Attack Redirection in Honeypots

Information Assurance Laboratory, University of Maryland

Julien VEHENT

Soutenance de Stage

Master Management de la Sécurité des Systèmes Industriels et des Systèmes d'Information

Promotion 2007

L'Université du Maryland

- 35,000 étudiants
- Plus de 7,500 professeurs et chercheurs
- Classée 13ème au niveau mondial en « *Engineering/Technology and Computer Sciences* » (source IHE, Shanghai)
- Budget 2007 : 1, 352 millions de dollars

Information Assurance Laboratory

- Co-Dirigé par le Dr. Michel Cukier
- Financement : NASA, NSA, DARPA, ...
- Travaille sur l'évaluation du risque et la vulnérabilité des systèmes

La problématique des Honeypots

Une question de fond : comment protéger efficacement les systèmes d'information des menaces extérieures ?

Sun Tzu, en 500 avant J.C., donne un élément de réponse :

知彼知己，百戰不殆；不知彼而知己，
一勝一負；不知彼，不知己，必敗

Know your enemy

1. Avoir conscience des menaces qui pèsent sur un système
2. Connaître le déroulement d'une attaque
3. Analyser cette attaque
4. Utiliser ces informations pour améliorer la protection

La problématique des Honeypots

La théorie

Objectif : simuler une cible intéressante pour attirer les intrus

Techniques : 2 écoles

- Low-Interaction Honeypot : le leurre en carton, facilement détectable mais couvre une surface importante;
- High-Interaction Honeypot : un serveur quasi-réel qui contient de fausses données, permet d'observer en profondeur le déroulement d'une attaque.

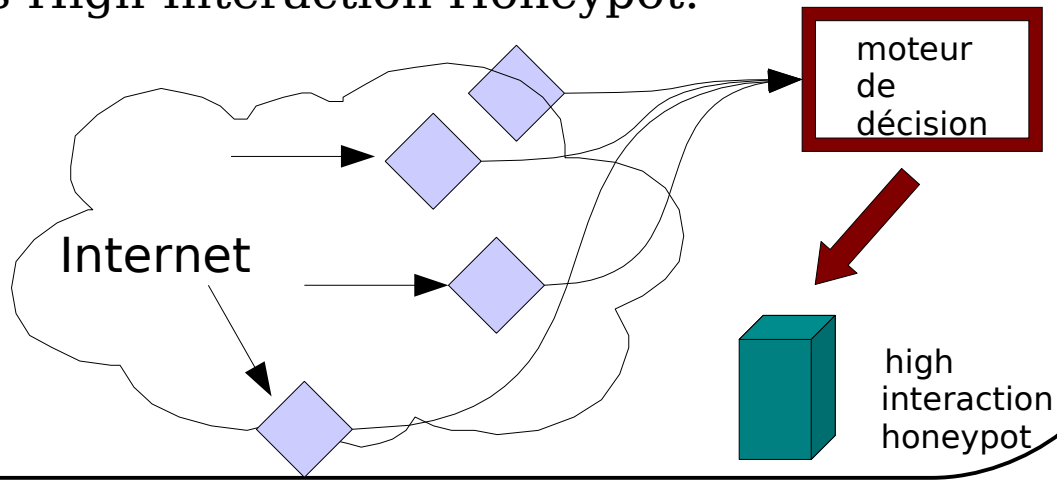
Problème : Il faut choisir entre quantité et qualité...

La problématique des Honeypots

Hybrid Honeypots

Objectif : améliorer la collecte d'attaques pour réduire les temps d'analyse et de réaction.

Méthodes : créer un système ayant les capacités de couvertures des Low-Interaction Honeypot et les capacités d'interaction des High-Interaction Honeypot.



