MUNI
C4E

Graph-based models in prediction and projection of cyber attacks

The 1st International Workshop on Graph-based network Security

Martin Husák
husakm@ics.muni.cz

Institute of Computer Science, Masaryk University

April 24, 2020

Section 1

Introduction

Presenter's Biography

Martin Husák, Ph.D.

- Researcher at Institute of Computer Science, Masaryk University, Czech Republic
- Member of **CSIRT-MU**, university's cybersecurity team (`https://csirt.muni.cz/?lang=en`)
- Formerly a visiting research at Florida Atlantic University, USA
- Contributor to The Honeynet Project

Research Interests

- Network security – traffic monitoring, honeypots, intrusion detection
- Operational security – incident response, CSIRT operations
- **Cyber situational awareness** – information sharing, **attack projection**

Outline

Section 2

Graphs and Security

Use Cases

How are graphs used in cybersecurity?

- **Attack graphs** are used for modeling attacks
- Topology graphs are used for modeling the networks we defend
- Connection graphs allow detection of malicious patterns
- Dependency graphs show critical systems and their dependencies
- **Alert correlation** can use graphs
- ... and many other applications

Use Cases

What can we model using the graphs?

- Attacks
  - Attack graphs
- Defenses
  - Network topology graphs
  - Critical missions and dependencies
- Events
  - Network connection graphs
  - Alert correlation
- Combinations of everything
  - Graph-based models for cyber situational awareness

Modeling the Attacks

Attack Graphs

- Models of attacks with many forms and existing extensions
- Useful for security assessment and strategic decisions
- More on that later in this talk

Modeling the Defenses

Network topology graphs

- Very common for networking operations, useful also for security
- Which host is connected where?

Missions and dependencies

- Enterprise missions / business processes and their dependencies
- Which hosts and service in the network are critical for the organization?
- Critical for prioritization of actions and modeling attack impacts

Modeling the Events

Network connections graphs

- Graph-based representation of network communication
- Who talked to whom?
- Useful for anomaly or intrusion detection, e.g., scanning, botnet activity

Graph-based Alert Correlation

- Attacker's action from the perspective of a defender
- Graph-based representation of relationships between alerts from IDS
- More actionable for operational cyber defense

Modeling Everything

Cyber situational awareness

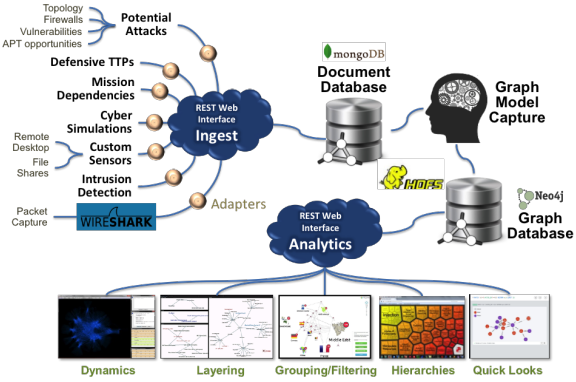
- **Perception** of the elements in the environment,
- **Comprehension** of the situation,
- **Projection** of future state and events

Proposed tools and models

- CyGraph, CAULDRON, ... (MITRE)
- VirtualTerrain (Rochester Institute of Technology)
- CAMUS, M2D2, and many others

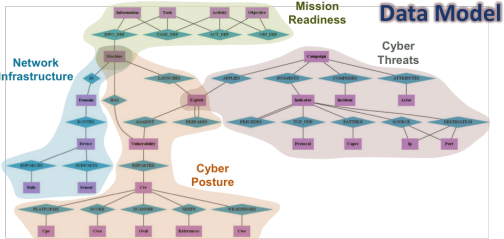
CyGraph

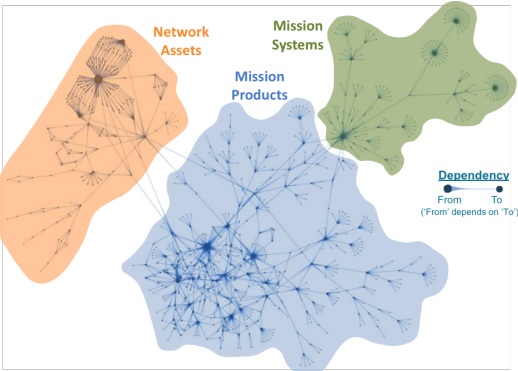
- Graph-based data model for cyber situational awareness
- Detailed representation of almost everything in the network
- Cooperates with other tools by MITRE



