Graph Analysis for forensics analysis

Security-Systems Summer Week 2023

Samedi 1 juillet 2023

Pierre Parrend

EPITA

ÉCOLE D'INGENIEURS EN INFORMATIQUE

Joint ML & Sec (unformal) Team EPITA/ICube

Pierre Parrend

Badis Hammi

Nidà Meddouri

Rabih Amhaz

Aline Deruyver

Amani Abou Rida

Julien Michel

Majed Jaber

Côme Frappé-Vialatoux

Artificial intelligence for cybersecurity

Challenge:

Detecting complex attacks in dynamic digital environments generating huge data volumes

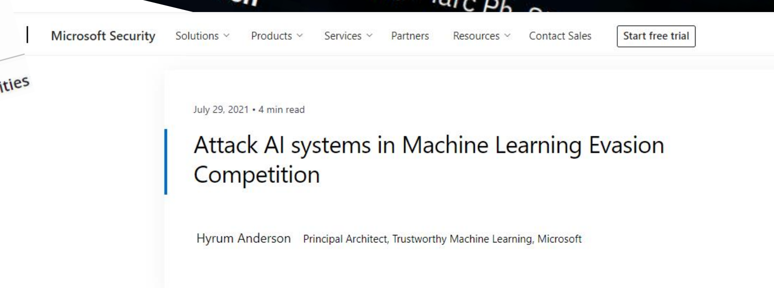
Teaching

Protecting Data, protecting through data, Unistra/TPS

ML & Security, EPITA SCIA

Trusted IA, EPITA ING1

Artificial Intelligence AGAINST cybersecurity ?



AI for Cybersecurity
Research challenges

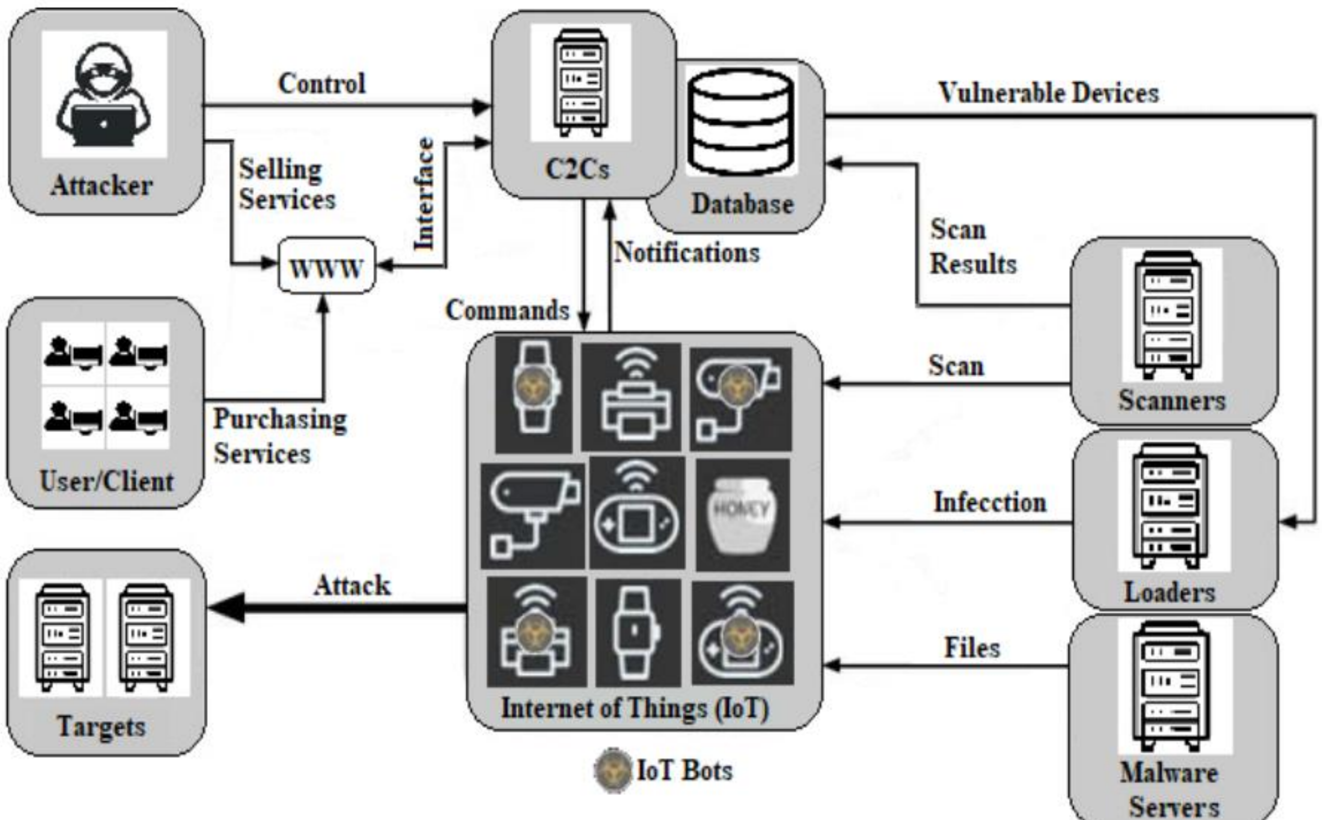
How to **model** attacks for an explicable and transferable detection ?

How to **detect** complex, multi-step attacks in system traces ?

How to **learn** new attacks to adapt analysis and prepare reaction ?

And how graphs can bring a solution ?

Running example:
UNSW IoT Botnet detection



Elsayed, Nelly, Zag ElSayed, and Magdy Bayoumi. "IoT Botnet Detection Using an Economic Deep Learning Model." *arXiv preprint arXiv:2302.02013* (2023).

Bot-IoT Dataset: Koroniotis, Nickolaos, et al. "Towards developing network forensic mechanism for botnet activities in the IoT based on machine learning techniques." *Mobile Networks and Management: 9th International Conference, MONAMI 2017, Melbourne, Australia, December 13-15, 2017, Proceedings 9*. Springer International Publishing, 2018.

