Karlsruhe Institute of Technology

TECHNISCHE UNIVERSITÄT BERGAKADEMIE FREIBERG
The University of Resources. Since 1765.

Attack Forecast and Prediction

Kaiser Florian; Budig Tobias; Goebel Elisabeth; Fischer Tessa; Muff Jurek; Wiens Marcus; Schultmann Frank

Introduction

- Attackers seem to have a *first mover advantage*[1] in a „*dynamic cat and mouse game*“[2]
- A main goal should be the minimization of this first mover advantage - Attack forecasting and prediction however is only hardly used[3]
- Projecting and predicting future developments furthermore is oftentimes based on experiences, subjective perceptions and gut feelings of experts
  - Prone to biases
  - Time consuming
- Low levels of automation in attack forecasting

Motivation

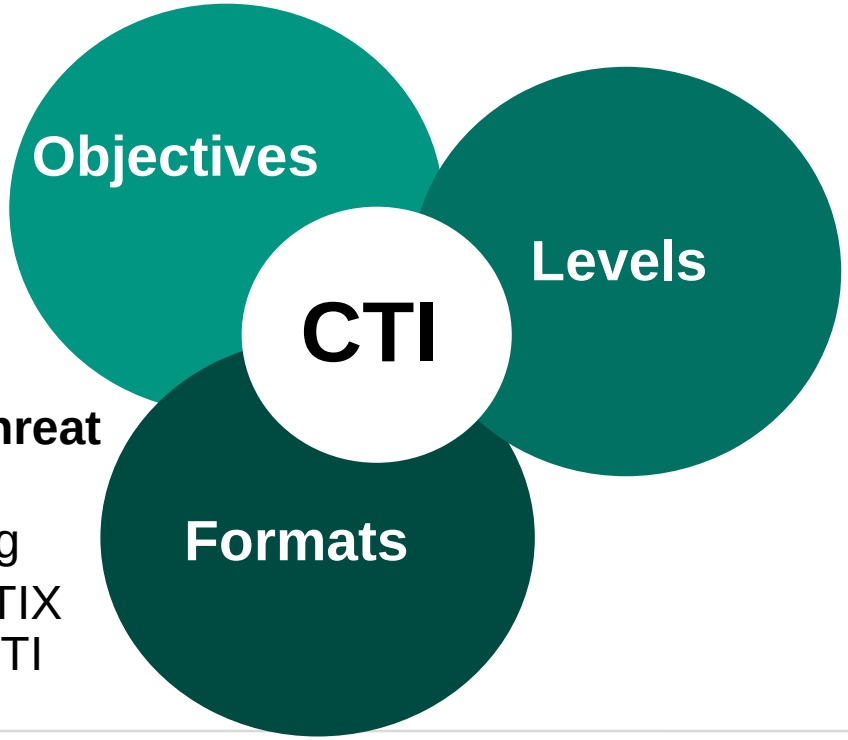
- “Although many solutions have been proposed, there is still no definite answer on how to effectively and precisely predict cyber attacks.”[3]
- Predictions mainly focus on a short term horizon rather than a medium- to long-term horizon
- Attack prediction and forecasting “is still an open and an imperative, desirable research problem”[3]

Cyber Threat Intelligence

Cyber Threat Intelligence (CTI) defines structured, actionable information for identiying adversaries and their motives, goals, capabilities, resources and tactis.[2]

- Powerful means of **increasing** the **efficiency** and **automation** of various security solutions
- CTI can be used for automated reasoning (**data driven analytics**) in cyber risk management

→ Threat Hunting; Attack detection; Attack prediction; Forensic investigations



- Technical CTI
- Operational CTI
- Tactical CTI
- Strategic CTI

- Importance of CTI lies in itst ability to **share threat information** among partners [2]

→ *steamlined* and *structured* information sharing

→ Structured Threat Information eXpression (STIX language) as a standard language for sharing CTI

Research objectives

- Can any patterns or trends be extracted form CTI and used for crafting strategic medium to long term predictions on the threat landscape?