S. Noel et al. CyGraph: graph-based analytics and visualization for cybersecurity. In Handbook of Statistics. 2016

CyGraph



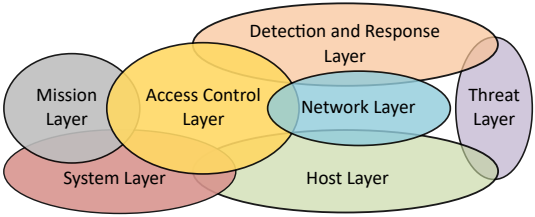


https://neo4j.com/blog/cygraph-cybersecurity-situational-awareness/

CRUSOE Project

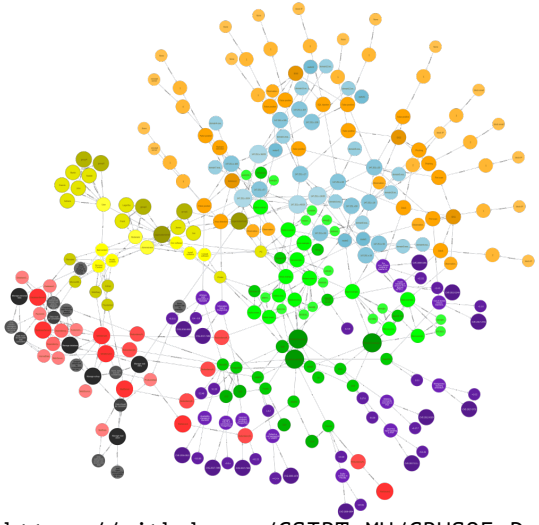
CRUSOE Project at Masaryk University

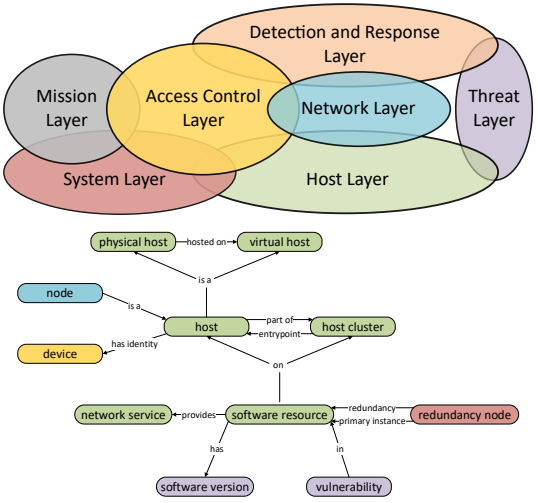
- Development of a toolset for achieving cyber situational awareness
- Inspired by CyGraph, more lightweight and automated
- Similar graph-based data model



J. Komárková et al. CRUSOE: Data Model for Cyber Situation Awareness. In Proceedings of the 13th International Conference on Availability, Reliability and Security. 2018

CRUSOE Project





https://github.com/CSIRT-MU/CRUSOE-Data-Model

Section 3

Prediction, Projection, and Forecasting

Motivation and Use Cases

- Predictive analytics allow for anticipatory cyber defense
- Better readiness for upcoming events
- Preemptive or early mitigation of threats

Four distinct use cases for predictive analytics in cybersecurity

1. Attack Prediction
2. **Attack Projection**
3. Attack Intention Recognition
4. Network Security Situation Forecasting

M. Husák, J. Komárková, E. Bou-Harb, P. Čeleda. Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials. 2018

1. Attack Prediction

What type of attack will occur, when, and where?

