Cryptography for Software and Web Developers

Part 5: Don’t believe the crypto hype

Hanno Böck

2014-05-28
The NSA scandal was the biggest boost for snake oil crypto of all time

Threema, Telegram, Cryptocat, whistle.im, chiffry, tutanota, myEnigma, Hike, Kontalk, ...
At the moment a lot of people will try to sell you the latest easy-to-use super-secure crypto solution

In most cases these should not be considered trustworthy
Telegram has a contest: They’ll pay you $200,000 if you can decrypt their sample messages.

Sounds good, right?

But it only applies to passive attacks. No sidechannels, authentication issues, software bugs like buffer overflows, known-plaintext-attacks, ...

Moxie Marlinspike challenged the Telegram developers with a similar contest by defining a completely insecure protocol. They haven’t responded.
➤ Threema is proprietary

➤ But they provide a ”validation” feature: App can log data packages and a small tool that’s available in source form can verify if that’s really the message encrypted with the corresponding private key

➤ How do you know if the logged package is the same that was sent?

➤ How do you know they don’t embed secret data in the nonce?

➤ You just don’t. The whole Threema validation is a scam.
We really could need some better crypto message systems

Some people will tell you: ”What’s the matter, we have PGP and Jabber with OTR, that’s all you need”

Except that they’re mostly unusable for normal users and have tons of strange properties

PGP doesn’t encrypt the Subject, has two modes where only one protects certain metadata, doesn’t provide forward secrecy

OTR only works if your communication partner is online, else it will be unencrypted
From everything I’ve seen lately there are only two systems I find interesting: Pond and Textsecure

- Free software, source available
- Well documented strong crypto technologies that seem to make sense
- Created by people who know a lot about crypto
I find it hard to believe, but this is a real problem

”E-Mail Made in Germany”,”SecurlTy made in Germany / TeleTrusT” etc.

Peter Tauber (member of german parliament, CDU) wants german encryption

Recently got a mail proposing a secure chat and phone system that uses ”german elliptic curves with 512 bit”. (I assume they mean the Brainpool curves, however Brainpool has no curve with 512 bit)

”Don’t use AES, it’s a US-standard from the NSA” - except that it has been created by researchers from Belgium
- Crypto is good when it has been created in a trustworthy process.
- It doesn’t matter what kind of passport the researcher / developer creating the system has.
- And finally: Be aware that Germany does not have a lot of high profile cryptographers.
Some reasonable questions you may ask:

”Crypto is hard. Do you have a crypto expert in your development team or has your software been reviewed by a crypto expert?”

”Can I see the technical details of the protocol?”

”Can I see the source code?”

If the answer to any of these is ”No” just ignore it
TextSecure https://whispersystems.org/
Pond https://pond.imperialviolet.org/