Lab: Charles Delaunay Institute (UMR CNRS 6281) of UTT

Title: Reconstruction of cyber-attack paths

PhD supervisors: Patrick LALLEMENT (Prof) and Marc LEMERCIER (Assistant Prof)

PhD location : Institute for Technology Research (IRT) System X, NANO-INNOV building, 8 Avenue de la Vauve, 91120, Palaiseau, FRANCE. (http://www.irt-systemx.fr/)

Key-words: cyber-security, forensics, graphs, modelling

Detailed presentation: the PhD thesis will be hosted in the EIC project team (*Environment for Cybersecurity Interoperability and Integration*) and will use the CHESS platform (*Cybersecurity Hardening Environment for Systems of Systems*) that has been developed to evaluate cybersecurity technologies for use-cases concerning smart-grids, factories of the future (FoF), autonomic transport systems, Internet of Things (IoT) services. The main PhD objective is to be able to reconstruct attacks paths by using the interactions tracks between all items involved: OS, terminals, networks, servers, middleware. For this, a representation model is necessary that represents both structural and temporal aspects of these interactions (causal temporal graphs, Petri nets). It will then be possible to reconstruct attacks scenarios and replay them by simulation.

Domain: Computer science

Funding: EIC project (http://www.irt-systemx.fr/project/eic/)

Objectives: the aim is to implement new solutions for further tools developments for aided-analysis and understanding of feared attack paths and also post-mortem or post-incident investigations for use-cases of the EIC-project.

Context: the PhD student will work within the IRT (Research & Technology Institute) System-X, located on the « plateau de Saclay », in the frame of the EIC project, where many industrial actors and academics are involved. This context represents a very stimulating environment with the best French labs (INRIA, CEA, Mines-Télécom Institute, Paris-Saclay University, UTT) and with the collaboration of major industries (Airbus Group, Thales, Gemalto, Engie).

Method: from the knowledge of conventional architectures (state of the art on existing paths of attack patterns) it would be able to propose an evolution adapted to hyper connected architectures.

Expected results: The final objective is to validate the model on a testing architectures that will be implemented in the CHESS platform, on which will be replayed scenarios of attacks. The relevance evaluation of the model will be based on traces collected via these new heterogeneous systems that require efficient algorithms to find associations between them.

References

R. Sulo Caceres and T. Berger-Worf, *Temporal Scale of Dynamic Networks*, in Temporal Networks, Springer, 2014

A. Casteigts, P. Flocchini, W. Quattrociocchi and N. Santoro, *Time-varying graphs and dynamic networks*, IJPEDS 27(5), 2012

N. Meghanathan, S. Reddy Allam and L.A. Moore, *Tools and Techniques for Network forensics*, Int. J. of Networks Security & Its Applications (IJNSA), 1 (1), 2009

C.Kruegel, F. Valeur and G. Vigna, *Intrusion detection and correlation: Challenges and solutions*, Springer, 2004

P.A. Khand, *System level security modeling using attack trees*, Proc. of 2nd Int. Computer Control and Communication Conf. (IC4), pp. 1-6, Feb. 17-18, Karachi, 2009

L. Piètre-Cambacédès and M. Bouissou, *The promising potential of the BDMP formalism for security modeling*, supplemental volume of the proc. of the 39th annual IEEE.IFIP Int. Conf. on Dependable Systems and Networks (DSN 2009), Estoril, Portugal, June 2009

Profile of the candidate: UE resident, master degree (or engineer) graduated, the applicant will be communicative, dynamic, autonomous, with a good spirit of initiative. French language proficiency can be useful.

Beginning: the PhD can begin as soon as the candidate is selected and allowed (if not French).

Contacts : Philippe Wolf : philippe.wolf@irt-systemx.fr

Patrick Lallement : patrick.lallement@utt.fr

Marc Lemercier : marc.lemercier@utt.fr