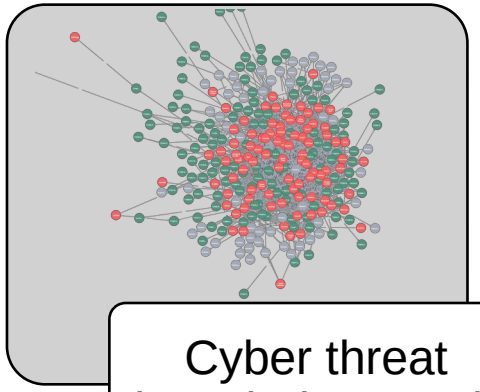
- How do different algorithms perform to predict future malware in a medium to long term?

- Can graph analytics be used to increase automation and precision in attack prediction and forecasting

Contributions

i. Utilizing CTI to **infer automatically** and **improve hypotheses on new attacks**
ii. Achieving a **higher level of automation** by automatic construction of hypotheses, supporting the analyst‘s decisions, saving scarce time
iii. Improving the **accuracy of hypotheses** provided by an analyst (minimizing biases due to subjective perspectives)
iv. Providing medium- to long-term predictions

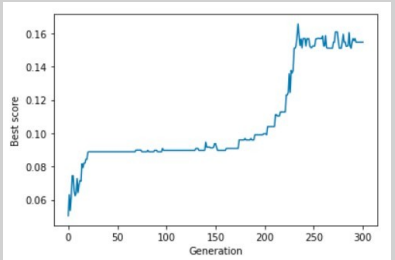
Methodology



Cyber threat knowledge graph

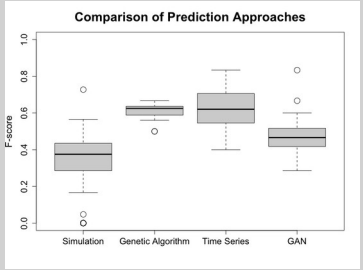
Generating test and training dataset

	2017	2018	2019	2020
T1548.002	0.006390	0.00468	0.003799	0.003361
T1134	0.001597	0.00156	0.001899	0.001681
T1134.002	0.000000	0.00078	0.004748	0.001681
T1134.001	0.001597	0.00156	0.000000	0.003361
T1087.002	0.003195	0.00234	0.001899	0.000000
...	...	...	...	...



Attack Forecast and Prediction

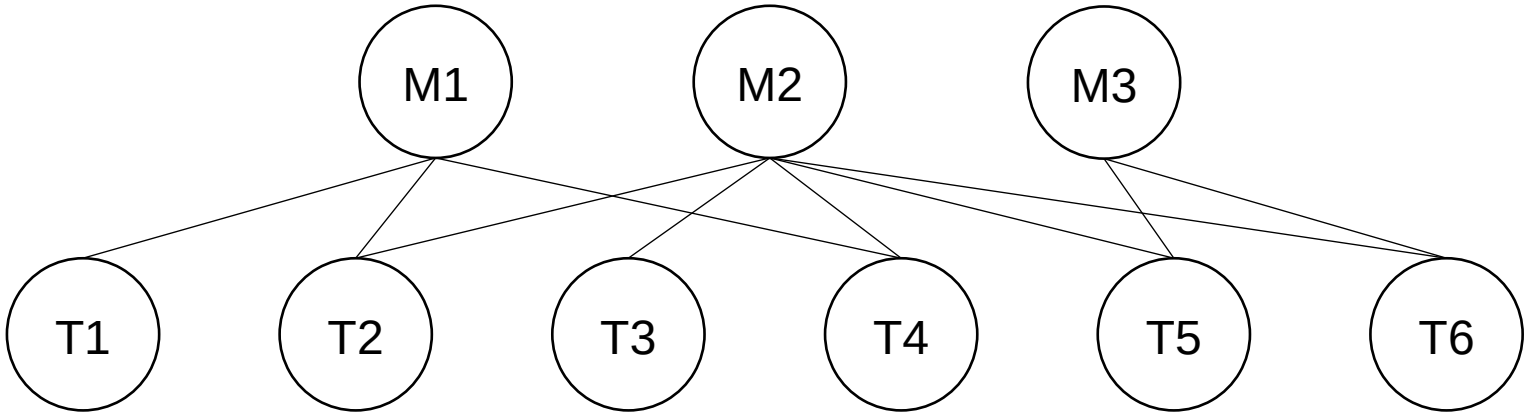
Evaluation



Cyber Threat Knowledge Graph

- Multi-level threat ontology based on CTI scraped from MITRE ATT&CK
- Analyzed relying on different algorithms for graph analytics for crafting attack predictions and forecasts