Modeling

Technical Properties of Graphs

➔ Towards trusted graphs

Transparency

Accountability

Human oversight

Privacy and data governance

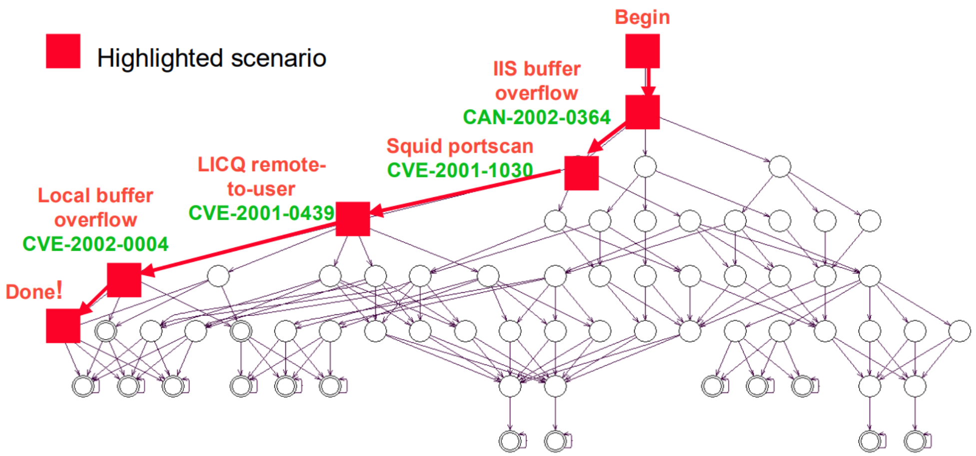
Security

Diversity, non discrimination and fairness

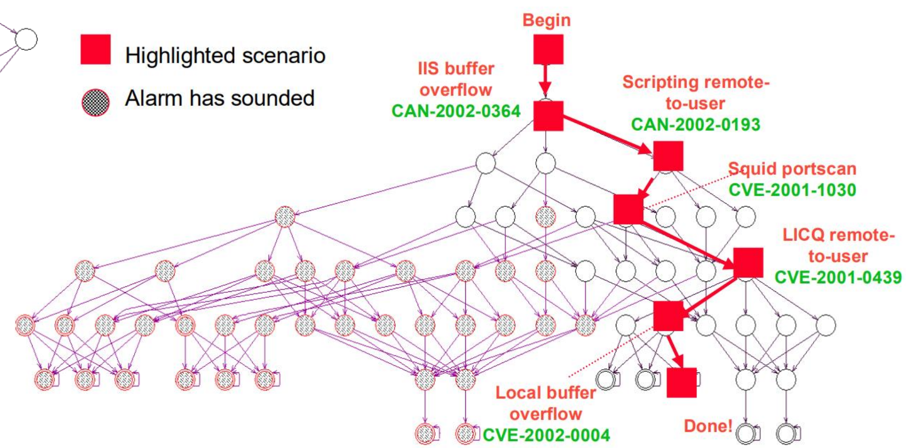
Societal and environmental wellbeing

Expert Knowledge
At the origin where … attack graphs

Modeling



Example Attack Graph



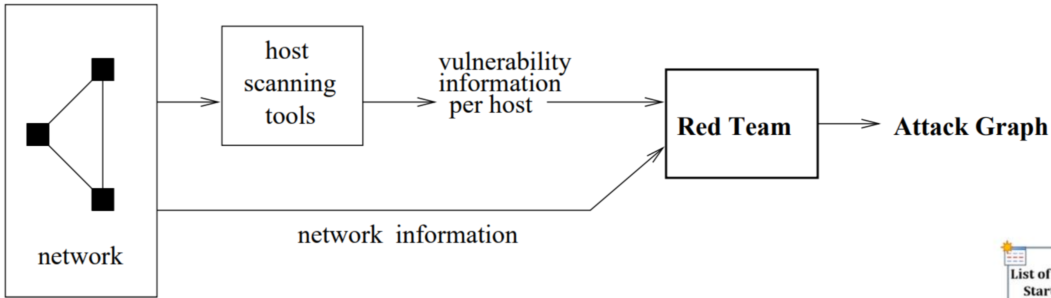
Alternative Attack Scenario Avoiding the IDS

Attack graphs for vulnerability analysis

→ Formalism for attack representation
→ Patterns for Intrusion Detection Systems
→ Enable to share knowledge visually

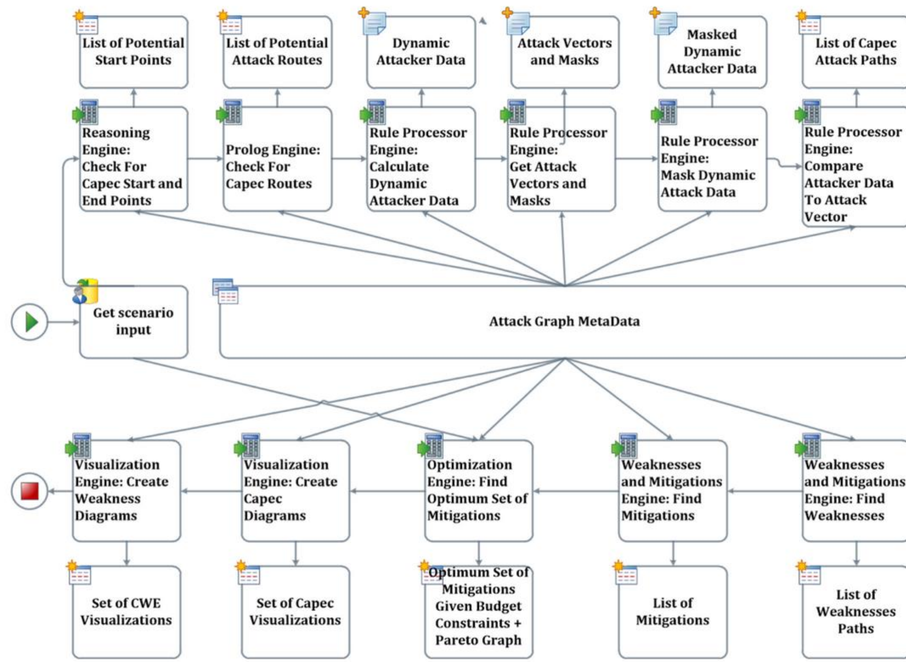
Sheyner, Oleg Mikhail. *Scenario graphs and attack graphs*. Carnegie Mellon University, 2004.

Attack graphs: Limitations



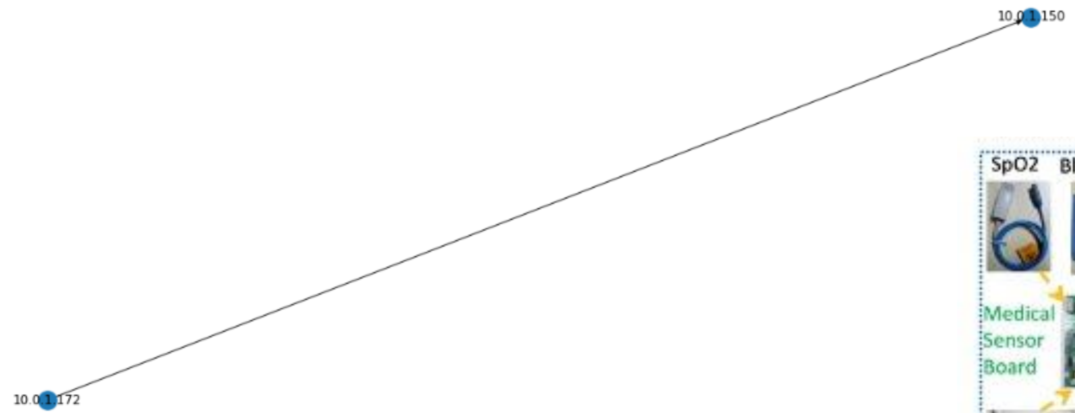
<u>Vulnerability Analysis of a Network is a tedious process</u>
→ Time costly
→ Error prone
→ Non-transferable

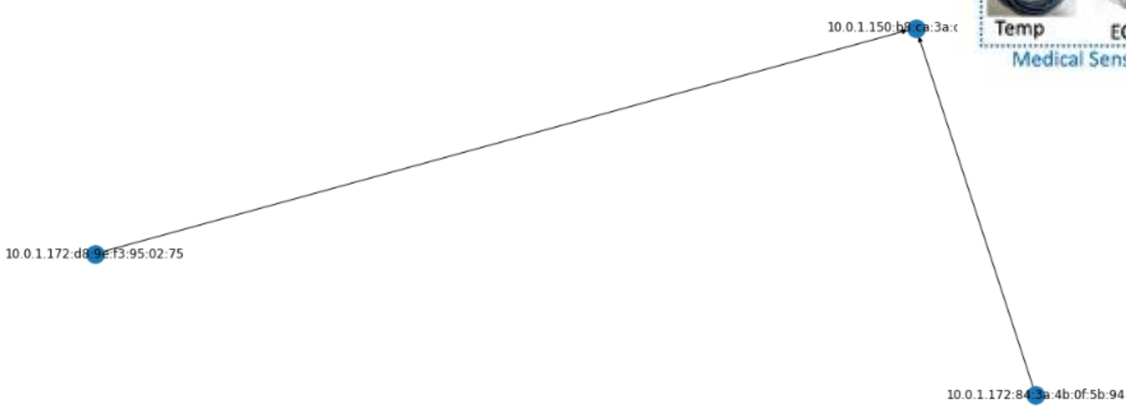
<u>The meta-model has gone more complex</u>
→ Some automation
→ Still relying on expert knowledge
  → A lot of manual documentation
  → Highly dependant on third party knowledge bases
→ Tool not available
→ Analysis tool uncoupled from detection or reaction capability

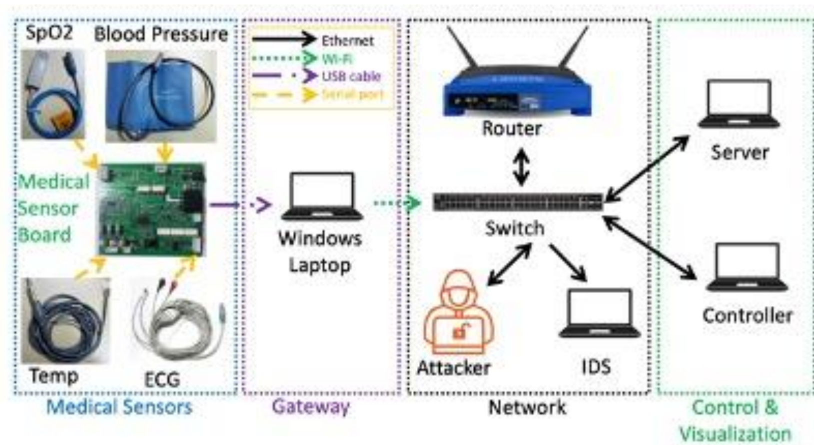


Hankin, Chris, and Pasquale Malacaria. "Attack Dynamics: An Automatic Attack Graph Generation Framework Based on System Topology, CAPEC, CWE, and CVE Databases." *Computers & Security* 123 (2022): 102938.

