Applied Crypto Hardening Project is looking for Help

Posted on **April 25,2017** by **lynx**

Hopefully many of you know the Applied Crypto Hardening (ACH) project, also known as BetterCrypto.org. The project was announced at DeepSec 2013. The idea was (and is) to compile hands-on advice for system administrators, dev ops, developers, and others when it comes to selecting the right crypto configuration for an application. The BetterCrypto.org document covers far more protocols than HTTPS. OpenSSH, OpenVPN, IPsec, and more topics are described in the PDF guide. The project is run by volunteers. This is where you come in.

The ACH project needs more volunteers to keep going. New GNU/Linux distributions are around the corner (the apt store never sleeps). Some vendors really do upgrade their code base. Libraries change and bleed less. Algorithms get tested, improved, and re-evaluated. The field of cryptography is moving forward, as it should. So if you have some mathematics skills, know your way around configurations, like to work with text fragments and documents, and would like to help improving the crypto capabilities of the software around you, then there is a way to express yourself. Join the mailing list. Get a Github account or use you existing one. Send pull requests. Help with the reviews.

Just because some vendors and some developers haven't been fast asleep for the past four years, the effort to promote, test, and deploy solid cryptographic configurations does not happen automagically. It's not all about OpenSSL cipher strings. It is about all applications that use cryptography. Help with your skills. We do.

Plus you can even submit a talk for the DeepSec 2017 Call for Papers and talk about how you did things cryptographically right. We had some talks about this in the past. Don't be a pre-quantum crypto couch potato!

Posted in:High Entropy,Internet | Tagged:Crypto,Development,Mindset | With 0 comments