TELECOM SudParis

INSTITUT Mines-Télécom

Detecting threats in cloud environments

Pamela Carvallo

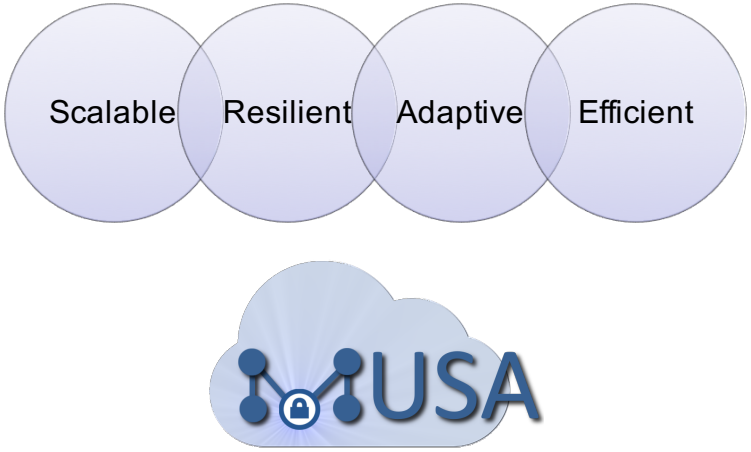
PhD Student

Advisor: Prof. Ana Cavalli

université PARIS-SACLAY

Motivation

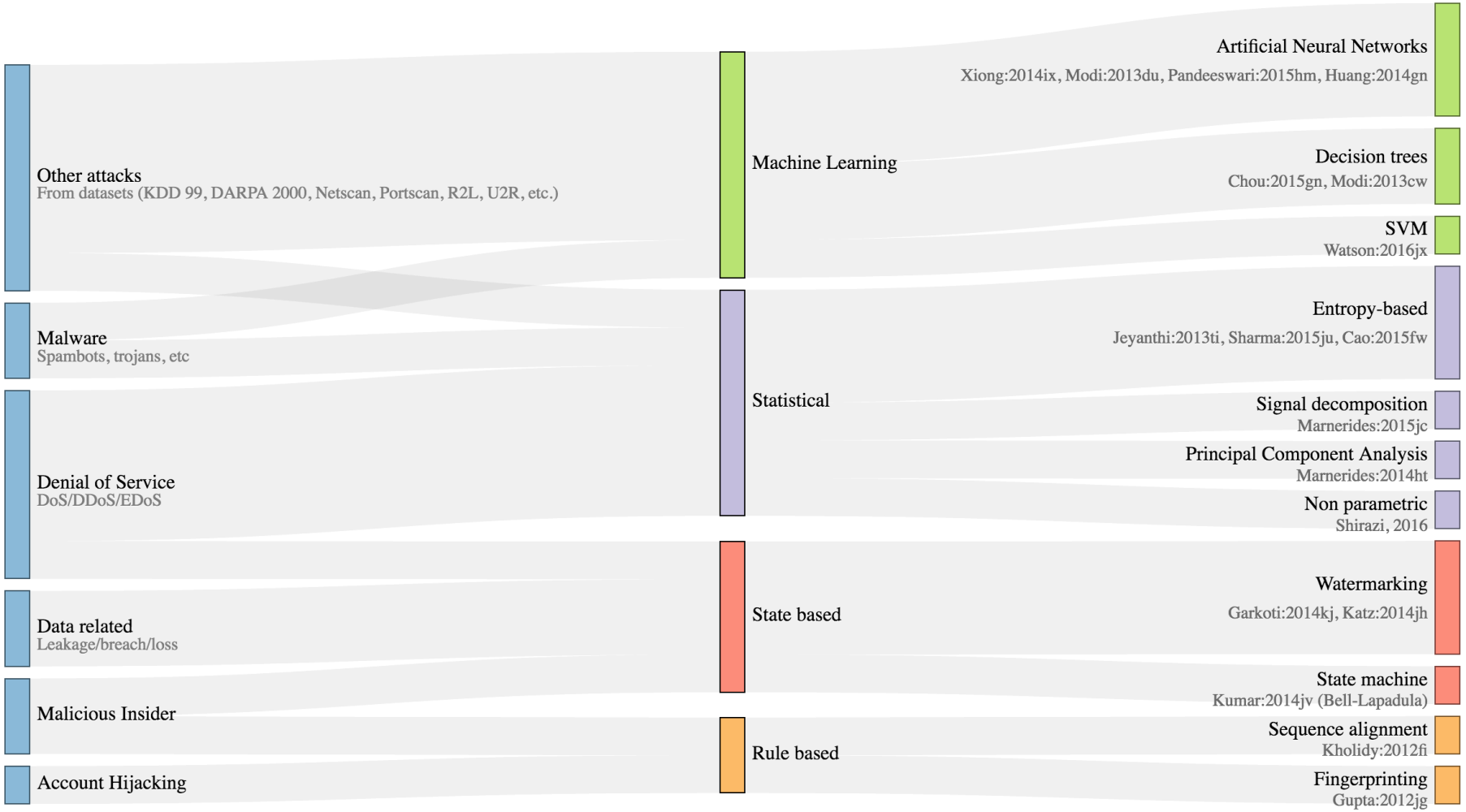
- Threats will come
- Cloud is attractive but security is one of the main obstacles
- Deploying more efficient threat detection systems in cloud is essential