An example with graphs: Spoofing







WUSTL-EHMS-2020 testbed

https://www.cse.wustl.edu/~jain/ehms/index.html

Hady, Anar A., et al. "Intrusion detection system for healthcare systems using medical and network data: A comparison study." *IEEE Access* 8 (2020): 106576-106584.

Modeling

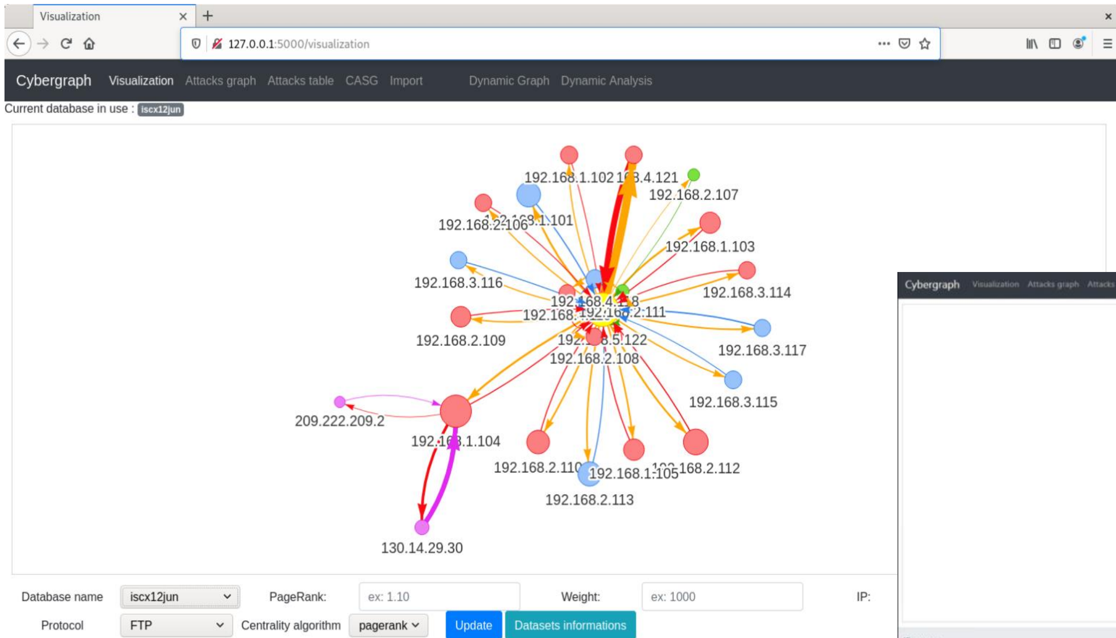
Pattern extraction through Cybergraph tool

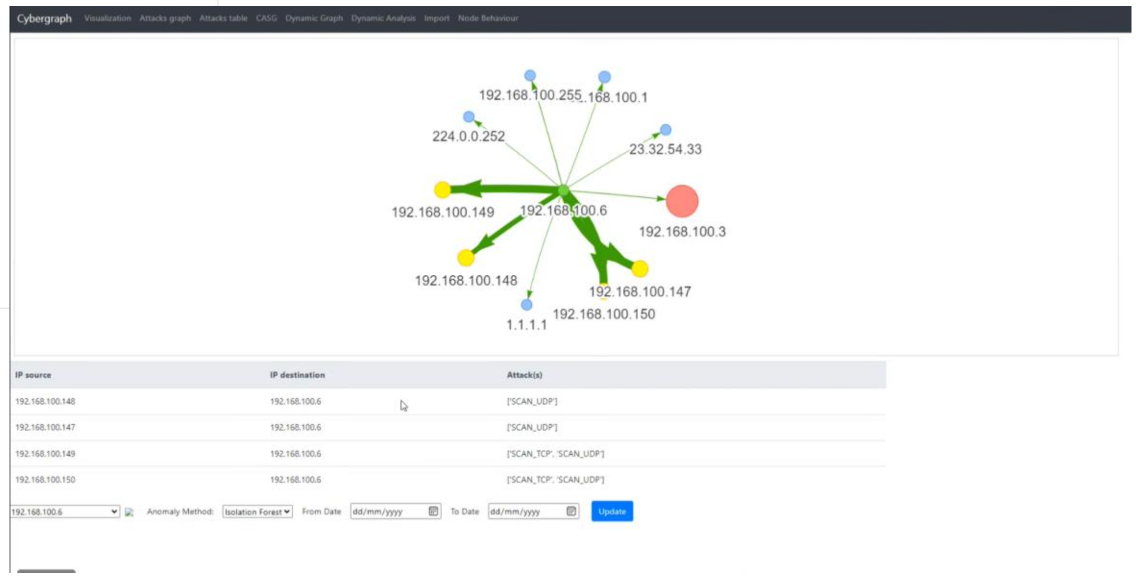
[Cybergraph]

`https://gitlab.cri.epita.fr/laboratoires/lse/research-devs/cybergraph`

[Graphseclearn]

`https://gitlab.cri.epita.fr/laboratoires/lse/research-devs/graphseclearn`





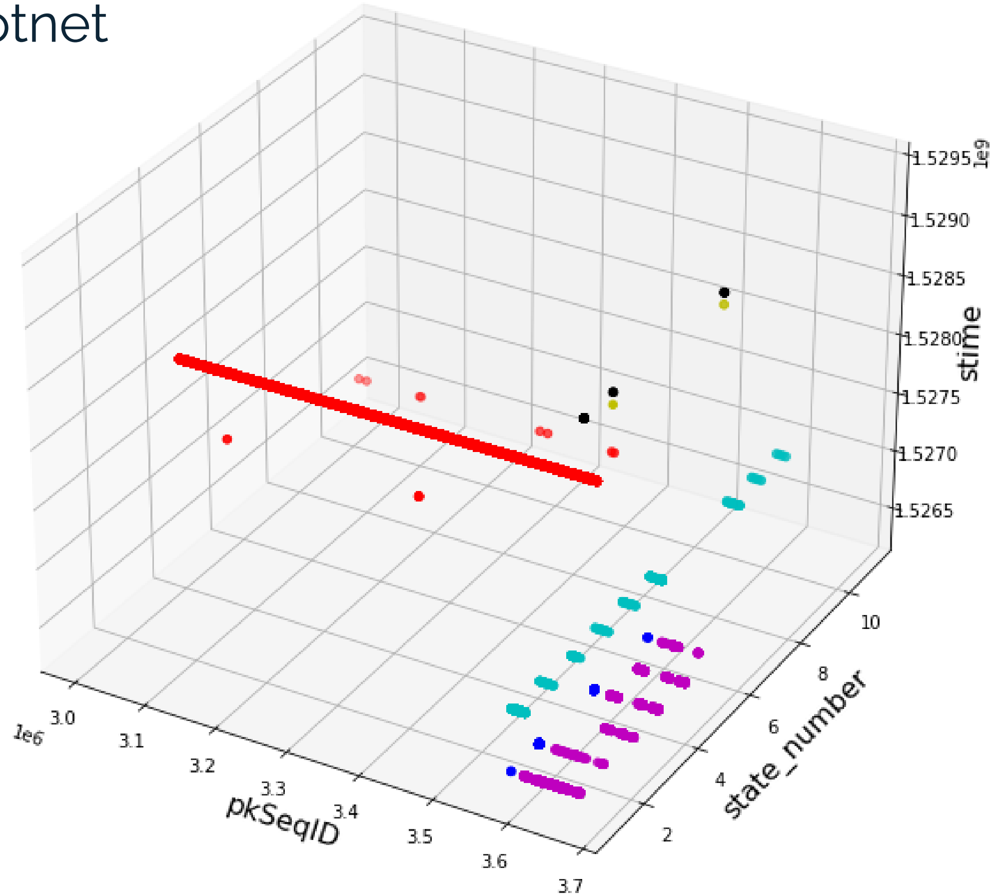
Graph structural queries

→Man in the Middle and Island Hopping
→ Uses GQL requests
→ Low hanging fruits and dangerous patterns (but not necessarily malicious)

