Sébastien Salva
LIMOS – Université d'Auvergne

Qui suis-je?

```
Public void setUp(){
Identity id=new Identity(‘’salva’’);}

Public void testid (){
assertEquals(id.surname, ’’sébastien’’);
assertEquals(id.name, ’’salva’’);
assertEquals(id.labo, ’’LIMOS’’);
assertEquals(id.city ’’Clermont-Ferrand’’);

assertArrayEquals(i.recherche, new String[] {‘’test basé modèle’’, ‘’sécurité’’, ’’inférence de modèles’’});
}
```

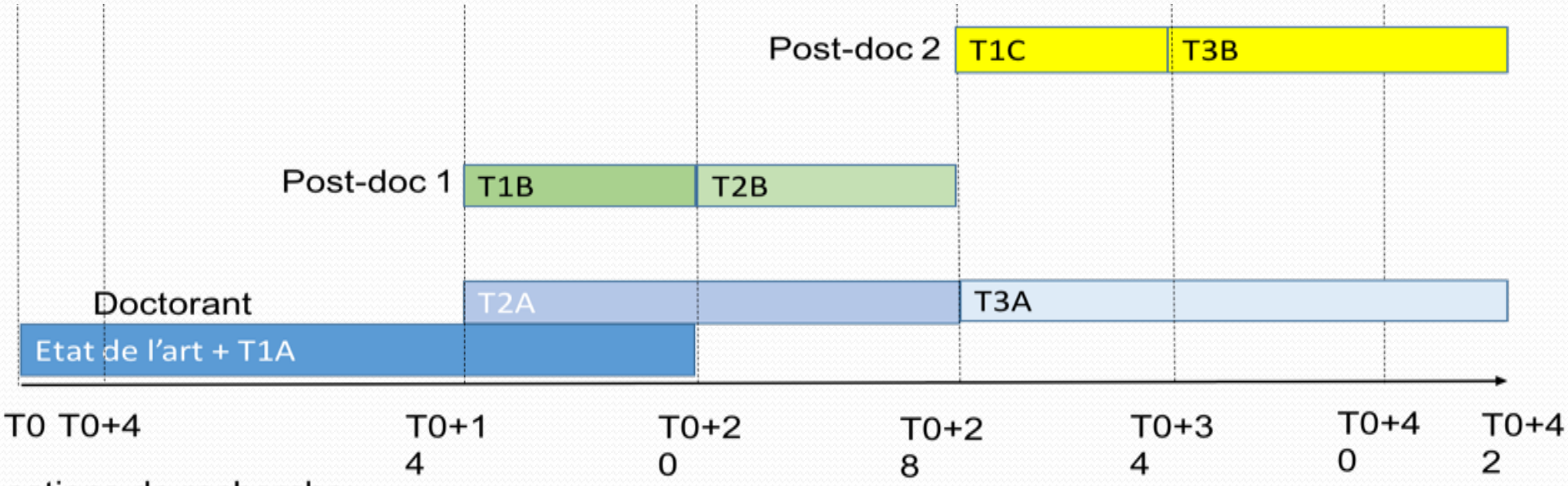
Projet VASOC

- Vers l'Audit de Sécurité des Objets Connectés

- UCA- LIMOS
  - ->software
- Université Saint-Etienne, Lab Hubert Curien
  - ->hardware

- Object-As-A-Service, Agaetis, Openium, Braincube, Elkya, Les Mowdoo

Déroulement



Allocations de recherche:
Doctorant: T0+4->T0+40 Post-doc 1 : T0+14->T0+26
Post-doc 2:T0+28->T0+40

Déroulement

T1 Développement d'une base de connaissances

a. Etat de l'art + création d'une base d'attaques et de contre-mesures : phase d'acquisition et d'intégration de données de sécurité dans une base publiquement disponible ; ;
b. Ajout de la notion de patron de sécurité: lintégration des patrons de sécuriténtégration des patrons de sécurité ;
c. Collecte de vulnérabilités, d'attaques liées au matériel. (solution de conception aux problèmes de sécurités récurrents) ;

T2 Analyse de risques :

a. Aide à la mise en place d'une phase d'exigences de sécurité ; : à partir de la base de connaissances, nous inférerons automatique des modèles de menaces ;
b. Mise en place de défenses via des patrons de sécurité , utilisable pour l'Audit de code ;

T3 Aide à l'Audit de sécurité :

a. Aide à la génération de test de sécurité Mise en place d'une phase de test d'intrusion;: aide à la génération de test de sécurité ;
b. Proposition d'un ensemble de techniques pour la sécurisation matérielle. ???????

IOT?

- Devices, network, gateway, cloud, mobile apps

- Plusieurs facettes
  - personnes (manufacturer, dev., revendeurs, utilisateur)
  - Interface d'accès (memory, code, physical interfaces, Web interface, firmware, update,local data storage, network, network services,)
  - Localité
  - Consommation, puissance CPU,
- Plusieurs Niveaux de risque

IOT?

- Standards (?) http://www.onem2m.org/

- Plateformes d'exp: Iot-lab
- Débuts de certification européennes Truste
- Certif FR CSPN, Besoin de métriques-> niveaux de certification

  - Proposition de qques scénarios de test -> mesures -> labels de certif
  - **Besoin de retours, d'ex. tests, de modèles, de mapper, de plateformes, etc.**

Top ten owasp Vulnérabilités

Main | OWASP Internet of Things Top 10 for 2014 | Project Details

The OWASP Internet of Things Top 10 - 2014 is as follows:

- I1 Insecure Web Interface
- I2 Insufficient Authentication/Authorization
- I3 Insecure Network Services
- I4 Lack of Transport Encryption
- I5 Privacy Concerns
- I6 Insecure Cloud Interface
- I7 Insecure Mobile Interface
- I8 Insufficient Security Configurability
- I9 Insecure Software/Firmware
- I10 Poor Physical Security

Pleins de challenges

- Bases de vulnérabilité ? D'attaques
- Design avec solutions sécurisées
- Auth + Chiffrement (local, distribué)

- Protection du matériel (voir actualité d'en ce moment…)
- Tester (notamment quand on fait appel à de la presta)
  - Quelques outils, mais pas trivial et très technique

Quelques Pistes générales?

- Classification vulnérabilités, attaques
- Architecture design, secuiryt pattern pour IOT (-> etudiants)
- Gen. De modèles de menaces (idela pour audit)
- Aides à la génération de tests
- **Inférence de modèles à partir de log ou test + learning** (->elliot)
- Def. De signatures pour reconnaitre IOT malware
- Gen de moniteurs dynamiques pour capturer traces

Quelques Pistes générales?

- Tests sur les données -> def. D'invariants temporels et test d'envoi de mauvaises données
  - Tester la conséquence d'envoyer des mauvaises données sur chaine d'analyse
- Protection gateway par monitoring et learning
- Analyse de composition de devices et proposition de re-composition sur multi-critères
- Analyse code source ou binaire
  - + association avec model learning
- Generateur de regles d'IDS pour gateway

Indutriels ?

- Qu'attendez vous du projet ?

- Transfert de savoir ?
  - Bases ? (CVE ? Etc.) méthodologie ?
- Etude / travail commun ? (stages ?)
- Outils ?

Plan d’actions ?

- Reunions ?

Merci