Master 1 Informatique

PJI - Projet Individuel - Sujet no 104

Systèmes de détection d'intrusion pour l'Internet des Objets

Auteurs :
M. Théo Plockyn
M. Rémy Debue

Encadrant :
Pr. Gilles Grimaud

Version 0.5 du
1er mai 2016

Remerciements

Nous remercions tout d'abord l'équipe pédagogique, administrative et intervenants du Master 1 informatique pour nous avoir encadré, aidé et assuré les enseignements dont nous avons disposé cette année.

Nous tenons aussi à remercier et à témoigner notre reconnaissance aux personnes suivantes :

Gilles Grimaud, notre encadrant, pour nous avoir proposé le sujet, nous avoir suivi et conseillé tout au long de ce projet.

Michaël Hauspie, pour ses consignes et sa participation dans les décisions du déroulement du projet.

Nadir Cherifi, pour son aide précieuse et ses connaissances des technologies utilisées qui nous ont débloqué à plusieurs reprises.

Samuel Hym, François Serman, Christophe Bacara, Quentin Bergougnoux, et toute l'équipe 2XS pour leur accueil sympathique et leur soutien tout au long de ce projet.

Table des matières

Table des figures

Liste des sigles et acronymes

6LoWPAN	*IPv**6** **Lo**w power **W**ireless **P**ersonal **A**rea **N**etworks*
IRCICA	**I**nstitut de **r**echerche sur les **c**omposants logiciels et matériels pour l'**i**nformation et la **c**ommunication **a**vancée de Lille
2XS	*e**X**tra **S**mall e**X**tra **S**afe* – L'équipe de recherche
CFS	*__C__offee __F__ile __S__ystem* – Le système de fichier de Contiki
PJI	**P**roj**j**et **i**ndividuel

Introduction

Dans le cadre de notre cursus en Master Informatique à Lille 1, nous avons eu lopportunité de réaliser un projet sur lensemble du semestre appelé PJI. Chaque étudiant ou binôme pouvait choisir un sujet sur lequel travailler parmi une liste mais également proposer le sien. Nous avons choisi de nous intéresser à un sujet proche de l'informatique embarquée, plus particulièrement dans le domaine de l'Internet des Objets. Notre sujet se porte sur la détection d'attaques dans un réseau 6LoWPAN.

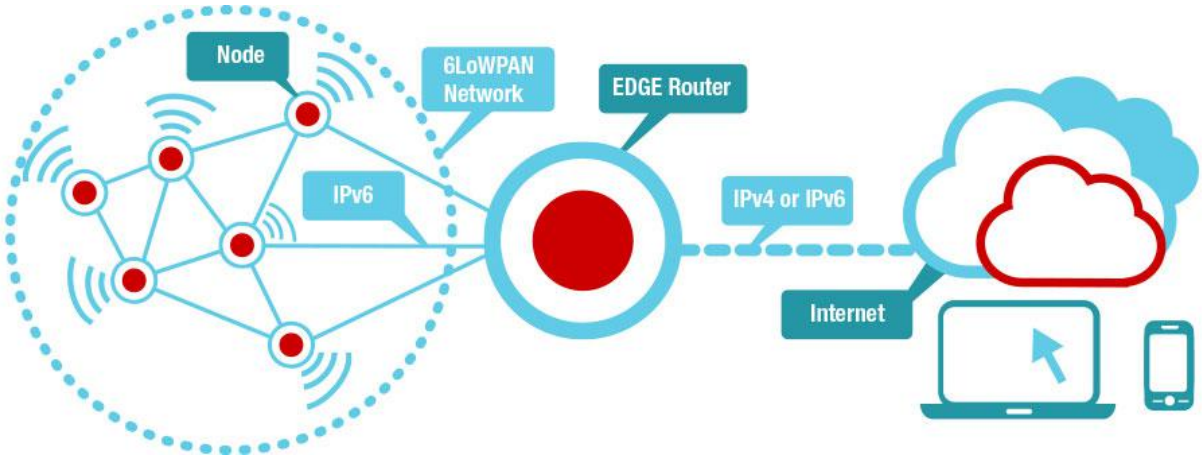

FIGURE 1 – Diagramme d'explication de 6LoWPAN.

