

Compte rendu de la journée RGE du 4 octobre 2012 à Troyes, organisée par l'UTT

Stéphane Vialle

Le RGE a tenu une réunion le 4 octobre 2012 à l'Université Technologique de Troyes. L'organisateur de la journée était Guillaume Doyen (UTT). Cette réunion a rassemblé un total de 49 participants (40 chercheurs académiques et 9 personnes du monde industriel), auxquels se sont ajoutés 20 étudiants du Master SSI (Sécurité des Systèmes d'Information) de l'UTT. Les laboratoires du RGE représentés le 4 octobre 2012 étaient les suivants : CRESTIC, LE2I, LIFC, LORIA & INRIA Nancy Grand Est, SUPELEC, UTT, implantés dans les villes de Besançon, Dijon, Metz, Nancy, Reims et Troyes. Nos 9 collègues industriels venaient de Champagne-Ardenne et de Paris.

Cette journée RGE était une journée thématique sur la « cyber-sécurité ». Elle incluait trois exposés invités : un exposé industriel de Thalès Défense et Sécurité sur la *vision R&D (de Thalès) des problématiques de cybersécurité actuelles*, un exposé industriel de la PME TREKK SAS présentant un *cas pratique de protection de site stratégique (hébergement de site de campagne pour l'élection présidentielle)*, et un exposé académique sur *les problématiques traitées par le Laboratoire de Haute Sécurité (LHS) de Nancy*. La journée comprenait aussi 6 exposés scientifiques des membres du RGE. Comme à l'accoutumé une table ronde a clôturé la journée, pendant laquelle la future journée RGE du 14 février 2012 à Belfort a été présentée, et quelques informations ont été échangées sur le fonctionnement du RGE.

Exposés invités :

1. Emmanuel Miconnet, Thalès Défense et Sécurité. *Vision R&D des problématiques de cybersécurité actuelles*

Les systèmes d'information sont devenus les centres nerveux de nos entreprises et organisations. Pourtant, la perception du risque d'attaque informatique est encore imparfaite et le passage d'une « vulnérabilité technique » à une crise d'ampleur importante reste un scénario encore sous-estimé par les entreprises. L'objet de cette intervention est double, tout d'abord il est de décrire le passage du simple « fait technique » à la crise potentielle, et d'autre part de préciser les activités R&D actuellement menées au sein de Thalès Défense & Sécurité dédiées à l'analyse et à l'anticipation de ce type de menaces.

2. Freddy Baudinet, TREKK SAS. *Cas pratique de protection de site stratégique : hébergement de site de campagne pour l'élection présidentielle*.

En novembre 2011 TREKK remportait un appel d'offre proposé par une agence de communication parisienne mandatée par un des principaux partis politiques français. Il s'agissait de mettre en place et de maintenir en condition opérationnelle des infrastructures d'hébergement hautement sécurisées pour les sites de campagne de l'élection présidentielle 2012. Plusieurs phases d'implémentation et un calendrier ont été établis, calés sur les événements de campagne (manifestations d'avant élections, 1er tour et deuxième tour).

3. Frédéric Beck, INRIA Grand Est, SED – Service d'Expérimentation et de Développement. *Le laboratoire de Haute Sécurité : LHS*

Le Laboratoire de Haute Sécurité (LHS - <http://lhs.loria.fr/>) est une plate-forme de recherche unique dans le monde académique hébergée à l'INRIA Nancy Grand Est et au LORIA. Il est composé de deux projets principaux:

- un télescope réseau dont l'objectif est de réaliser la collecte à grande échelle de codes malicieux et de traces d'attaques en vue de leur analyse,
- l'étude des codes malveillants et la définition de nouveaux mécanismes de défense pro-actifs permettant de se prémunir contre les malwares inconnus.

Le but de cette présentation est de présenter cette infrastructure ainsi que les diverses activités qui y sont menées.

Exposés scientifiques traditionnels :

4. Florent Nolot, SysCom/CRESTIC. *Sensibilisation aux failles de sécurité : le cas des chevaux de troie.*
5. Florian Legendre, SysCom/CRESTIC. *Cryptanalyse logique des fonctions de hachage.*
6. Frédéric Beck, INRIA Grand Est, SED. *La virologie au LHS : une histoire de codes malveillants.*
7. Remi Badonnel, Madynes/LORIA. *Gestion de configuration sûre dans les réseaux et systèmes autonomes.*
8. Remi Cогranne, LM2S/STMR. *Application des tests statistiques d'hypothèses à la criminalistique des images.*
9. Yanbo Shou, DISC/FEMTO-ST. *Utilisation de la cryptographie basée sur les courbes elliptiques dans les réseaux de capteurs.*

