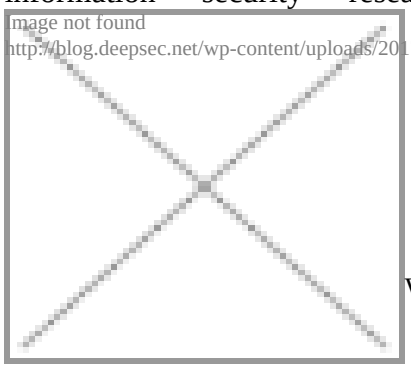
The only responsible Encryption is End-to-End Encryption

Posted on **October 30,2017** by **lynx**

Last week the Privacy Week 2017 took place. Seven days full of workshops and presentations about privacy. This also included some security content as well. We provided some background information about the Internet of Things, data everyone of us leaks, and the assessment of backdoors in cryptography and operating systems. It's amazing to see for how long the Crypto Wars have been raging. The call for backdoors and structural weaknesses in encryption was never silenced. Occasionally the emperor gets new clothes, but this doesn't change the fact that some groups wish to destroy crypto for all of us. The next battle is fought under the disguise of *responsible encryption*. Deputy Attorney General Rod J. Rosenstein invented this phrase to come up with a new marketing strategy for backdoors.

Once you have backdoors in any technology, it ceases to be secure. Technology companies, academics, and information security researchers have all worked to improve hardware and software



we use on a daily basis. Even governments rely on secure applications and protocols. It is technically impossible to have security in anything that is backdoored. It is really that simple. The discussion has been raging since the ill-advised Clipper Chip, basically ever since strong encryption was available for businesses and private persons in the world of IT.

Kurt Opsahl wrote an analysis which we highly recommend. In case you hear someone mumbling about responsible encryption, please make sure that you explain to this someone that strong crypto is the correct answer. Anyone not believing this should attend DeepSec. We love to discuss and analyse all different approaches. Warning: The discussion will probably get really short.

Update: Dear journalists, please refrain from using the terms *responsible encryption* and *going dark* as actual technologies of information technology. Always use quotes („“ or "") to mark these terms as vague. It makes the job of the security researchers much easier. Thank you!

Posted in:High Entropy,Security | Tagged:Crypto | With 0 comments