Detection

The baseline: Detection with Machine Learning

Visualisation of UNSW-IoT-Botnet

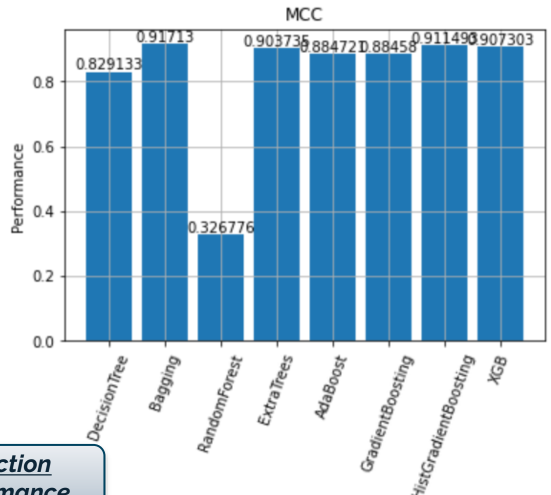


<u>*Machine learning*</u>

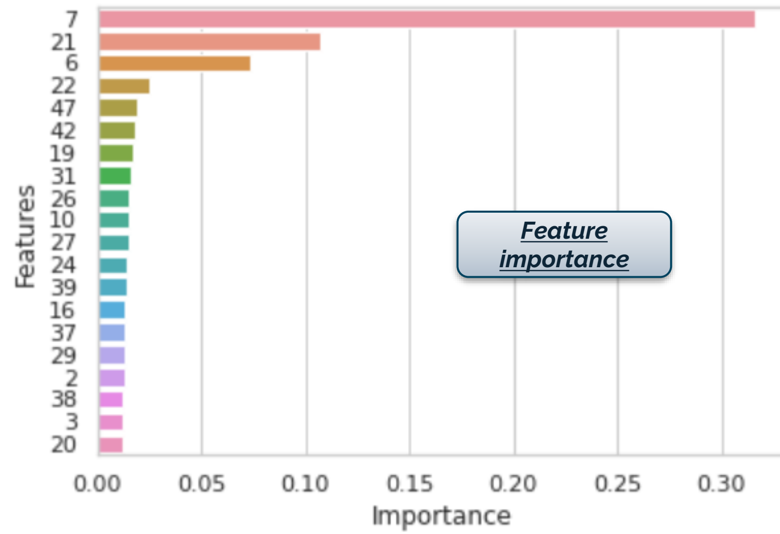
→ *(Somewhat) stable knowledge corpus*
→ *(not so) widely deployed*
→ *Relies on paquet features (or any punctual data)*
→ *Unable to consider connections between machines*
→ *Unable to go beyond projection of past events*

Learning

Key features of ML for cybersecurity

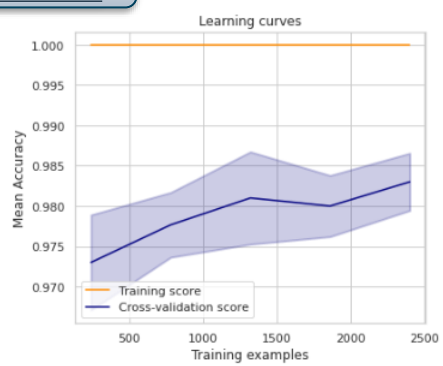


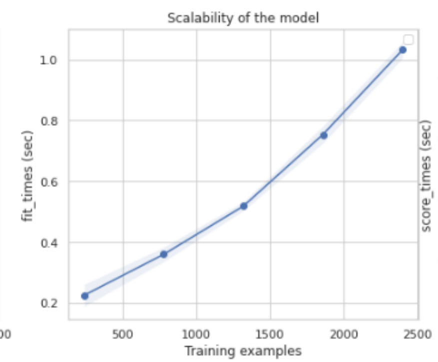
Detection performance

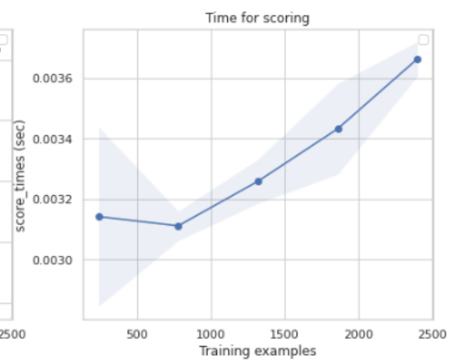


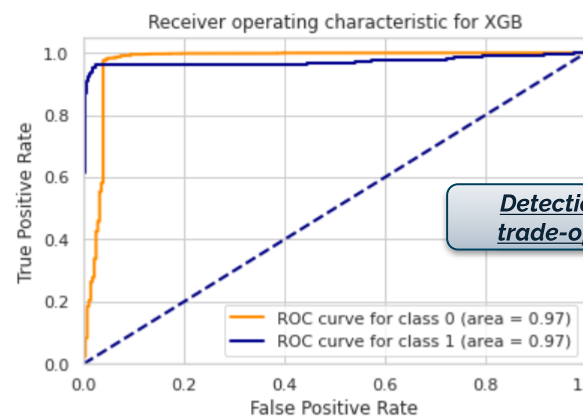
Feature importance

Time performance



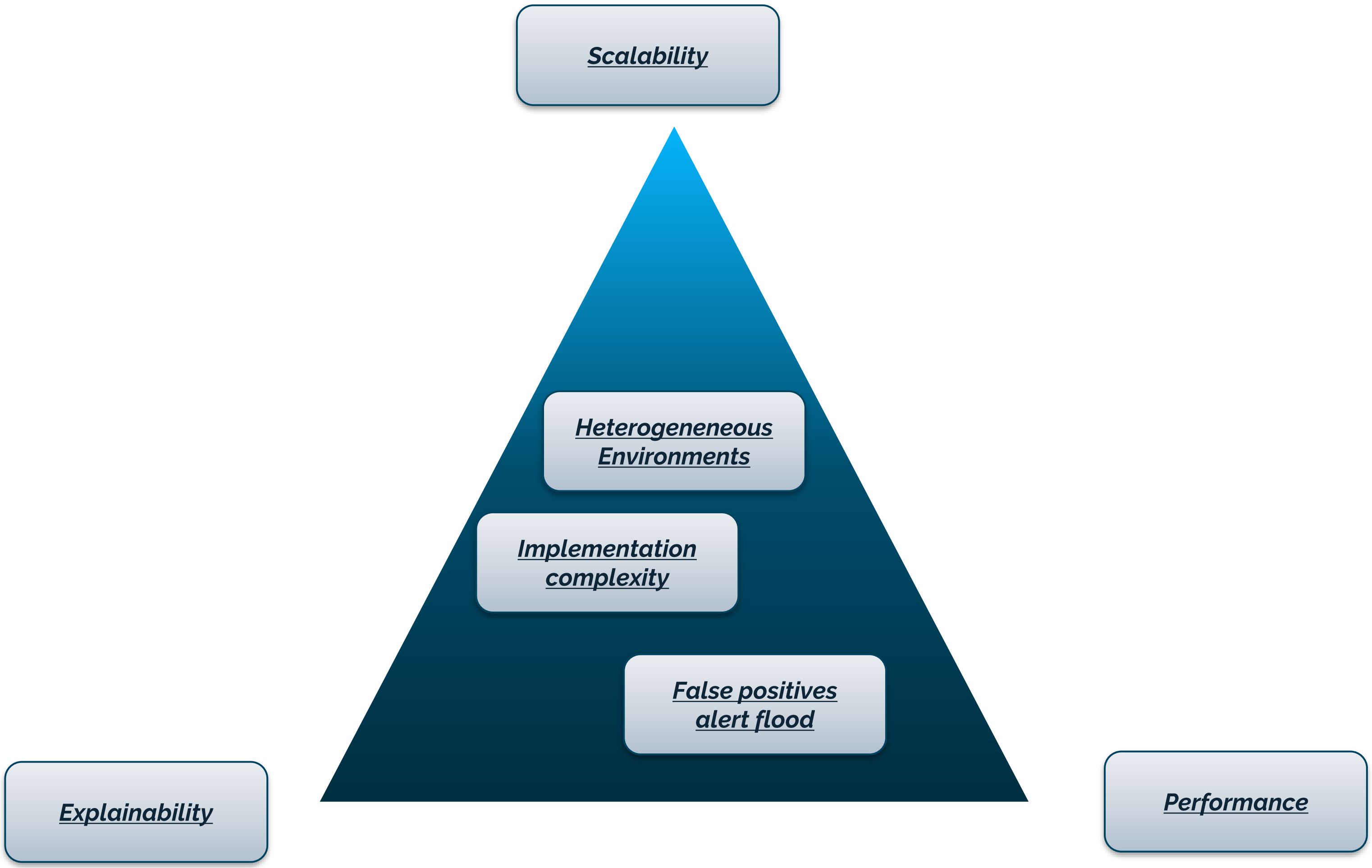






Detection trade-offs

Hard points


Scalability
Heterogeneous Environments
Implementation complexity
False positives alert flood
Explainability
Performance