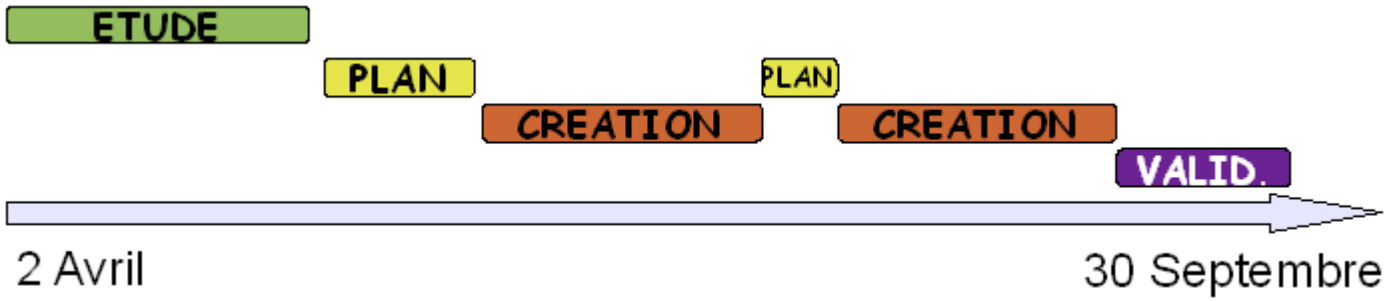
Le projet ArgusProxy

Objectifs

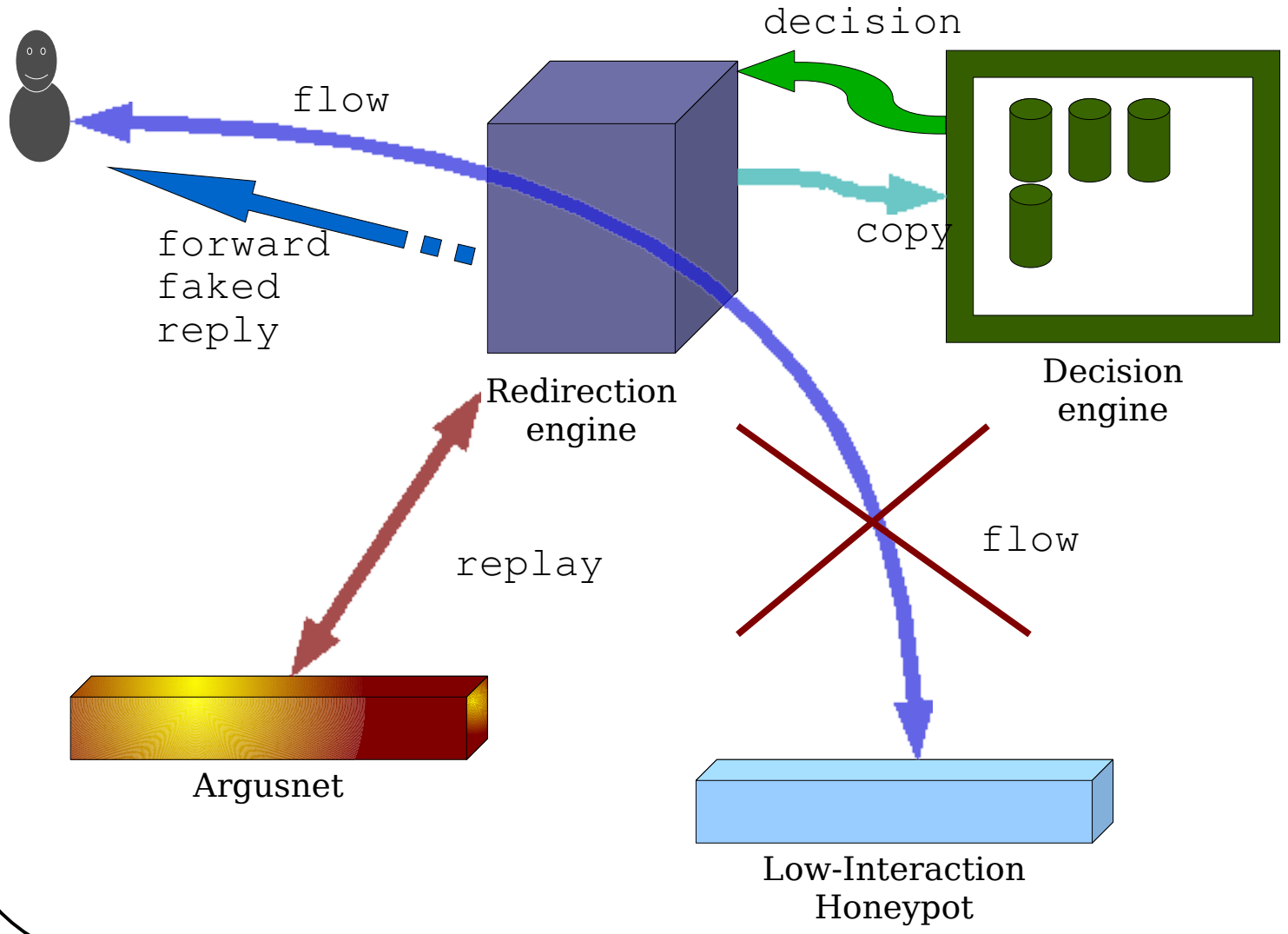
Du projet : Créer une architecture basée sur la théorie des Hybrid Honeypots, l'améliorer et la déployer à l'UMD.

