2nd Annual DefMal Workshop[1]

12 Place Chateaubriand

35400 SAINT-MALO

Monday, June 3

9h00 - 9h30: PEPR Introduction by Prof. Dr. Jean-Yves MARION, Scientific Responsible for the DefMal target PEPR project

9h30 - 10h20: Dr. Nils Ole TIPPENHAUER, CISPA Helmholtz Center for Information Security - **"Out of control: Attacking and defending Industrial Control Systems"**

10h20 - 10h40: Coffee break

10h40 - 11h30: Dr. Roberto GIACOBAZZI, Arizona University – "**A Complete Journey into (in) Completeness: Hacking program analysis**"

11h30 - 12h20: Prof. Dr. Jacques KLEIN, Luxembourg University - **"AI for Software Vulnerabilities and Android Malware"**

12h30 - 14h00: Lunch break

14h00 - 15h30: Post-it collaboration exchange – An icebreaker moment about our project

15h30 - 15h50: Coffee break

Talks

15h50 - 16h00: Sébastien LARINIER, ESIEA – "**Malware analysis using CAPA and machine learning**".

16h00 - 16h30: Prof. Dr. Pierre-François GIMENEZ, CentraleSupélec - IRISA, "**Robust malware detectors by design**"

16h30 - 17h00: Dr. Nicolas BELLEC and Vidal ATIAS, CEA List – "**Advances in Deobfuscation**"

Short break

17h10 - 17h40: Prof. Dr. Tayssir TOUILI, CNRS - IRIF, "**Reachability Analysis of Concurrent Self-Modifying Code**"

17h30 - 18h00: Prof. Dr. Simone AONZO, EURECOM, "**Unmasking the Veiled: A Comprehensive Analysis of Android Evasive Malware**"

19h00: Dinner at "Le 5 – Restaurant Panoramique"

Tuesday, June 4

9h00 - 09h30: Dr. Yufei HAN, INRIA – IRISA, "**The use of LLM in cyber security knowledge encoding**"

Focus on WP 5 - Malware Ecosystems

9h30 - 10h00: Dr. Paul LABIC, Université de Strasbourg - **"Triptyque corruption-blanchiment-criminalité cyber-facilitée, taxonomie des auteurs et temporalité"**

10h00-11h00: Table discussion with Dr. Éric FREYSSINET, Senior Adviser on Cybercrime & Cybersecurity, Jean-Yves MARION, Scientific Responsible of DefMal, Dr. Paul LABIC, Strasbourg University and Maira NASSAU, DefMal Project manager.

11h00 - 11h20: Coffee break

11h20 - 12h10: Focus on WP 6 - Shared Platform: How to advance, what are the real needs?

12h30 - 14h00: Lunch break

DefMal PhD Talks

14h00 - 14h20: Jean-Marie MINEAU, CentraleSupélec -IRISA, "**Android Malware Manipulation for Improved Investigation**"

14h20 - 14h40: Vincent RAULIN, INRIA, IRISA, **upcoming title**

14h40 - 15h00: Antonino VITALE, EURECOM, "**Study of Similarity and Diversity Among Malicious Samples**"

15h00 - 15h20: Leo BERTRAND, Université de Lorraine, LORIA, "**Offensive aspect of the fight against malware**"

15h20 - 15h40: Coffee break

15h40 - 16h00: Quentin JACQMIN, Université de Lorraine, LORIA, "**Static symbolic execution of obfuscated binaries**"

16h00 - 16h20: Gabriel SAUGER, Université de Lorraine, LORIA, "**Inducing systematic targeted mismatches to ML-based binary function classifiers**"

16h20 - 16h40: Alexandre DOYEN, CEA List, "**Automatic detection of backdoors in security protocol implementations**"

16h40 - 17h00: Conclusions