14 June 2016 Study · Digital Identity · Web & Cloud

Dynamic Key Usage Policies

The full text is currently only available in the Deutsch version. A translation will follow.

Archived. This content is no longer updated. It remains available for reference.

Source https://technology2.a-sit.at/en/publications/dynamic-key-usage-policies/

More and more data and resources are moved to the cloud. Even cryptographic primitives do benefit from the advantages of the cloud. However, state-of-the-art authentication methodologies and defense strategies mostly cannot cope with attacks while simultaneously allowing the legitimate user to use the service. The legitimate user is often required to perform manual steps to gain access to the service again. Denial-of-Service attacks against a user therefore persist.

This work presents a slightly different approach on how such systems can be protected. The goal is to autonomously react to changes of the systems status by changing authentication methodologies on the fly. By changing the authentication requirements, an attack might be stopped, the legitimate user can use the service during the attack, and the user can be presented with the least complex authentication requirement feasible for the current system status.

This work presents an architecture based on strategies, actions and policies which is capable of meeting the aforementioned requirements. Further, the target system does not need to be altered significantly. Two prototypes demonstrate two real use cases.