Déroulement d'une attaque sur un système

Introduction

Ce document présente le déroulement d'une attaque sur un système. L'attaque se déroule en deux étapes :

- **Reconnaissance du système,** lors de cette étape l'attaquant tente d'obtenir le plus d'information possible sur le système sans interagir avec ce dernier (observation, piratage de boîtes mail, …)
- **Découverte du système,** lors de cette phase l'attaquant interagit avec le système dans le but d'en comprendre l'architecture interne.

Table des matières

Cas d'étude

Nous baserons notre exemple sur un système simple de détection de forme. Le système est composé d'une caméra relié à un FPGA lui-même relié à un processeur ARM et un disque dure SSD. Le système dispose d'une connexion internet via le processeur ARM.

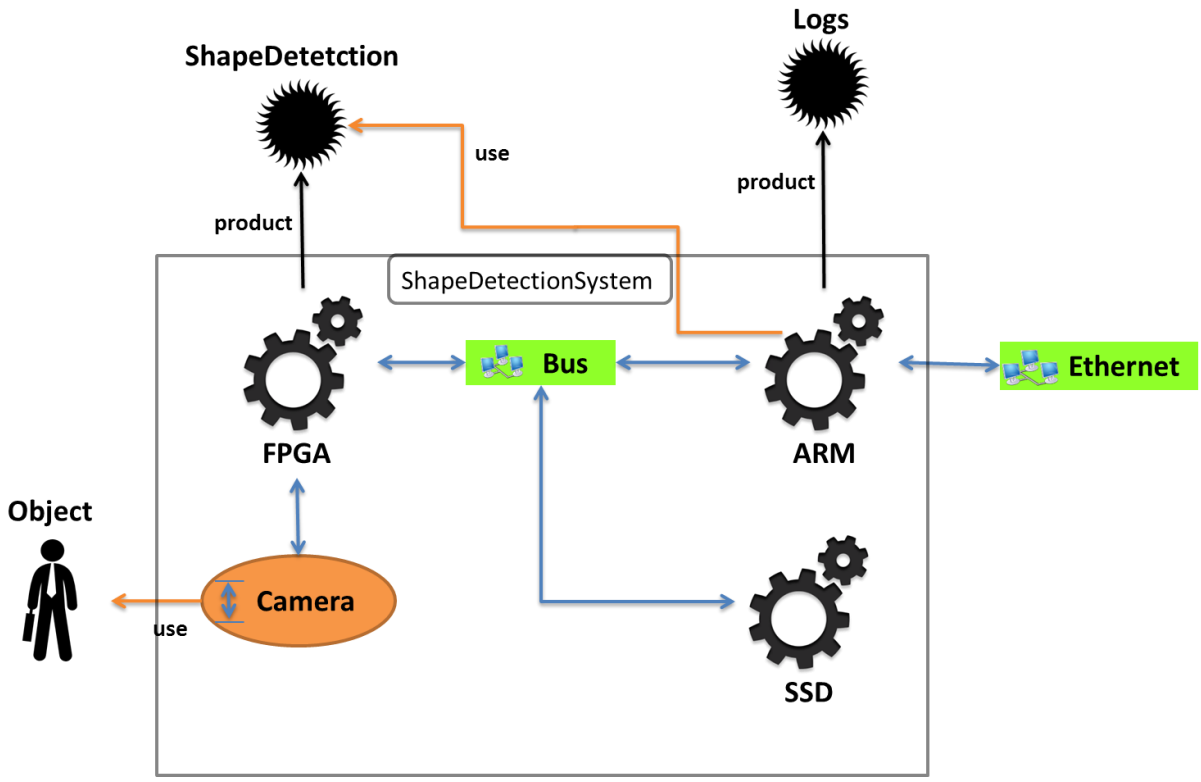

Figure 1: Schémas du système réel dans son ensemble

Le figure ci-dessus représente le système réel dans son ensemble, c'est cette information que l'attaquant cherche à obtenir lors de la 1er phase de l'attaque (Reconnaissance du système).