Du stage :

- **Etudier** les besoins, la faisabilité, la technique;
- **Plannifier** les phases de Génie Logiciel;
- **Créer** le moteur de redirection;
- **Valider** son fonctionnement.



ArgusProxy : architecture



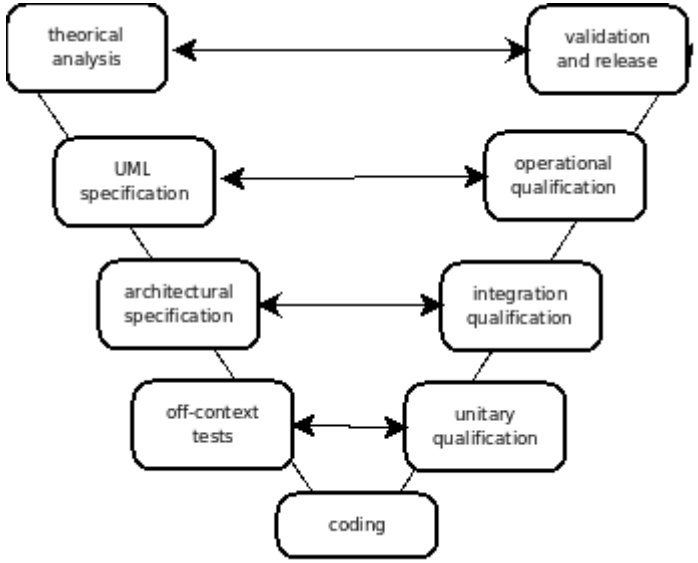
Le projet ArgusProxy

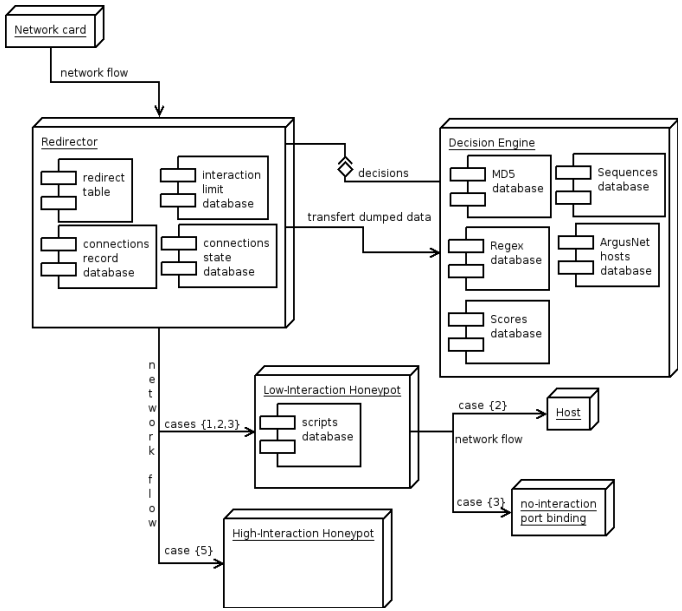
Méthodologie

Génie logiciel : modèle en V

Spécification :

Unified **M**odeling **L**anguage





Programmation :

Gnome Lib, Trac, Valgrind, ...

trac
Integrated SCM & Project Management

Valgrind

Le projet ArgusProxy

Résultats et validation

3 points de contrôles :

- **Vitesse** d'exécution : le temps de process doit être inférieur à la latence de la connexion;
- **Intégrité** des données : stockage d'informations et re-jeu de connexions ne doivent pas modifier l'information;
- **Stabilité** : exécution fiable par réduction des problèmes courant en C.

