framatome

UNIVERSITÄT BIELEFELD

Consideration of Artificial Intelligence for Cybersecurity Aspects of I&C Systems

Ines Ben Zid

Vienna, 12/02/2020

1 . Introduction

2 . Applications

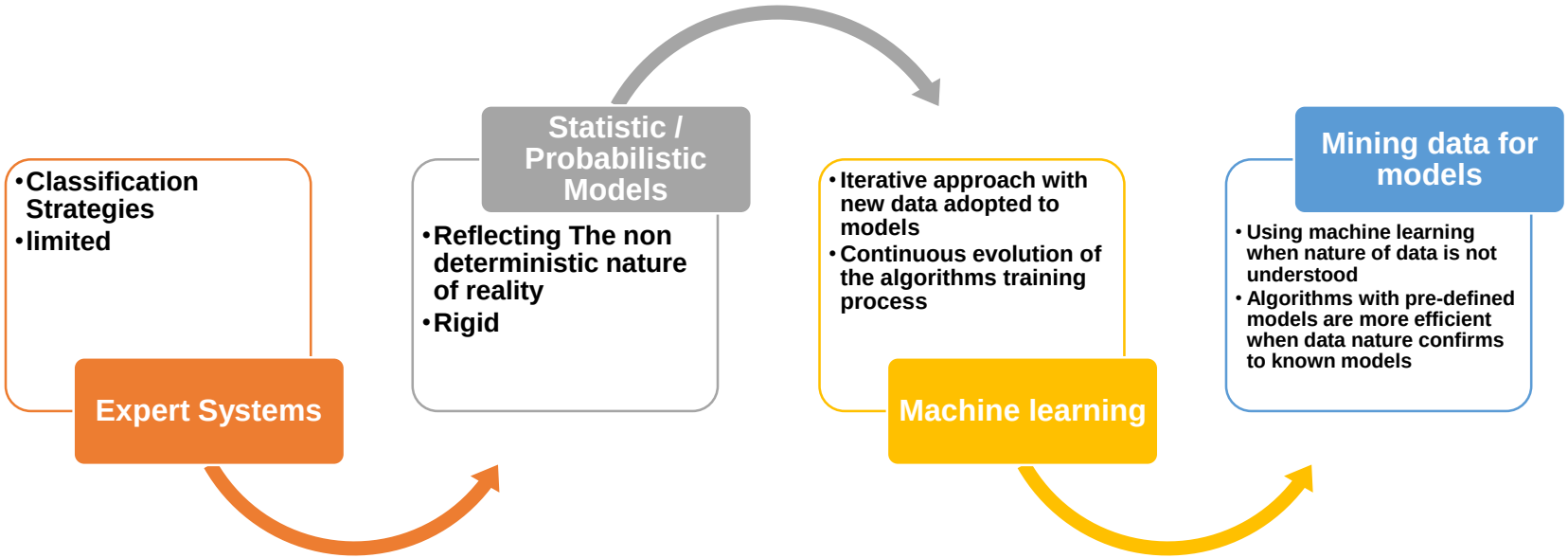
3 . Implementation

4 . Challenges and Boundaries

5 . Conclusion

1 . Introduction

Introduction (1) AI Evolution



Introduction (2) AI for CS

An experimental research area

- Still have some problems
- Results so far are promising

Rising use of autonomous analysis tool

- Rapid response to current and future cybersecurity challenges

2 . Applications

Applications (1)

Create Predictions

- Detecting email cybersecurity threats
- Detecting malware threats
- Detecting network anomalies

Plan Preventions

- Securing user authentication and identification

Take Actions

Applications (2) Creating predictions

Anomalies detection :

- software malware detection
- data stream anomalies
- Intrusion prevention and detection system IPDS
- Avoiding false positive alarms
- Detection of malicious software using

Methodologies:

- Algorithms trained with normal states of the system
- Extension may include classification of alarms and attacks

Applications (3) Planning preventions

Identification and authentication:

