ILAB: An Interactive Labelling Strategy for Intrusion Detection

Anaël Beaugnon, Pierre Chifflier, Francis Bach

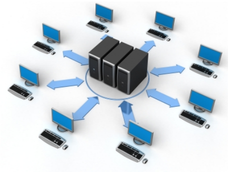
anael.beaugnon@ssi.gouv.fr

ANSSI, ENS Paris, INRIA

RAID 2017

Outline

Intrusion Detection System



Communications

Information System

Detection System

Alerts

Traditional Detection Methods

Precise detection rules built by security experts

- ✓ Easy to control the false alert rate
- ✓ Alerts easy to interpret
- ✗ Not robust to attack variations or new attacks

Traditional Detection Methods

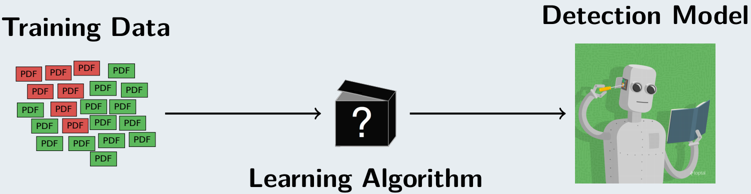
Precise detection rules built by security experts

- ✓ Easy to control the false alert rate
- ✓ Alerts easy to interpret
- ✗ Not robust to attack variations or new attacks

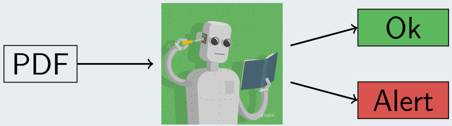
Machine Learning !

Machine Learning

Step 1: Training

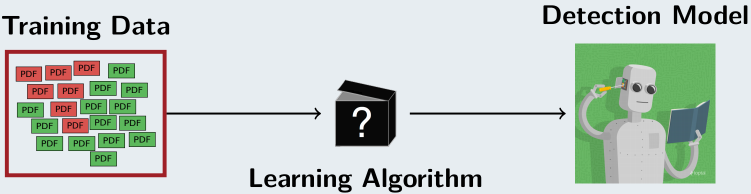


Step 2: Predicting

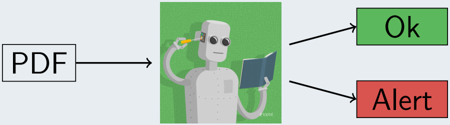


Machine Learning

Step 1: Training



Step 2: Predicting



Lack of Representative Training Data !

- ✗ Public datasets $\neq$ deployment environments
- ✗ Crowd-sourcing is not suited for Computer Security

Lack of Representative Training Data !

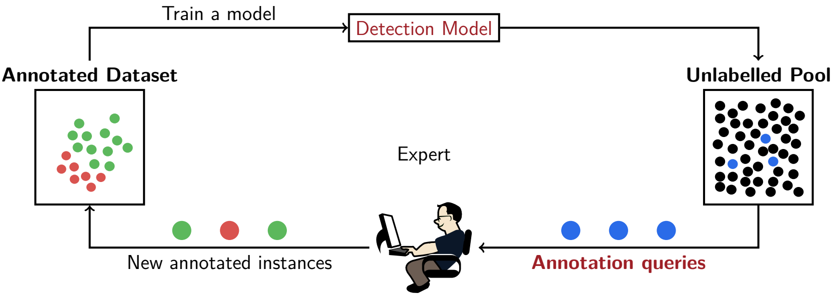
✗ Public datasets $\neq$ deployment environments