Reconnaissance du système

Regroupement des informations

Nous supposerons pour notre exemple que l'attaquant possède :

- **Une photo du système** : Cette photo a pu être prise par un drone ou grâce à un téléphone. Elle est de qualité moyenne mais permet tout de même d'obtenir quelques informations sur le système.
- **Des informations concernant la consommation énergétique du système :** Ces informations peuvent être déduites d'une image du système sur laquelle les sources énergétiques sont visibles ou via un autre moyen tel que le piratage d'une boîte mail.

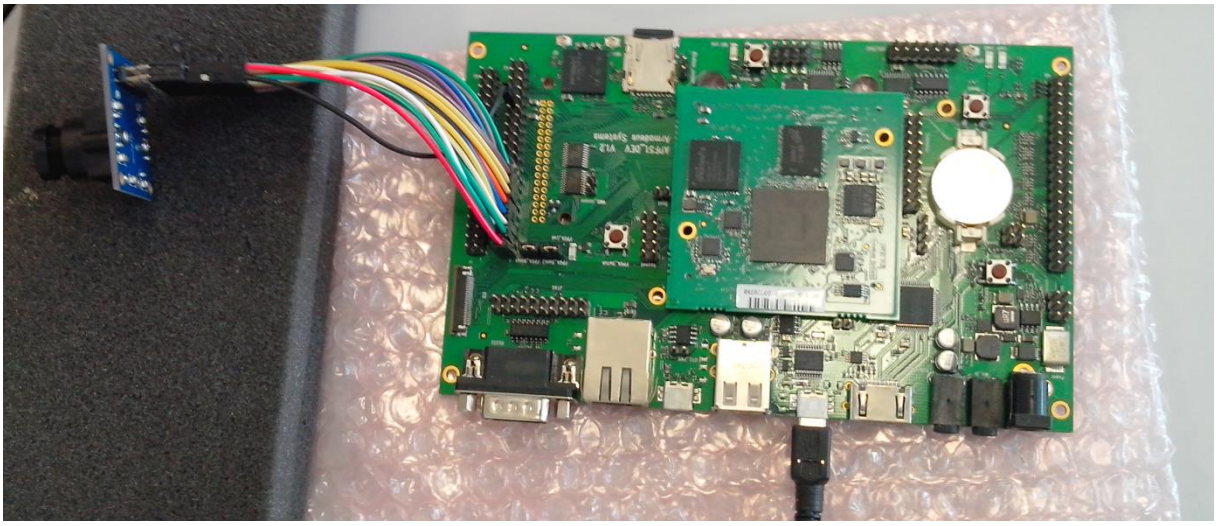

Figure 2: Photo du système

Sur la photo si dessus, prise par l'attaquant, il est possible de reconnaitre une caméra branché à un FPGA lui-même relié à plusieurs autres composants. Le système global semble relié au réseau via un port Ethernet. Les observations faites grâce à la photo permettent à l'attaquant de créer le modèle supposé du système via Pimca. Pour créer ce modèle l'attaquant doit faire des hypothèses sur le système. Dans un premier temps il suppose que le système possède un processeur I7, un disque dure HDD, de la mémoire RAM et un GPU.

Hypothèse 1 :

