Putting the Context into the Crypto of Secure Messengers

Posted on **January 21,2017** by **lynx**

Every once in a while the world of encrypted/secure/authenticated messaging hits the wall of usability. In the case for email Pretty Good Privacy (PGP) is an ancient piece of software. These days we have modern tools such as GnuPG, but the concept of creating keys, verifying identities (i.e. determining who is to trust), synchronising trust/keys with communication partners, and handling the software in case something goes wrong is quite a challenge. Plus things might change. People revoke their keys, devices get lost, data gets deleted, people create new keys or even (digital) identities, or do lots of things that is either anticipated by the software developers or not. Communication is not static. There are moving parts involved, especially the communication partners might move a lot.

So crypto is hard, we know this. Discussing secure messengers is also hard as The Guardian found out a couple of days ago. The author claimed that WhatsApp contains a „backdoor“ and that the messages can be re-encrypted and sent again. The whole story revolves around the generation of unique secrets keys and doing stuff with messages already being transported. Open Whisper Systems has commented on this article by providing the technical background, criticising the falsely used term „backdoor“, and explaining what is going on behind the scenes for WhatsApp and Signal. The reactions to the Guardian Article range from technically incorrect to o utrageously dangerous for WhatsApp users relying on the protection of their messages.

The question remains: What should a secure messenger do, when it detects that a communication partner has changed security parameters? The answer is different for WhatsApp and Signal. As you know from network security you can default to accept or deny/drop. With messages you can either drop the message until the communication partner has confirmed the change and possibly re-verified the identity of the communication partner; or you can route the message. Regardless what you do, it is a valid choice provided the encryption is sound and you tell the user(s) about it. The preferred choice depends on the context. If you have very disciplined communication partners, then this event is an indication that something is wrong. If you communication partners periodically change devices, don't do any backups, eat SIM cards for breakfast, and play around with installed apps, then this might be nothing to worry about.

Examining the context is often all you can do. The tools are there to help you. Even PGP with the dreaded Web of Trust and its 1990s usability offers you some information to make a decision. The crucial point of secure communication is to keep track of identities and do the verification of contacts right. Given your threat model you can do this by a phone call or a personal meeting. It's your decision.

Posted in:Communication,Discussion,Internet | Tagged:Crypto,Design,Mindset,Mobile | With 0 comments