- Early detection and prediction
  - Rising number of requests implies a starting DDoS
- Entity reputation and scoring
  - Certain IP address performs network scanning regularly and will probably continue
  - An entity behaves like an attacker from the past – it may be the same attacker
- Predictions based on other sources
  - When a new vulnerability is disclosed, exploit attempts are expected
  - Phishing campaigns often follow breaking news

V. Bartoš, M. Žádník, S. Mahbub Habib, and E. Vasilomanolakis. Network entity characterization and attack prediction. In Future Generation Computer Systems. 2019
A. Okutan, S. J. Yang, K. McConky, and G. Werner. CAPTURE: Cyberattack Forecasting Using Non-Stationary Features with Time Lags. In 2019 IEEE Conference on Communications and Network Security (CNS)

2. Attack Projection

What is an adversary going to do next?

- Most often uses attack models and model matching
  - Created by human experts – very laborious
  - Constructed from historical records – data mining
- If a starting sequence of attack is found, the remainder is predicted
- If there are multiple options, we can select the probable by using:
  - assigned probability
  - frequency in historical records
- The output is typically the next predicted action of an attacker

S. J. Yang, H. Du, J. Holsopple, and M. Sudit. Attack Projection. In Cyber Defense and Situational Awareness. Springer. 2014

3. Attack Intention Recognition

What is the ultimate goal of an adversary?

- Very similar to attack projection, different outputs and goals
- Tied to attacker's motivation and criticality of protected assets
- Attacker has a variety of options how to act, such as:
  - picks the targets – probably a motivated attacker
  - sequentially or randomly scanning the network for targets – probably not motivated
- Different parameters of projecting the attack:
  - attack complexity – differentiate motivated attackers from script kiddies
  - attacker's gain, defender's loss – effect of past steps suggest motivation

A. A. Ahmed and N. A. K. Zaman. Attack intention recognition: A review. In International Journal of Network Security. 2017

4. Network Security Situation Forecasting

How is the overall situation going to evolve?

- For example, increase or decrease in number of expected attacks
- Often attempts to represent cybersecurity situation in a few values
- Mostly applicable for assessing network-wide or global security situation
- No information on particular attacks (lists of attackers and targets, timing)

Y.-B. Leau and S. Manickam. Network Security Situation Prediction: A Review and Discussion. Springer. 2015

Section 4

Graphs and Attack Projection

Approaches to prediction, projection, and forecasting

- Discrete models
  - **Attack graphs**
  - **Bayesian networks**
  - **Markov models**
  - Game-theoretical models
- Continuous models
  - Time series
  - Grey models
- Machine Learning and Data Mining
- Other approaches
  - including specialized methods, e.g., DDoS forecasting

M. Husák, J. Komárková, E. Bou-Harb, P. Čeleda. Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials. 2018

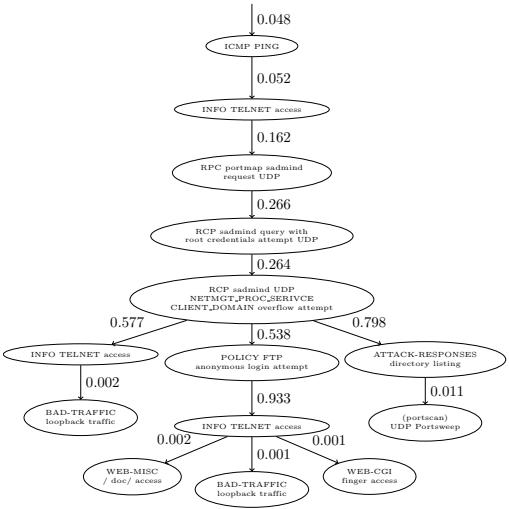
Attack Graphs

Attack Graphs

- Introduced in 1998, still widely used
- Many existing variants and extensions
- Used for attack projection from 2003