- Each Malware (M) can be described as a combination of techniques (T)



Statistics

- MITRE ICS, Enterprise & Mobile

- 13 tactics
- 552 techniques
- 585 different softwares (malwares)

Dataset splitting

- Excluded „degenerated“ malware
  - 449 remaining attacks – malware

- Data was time sorted

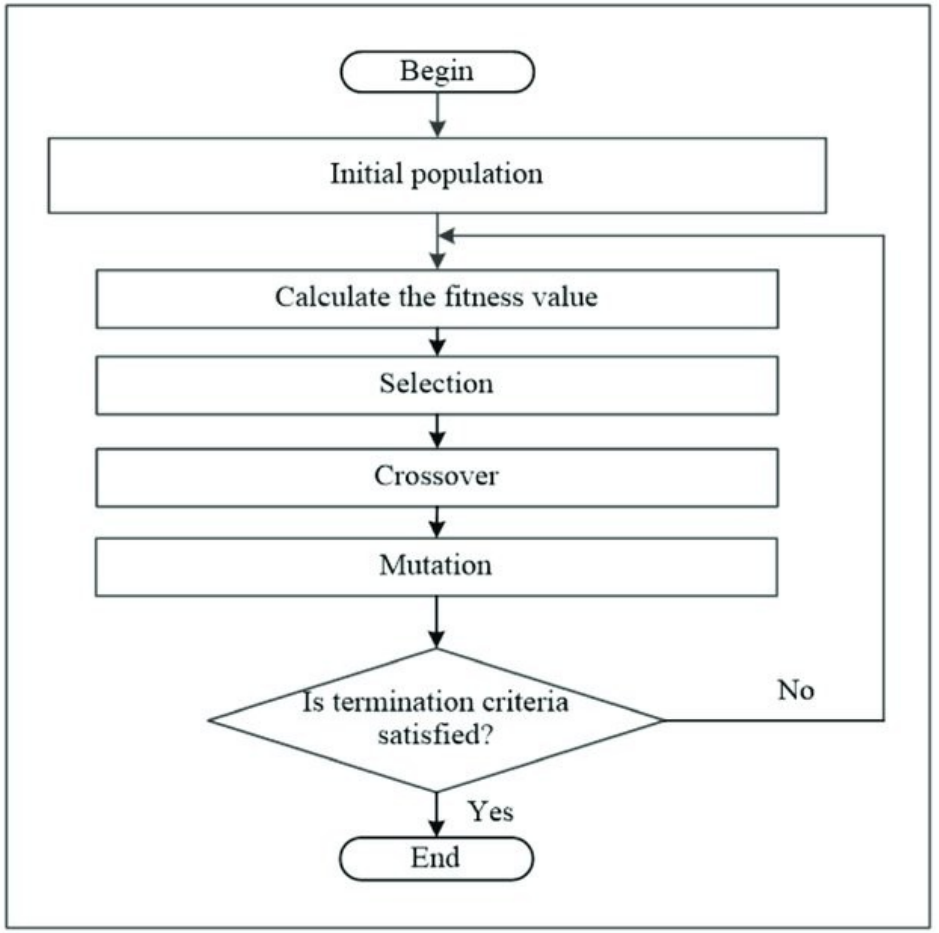
- 80/20 - splitting
  - Training set: 358 oldest attacks of
    - 31.5.2017 - 10.6.2020
  - Test/ evaluation set: 91 newest attacks
    - 10.6.2020 - 13.4.2021

Algorithms for forecast and prediction generation

- Classical graph analyric algorithms
  - Hierarchical Clustering
  - Principal Component Analysis
  - Time series and regression analysis