✗ Crowd-sourcing is not suited for Computer Security

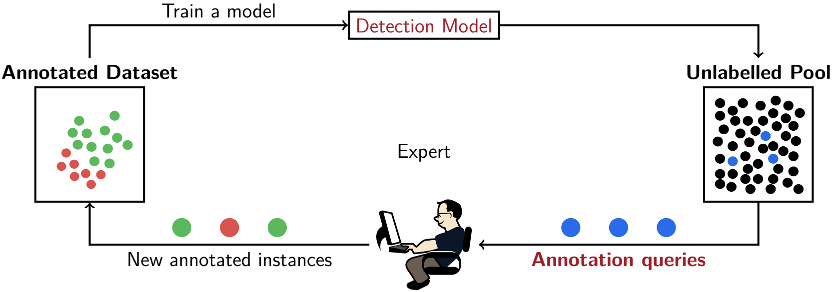
In-situ labelling with Active Learning

Annotate data from the deployment environment

Active Learning



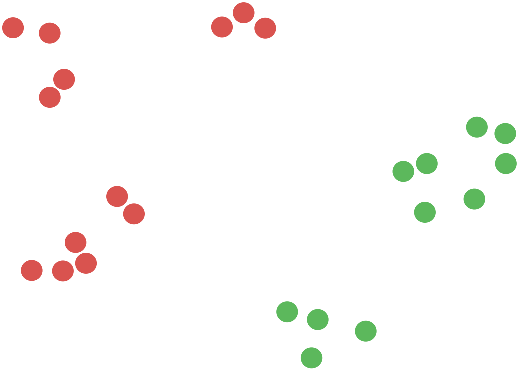
Active Learning



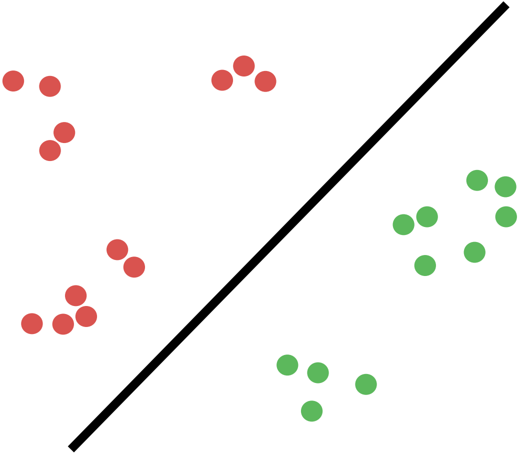
Issues

- Waiting-periods
- Sampling bias

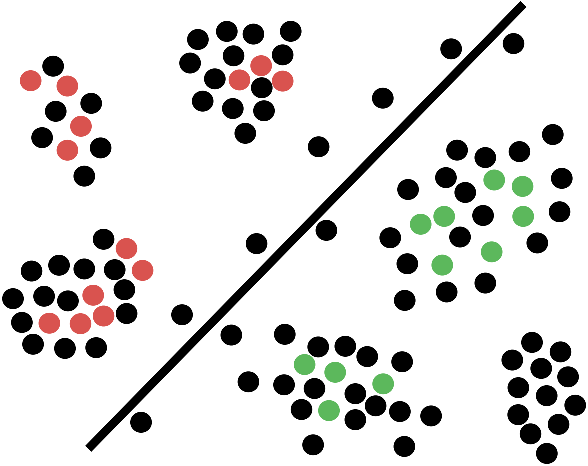
Sampling Bias Issue



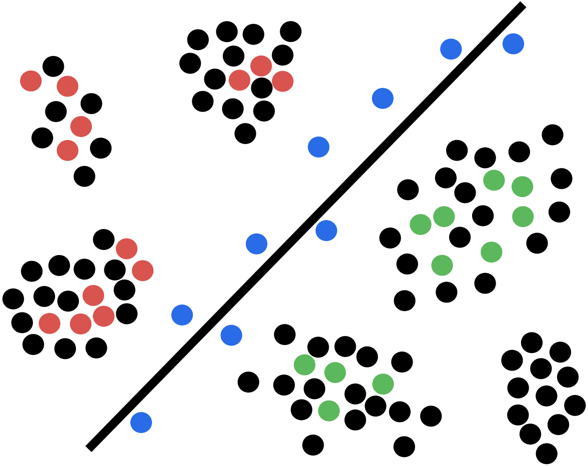
Sampling Bias Issue



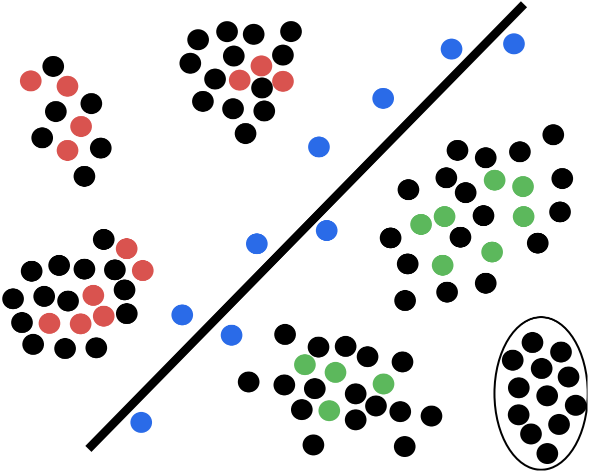
Sampling Bias Issue



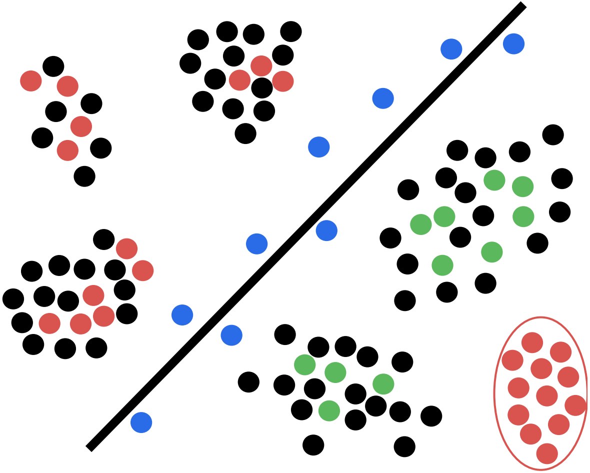
Sampling Bias Issue



Sampling Bias Issue



Sampling Bias Issue



Objective

Maximize the performance of the detection model
for a given expert time spent annotating.