- I7
- HDD
- RAM
- GPU

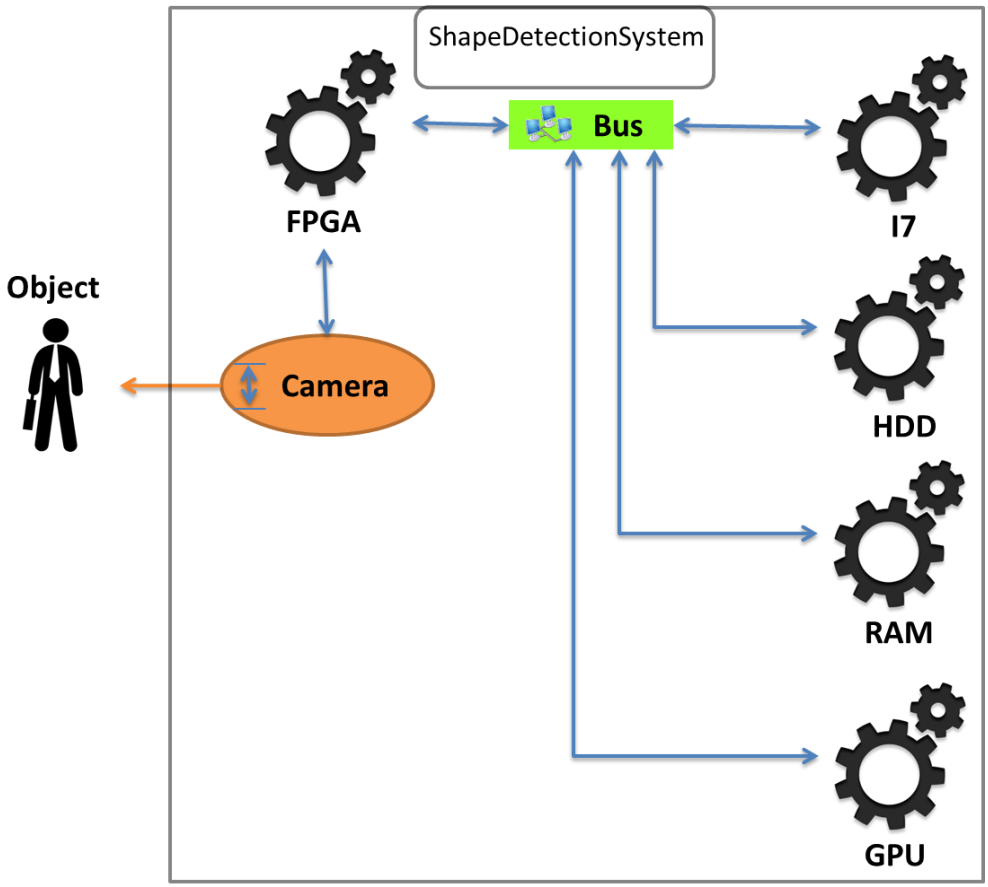

Figure 3: Modèle du système supposé créait grâce aux hypothèses 1

En plus de la photo du système l'attaquant a réussi à intercepter un échange d'email entre plusieurs acteurs du projet :

A : [redacted]
Cc:
Cci :
Objet : Re: COnfig pour le proxy git
De : [redacted] 2015 11:03

Sans Serif 10

----- [redacted] a écrit : -----
A : [redacted]
De : [redacted]
Date : 04/11/2015 18:13
Objet : COnfig pour le proxy git

git config --global http.proxy http://proxy:8080
git config --global https.proxy https://proxy:8080

PS: N'oublie pas de coupé le système quand tu auras fini de le configurai, il consomme tout de même 10kW/h

Figure 4: Email provenant d'une boite mail piraté

L'Email présenté dans la figure ci-dessus permet à l'attaquant d'obtenir une connaissance approximative de la consommation du système (10kW/h). L'attaquant peut alors ajouter cette information à un fichier Excel que l'on nommera *informationsComplementaires.xlsx.*

Simulation du modèle du système supposé

Une fois que l'attaquant a regroupé des informations sur le système et qu'il les a misent en forme grâce à plusieurs outils (Pimca et Excel), il peut tester les hypothèses qu'il a formulé. Pour ce faire l'attaquant utilise Role4All ce qui lui permet de lier le modèle du système supposé, fait sur Pimca, et les informations complémentaires contenus dans le fichier Excel. Une fois ces données reliées le système supposé est virtualisé et testé grâce à Morphose. Morphose effectue alors plusieurs mesure (consommation, température, …) sur le système virtuel et les comparées aux mesures effectuées sur le système réel.