Simple attack graph for attack projection

- Nodes – attacker's actions
- Edges – predictability

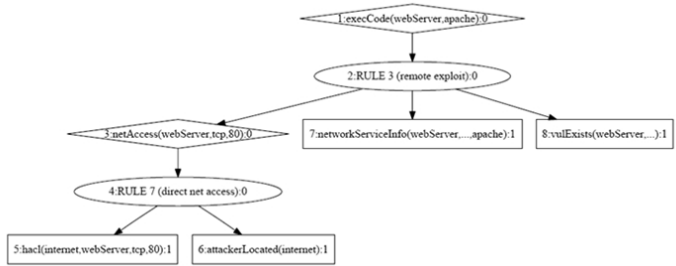


Attack Graphs

MulVAL

- Well-known AG tool
- Vulnerability assessment
- Network topology-aware
- Shows possible attack paths and vectors
- No probabilities

`http://people.cs.ksu.edu/~xou/mulval/`



Taken from `http://forge.fiware.org/`

Bayesian Network

Bayesian network (BN)

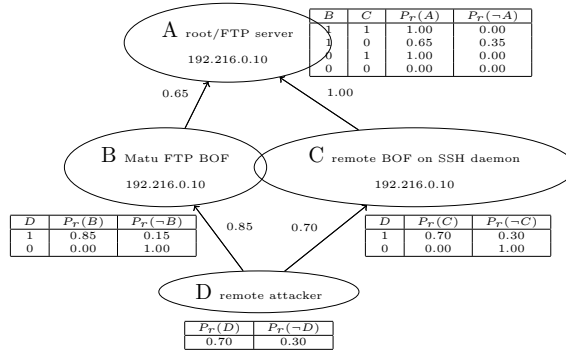
- DAG of random variables (nodes) and their relationships (edges)
- Each variable has a conditional probability table attached

Bayesian attack graph

- BN constructed from an AG

Causal network

- Requirement on causality of the relationships



Example of BAG – attacker (D) can use two buffer overflow exploits (B, C) to get access to a server (A)

Markov Models

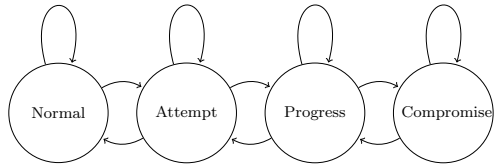
Hidden Markov models

- Add hidden (unobserved) events
- Not everything can be detected by IDS!

State-of-the-art

- Variable-length Markov models
- Projects by prof. Yang (RIT)

`https://people.rit.edu/~sjyeec/research.html`



Other Graph Models

Petri nets

- Powerful modeling tool, high explainability
- Not very practical for projection use cases

Game-theoretical models

- For specific purposes
- Computationally intensive

Issues and Challenges

Attack Libraries

- There is a need to build a library of attack models
- Manual construction is extremely laborious

Up-to-date Content

- The attack libraries may obsolete fast
- Models and model parameters may change daily

Data Mining and Machine Learning as a solution?

- Automated construction of attack library
- What data to process and how?

How can Data Mining help?

Main goals

- Use data mining and machine learning to build attack libraries
- Continuously update the libraries

Milestones

- Select suitable methods and data
- Tune parameters
- Check sanity of the results
- Evaluate predictive capabilities of the outputs