Open questions

What about:

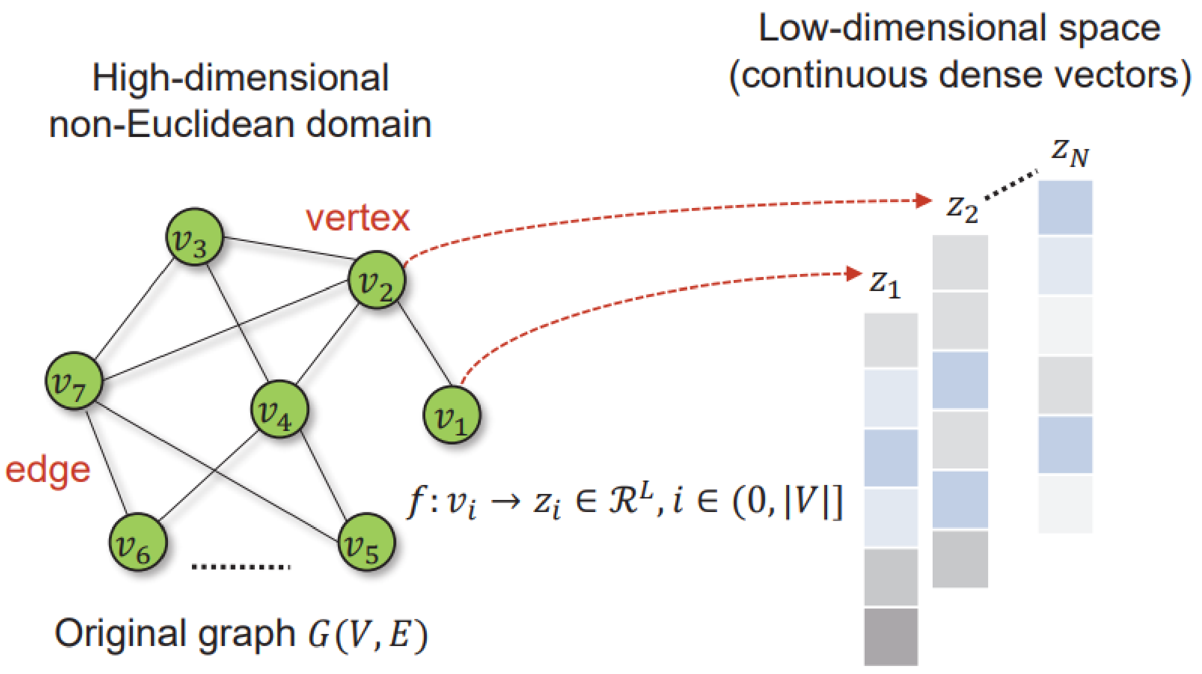
Interactions ?

Scalability ?

Novel attacks ?

Graph learning: Embedding

Principles



Xu, Mengjia. "Understanding graph embedding methods and their applications." *SIAM Review* 63.4 (2021): 825-853.

Embeddings

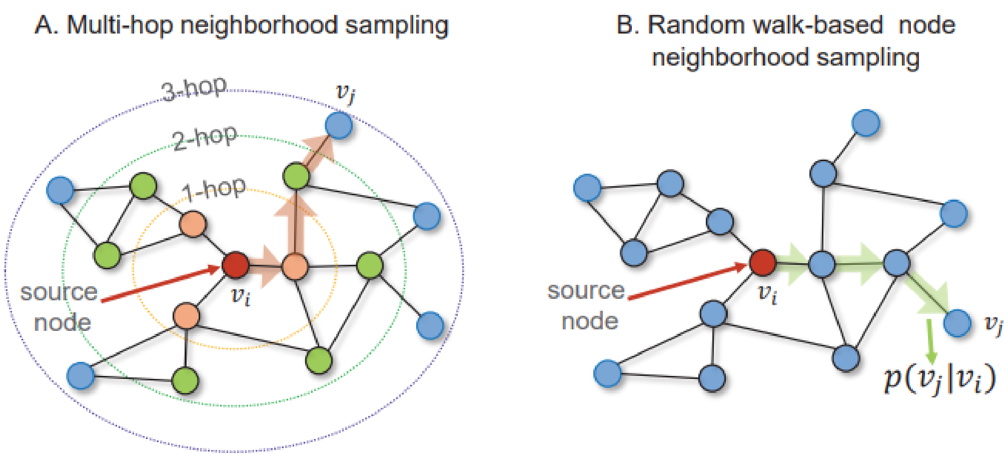
→ Node2Vec, Graph2Vec, GraphSage

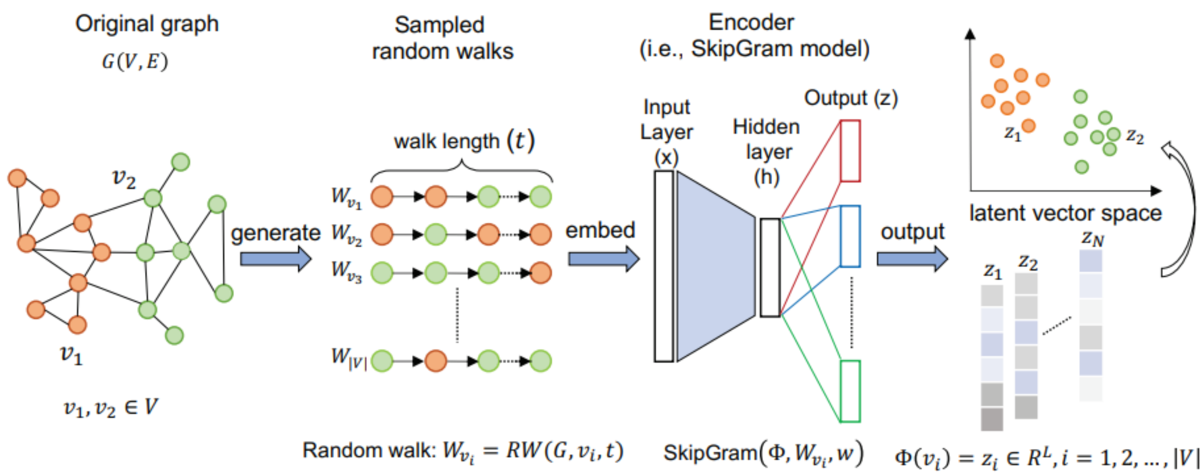
→ Takes the neighborhood into account

→ *Very static approach*

Graph learning: Embedding

Internals

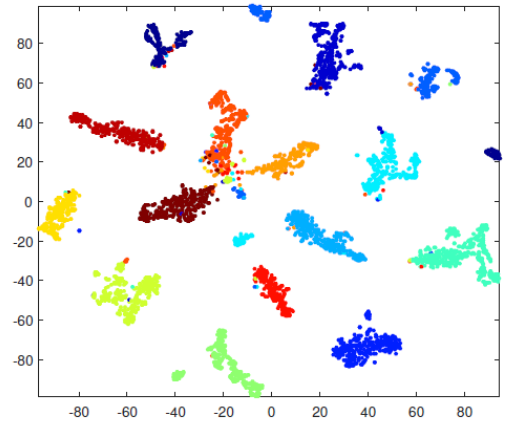




Xu, Mengjia. "Understanding graph embedding methods and their applications." *SIAM Review* 63.4 (2021): 825-853.