Cette journée sur le thème de la cyber-sécurité a donc réuni près de 50 chercheurs et ingénieurs, et a profité également à une promotion de Master de l'UTT. La plupart des exposés ont fait l'objet de questions-réponses motivés, et ont abordé des aspects variés de la cyber-sécurité. Les exposés invités ont soulevé principalement les questions de (1) l'identité et la motivation des attaquants dans l'espace cyber qu'est l'Internet et (2) notre capacité à les traiter efficacement. Les problématiques actuelles de quantité d'information (*Big data*), corrélation, criticité et automatisation de la réaction (isolation, contre-mesure...) ont été abordées. Des questions d'ordre législatif ont aussi été soulevées notamment lors de la présentation du laboratoire de haute sécurité pour comprendre notamment jusqu'où peut aller une investigation de recherche dans un contexte de cyber-attaque et sous quel cachet cette dernière pouvait avoir lieu. Les exposés scientifiques ont quant à eux suscité des questions scientifiques plus précises sur les thèmes abordés. On note par exemple les questions méthodologiques de cryptanalyse soulevées lors des exposés sur l'utilisation de méthodes SAT pour le cassage de fonctions de hachage mais aussi sur l'utilisation de courbes elliptiques dans les réseaux de capteurs.

Table ronde :

Comme à l'accoutumé, la table ronde fut l'occasion de donner des nouvelles diverses et de planifier les futures journées RGE.

- L'évolution du RGE proposée lors de la réunion précédente, a été acceptée depuis par le comité de pilotage du GDR ASR. Partant de l'observation que les journées thématiques sont appréciées et remportent habituellement un réel succès, alors que les journées non-thématiques réunissaient de moins en moins de participants (et se révélaient de plus en plus difficile à organiser), nous avons opté pour des journées thématiques régulières.

Nous aurons toujours 3 journées par an, mais organisées selon le schéma suivant :

- Une journée thématique autour des thèmes des « réseaux informatiques » et de leurs nouveaux défis.
- Une journée thématique autour des thèmes et défis associés au « calcul » (intensif et parallèle).

- Une journée sur un thème émergent, de préférence à la limite des réseaux et du calcul, ou une journée pluridisciplinaire si la demande se fait sentir.

- La principale nouvelle du GDR ASR est le prochain changement de responsable. Marc Daumas ayant pris ses nouvelles fonctions à l'ambassade de France à Washington, il assure la direction du GDR ASR jusqu'à la fin du quadriennal (fin 2012), en biseau avec le nouveau responsable. A ce jour nous ne connaissons pas encore le nom du futur responsable.

- Nous avons confirmation de l'organisation de la prochaine journée (14 février 2013) RGE à l'IUT de Belfort, sur un thème « calcul » (voir ci-dessous).

- Nous avons décidé d'organiser la journée RGE suivante le 30 mai 2013 à Besançon autour du thème des Systèmes d'Exploitation (sur une proposition de Bertil Foliot lors de la dernière réunion de pilotage du GDR ASR). Nous nous attacherons toutefois à relier cette journée à des thèmes traditionnels du RGE, par exemple en étudiant les aspects des systèmes d'exploitation utiles aux réseaux de capteurs ou aux systèmes de calculs distribués.

- Nos collègues de Dijon attirent notre attention sur le fait que l'Université de Bourgogne tend à renouveler des postes d'Enseignant-Chercheur (MC) par des postes d'enseignants à 100% (PRAG en Informatique). Les autres participants de la table ronde n'ont pas connaissance de faits similaires dans leurs Universités.

- Enfin, Stéphane Vialle a annoncé sa volonté de passer la main à un autre responsable RGE à la suite de la journée de juin 2013. Cela fait maintenant 7 années qu'il est responsable du RGE, et il lui semble temps de renouveler la tête de notre « action régionale pérenne » (au sein du GDR ASR). Cette transition interviendrait à la fin de l'année académique en cours, et après une année du nouveau fonctionnement du RGE. Les collègues intéressés sont donc invités à se faire connaître.

Dates des prochaines journées RGE :

- Jeudi 14 février 2013 à l'IUT de Belfort : journée thématique en algorithmique et programmation pour accélérateurs matériels (GPU, FPGA, MIC...)
Organisateur : Raphaël Couturier (Raphael.Couturier@univ-fcomte.fr).
- Jeudi 30 mai 2013 au LIFC à Besançon : journée thématique sur les systèmes d'exploitation, avec des focus sur les besoins des réseaux de capteurs et des plates-formes de calculs distribués.
Organisateur : Hervé Guyennet (Herve.Guyennet@femto-st.fr).

Journée à organiser en liaison avec Bertil Folliot (Paris 6 – GDR ASR).