FUI SecurOCaml

Fabrice LE FESSANT

Réunion de Kick-Off
16 Janvier 2015

OCaml PRO

Kick-Off SecurOCaml

- 10h-10h10: introduction
- 10h10-10h30: présentations des financeurs
- 10h30-10h40: questions aux financeurs ou pause
- 10h40-12h: présentations des partenaires (10-15min par partenaire)

  (présentation du partenaire, intérêt dans le projet, technique et économique)
- 12h-12h10: petite pause
- 12h10-13h: début des discussions techniques (revue des sous-projets et des délivrables, discussion sur l'état actuel d'OCaml par rapport à ces objectifs, établissement d'un calendrier des réunions suivantes, etc.)
- 13h: fin et déjeuner (pour les inscrits)

SecurOCaml

Conception d'un environnement pour développer des applications de sécurité en OCaml

- Labelisé par le GTLL de Systematic
- Financé dans le cadre du FUI 18 :
  - 849 kEuro d'aide sur 1988 kEuro de dépenses
  - CG91 et BPIFrance
- Début du projet : 16 janvier 2015
- Durée du projet : 36 mois

OCaml

- 20 mars 2014: Facebook annonce qu'ils utilisent en interne un nouveau langage, Hack, pour développer leur site. Hack est écrit en OCaml.

Another long-term design goal -- more implied by the language's construction than explicitly stated by Facebook -- is making Hack safer with fewer inherent vulnerabilities than PHP. In addition to the type-checking constraints now available in the language, there's also the way Hack was written; rather than being coded in C, as PHP was, Hack was designed using the OCaml language -- the same platform used by the Xen Project folks to develop its **secure-by-design Mirage OS**. PHP has had its share of **low-level vulnerabilities** over the years, **not all of them obvious** (or specific to that platform), so it makes sense to adopt a new design methodology that makes casual exploits more difficult to pull off.

OCaml

- Cloud: Citrix XenServer → 15% du marché de la virtualisation (Amazon). Le logiciel qui contrôle chaque machine Xen est écrit en OCaml.
- Finance: Jane Street Capital, l'une des 10 plus grandes firmes de ”proprietary trading” avec 10 Milliard$ de transaction par jour. Toute leur infrastructure est écrite en OCaml.
- Logiciel: Microsoft diffuse Terminator, outil d'analyse des drivers sous Windows. Terminator est écrit en OCaml.

OCaml

- Scade 6 chez Esterel-Technologies :
  - Compilateur KCG migré de C à OCaml
  - Un des seuls compilateurs certifié au niveau A de la norme DO-178B

- Frama-C et Astrée, utilisés chez Airbus
  - Frama-C: framework d'analyse de code C développé au CEA, appliqué à prouver la correctoin fonctionnelle de 10k lignes de C
  - Astrée: détecteur d'erreurs à runtime, développé à l'ENS, appliqué à 1M lignes de C

OCaml

- Langage développé à l'INRIA depuis 30 ans
- Le ”typage statique fort” d'OCaml:
  - La rapidité de développement (peu de bugs/tests)
  - La performance à l'exécution
  - La portabilité (y compris vers JavaScript)
  - La maintenabilité du code dans le temps
- Communauté en pleine croissance
  - OCamlPro, OCamllabs, ocaml.org
  - OPAM : de 200 à 750 contributions depuis 2013

SecurOCaml

- L'**ANSSI** a commandé deux études de trois ans sur la sécurité des langages :
  - L'étude **JavaSec** → quasi-impossible de sécuriser Java
  - L'étude **LaFoSec** → OCaml surclasse en sécurité les autres langages fonctionnels, mais :
    - Recommandations d'évolution pour améliorer encore le langage
    - Besoin d'outillage pour l'audit de code pour la certification (CESTI)
- **Objectif** : Fournir un **langage de programmation** combinant ***sûreté de fonctionnement*** et ***sécurité,*** avec une **trousse à outils d'audit de code**.

Les partenaires

- 4 PME, 3 académiques, 2 « observateurs »:
  - OcamlPro (porteur du projet → outillage OCaml)
  - LexiFi (gestion de contrats financiers en OCaml, Bloomberg, SimCorp, contributeur OCaml)
  - SafeRiver (audit en sécurité, porteur LaFoSec)
  - Trust-in-soft (outils de Cyber-Sécurité en OCaml)
  - INRIA (maintenance Ocaml)
  - ENSTA (contributeur important)
  - CEA List (utilisateur important)
  - TrustedLabs (sécurité et cartes à puce)
  - ANSSI (sécurité des infrastructures informatiques)