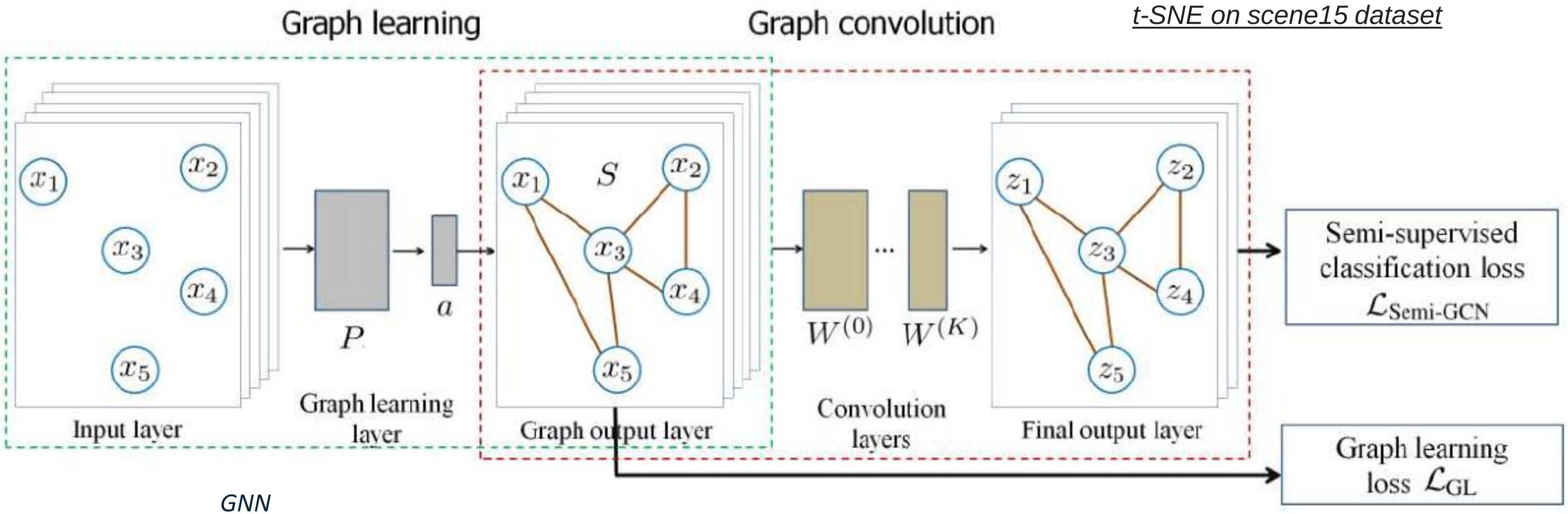
Graph learning with GNN

Unsupervised Detection



t-SNE on scene15 dataset

https://figshare.com/articles/dataset/15-Scene_Image_Dataset/7007177



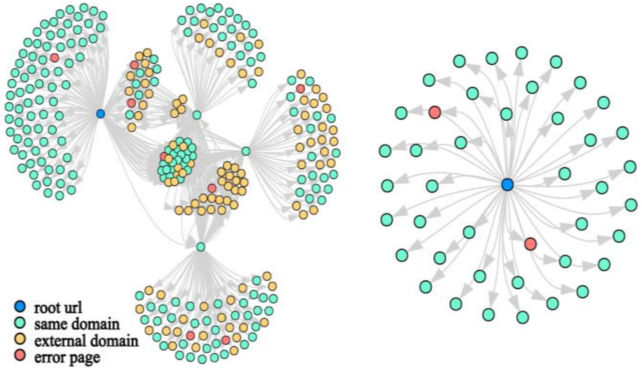
Jiang, Bo, et al. "Semi-supervised learning with graph learning-convolutional networks." *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*. 2019.

GNN

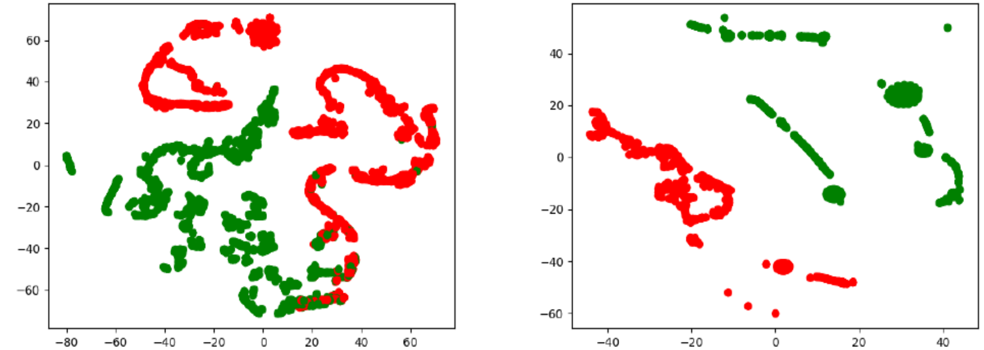
→ Process is very specific to each problem
→ *Graph extraction adds complexity*
→ *Ad hoc Graph learning layer !!*

Yet another application: Phising detection

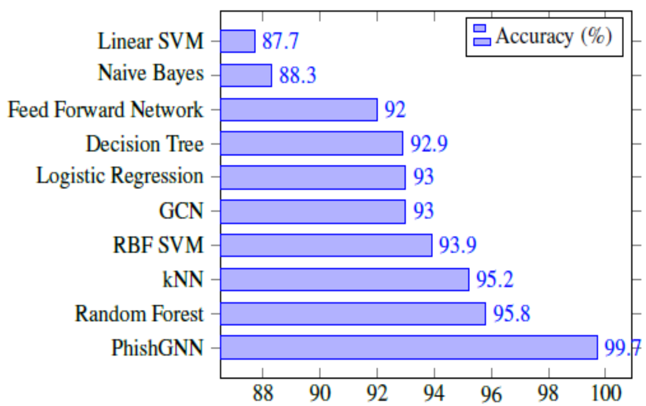
https://github.com/TristanBilot/phishGNN



Graph representation of two websites after crawling with depth=1. Graph on the left contains multiple children URLs already crawled in previous iterations so their children are inserted in the graph as nodes of depth 2. Graph on the right contains children URLs never crawled before. Node in dark blue is the root URL, nodes in cyan and yellow are respectively URLs from the same domain and different domain, while red nodes are URLs returning an error code (HTTP status not in range 200-299)



Embeddings of two models trained on our dataset. GCN2 without PhishGNN framework (left) and with PhishGNN framework (right). Green: Benign; Red: Phishing



Classification accuracies between traditional Machine Learning methods, GCN and PhishGNN

	Benign	Phishing	Total
Benign	688	3	691
Phishing	2	802	804
Total	690	805	1495

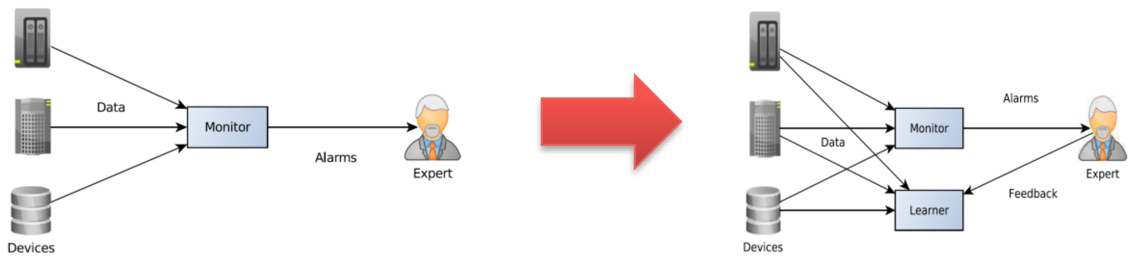
Confusion matrix for a test set of 1495 examples

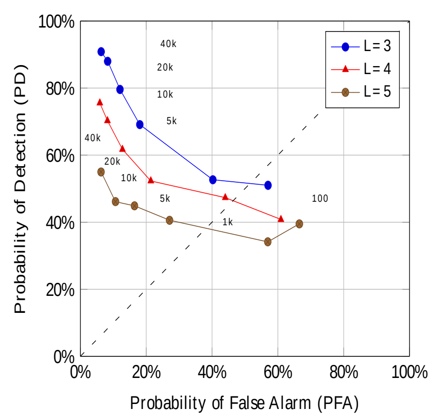
Bilot, Tristan, Grégoire Geis, and Badis Hammi. "PhishGNN: A Phishing Website Detection Framework using Graph Neural Networks." (2022).

