TELECOM SudParis
INSTITUT Mines-Télécom

Intrusion detection on Software Defined Network (SDN) using a Machine Learning approach

18
RESEARCH

Authors

Charles MURE
Félix MOLINA

Supervisors

Gregory BLANC
Mustafizur SHAHID

Partners

cassiopée
TELECOM SudParis

Technologies

Alcatel·Lucent
sFlow
argus
Keras
A deep learning library

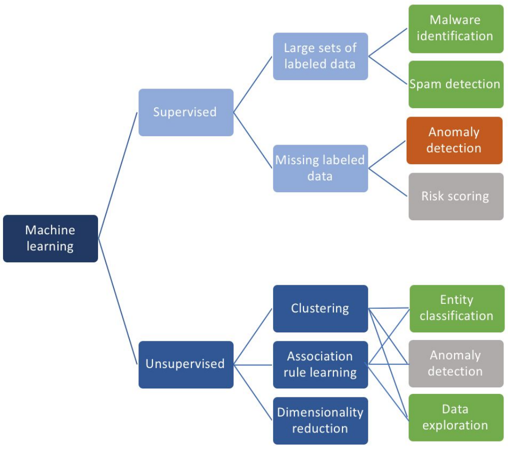
Dataset from

UNSW SYDNEY

- *This project proposed a new* ***machine learning-based IDS*** *(Intrusion Detection System) software using* ***Deep Learning*** *and* ***flow-based*** *approach.*

CYBERSECURITY IN SDN

- Today, intrusions happen too fast for anyone to respond effectively, and terabytes can be siphoned off overnight. Unfortunately, the gap is widening between the speed at which compromises happen and that at which they are discovered.
- Software Defined Network and network/flow programmability offer a **custom-made network** giving access to an easy way to collect network data in a **centralized** way. The SDN switches can have the same role as a router on which it is possible to run applications. These applications can improve the network security analyzing traffic with Machine Learning algorithms and then detect intrusion. In addition, some protocols like sFlow or IPFIX have been created to extract, from network flows, network features.



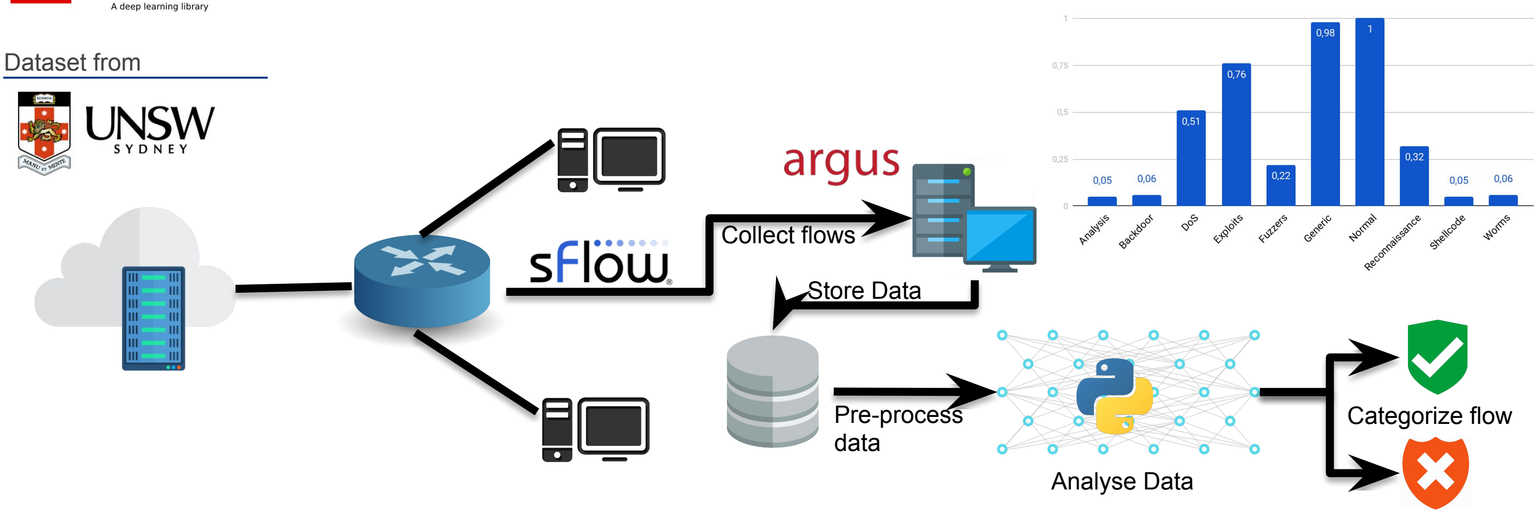
MACHINE LEARNING FOR CYBERSECURITY

- A network generates **lots of data**.
- It is now possible to analyse **anomalous flows** on the network instead of using a naive rule-based system.
- However, it is very difficult to develop a **flexible and effective IDS for unforseen attacks**. **Deep Learning** are capable of automatically finding correlation in complex data with a **high accuracy**. It is the most promising method for the next generation of IDS.

PROTOTYPE OF A DEEP LEARNING IDS

- We propose a simple implementation in **Python** of an **IDS based on Convolutional Neural Network**. The idea is to monitor in **real-time** the **network flows**, **extract features** from them, pre-process the data and then **categorize this flow** as **normal** or as one of the **7 types of attacks**. The complete stream process takes less than a second on a simple laptop.
- However, our system does not yet exploit the full potential of SDN protocols to collect flows because sFlow is not specific to SDN.

Precision over classes with UNSW-15 Dataset



Contact
charles.mure@telecom-sudparis.eu
felix.molina@telecom-sudparis.eu

Site web
www.cassiopee.wp.tem-tsp.eu
github.com/CharlesMure/cassiope-NIDS