EUROPEAN COMMISSION
DIRECTORATE-GENERAL
JOINT RESEARCH CENTRE
Directorate B - Resources
Recruitment and Training

2014-IPR-G-000-3495 **P2TIC Contextualised Decryption**

Position for:

Trainee

Short description of activity:

In cooperation with the European Cyber-Crime Centre (EC3) of Europol, the Digital Citizen Security Unit is conducting evaluations of technics that measures the strength of passwords and passphrases. Many tools exist nowadays to perform password recovery based on exhaustive search (testing all the possibilities) or using more clever technics such as using a dictionary. On the opposite, technics to recover passphrases are quite limited and mainly limited to exhaustive combination of words from a dictionary with unfortunately a low chance of success.

The successful candidate will contribute to conduct research in this field in order to increase the quality of the existing tools by considering the two following approaches:

1. Enrich the dictionary with contextual information about the targeted user (e.g. name of relatives, wedding date, favourite books…) can constitute a good method to increase the success of the recovery as these data are often used to build passwords and passphrases. But the dictionary must remain "small" to maintain an acceptable complexity for the recovery. Consequently, the candidate will support the research team in order to define clever way to preserve only pertinent data among the large set of existing one.

2. The second approach focuses on the definition of a "grammar" of passwords and passphrases. Semantic analysis of those elements will contribute to the fine tuning of the methodology. Even if it is strongly recommended to use fully random passwords, statistics from password leakage tend to show that users generally use a specific structure to build their passwords. The candidate will collaborate on the exploring of the possible use of semantic analysis, computational linguistic and machine learning technics on existing sets of data in order to envisage new strategies.

As a trainee, he/she will be supported and followed by a senior researcher. However, he/she should be able to work autonomously, especially regarding to software development.

The successful candidate will join a young, multidisciplinary and multinational group of researchers. During the course of the appointment, he/she will have the possibility to develop contacts with major European institutions and companies working in the field of digital media forensics. It is expected that the results of the appointment will lead to the publication of scientific papers in peer-reviewed conferences and journals.

Qualifications:

The ideal candidate is required to have solid knowledge of Python programming language, or equivalent high level language.

Knowledge of computational linguistics and machine learning techniques or natural language Processing is highly desirable.

Practical cryptography skills (symmetric and asymmetric), including cryptography tools and development skills under GNU/Linux will be an advantage.

Excellent knowledge of English is an advantage given that the work to be carried out will mostly be conducted in that language.

Institute **Unit** **Action**	Institute for the Protection and Security of the Citizen Digital Citizen Security Unit Further information: http://ipsc.jrc.ec.europa.eu
Indicative duration **Preferred starting date**	5 months As soon as possible
JRC Site **Country**	Ispra Italy
JRC contact details	For any technical problems with your application, please contact: JRC-ESRA@ec.europa.eu
JRC trainees rules	**For general eligibility requirements, please read the rules governing the traineeship scheme of the JRC:** https://ec.europa.eu/jrc/en/working-with-us/jobs/temporary-positions/jrc-trainees