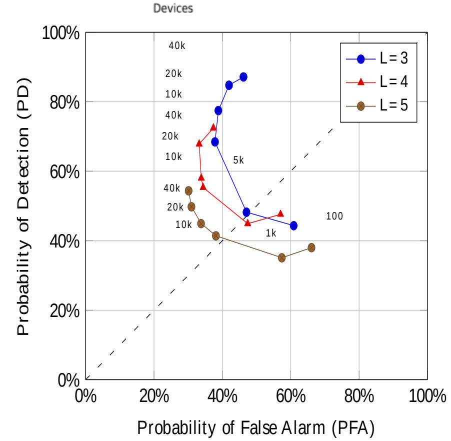
Learning

Learning with human feedback

Attack graphs as daemon detectors





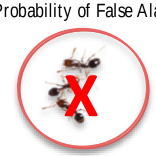


<u>*Morwilog*</u>

→ Stochatic process

→ *Enables to push the border of noiseless detection*

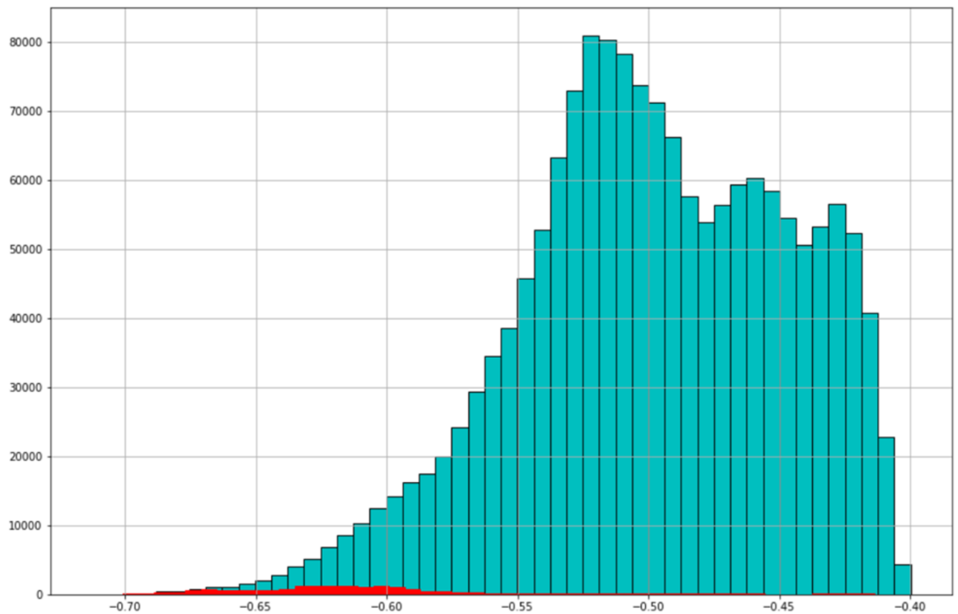
→ *Relies on feedback from human operator, for instance through a dedicated monitoring tool*

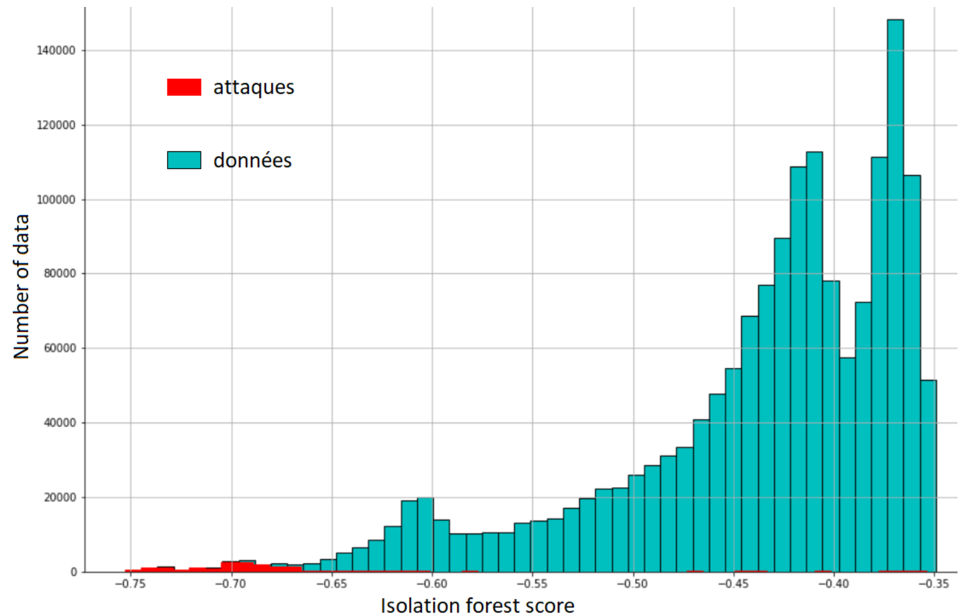


J. Navarro, A. Deruyver, P. Parrend, <u>Morwilog: an ACO-based System for Outlining Multi-Step Attacks</u>, IEEE Symposium Series on Computational Intelligence (IEEE SSCI 2016), Athènes, Greece, décembre 2016

Learning autonomously

Unsupervised learning with isolation forrests and community features





V1:

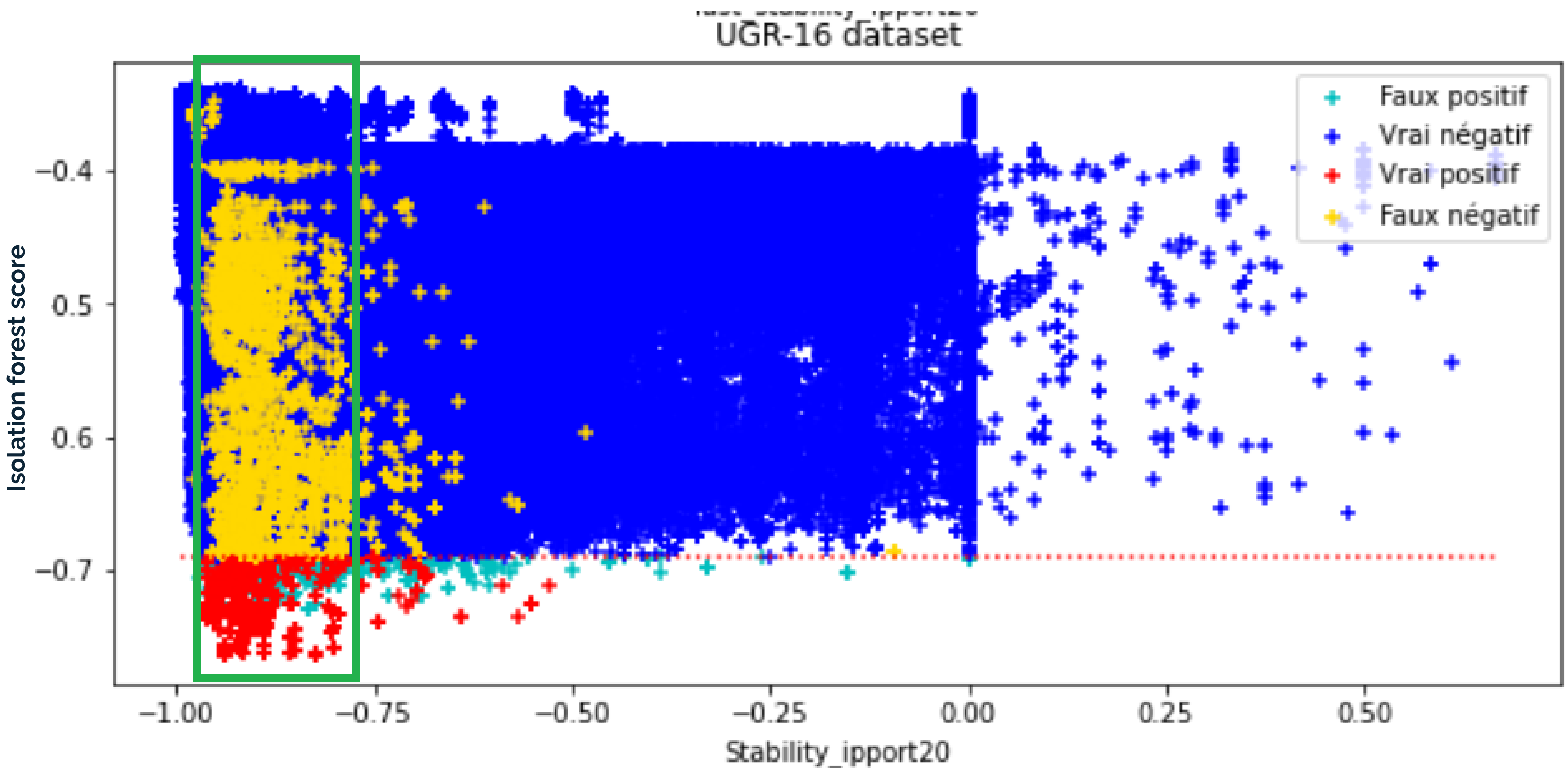
- *Difficulty dissociating attacks from other data by score*
- *Most attacks remain a minority in their detection score range*