Work planning

- **To study state of the art - Survey's contribution**
  - Establish a closer relationship between threats and detection techniques
  - Compare detection techniques suitable for cloud
- **To contribute to the existing techniques and tools -Detection systems**
  - Approaches
    - Signature-based
    - Behavior-based
      1. Sensor positioning and collecting
      2. Processing
      3. Training / Testing
      4. Prediction
  - Architecture

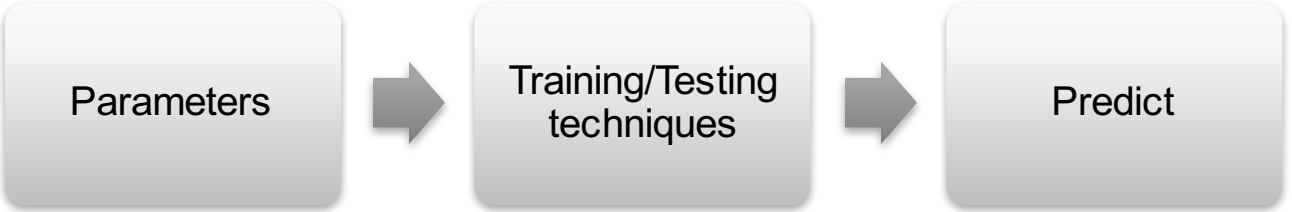
Current results – a closer relationship between threats and existing detection techniques



Next steps (short term) – for survey

- **Perform some experiments of *some* techniques for *some* threats**
  - Which threats?
  - Which techniques?
- **What if some edges can be added to established relation?**
  - Which techniques were not used for which threats?
  - Why is it?

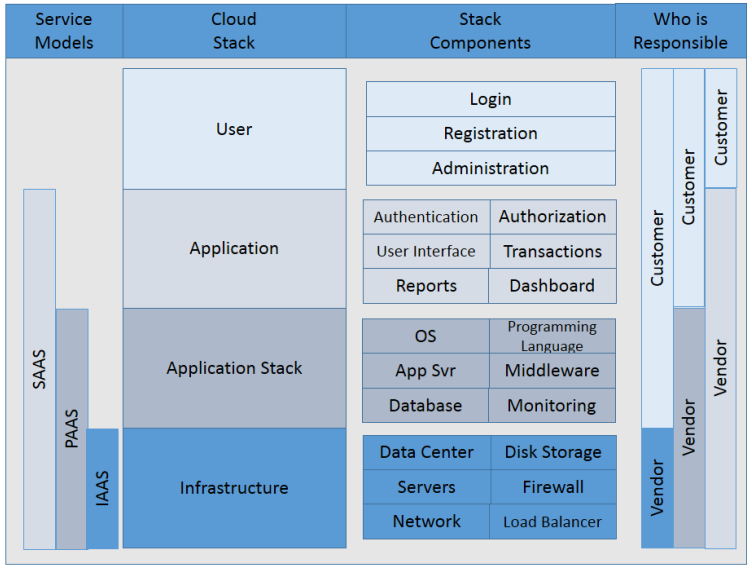
One of the problems statements of the thesis – threat prediction issues



What / Where to collect

Which technique(s) and which tests

How / When / Where



Questions, comments

Thank you!