

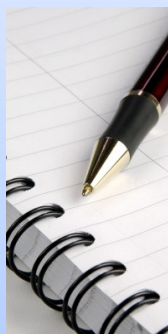


## Workshop: Conception de tests et hacking applicatif

Ce cours adresse la sécurisation opérationnelle d'un système applicatif, du point de vue de la conception et de la validation par les tests. On se concentre plus particulièrement, sans s'y restreindre, aux systèmes d'information ouverts sur internet (applications web, SOA).

À cet effet, les principales menaces de sécurité logicielles sont exposées, ainsi que les détails sur les solutions de sécurité possibles (politiques de sécurité basées sur le contrôle d'accès, contrôle des entrées contre les injections de code, XSS). Pour bien comprendre les interactions d'un mécanisme de sécurité avec les autres caractéristiques d'un système (fonctionnalité, disponibilité, performance), il est nécessaire de revenir sur les règles de conception des applications. Nous utiliserons le langage de modélisation UML dont on rappellera les éléments utiles à la formation. Afin de garantir la bonne implémentation et le fonctionnement des mécanismes de sécurité, les critères et les techniques de sélection de tests de sécurité seront détaillés.

Les techniques de hacking permettent d'auditer et de tester la sécurité d'un système applicatif. Malgré les aprioris sur les hackers et leurs techniques, une méthodologie leur est nécessaire afin de pouvoir exploiter efficacement ces applications. Cette méthodologie sera exposée lors de cette formation. Elle sera complétée par l'utilisation technique de framework d'exploitation tel que metasploit et d'outils de fuzzing pour la découverte de failles.



### Détails de la formation

Lieu	itrust consulting, Foetz, Luxembourg
Date, durée	<b>Janvier 2012 - 3 jours</b>
Intervenants	<p><b>Prof. Yves Le Traon</b>, professeur à l'Université du Luxembourg, dirige l'équipe SERVAL du Snt (Security Reliability and Trust Interdisciplinary Research Center), spécialisée dans la conception, le déploiement et la validation de solutions de sécurité pour les systèmes et réseaux. Membre de l'IEEE Computer Society, co-fondateur de l'IEEE International Conference of Software Testing, Verification and Validation (ICST), il est un expert reconnu dans ces domaines qu'il enseigne à l'Université et auprès d'entreprises (ALCATEL, Mitsubishi, Thales et France Télécom).</p> <p><b>Paul Rascagnères</b>, IT Security consultant chez itrust consulting, est très actif dans la communauté OpenSource ainsi que dans la recherche de vulnérabilités. Il a développé de nombreux "proof of concept", p.ex. sur IBM, détecté des vulnérabilités sur des applications Web et des Firmware, publié des CVE (Common Vulnerabilities and Exposures).</p>
Langue	<b>Français</b>



## Résultats d'apprentissage:

A l'issue de la formation, les participants seront capables de:

- mettre en œuvre des tests de sécurité et d'intrusion grâce aux travaux pratiques
- comprendre les mécanismes de sécurité internes au logiciel et les principales menaces et attaques associées
- appréhender un modèle UML décrivant les interactions entre les composants de sécurité et classes du logiciel
- décrire une politique de contrôle d'accès, et comprendre comment l'intégrer dans une application
- proposer des améliorations réalisables dans la refonte d'une architecture logicielle existante (legacy)
- tester un logiciel vis à vis des propriétés de sécurité (accès, injection de code) en tenant compte de la correction fonctionnelle et des performances
- comprendre la méthodologie utilisée par les hackers
- utiliser le framework d'exploitation libre metasploit et les outils de fuzzing
- réaliser un audit de sécurité pertinent en utilisant les techniques des hackers

### Informations générales

Adresse du centre de formation	Bâtiment Ecostart2, Rue du commerce, L-3895 Foetz	
Inscription	<b>Pours'inscrire:</b> <a href="http://www.itrust.lu">www.itrust.lu</a> (section Training) <b>+352 26 176 212</b> <b>training@itrust.lu</b>	
Repas	Inclus: repas au restaurant, boissons etc..	
Paiement	Le paiement doit être effectué avant la formation par virement bancaire. Les informations de paiement seront fournies au moment de l'inscription.	
Programmation de la journée	Enregistrement et café: 8h30 – Formation: 9h à 12h / repas / 13h30 à 17h	
Conditions générales	<ul style="list-style-type: none"> <li>• En cas d'annulation, 50% du montant de la formation sera dû;</li> <li>• Itrust consulting se réserve le droit d'annuler la formation. Dans ce cas, tout paiement réalisé sera intégralement remboursé.</li> </ul>	
Tarif par participant	450€ H.T. par jour, soit 1 350 € H.T. pour cette formation (1390 € T.T.C. TVA3%)	
Tarif de groupe (par société)	2 <sup>nd</sup> participant:	-20%
	3 <sup>rd</sup> participant:	-40%
	Au-delà:	-60%

## Itrust training center

- Intervenants avec une forte expérience théorique et pratique, fréquemment co-auteurs de standards ou Professeurs d'université
- Repas inclus pour favoriser les échanges entre participants
- Supports de formation sur papier et DVD
- Exercices et travaux pratiques inclus
- Disponibilité des intervenants pour toute question après la formation
- Certificat de formation fourni
- Flexibilité: formations sur mesure
- Plus d'informations sur: [www.itrust.lu/index.php/Training.html](http://www.itrust.lu/index.php/Training.html).

