Durcissement de programmes C avec SIDAN

SSTIC 2012

2012-06-07T1215+0200

Pierre KARPMAN

École Normale Supérieure de Cachan & Supélec

pierre.karpman@rennes.supelec.fr

Approche par invariants pour la détection d'attaques

Objectifs :

- Chercher des propriétés invariantes sur l'état du logiciel
- Instrumenter le logiciel avec des assertions exécutables dérivées des invariants
- Détecter des attaques quand les assertions échouent à l'exécution

Invariants utiles pour la sécurité

- Invariants sur le flot de contrôle du programme
  (pas de transferts de flot illégaux)
- Invariants sur le flot de données du programme
  (pas d'écriture dans la mémoire depuis des endroits illégaux)
- Invariants sur la valeur des données du programme
  (les variables contiennent des valeurs vraisemblables)

Invariants dans SIDAN

- But : vérifier la cohérence des données d'un programme avant (et après) chaque appel de fonction (si possible)
- Deux types d'invariants :
  - vérifier que les variables prennent des valeurs dans leur *domaine de variation* théorique
  - vérifier l'intégrité des variables supposées rester constantes après des appels de fonction

Premier exemple

- Assertions pour des invariants sur les domaines de variation :

```
coninva_assert(t1 >= -117 && t1 <= 210
                    && argc == 2);
t2 = strcmp(*(argv + 1), "--vers");
coninva_assert(t2 >= -45 && t2 <= 210);
```

Second exemple

- Assertions pour des invariants sur les variables constantes :

```
register in_addr_t __babar171;
__babar171 = sa.sin_addr.s_addr;
ip = ntohl(sa.sin_addr.s_addr);
coninva_assert(sa.sin_addr.s_addr
                    == __babar171);
```

L'implémentation, dans tout ça ?

- SIDAN est implémenté sour la forme d'un plugin dans *Frama-C*
- Frama-C est un framework d'analyses statiques pour programmes C développé par le CEA
- L'ajout d'assertions se fait par modification directe de l'arbre de syntaxe abstraite des programmes, avant la compilation

It's show time!

Une petite démonstration ?

Pour en savoir plus...

- Page web de SIDAN :
  http://www.rennes.supelec.fr/ren/rd/cidre/tools/sidan
  (sera *bientôt* à jour)
- Pour les plus motivés :
  http://perso.eleves.bretagne.ens-cachan.fr/~pkarp892/rapp_m2.pdf
- Et sinon... :
  pierre.karpman@{rennes.supelec.fr, eleves.bretagne.ens-cachan.fr}
  {eric.totel, frederic.tronel}@supelec.fr