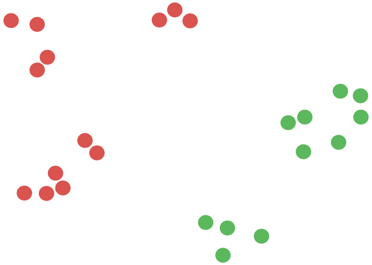
Challenges

1. Avoid sampling bias
2. Maintain short waiting-periods

Outline

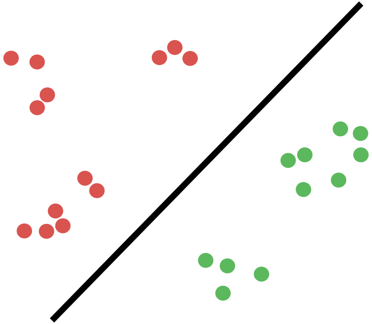
Avoid Sampling Bias

Annotation: label and family



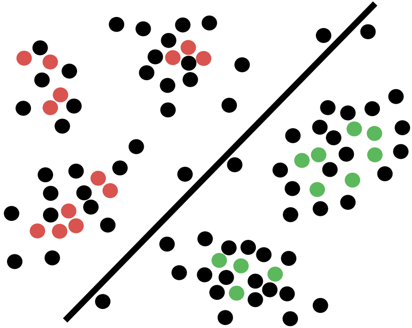
Avoid Sampling Bias

Annotation: label and family



Avoid Sampling Bias

Annotation: label and family

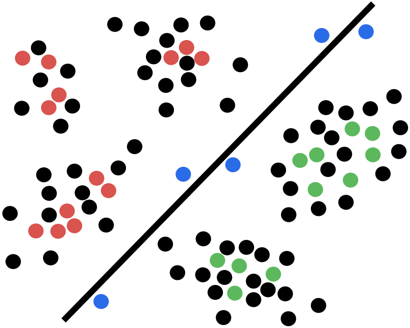


Avoid Sampling Bias

Annotation: label and family

Annotations Queries

- Close to the decision boundary

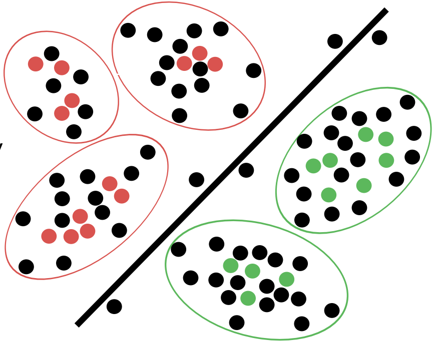


Avoid Sampling Bias

Annotation: label and family

Annotations Queries

- Close to the decision boundary



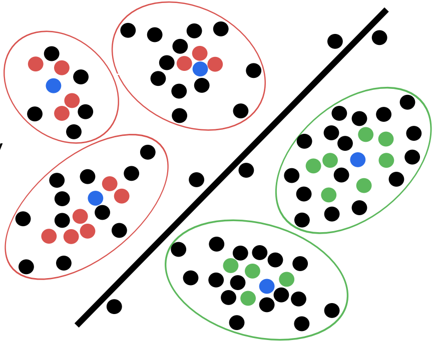
Clusters = User-defined Families

Avoid Sampling Bias

Annotation: label and family

Annotations Queries

- Close to the decision boundary
- Center of the clusters



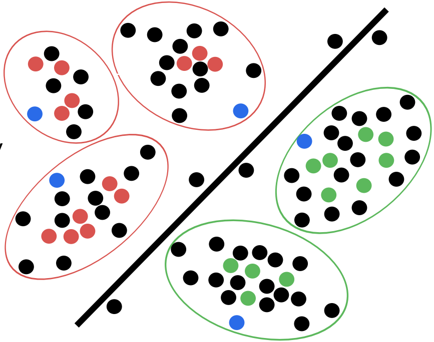
Clusters = User-defined Families

