Crypto Agility Spider Chart

Leonie Wolf

Fraunhofer SIT

To mitigate the expectable loss of security, cryptographic schemes need to be replaced consistently. The ability to execute this exchange fast and with little effect on the overall system is often referred to as crypto(-graphic) agility. Although it is frequently demanded, there is little common understanding what crypto agility is or how it can be achieved and measured.

We present a scale to define crypto agility in various dimensions. Part of the scale are technical dimensions, like algorithmic agility and hardware/software properties, as well as organisational and human-centered dimensions. This offers a comprehensive view of all the dimensions affecting the crypto agility of a system. With this multidimensional definition we hope to facilitate a comparison of different crypto agility strategies and further research in this area.

Keywords: Crypo-agility, security metrics, security management