Journée thématique organisée par l'action RGE et supportée par le pôle ResCom du GDR ASR CNRS et l'agence Carinna sur le thème de la

Cyber-Sécurité

Jeudi 4 octobre 2012 à
L'Université de Technologie de Troyes

Programme

9h30 Accueil des participants (Salle M104)

10h00 *Sensibilisation aux failles de sécurité : le cas des chevaux de troie* (Florent Nolot, SysCom/CRESTIC – Systèmes Communicant/Centre de Recherche en STIC)

Résumé : *De très nombreuses personnes négligent les mises à jour de leur système d'exploitation ou de leurs applicatifs. Pourtant, avant de parler de techniques avancées pour sécuriser un réseau, un système ou des échanges entre équipements, il est impératif de vérifier que les recommandations de sécurité informatique les plus simples soient respectées. A l'occasion de cette présentation, des démonstrations sur le vol d'informations à l'insu d'un utilisateur et la prise de contrôle à distance d'un ordinateur seront effectuées, à l'aide de virus et chevaux de troie, afin de montrer l'importance d'être muni d'un anti-virus, d'un détecteur d'intrusion et d'un firewall sur son poste de travail.*

10h30 *Vision R&D des problématiques de cybersécurité actuelles* (Daniel Pays, Thalès Défense et Sécurité)

Résumé : *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.*

11h15 Pause (Salle M104)

11h45 *Cas pratique de protection de site stratégique : hébergement de site de campagne pour l'élection présidentielle* (Freddy Baudinet, TREKK SAS, fournisseur de solutions d'hébergement à valeur ajoutées)

Résumé : *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).*

Notre présentation présente la façon dont nous avons abordé ce projet, nos relations avec les concepteurs du site, celles avec le service multimédia interne du parti politique, la façon dont nous avons imaginé l'infrastructure sécurisée, son dimensionnement au fil du temps, enfin les services de pilotage et d'astreinte mobilisés. Nous terminerons par le bilan de l'opération et les questions éventuelles. Le nom du parti en question ne peut être diffusé.

12h15 *Cryptanalyse logique des fonctions de hachage* (Florian Legendre, SysCom/CRESTIC – Systèmes Communicant /Centre de Recherche en STIC)

Résumé : *Ces dernières années, le problème SAT a vu son champ d'applications potentielles croitre de façon significative et permet, à ce jour, de résoudre efficacement bon nombre de problèmes fondamentaux et industriels. Au début des années 2000, un nouveau champ d'application du problème SAT, nommé Cryptanalyse Logique, a fait son apparition. Ce nouveau domaine d'étude consiste à modéliser sous une forme logique le processus mis en place dans les fonctions cryptographiques, pour ensuite appliquer un solveur SAT sur l'instance générée afin de la résoudre.*

Nous décrirons dans un premier temps ce qu'est la cryptanalyse logique puis dans un deuxième temps, nous prendrons l'exemple de la fonction de hachage MD5 pour illustrer nos travaux. Ainsi, nous montrerons de quelle façon SAT peut être utilisé pour se comporter comme un "reverse-engeeniring" sur des versions réduites de fonctions de hachages. Par ailleurs, nous proposons différents angles de résolution pour une instance SAT générée et déboucherons sur le problème de la collision ainsi que sur l'extension de cette technique sur diverses fonctions cryptographiques.

12h45 Repas (Salle M104)

14h15 *Le laboratoire de Haute Sécurité : LHS* (Frédéric Beck, INRIA Grand Est, SED - Service d'Expérimentation et de Développement)

Résumé : *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.

14h30 *La virologie au LHS : une histoire de codes malveillants* (Frédéric Beck, INRIA Grand Est, SED - Service d'Expérimentation et de Développement)

Résumé : *L'objectif de cette présentation est de présenter un panorama des activités de recherche liées à la virologie réalisées au sein du LHS à travers divers cas d'étude. Tout d'abord, nous illustrerons le fonctionnement et les avantages de l'analyse morphologique à travers les virus Stuxnet et Duqu. Ensuite, nous présenterons une expérience de neutralisation du botnet waledac au sein du LHS, avant de conclure avec une autre*

application possible du moteur morphologique dans le cadre de la synchronisation de codes entre Waledac et OpenSSL.

15h00 *Gestion de Configuration Sûre dans les Réseaux et Systèmes Autonomes* (Remi Badonnel, Madynes/LORIA – Management of Dynamic Networks and Services/Laboratoire Lorrain de Recherche en Informatique et ses Applications)

Résumé : *La dynamique croissante des réseaux et la multiplication de leurs services a considérablement augmenté la complexité de l'activité de gestion. Si l'automatisation de cette activité est devenue indispensable, elle pose de nouveaux défis. En particulier, les réseaux et systèmes autonomes doivent être capables de prendre en charge tout ou partie de leur propre gestion. Or les changements opérés pour réaliser les différentes opérations d'auto-configuration peuvent placer le système dans un état vulnérable. Aussi, cette automatisation ne sera réellement possible qu'à la condition qu'elle intègre des mécanismes permettant de prévenir et traiter de telles vulnérabilités de configuration. Nous présenterons ici un aperçu de nos travaux contribuant à maintenir une configuration sûre des environnements autonomes au regard de la sécurité, et s'appuyant notamment sur le langage standardisé OVAL (Open Vulnerability and Assessment Language).*

15h30 Pause (Salle M104)

16h00 *Application des tests statistiques d'hypothèses à la criminalistique des images* (Remi Cogranne, LM2S/STMR – Laboratoire de Modélisation et Sureté des Systèmes/Sciences et Technologies pour la Maîtrise des risques)

Résumé : *Avec l'avènement du réseau Internet et de la photographie numérique, de nombreuses images naturelles (acquises par un appareil photographique) circulent un peu partout dans le monde. Par ailleurs, le développement des logiciels de retouche d'image est, depuis quelques années, suffisamment avancé pour permettre à un utilisateur novice de modifier ses images à fins légitimes ou malveillantes. Ainsi, des questions sur la valeur probatoire de tels médias se posent désormais. Dans ce contexte, la principale difficulté est de concevoir des tests fiables dans le sens où leurs probabilités d'erreurs doivent être maîtrisées. Dans cet exposé, cette problématique est abordée en utilisant la théorie des tests d'hypothèses associée à un modèle statistique des images. Les deux applications proposées sont la détection d'informations cachées (stéganographie) ainsi que l'identification de l'appareil photographique ayant capturé une image donnée.*

16h30 *Utilisation de la cryptographie basée sur les courbes elliptiques dans les réseaux de capteurs* (Yanbo Shou, DISC/FEMTO-ST - Département d'Informatique des Systèmes Complexes/ Laboratoire d'Informatique de l'université de Franche-Comté)

Résumé : *In event-driven sensor networks, when a critical event occurs, sensors should transmit quickly and securely messages back to base station. We choose Elliptic Curve Cryptography to secure the network since it offers faster computation and good security using shorter keys than RSA protocol. In order to minimize the computation time, we propose to distribute the computation of scalar multiplications on elliptic curves by involving neighbor nodes in this operation. The results of performance tests show that parallel computing certainly consumes much more resources, however it reduces considerably the computation time of scalar multiplications. This method is applicable in event-driven applications when execution time is the most critical factor.*

17h00 Table ronde

Accès wifi

Nom du réseau (SSID) : RGE2012
Mot de passe : RGE2012UTT