protocols.

Some valuable services can only be implemented using servers (with today's technology). But enable end-to-end encryption whenever possible.

All standards involved in communication are impacted. That includes communication between things which are used by humans.

A core problem: Combining different levels of encryption/security. Example: secure c2s - insecure s2s - secure s2c: no e2e security. That is typical for federated protocols like mail (SMTP) or messaging (XMPP). Maybe security labels [2] can be used here?

Levels of security should be visible to end users, similar to visibility of quality issues in public issue trackers. Use of c2s encryption or absence of it can be displayed by user interface, but what about s2s encryption? Can servers be prevented from lying to clients regarding absence of s2s encryption?

Do not support insecure technologies like DRM. Some standards can be dangerous [3].

Due to the human, social and political costs of privacy violations strong technical privacy protections are justified. For some people extremely strong (above average) protections are appropriate. Such protections should be possible using standard protocols.

[1] A Public Statement Regarding Ubiquitous Encryption on the XMPP Network, https://github.com/stpeter/manifesto/blob/master/manifesto.txt

[2] XEP-0258: Security Labels in XMPP,
http://xmpp.org/extensions/xep-0258.html

[3] Encrypted Media Extensions, http://www.w3.org/TR/encrypted-media/