AFCEA Europe Cryptography workshop

in partnership with secunet secusmart | BlackBerry Subsidiary

13 September 2018, Pullman Brussels Centre Midi, Belgium

Everything Secret, Complete Insecurity?

Are today's policies matching modern cryptography and operational requirements?

An increasingly joint, even integrated environment for military and security operations naturally asks for improvements in the handling of highly sensitive/classified information and therefore encryption systems. Different national encryption systems, advanced attack potential, and an increasing request for more convenience by users with regard to speed, capacity, comfort in handling ever larger amounts of data require highly capable, yet highly secure and interoperable crypto systems. This means a challenge for both the technology and procedures, especially when it comes to the most efficient employment of up-to-date cryptographic tools in stationary and mobile applications.

The first step in approaching this challenge is to understand the general capability and capacity of existing, most-advanced modern crypto technologies. Limitations, generated by procedural or policy implications, need to be addressed, for instance certification and approval schemes, product lifecycle issues and crypto-related policies. Conclusions need to be drawn, before entering the new era of encryption, the post-quantum era.

Policy and implementation of crypto are also relevant in situations, where you wouldn't necessarily expect it: Multi-tenant and Multi-level systems are in strong need in missions, due to space and power limitation, yet partner nations still must work individually with a multitude of (differently classified) data.

The true challenge will come with the new disruptive, paradigm shifting technology of quantum computing, especially with regard to its application in the field of encryption. Despite its (im)maturity in practice, chances and risks have to be addressed today. For example, encrypted data can be stored in today's world and broken later by the new technology. Together with a clear vision of its implementation, questions of policy and handling need to be addressed well in advance in order to avoid unwanted surprises and being overtaken by the potential result of new incompatibilities and operational limitations in the future of this up-and-coming technology.