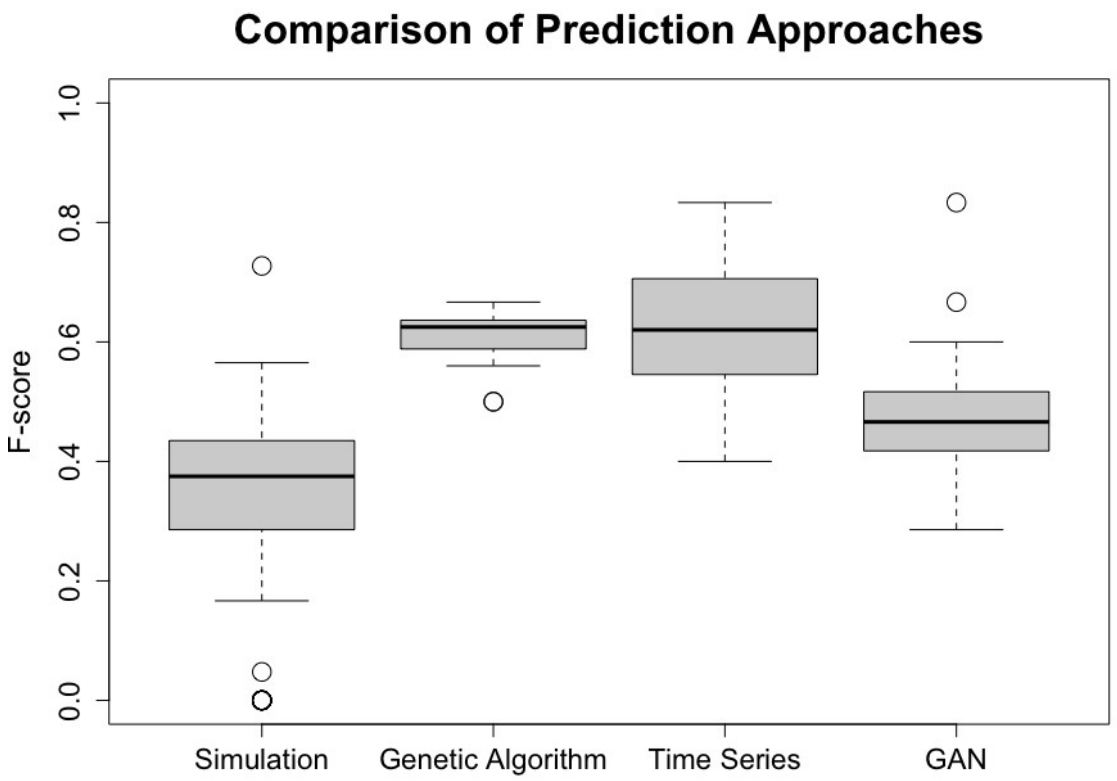
- Genetic algorithms
  - Fitness derived from technique utilization as a proxy for the promissed utility (frequency & correlation)
  - Roulette wheel selection & tournament selection
  - Uniform crossover, one point crossover, two-point crossover

- Neural network
  - Generative adversial network



Evaluation

- Walk forward validation (1 year ahead)
- Test dataset consisting of historic attacks from since 2020
- F-Score
- Baseline
  - „Simulation“ – extrapolation based on current observations



Conclusion

- AFP is an **automated attack predictor** able to **forecast** new malware developments
- Showed and validated the predictive power based on walk forward validation with **a time horizont of one year**
- Predictions are not exact rather, **real software deviates slightly from most predictions**
- AFP increases cyber security maturity and cyber situational awareness through ist high predictive capability
- The results of AFP can be used to prepare proactively for future attacks and improving investment decisions/ research spending of defenders, develop security measures **before they were observed in the wild**.
- AFP suffers from data quality and low data availability

M. Sc. Florian Kaiser

Research Associate
Karlsruhe Institute of Technology (KIT)
Institute of Information Security and Dependability &
Competence Center for Applied Security Technology
(KASTEL)

florian-klaus.kaiser@kit.edu

Thank you for your attention

References

[1] Hausken, K., & Bier, V. M. (2011). Defending against multiple different attackers. European Journal of Operational Research, 211(2), 370-384.

[2] Elitzur, A., Puzis, R., & Zilberman, P. (2019, November). Attack hypothesis generation. In 2019 European Intelligence and Security Informatics Conference (EISIC) (pp. 40-47). IEEE.

[3] Husák, M., Komárková, J., Bou-Harb, E., & Čeleda, P. (2018). Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials, 21(1), 640-660.