V2:

- *Highest detection scores are attacks only*
- *Most attacks are majority in their detection score range*

Learning autonomously

Handling False Positives



Leveraging graphs for learning novels attacks

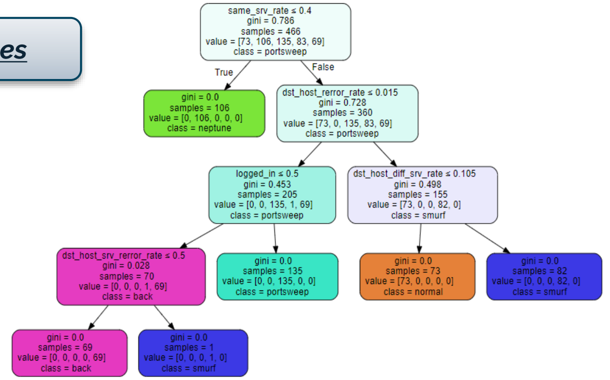
- Reinforcement through human feedback
- Unsupervised learning through discriminating features
- False positive reduction through suitable scoring

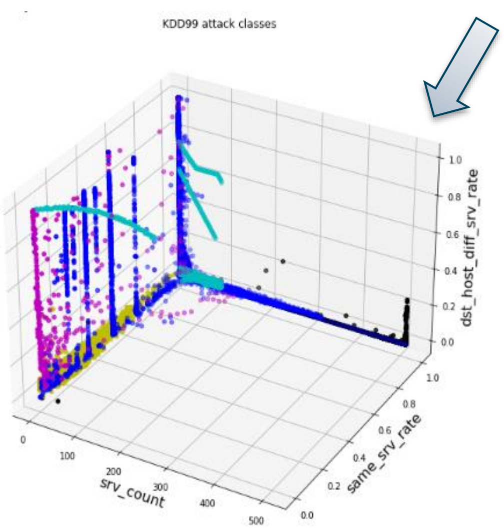
A necessary – and efficient ! – step towards explainable attack detection on heterogeneous networks

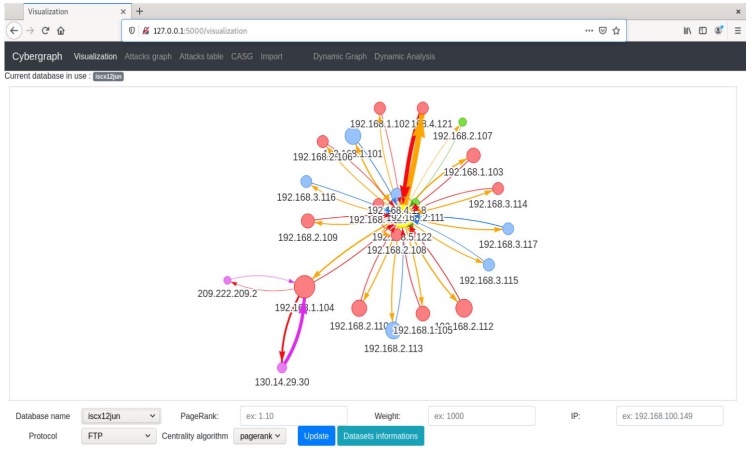
Conclusion

Learning with trust

Decision trees



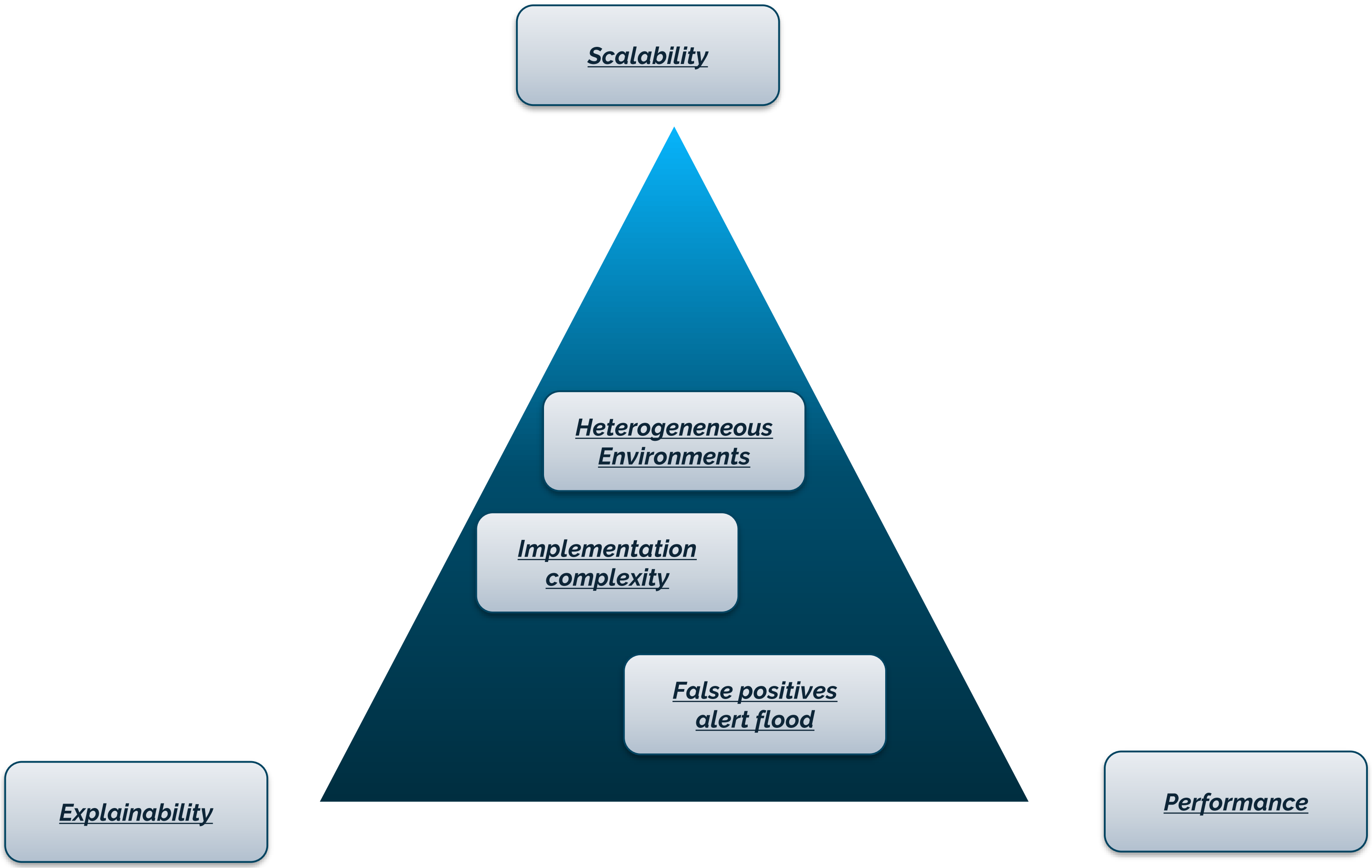




Machine learning

Graph learning

Graph learning proves to be performant for key issues in modeling, detection and learning



Thanks !!

EPITA
ÉCOLE D'INGENIEURS EN INFORMATIQUE