

Thematic section : Explicability and Threat Modeling

- N. Lamhari, V. Legrand, G. E. Jaramillo, Rojas, O. Atig. "An Ontology for cyber incident root cause analysis from event logs". IBIMA. 2019.
- Julio Navarro, Véronique Legrand, Aline Deruyver, Pierre Parrend, « OMMA: Open Architecture for Operator-guided Monitoring of Multi-step Attacks », Eurasip Journal on Information Security, 2018,6. Published on: 2 May 2018 <https://doi.org/10.1186/s13635-018-0075-x>.
- Julio Navarro, Véronique Legrand, Sofiane Lagraa, Jérôme François, Abdelkader Lahmadi, GiuliaDe Santis, Olivier Festor, Nadira Lamhari, Fayçal Hamdi, Aline Deruyver, Quentin Goux, Morgan Allard and Pierre Parrend, "HuMa: A multi-layer framework for threat analysis in a heterogeneous log environment", in FPS, ser. Lecture Notes in Computer Science, vol. 10723, Springer, 2017, pp. 144–159.
- Sofiane Lagraa, Véronique Legrand, Marine Minier. Behavioral change-based anomaly detection in computer networks using data mining. International Symposium on Recent Advances in Intrusion Detection, 2017.
- V. Legrand, P. Parrend, O. Gaouar, « ArchiTrace : Apprentissage de la sécurité par les traces », Conference: WESSI - 1er Workshop sur l'Enseignement de la Sécurité des Systèmes d'Information, 2014.
- V. Legrand, « Confiance et risque pour engager un échange en milieu hostile », Thèse de doctorat, INSA Lyon, soutenue le 19/6/2013.
- Legrand, V., Parrend, P, « DIM: A cognitive architecture for detecting anomalies in complex IT ecosystems », ECCS, European Conference on Complex Systems, 2014.
- V. Legrand, P. Parrend, S. Frénot, P. Collet, M. Minier, Vers une architecture 'big-data' bio-inspiree pour la détection d'anomalie des SIEM, C&ESAR 2014: Détection et réaction face aux attaques informatiques, Rennes, France, novembre 2014
- J. Saraydaryan, F. Benali, G. Jombart, V. Legrand, and S. Ubéda. L'Apport d'une Ontologie pour la Sécurité des Systèmes d'Information.. In 2èmes Journées Francophones sur les Ontologies. Lyon, December 2007.
- F. Benali, V. Legrand, and S. Ubéda. An Ontology for the Management of Heterogeneous Alerts of Information System. In The 2007 International Conference on Security and Management (SAM'07), Las Vegas, USA, June 2007.
- J. Saraydaryan, V. Legrand, and S. Ubéda. Evaluation of Deviating Alerts coming from Behavioral Intrusion Detection. In International Conference on Emerging Security Information, Systems and Technologies SECURWARE, 2007.
- F. Benali, S. Ubéda, and V. Legrand. Préparation des messages de sécurité pour la classification automatique de messages.. In Ecol'IA 2008 : Apprentissage et fouille de données : de la théorie à la pratique, Tunisie, March 2008. Best Paper Award.
- V. Legrand, R. State, and Paffumi. A Dangerousness-Based Investigation Model for Security Event Management. In Internet Monitoring and Protection (ICIMP), 2008.
- V. Legrand, S. Ubéda, and R. State. Enriched Diagnosis and Investigation Models For Security Event Correlation. In IEEE ICIMP, San Jose, 2008.
- J. Saraydaryan, V. Legrand, and S., Ubéda, « Détection d'Anomalies Comportementales Appliquées à la Vision Globale ». In Atelier Intégration, interrogation et analyse de « logs ». (ILO2008), 2008.
- J. Saraydaryan, V. Legrand, and S. Ubéda, « Modeling of Information System Correlated Events Time Dependencies », In 8ème Conférence Internationale sur les Nouvelles Technologies de la Répartition (NOTERE 08), 2008.
- F. Benali, S. Ubéda, and V. Legrand. Automatic Classification of Security Messages Based on Text Categorization.. In 8ème Conférence Internationale sur les Nouvelles Technologies de la Répartition (NOTERE), Lyon, June 2008.
- F. Benali, S. Ubéda, and V. Legrand. Collaborative Approach to Automatic Classification of Heterogeneous Information Security.. In The Second International Conference on Emerging Security Information, Systems and Technologies SECURWARE, Cap-Esterel, August 2008. Note: Best Paper Award.
- J. Saraydaryan, F. Benali, S. Ubéda, V. Legrand, « Comprehensive Security Framework for Global Threats Analysis », International Journal of Computer Science Issues (IJCSI) (08/2009).
- Véronique Legrand, Farid Naït-Abdesselam et Stéphane Ubéda – « Etablissement de la confiance et réseaux ad-hoc: Un état de l'art » - Laboratoire CITI – INRIA ARES - Conférence SAR 2003.

