SUPAERO – 2014-2015

Propositions de sujet d'étude

L'évaluation de ce cours s'effectuera en fonction d'un rapport rédigé sur un des sujets suivants.

Modalités :

- rapport à réaliser en binôme (monôme accepté)
- choix des binômes et choix du sujet avant la mi-janvier 2015
- plan à communiquer (cf. commentaires ci-dessous)
- contact : rodolphe.ortalo@carsat-mp.fr (réponse sous 24/48h)
- rapport final à rendre avant le 28 février 2015 (à valider avec la direction des études).

Liste de sujets d'étude :

1 Sous réserve d'accord préalable, vous pouvez choisir un sujet personnel (qui peut être l'étude d'un document ou d'un outil).

2 Approfondir l'étude quantitative (statistique) de la base CVE du MITRE (cve.mitre.org) : ne pas se limiter à l'évolution du nombre d'alertes, mais étudier l'évolution par type de logiciel, par gravité, par origine, etc. pour proposer des causes.

3 Validation de l'utilisation des solutions cryptographiques (audit de code source, donc probablement pour des logiciels libres) : GnuPG, OpenSSL, (OpenSSH), Composants cryptographiques (ou assimilés) de Linux, (GNUTLS), (libgcrypt)

4 Étude, comparaison et critique des techniques et des propriétés de sécurité des composants logiciels de mémorisation des mots de passe de Mozilla Firefox et d'Internet Explorer.

5 Identifier les besoins de sécurité, les normes et les technologies utilisables pour la définition d'une carte d'identité électronique.

6 Identifier les technologies, les besoins de sécurité et les menaces associées à une machine à voter électronique.

7 État des fonctions d'authentification disponibles avec les navigateurs Web standards (en incluant l'infrastructure de sécurité associée à mettre en place).

8 Techniques de réalisation de vers, portes dérobées ou chevaux de Troie.

9 Étude d'une méthodologie de développement d'attaques avec l'environnement *metasploit* (www.metasploit.com) ou de tests de vulnérabilité avec OpenVAS (www.openvas.org).

10 Proposer des cas d'utilisation de l'*aberrant behaviour detection* avec RRDTool pour la détection d'anomalies de sécurité (ou autres approches statistiques).

11 État et comparaison des éditeurs de liens dynamiques (`.so`, `a.out`, `DLL`) vis à vis de la sécurité. (Comment se charge un programme?)

12 Découvrir les caractéristiques complètes d'un utilisateur au sens d'une machine – c'est à dire en termes techniques (*uid*, *pid*, mais aussi: *rootfs*, et d'autres?). Se focaliser sur les OS dont les sources du système d'exploitation sont disponibles.

13 Étudier X11 et la sécurisation (possibilité de se limiter au contexte *open-source*).

14 Étudier l'authentification Unix, et notamment la comparaison de PAM (Linux) et de l'authentification BSD. Étendre à la notion de session sous Unix?

15 Étudier et critiquer la sécurité d'un protocole de routage dynamique (OSPF, BGP, RIP)

16 Étudier et comparer la sécurité des technologies d'annuaires (NIS+, LDAP, A.D., autres?).

17 Proposer des algorithmes orientés vers le traitement des agrégations temporelles d'alertes, en visant le contexte d'un SGBD SQL.

18 Identification et caractérisation des mécanismes de sécurité présents dans le protocole et les échanges *Bluetooth*.

19 Identification et caractérisation des mécanismes de sécurité présents dans le protocole et les échanges *WiFi* (802.11a, 802.11b et 802.11g).

20 Étude et caractérisation technique de TPM (Trusted Platform Module) produit par l'initiative TCPA (Trusted Computing Platform Alliance). Débouchés et impact sur les technologies de l'information (généralités) *ou encore* étude d'une implémentation spécifique (LaGrande, Palladium, etc.).

21 Etude et commentaire de l'ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

22 Utilisation des annotations `sparse` (http://lwn.net/Articles/87538/) pour la détection par analyse statique à la compilation d'erreurs de programmation induisant des failles de sécurité dans le source du noyau Linux.

23 Étude, analyse et exploitation des traces Windows (évènements) : identification des documentations de référence, analyse des évènements intéressants du point de vue de la génération d'alertes de sécurité, mise en œuvre éventuelle (dans un analyseur de traces open-source par exemple).

24 Etat des lieux des derniers développements concernant les fonctions de hachage cryptographiques (*quid* de SHA-1, SHA-3 *césaco* ?).

25 Vue générale de l'utilisation et de la mise en oeuvre des technologies biométriques dans le domaine informatique.

26 Comparaison des systèmes embarqués et des systèmes informatiques généralistes vis à vis de la sécurité.

27 Analyse critique et recherche d'alternatives à la diffusion de correctifs de sécurité.

28 Spécification générale des besoins de sécurité envisageables pour un téléphone portable récent (GSM, GPS, Bluetooth+WiFi)

29 Etude d'un logiciel d'analyse de code source (par exemple : `splint`) pour la recherche et l'élimination de failles de sécurité.

30 Etude des fonctions de protection et de prévention des failles de sécurité disponibles au niveau d'un compilateur (avec ou sans *patch* spécifiques).

31 Etude du processus de gestion des créations d'utilisateurs et des autorisations dans une entreprise de grande taille et spécification des principales fonctions d'un logiciel de gestion de ces autorisations.

32 Suivi de la qualité des mots de passe : outillage, traitements à mettre en place et surtout définition et comparaison des statistiques utilisables pour un suivi efficace.

33 Dans le cas d'un poste de travail ou d'une station de travail « standard », étude des besoins d'assistance d'un utilisateur en matière de sécurité et spécification générale d'une IHM permettant d'aider/alerter/sensibiliser l'utilisateur aux aspects relatifs à la protection de son poste de travail. (NB : Possibilité de faire un état des lieux des IHM utilisées par certains constructeurs actuels.)

Commentaires : L'étude de ces thèmes doit bien évidemment se faire dans une optique résolument tournée vers les problèmes de sécurité informatique. Pour le sujet choisi, vous devrez vous adapter aux sources d'information disponibles, au périmètre et au niveau de détail que vous avez la possibilité d'explorer dans les délais impartis. Si elle est possible, une expérimentation sera très appréciée.

Je souhaite valider le plan détaillé du document que vous comptez produire avant que vous vous engagiez dans la construction du rapport complet. Merci de me le communiquer, par e-mail de préférence. Cette étape intermédiaire n'aura aucune incidence sur la notation finale, il s'agit de vous orienter. Par ailleurs, n'hésitez pas à m'envoyer les questions que vous vous poserez sur votre sujet, je tacherai d'y répondre (à moins qu'elles ne conduisent à réaliser votre propre travail bien sûr).

Nota : Enfin, gardez à l'esprit le domaine que vous étudiez, la sécurité. Toute action concrètement dangereuse pour d'autres ou pour vous (notamment pour les sujets visant à vous faire approfondir les menaces informatiques) sera *pénalisée*, indépendamment du niveau de technicité dont elle fera preuve.