Avoid Sampling Bias

Annotation: label and family

Annotations Queries

- Close to the decision boundary
- Center of the clusters
- Edge of the clusters

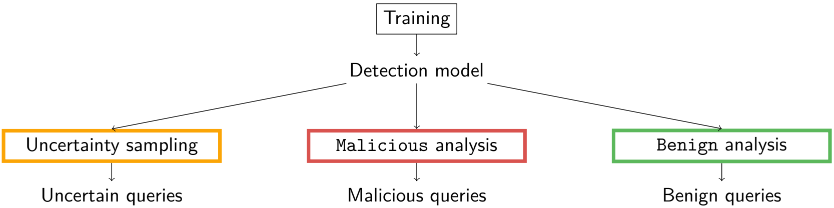


Clusters = User-defined Families

Reduce Waiting-Periods

Divide and conquer approach

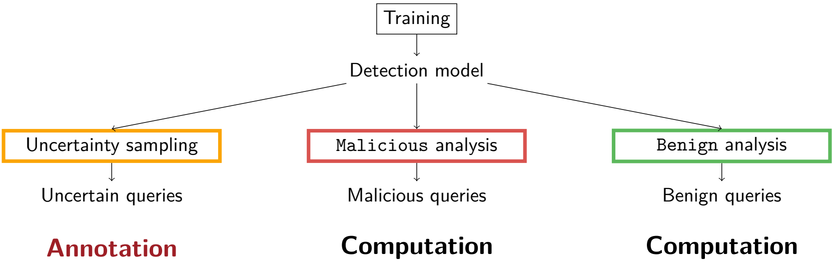
- Reduced complexity
- Annotations during computations



Reduce Waiting-Periods

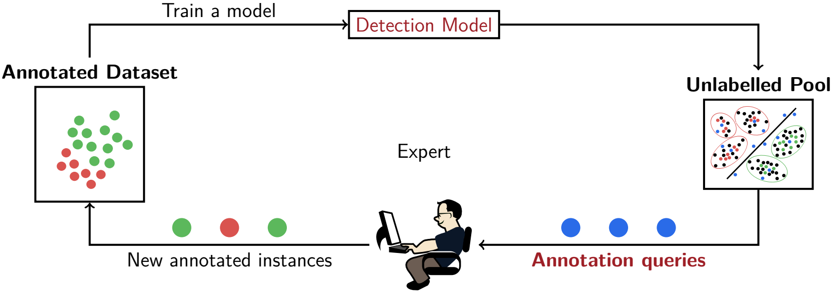
Divide and conquer approach

- Reduced complexity
- Annotations during computations



ILAB Active Learning Strategy

Avoid sampling bias while keeping short waiting-periods



Outline

Comparison with state-of-the-art methods

Simulations on Fully Labelled Datasets

	#instances	#features
Contagio_10%	10,000	113
NSL-KDD_10%	74,826	122

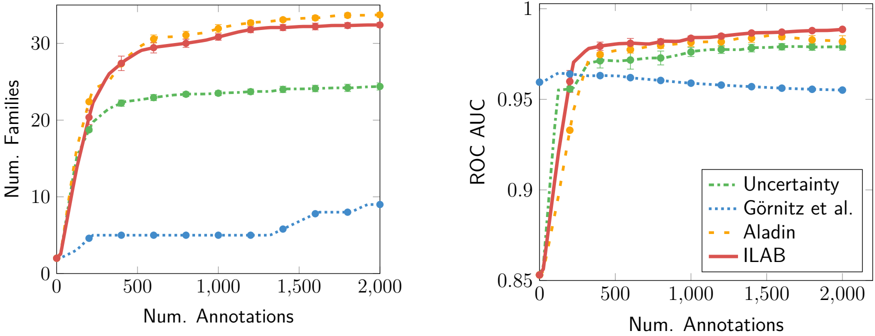
State-of-the-art methods

- Uncertainty sampling [1]
- Görnitz et al. [2]
- Aladin [3]

