ERCIM "ALAIN BENSOUSSAN"
FELLOWSHIP PROGRAMME

ERCIM
European Research Consortium
for Informatics and Mathematics

Scientific Report

First name / Family name	Gábor György Gulyás
Nationality	Hungarian
Name of the *Host Organisation*	INRIA
First Name / family name of the *Scientific Coordinator*	Claude Castelluccia
Period of the fellowship	01/06/15 - 31/05/16

I – SCIENTIFIC ACTIVITY DURING YOUR FELLOWSHIP

After my arrival to the Privatics Team at INRIA, we've chosen the crossroad of machine learning and privacy as my main topic. In particular, the goal of my research was to research, design and implement machine learning models as parts of generic and automatic re-identification algorithms, which can be implemented as tools. As machine learning was almost a completely new area for me, first I was reading papers, tutorials and following (video) lectures, in order to be able to work with different machine learning techniques. Next, I did a literature survey on works where machine learning was used for de-anonymization.

I was working on how machine learning can be used in structural de-anonymization of social networks. At the time of writing this report, we are working on a publication that contains our results; we plan to submit this paper to WPES 2016 [C3]. During the fellowship period I have also submitted a work that was in part related to my work before obtaining the degree of PhD [C2].

Related publications and talks: [C2, C3, T1-3, T6]

I was also studying uniqueness and re-identification: we analyzed a privacy-preserving scheme that is used in real-world systems (such as Apple iOS 9), in which access to properties were limited. We showed that due to conceptual problems, this scheme is vulnerable to attacks.

Related publications and talks: [C1, T4-5]

II – PUBLICATION(S) DURING YOUR FELLOWSHIP

[C1] Gábor György Gulyás, Gergely Ács, Claude Castelluccia: *Near-Optimal Fingerprinting with Constraints*, accepted at PET Symposium 2016.

[C2] Gábor György Gulyás, Benedek Simon, Sándor Imre: *An Efficient and Robust Social Network De-anonymization Attack*, submitted to ESORICS 2016.

[C3] Gábor György Gulyás, Luca Melis, Claude Castelluccia: *Efficient Social Network Re-identification with Machine Learning*, to be submitted to WPES 16.

III – ATTENDED SEMINARS, WORKHOPS, CONFERENCES

[T1] Gábor György Gulyás: *Advanced social network de-anonymization attacks*, Seminar talk at INRIA, Montbonnot, France, 2015. 06. 23.

[T2] Gábor György Gulyás: *Machine learning for re-identification*, Privatics internal workshop, Corrençon-en-Vercors, France, 2016. 01. 21.

[T3] Gábor György Gulyás: *Machine learning and re-identification*, KDD Workshop 2016, San Giuliano Terme, Italy, 2016. 02. 23.

[T4] Gábor György Gulyás: *The illusion that comes with a price: privacy on the web*, Seminar at the KDD Lab (ISTI-CNR), Pisa, Italy, 2016. 02. 25.

[T5] Gábor György Gulyás: *Near-Optimal Fingerprinting with Constraints*, PrivaSki 2016, Corrençon-en-Vercors, France, 2016. 03. 09.

[T6] Gábor György Gulyás: *Taking Re-identification Attacks of Social Networks to the Next Level*, Seminar talk at UCL, London, Great Britain, 2016. 03. 31.

IV – RESEARCH EXCHANGE PROGRAMME (REP)

We've selected the KDD Lab in Pisa for collaboration, as it has an excellent reputation related to data mining (and machine learning), thus making the visit suitable for my research topic. During my research visit, I've met multiple researchers of the lab, and discussed common research interests. We have found multiple areas where we could work in cooperation. I have also participated in the group's annual workshop called KDD Workshop 2016 [T3], and I also gave a seminar talk at ISTI-CNR [T4].