Security Analysis of GDPR Subject Access Request Procedures

Coline Boniface[1], Imane Fouad[2], Nataliia Bielova[2], Cédric Lauradoux[1], and Cristiana Santos[3]

[1] Univ. Grenoble Alpes, Inria, France name.surname@inria.fr
[2] Université Côte d'Azur, Inria, France name.surname@inria.fr
[3] School of Law, University Toulouse 1 Capitole, France
cristiana.santos@ut-capitole.fr

The GDPR came in force in May 2018 and defines rights for data subjects, such as access right, but it is still unclear how subjects can exercise them concretely. Our recent paper [1] explores two critical questions: Is it safe for a data subject to exercise the right of access of her own data? When does a data controller have enough information to authenticate a data subject?

To answer these questions, we first identify the threats to the subject access request (SAR) procedure and significant privacy issues for the data subject, such as *impersonation*, *incorrect disclosure* and *abusive identity check*.

By analyzing the recommendations on SAR of 28 DPAs of the EU countries, we observe that four of them can potentially lead to *abusive identity check*. Fortunately, six of them are recommending to enforce the *data minimization principle* during authentication.

We have evaluated the authentication procedures when exercising the access right of the 50 popular websites and 30 third-party tracking services. Seven popular websites require to provide a national identity card or government-issued documents to authenticate the data subject. Among third-party tracking services, nine of them additionally to cookies demand *other personal data from the data subjects*, like the identity card or the full name, that are not needed to authenticate the user.

Interestingly, PETs, such as VPNs, anonymous networks like TOR, or cleaning cookies *make a strong impact on the SAR*: it becomes nearly impossible to identify the data subject and hence prevents her from being able to exercise her subject access rights.

Finally, we provide guidelines on how to authenticate data subjects safely while protecting their identities, and without requesting additional unnecessary information. We explain how data controllers and data subjects must interact and how digital identifiers can be redesigned to be compliant with the GDPR.

References

1. Boniface, C., Fouad, I., Bielova, N., Lauradoux, C., Santos, C.: Security analysis of subject access request procedures. how to authenticate data subjects safely when they request for their data. In: Annual Privacy Forum (APF'19) (2019), To appear.