1 Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004
2 Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013
3 Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008

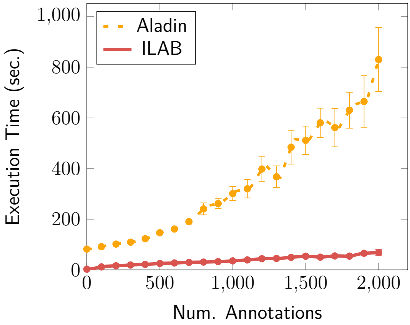
Comparison with state-of-the-art methods

ILAB avoids sampling bias as Aladin.



Comparison with state-of-the-art methods

ILAB induces shorter waiting-periods than Aladin.



Comparison with state-of-the-art methods

ILAB avoids sampling bias while keeping low waiting-periods.

	Uncertainty [1]	Görnitz [2]	Aladin [3]	**ILAB**
No sampling bias	✗	✗	✓	✓
Short waiting-periods	✓	✗	✗	✓

1 Almgren et al., Using Active Learning in Intrusion Detection, CSFW 2004

2 Görnitz et al., Toward Supervised Anomaly Detection, JAIR 2013

3 Stokes et al., Aladin: Active Learning of Anomalies to Detect Intrusions, 2008

Outline

ILAB in Practice

Anomaly detection from NetFlow data

Unlabelled Pool

Num. flows	$1.2 \cdot 10^8$
Num. IP	$463,913$
Num. features	134

ILAB in Practice

Anomaly detection from NetFlow data

Unlabelled Pool

Num. flows	$1.2 \cdot 10^8$
Num. IP	$463,913$
Num. features	134

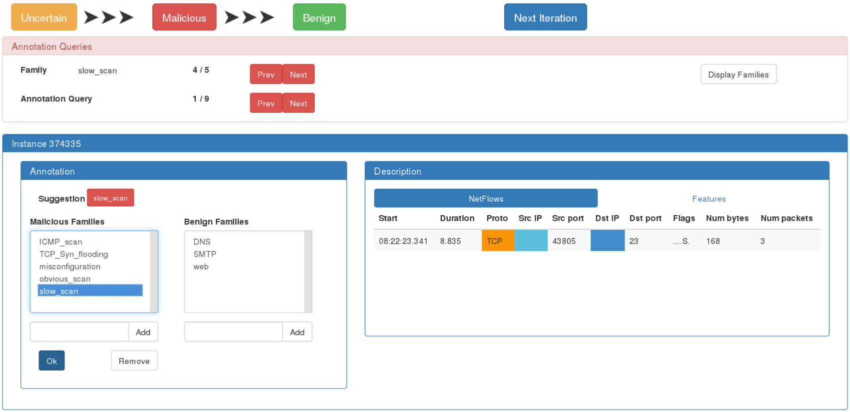
Initial Annotations

- 70 `Malicious`: `Obvious scans` (TRW alerts)
- 70 `Benign`: `Web`, `SMTP`, `DNS` (random sampling)

Only obvious scans: many ports, or many IP adresses are scanned.

ILAB in Practice

ILAB graphical user interface for annotating



ILAB in Practice

Annotation procedure: about 4 hours
10 iterations, 100 annotations at each iteration.

Only 0.21% of the IP addresses are annotated
Only 1,000 IP adresses are annotated out of the 463,913.

Many Families Discovered
`stealthy scans`, `TCP Syn flooding`, `backscatter`, etc.

The expert has spent 99% of his time annotating
The expert has waited less than 40 seconds between each iteration.

An effective Active Learning strategy
for Computer Security experts !

https://github.com/ANSSI-FR/SecuML

An effective Active Learning strategy
for Computer Security experts !

https://github.com/ANSSI-FR/SecuML