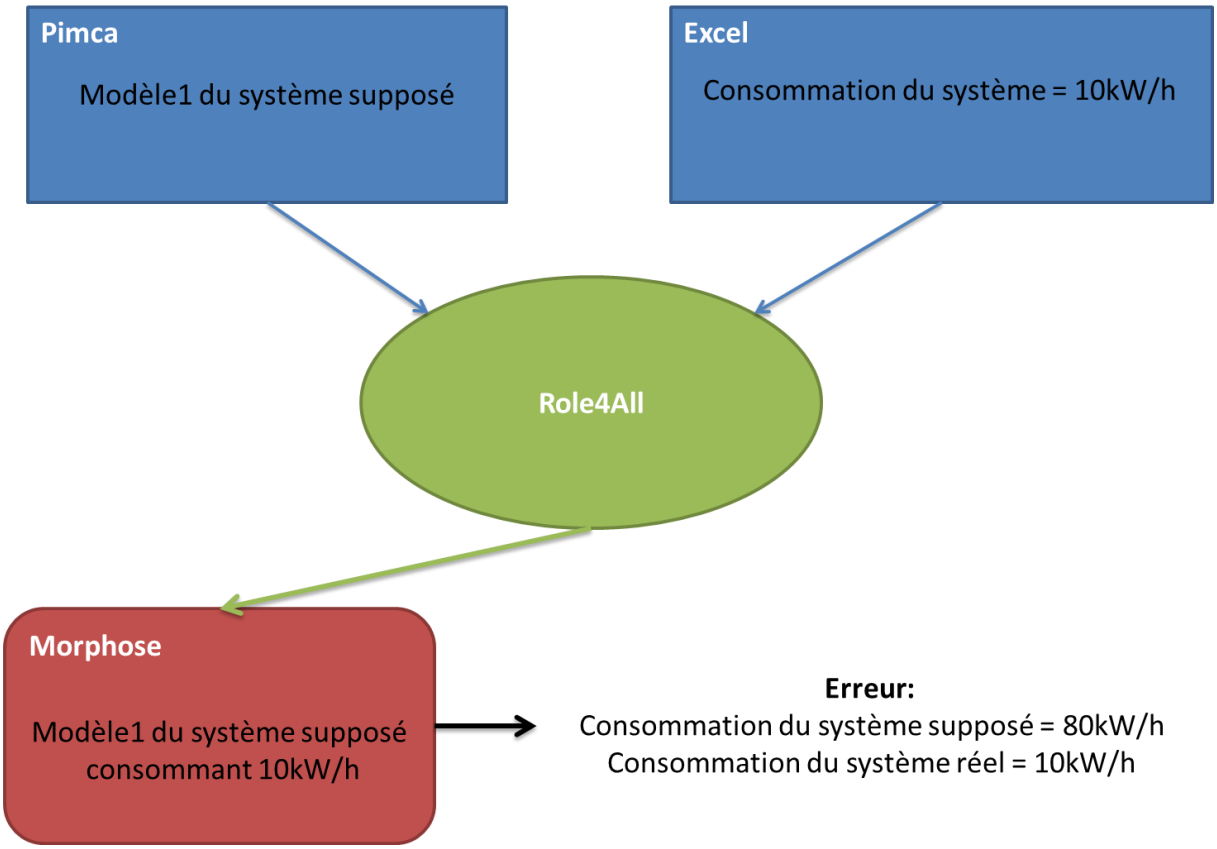

Figure 5: Teste des hypothèses 1

La figure ci-dessus schématise une phase de validation d'hypothèse. Le résultat des tests effectués nous permet de conclure que le modèle du système supposé ne représente pas le système réel. En comparant les consommations réelles et simulées on peut déduire que le modèle du système supposé est trop gourmand en énergie. L'attaquant peut alors modifier ses hypothèses en conséquence. Dans ce cas précis il décide de suppriment le GPU et la RAM.