V. Legrand, D. Hooshmand, and S. Ubéda, "Trusted ambient community for self-securing hybrid networks," INRIA, Research Report 5027, 2003.

V. Legrand, S. Ubéda, J. Morêt-Bailly, A. Rabagny, L. Guihéry, J-P. Neuville. "Vers un modèle de confiance pour les objets communicants : une approche sociale ». 3rd Conference on Security and Network Architectures, June 2004.

V. Legrand, S. Galice, S. Ubéda J-P. Neuville. « Identification pour les réseaux spontanés ». 4rd Conference on Security and Network Architectures, June 2005.

Galice, Véronique Legrand, Marine Minier, John Mullins, Stéphane Ubéda, Modelization and trust establishment in ambient networks, poster, International Symposium on Intelligent Environment, 2006.

Samuel Galice, Véronique Legrand, Marine Minier, John Mullins, and Stéphane Ubéda. The KAA project: a trust policy point of view. Research Report RR-5959, INRIA, 2006.

S., Galice, V., Legrand, M., Minier, J., Mullins, and S., Ubéda. A History-Based Framework to Build Trust Management Systems. In Second International IEEE SECURECOMM Workshop on the Value of Security through Collaboration (SECOVAL 2006), pages to appear, august 2006.

Legrand V, « Etablissement de la confiance et réseaux ad hoc - le germe de confiance », INSA de Lyon, Ecole doctorale EDIIS, Laboratoire CITI de Lyon, Rapport de DEA, Juin 2003.

Research projects

- [1] 2004-2008 : ACI sécurité informatique KAA (Key Authentification Ambient) : Rapport final ACI sécurité informatique Samuel Galice, Veronique Legrand, Frédéric Le Mouël, Marine Minier, Stéphane Ubéda, Michel Morvan, Sylvain Sené, Laurent Guihéry, Agnès Rabagny, Joël Moret-Bailly, Jean-Philippe Neuville, Jérôme Pousin.
- [2]. 2005 à 2009 : Deserec – DEpendability and Security by Enhanced REConfigurability - Montant Exaprotect : 1,1 M€ - 36 mois -- WP leader;
- [3]. 2005 à 2008 : Oppidum – IcareNg : des produits et services innovants pour la sécurité - Porteur et coordinateur;
- [4]. 2006 à 2010 : ReD – Reaction and Detection - Montant Exaprotect : 0,4 M€ - 30 mois - WP leader;
- [2014 à 2019 : HuMa – L'HUmain au cœur de l'analyse de données MASSives pour la sécurité – 4,5 M€ dont 1,4 d'aide - 36 mois - Porteur et coordinateur.

Prototypes

2016-2019 : HuMa : « Analysis by the threat modeling »

2013-2016 : HuMa : « Analysis by the pattern visualization »

2006- 2010 : « Modélisation et Classification Automatique des Informations de Sécurité » - java.

2005- 2009 : « Détection d'intrusion par analyse comportementale et statistique » - java.

2002- 2004 : « Protocole et méthode d'authentification pour la confiance dans les réseaux pair-à-pair » scripts.

2004-2004 : « implémentation de l'algorithme « ERIC, Risk Evaluation Protocol for the spontaneous network » - java.

2003-2003 : « Protocole adaptatif pour l'établissement de la confiance en réseaux ad hoc », (carte à puce mise à disposition par Gemplus).

2003-2003 : « Implémentation de l'algorithme de gestion de la confiance dans les réseaux ad hoc pour un échange sécurisé des ressources » (déploiement en environnement PKI MS Windows Server).

2002-2003 : « Développement d'un algorithme pour l'identification dans les Réseaux Ad hoc : Définition d'une Méthode d'Authentification basée sur l'Identité ».

2001-2002 : « Protocole et méthode d'authentification pour l'accès aux soins à domicile et au partage du « Dossier médicalisé »