

## Lambda functions for network control and monitoring

**Auteur** : Leduc, François

**Promoteur(s)** : Mathy, Laurent

**Faculté** : Faculté des Sciences appliquées

**Diplôme** : Master en sciences informatiques, à finalité spécialisée en "computer systems security"

**Année académique** : 2020-2021

**URI/URL** : <http://hdl.handle.net/2268.2/13159>

---

*Avertissement à l'attention des usagers :*

*Tous les documents placés en accès ouvert sur le site le site MatheO sont protégés par le droit d'auteur. Conformément aux principes énoncés par la "Budapest Open Access Initiative"(BOAI, 2002), l'utilisateur du site peut lire, télécharger, copier, transmettre, imprimer, chercher ou faire un lien vers le texte intégral de ces documents, les disséquer pour les indexer, s'en servir de données pour un logiciel, ou s'en servir à toute autre fin légale (ou prévue par la réglementation relative au droit d'auteur). Toute utilisation du document à des fins commerciales est strictement interdite.*

*Par ailleurs, l'utilisateur s'engage à respecter les droits moraux de l'auteur, principalement le droit à l'intégrité de l'oeuvre et le droit de paternité et ce dans toute utilisation que l'utilisateur entreprend. Ainsi, à titre d'exemple, lorsqu'il reproduira un document par extrait ou dans son intégralité, l'utilisateur citera de manière complète les sources telles que mentionnées ci-dessus. Toute utilisation non explicitement autorisée ci-avant (telle que par exemple, la modification du document ou son résumé) nécessite l'autorisation préalable et expresse des auteurs ou de leurs ayants droit.*

---

# **Lambda functions for network control and monitoring**

Author: François Leduc

Supervisor: Prof. Laurent Mathy (Uliège)

Master's Thesis

School of Engineering and Computer Science

University of Liège

Academic year 2020-2021

## **Abstract**

Monitoring a network in a precise manner is becoming more interesting in light of the volume of traffic that new infrastructures can accommodate. With the advent of programmable switches and routers, monitoring systems are turning to solutions that benefit from this new capability. There is also the establishment of a new back-end approach known as serverless computing, which consists in uploading lambda functions to the cloud. These functions offer backend services on an as-needed basis.

The goal of this work is to develop a monitoring system capable of detecting network attacks and specific events of interest to a network operator. To accomplish this, the two previously introduced notions are used, namely a backend architecture based on serverless computing and the assumption that the network is made up of programmable devices.

In terms of packet processing technology, we used XDP, which allows us to create a hook at the switch's network interface and execute a program. The program's goal is to save the headers of IP packets locally. These data are then formatted as custom events and transferred to an intermediate server. In order to do this, we have designed a protocol on top of UDP. The server will then trigger the execution of the lambda functions associated to the events. For their execution we decided to choose Kubeless, a Kubernetes-native serverless framework. A Proof of Concept was created to see if our solution was scalable and possible. We then evaluate the amount of network traffic generated by our approach and discuss protocol limitations.

We conclude by suggesting several sorts of prospective improvements ranging from security to better benchmarking and other architectural options.