Hypothèse 2 :

- I7
- HDD

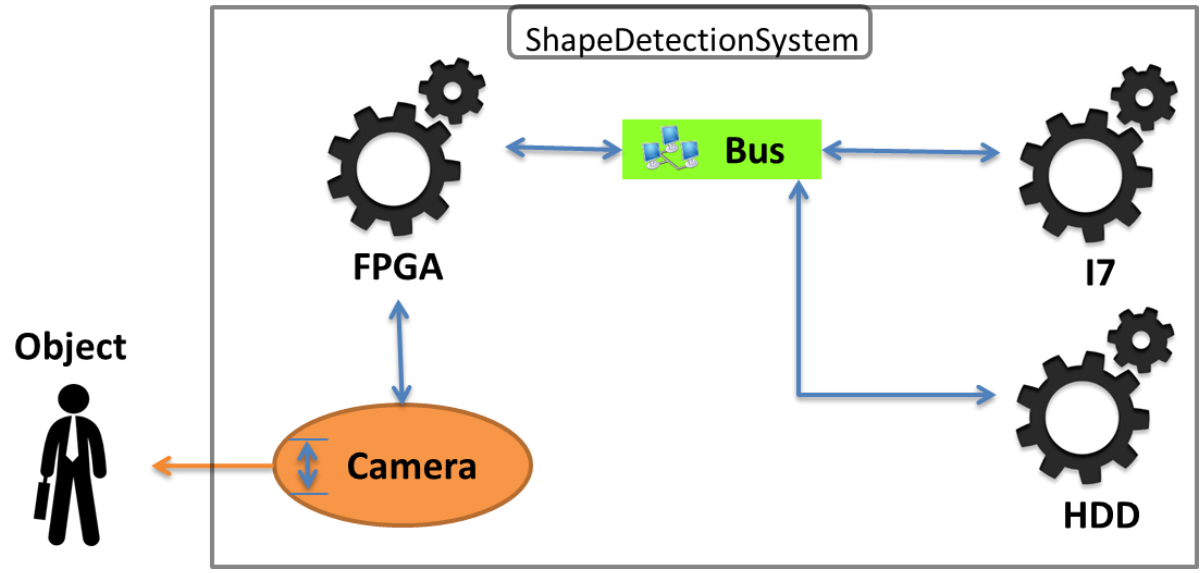

Figure 6: Modèle du système supposé créait grâce aux hypothèses 2

L'attaquant peut alors simuler son nouveau modèle en suivant le même cheminement que pour le modèle précédent.