L'équipe de recherche proposant ce sujet est le groupe 2XS **eXtra Small eXtra Safe** composée de notamment **Gilles GRIMAUD** notre encadrant, **Michael HAUSPIE** son collègue proche de ce sujet et bien sûr le reste de l'équipe. L'équipe se focalise sur les problématiques de sécurité dans les systèmes embarqués contraints, notamment fournir des solutions logicielles prouvées.

Chapitre 1

Contexte du sujet

— Expliquer le projet

1.1 Analyse de l'existant

1.1.1 Internet des objets

— Qu'est-ce que c'est ?
— Technologies utilisables (bluetooth, wifi, 6lowpan)

1.1.2 Technologies de communication

— 6lowpan qu'est-ce que c'est ?
  — définition
  — exemples (Linky, domotique, industrie)

1.1.3 Sécurité des communications

— Sécurité dans 6lowpan
  — RFC définissent sécurité
  — Dans les faits, pas vraiment mis en place

1.2 But du projet

1.2.1 Détail du projet

— mote qui sniffe, oui mais quoi ?
— système contraint en puissance et en mémoire

1.2.2 Où s'inscrit le projet ?

— Industrie, hopitaux, mobilier urbain (pas "simple domotique")

1.3 Réponse à un besoin de l'équipe

1.3.1 Focus sur la sécurité par 2XS

— Systèmes sûrs
  — Preuves formelles
  — Différents projets de sécurité
— D'accord, mais quid des communications ?

1.3.2 Disqus

— IDS – Système de détection d'intrusion

1.4 Technologies et systèmes utilisés

Ici on présente les technologies utilisées

1.4.1 Contiki OS

1.4.2 Outils de simulations

— Cooja
— InstantContiki3.0

1.4.3 Langage C embarqué et sa chaine de compilation spécifique

1.4.4 Git

Chapitre 2

Explications techniques

2.1 Contiki

2.1.1 Pile réseau de Contiki

2.1.2 Systèmes de stockage Contiki

Contiki file system

- Expliquer comment écrire dedans
- Expliquer pourquoi on ne l'a pas utilisé

Volatile

Listes

- Expliquer comment écrire dedans
- Expliquer pourquoi on ne l'a pas utilisé

Buffers cycliques

- Expliquer comment écrire dedans
- Expliquer pourquoi on l'a utilisé

2.2 6LoWPAN

2.2.1 Compression des headers

- Pourquoi compresser ?
- Comment ça marche (avec images)

2.2.2 Attaques possibles

- Qui nous intéressent pas directement
  - Attaques passives (écoute)
  - Brouillage des ondes
  - Inondation de paquets
- Qui nous intéressent
  - Spoofing
  - Paquets dupliqués
  - Paquets fabriqués
  - Sybil attack

Nos possibles solutions du coup

Chapitre 3

Déroulement du projet

3.1 Prise en main du sujet et des technologies

3.1.1 Contiki OS

— Embarqué
— simulations avec Cooja
— Pourquoi Contiki et pas un autre ?

3.1.2 Chaîne de compilation

— GCC
— architectures différentes
— contrôleurs radio différents

3.2 Programme développé

3.2.1 Comment c'est fait

3.2.2 Jusque où est on arrivé

3.3 Challenges et retours

3.3.1 Évolutions à court terme

— Plus de détections d'attaques

— Intégration dans disqus

3.3.2 Évolutions à long terme

— Grille de sniffers
— Triangulation des anomalies

3.3.3 Pourquoi c'était dur ?

— Logistique
  — Commencé en retard
  — Timing avec les cours
— Découvertes multiples
  — Embarqué
  — Technologies de communication
  — Spécifications
— Documentation parfois incomplète ou trop peu visible
  — Packetbuf avec différence de paquet entrant et sortant
— Exemples de code pas assez commentés

Conclusion et perspectives

Conclusion et ouverture
— Résumer le sujet, sa problématique et notre morceau de solution
— Ce qu'on a apporté
— Ce que ça nous a apporté
— Comment ce qu'on a appris va nous servir plus tard