Statut : Architecture générale en test sur le réseau public du laboratoire. Quelques corrections de bugs et améliorations sont en cours.

Bilans

Managérial :

- Premier projet de Génie Logiciel dirigé de la phase d'étude à la livraison finale;
- Application concrète des modules d'enseignement;

Technique :

- Premier contact avec l'univers de la recherche;
- Apprentissage des techniques avancées de développement, tests et validation;

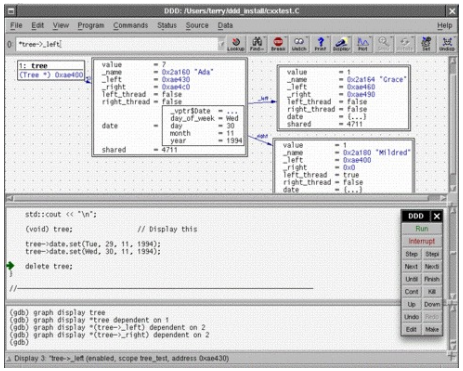
Humain :

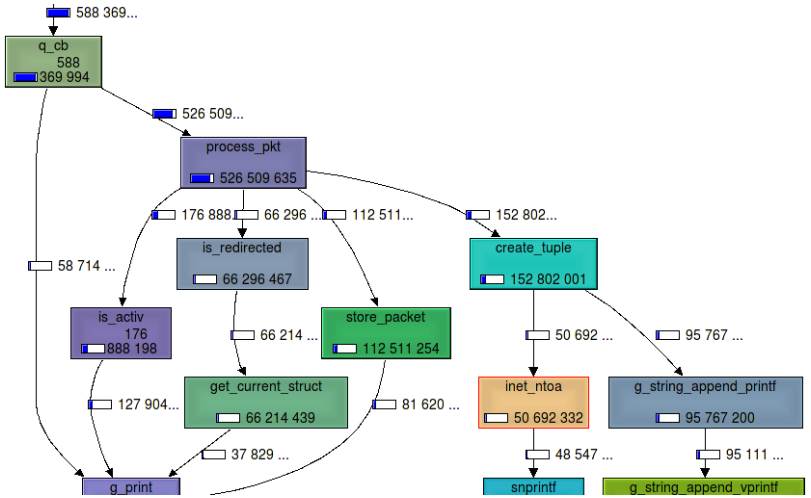
- 6 mois sur u[illegible] cam[illegible]us a[illegible]éricain !

Travaux Futurs

Redirection Engine :

- Terminer les tests et validations via Valgrind et GDB;
- Préparer le cahier des charges de la version 2;





Decision Engine :

- Définir le cahier des charges pour....
- préparer la spécification et le modèle en V et...
- programmer ! :)

Merci de votre attention !