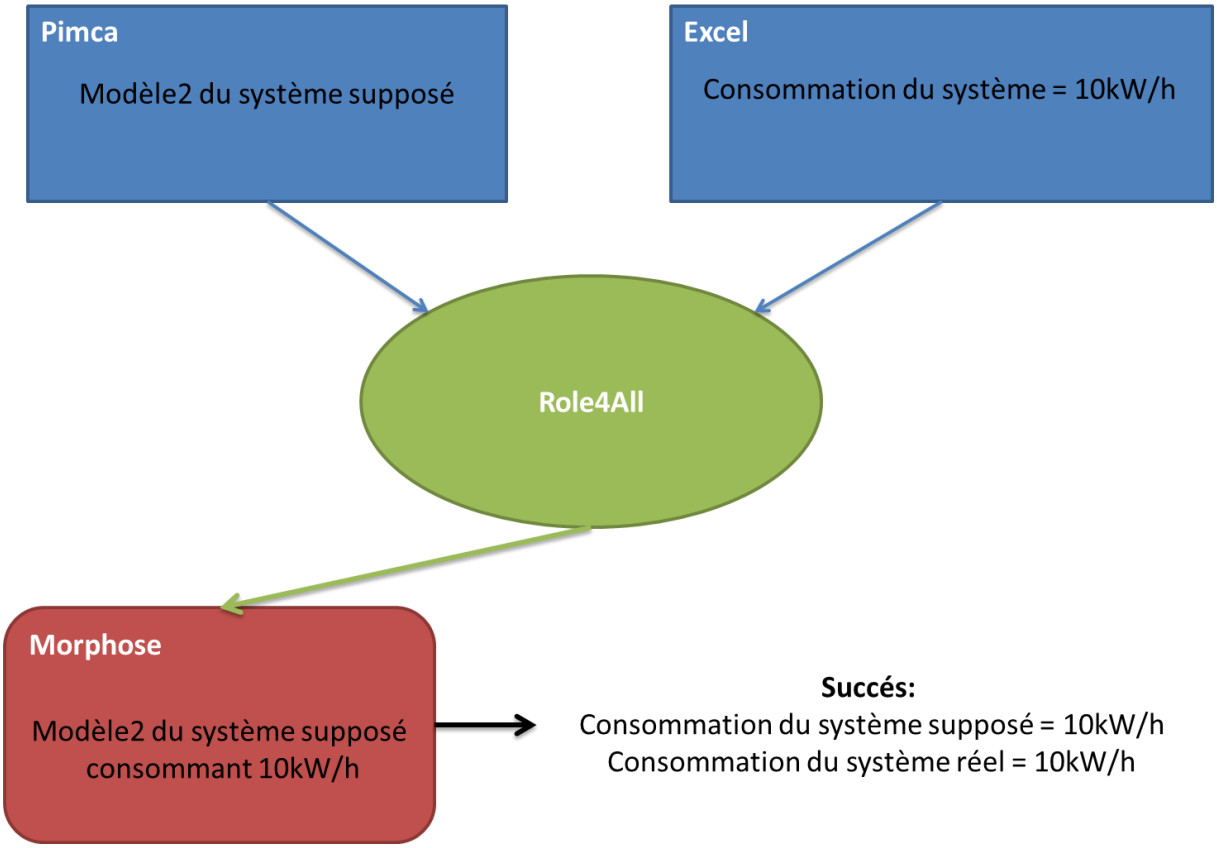

Figure 7: Teste des hypothèses 2

Le 2ème modèle proposé par l'attaquant semble cohérant. Avec les informations que possède l'attaquant (photos et consommations) il ne lui est pas possible de plus raffiné son modèle.

L'attaquant doit alors rechercher de nouvelles informations sur le système (temps de réponse, temps d'allumage, dégagement thermique, …). Ces informations seront alors formatées (Excel, Pimca ou autre) et injectées dans la simulation du système supposé. Ces nouvelles données permettront de raffiner la connaissance que l'attaquant a du système.

Nous supposerons que l'attaquant, grâce à de nouvelles sources d'informations, a réussis à raffiner ça connaissance du système jusqu'à arriver au modèle suivant :

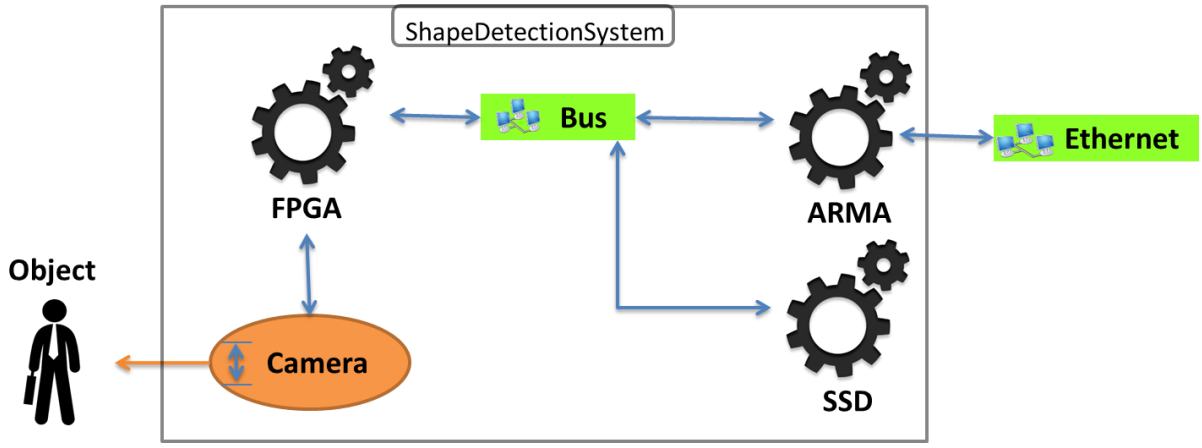

Figure 8: Modèle du système supposé

Conclusion

L'attaquant, grâce à un regroupement d'informations périphériques au système, a pu créer un schéma représentant l'architecture externe du système. Ce schéma sera utile lors de la prochaine étape qui consiste en la découverte de l'architecture interne du système.

Découverte du système

TODO