checking integrity of acquired information

checking typing patterns on keyboards or computerized handwriting

pattern recognition

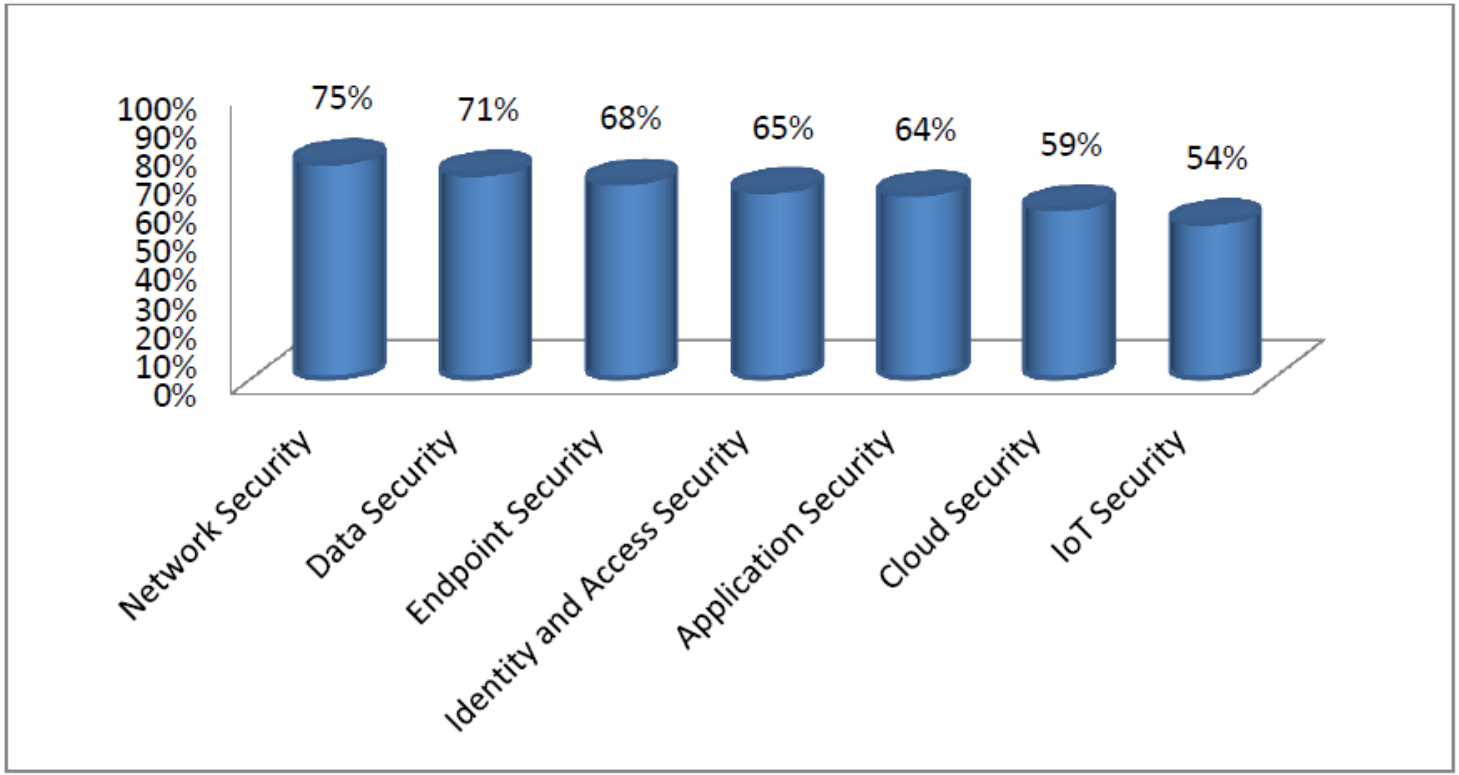
Applications (4) Taking Actions

Continuous evaluation:

Evaluating the algorithms performance and effectiveness

Evaluating the techniques that are potentially exploited by attackers

Applications (5)



3 . Implementation

Implementation (1) Methodologies

Machine learning:

Where the system or network are monitored in order to detect any anomalies as early as possible

Monitoring by analyzing the system features (application Programming Interfaces APIs, accessed hard disk partitions, consumed power)

Types:

The different types of machine learning vary based on the resulting output we want to achieve and the input we are providing

Implementation (2) Machine Learning Types

Machine learning

- Supervised learning
- Unsupervised learning
- Reinforcement learning

Implementation (3) Supervised Learning

Principle:

Algorithms are trained with known Input / Output sets

Through the training, the algorithm will figure out the relationship between the Input / Output

Example:

- Classification algorithms

malware classification; malware signature difference is very minor

Implementation (4) Unsupervised Learning

Principle:

The algorithms must try to classify the data without the aid of a previous Output provided by the analyst.

In the context of cybersecurity, unsupervised learning algorithms are important for malware attacks, frauds, and email spamming campaigns that are being detected for the first time.

Example:

Clustering (Hierarchical Cluster Analysis)

Implementation (5) Reinforced Learning

Principle:

A strategy that emulates the trial and error approach

The learning process is based on assigning either a positive or a negative reward at the end of the learning path and eventually at the end of the learning process

Example:

Markov process / Hidden Markov Models : detection of plymorphic malware threats.

Implementation (6) Integration

Specific awareness within the organization have to be recognized.

This awareness concerns mainly software requirements and their configuration.

The continuous monitoring and the scalability of the AI-based solutions has to be planned

4 . Challenges and Boundaries

Challenges and boundaries (1)

Trying to detect something which is not clearly known or defined

- This aspect usually rises the complexity of the anomaly detection tool which is an inevitable challenge

Examine the potential implications related either to the used method itself or the consequences of its deployment on the security posture of certain systems

- new vulnerabilities as well as new attack vectors created within either the office IT systems, the production OT systems or the used AI system itself

Challenges and boundaries (2) Criteria

The system

- The system characteristics, capabilities and capacities

The Integration

- The limitations and assumptions regarding the integration of the method

The security

- The associated security considerations (third party, supply chain, etc.)

The purpose

- The purpose to be served through the algorithm

Challenges and boundaries (3) Criteria

The two most important requirements we can state here are:

- the choice of the AI technique / algorithm
- the input data

Acquiring the right and especially most up to date input data for the learning algorithm can present some difficulties which will have an influence on the performance of the method.

5 . conclusion

Conclusion

- Artificial Intelligence for cybersecurity of I&C system shows promising results, especially with the shifting towards digitalized and intelligent infrastructures.
- There is a need to integrate the skills and knowledge that can meet with this advance
- Expert – machine conflict ?

It is rather a harmony of skills

AI tools: take care of the “exhausting” part that is the analysis of enormous amounts of data

Specialists / Experts: examine the highlighted threats which require more attention and studying

framatome