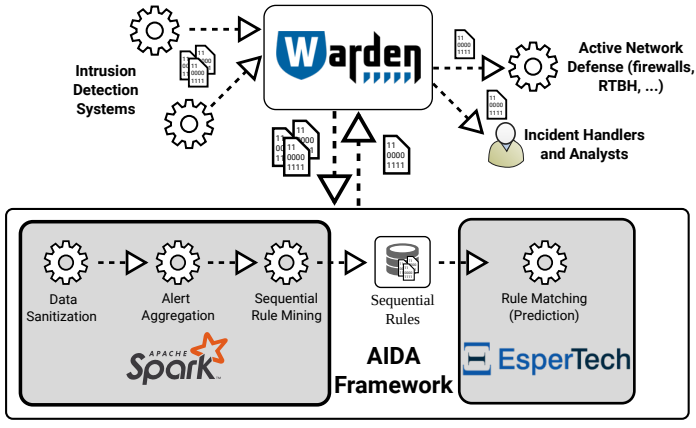
Experience with the AIDA Framework

AIDA Framework

- Correlation and prediction of alerts from IDS
- Deployed in SABU alert sharing platform
  (alerts from 20+ organizations, mostly universities in Czech Republic)
- Attack projection based on sequential rule mining and model checking
- Anonymized dataset publicly available for experiments

M. Husák and J. Kašpar. AIDA Framework: Real-Time Correlation and Prediction of Intrusion Detection Alerts. In Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES), 2019
M. Husák, M. Žádník, V. Bartoš, and P. Sokol. Dataset of intrusion detection alerts from a sharing platform. June 2019. http://dx.doi.org/10.17632/p6tym3fghz.1

Experience with the AIDA Framework



https://sabu.cesnet.cz/en/start
https://github.com/CSIRT-MU/AIDA-Framework

Experience with the AIDA Framework

Selecting the most suitable data mining method

- Sequential pattern and rule mining
- Graph mining methods were not evaluated (yet)

Pattern example

- *{IDS1, Scan, 22}, {IDS2, Scan, 22}, {IDS3, Scan, 22}*

Rule example

- *{IDS1, Scan, 22}, {IDS2, Scan, 22}* => *{IDS3, Scan, 22}*; *#CONF 0.8*

M. Husák, J. Kašpar, E. Bou-Harb, P. Čeleda. On Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts. In Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES), 2017

Experience with the AIDA Framework

Experimental results

- Evaluated in live environment and also with the dataset
- Mining Top-10 rules every day for prediction in the following day
- Most of the sequential rules make sense (8+ out of 10)
- Confidence values up to 0.9 (90 % predictability)
- Timely predictions leave 5 minutes to mitigate the attacks

M. Husák and J. Kašpar. Towards Predicting Cyber Attacks Using Information Exchange and Data Mining. In 14th International Wireless Communications Mobile Computing Conference (IWCMC), 2018

How would graphs help?

Where is the problem?

- Sequences are fine, works well, and give solid results. However...

Data Mining

- When mining more rules, there appears to be many similar ones
- Updating the existing rules might be tricky – everything is replaced at once
- Can we only update predictability scores?

Rule Matching

- For each rule, there is one running query over the stream of alerts
- Can we run just one query for all models?

How would graphs help?

Data Mining

- Mining graphs directly or modeling the outputs in a graph?
- Requires a well though-out design and implementation
- Many potential pitfalls

Rule Matching

- Traversing graphs instead of checking each rule separately
- Need to be careful about cycles and finite states
- Higher performance of rule matching tool

Related Work

Graph Mining in cyber security

- B. Aditya Prakash: Graph Mining for Cyber Security. In Cyber Warfare 2015
- L. Akoglu et al. Graph based anomaly detection and description: a survey. In Data Mining and Knowledge Discovery. 2014

Graph mining for attack projection

- Z. Li et al. A data mining approach to generating network attack graph for intrusion prediction. In Fuzzy Systems and Knowledge Discovery, 2007
- H. Farhadi et al. Alert Correlation and Prediction Using Data Mining and HMM. In ISeCure, 2011
- A. A. Ramaki et al. Real time alert correlation and prediction using Bayesian networks. In ISCISC, 2015

Section 5

Conclusion

Conclusion

Conclusion

- Graph-models can be found almost everywhere in cybersecurity
- Attack graphs and their derivatives allow projecting cyber attacks
- Projection and preemptive mitigation is a novel approach to cyber defense

Challenges and Future Work

- Building the graph models is hard and they get obsoleted quickly
- ML&DM-supported approaches seems promising
- Graph mining for attack projection would combine benefits of DM and graph models

Thank You for Your Attention!

MUNI
C4E

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