MUNI
C4E

Predictions of Network Attacks in Collaborative Environment

NOMS 2020 Dissertation Digest Session

Martin Husák
husakm@ics.muni.cz

Institute of Computer Science, Masaryk University

April 23, 2020

Part I

Introduction

Motivation & Goals

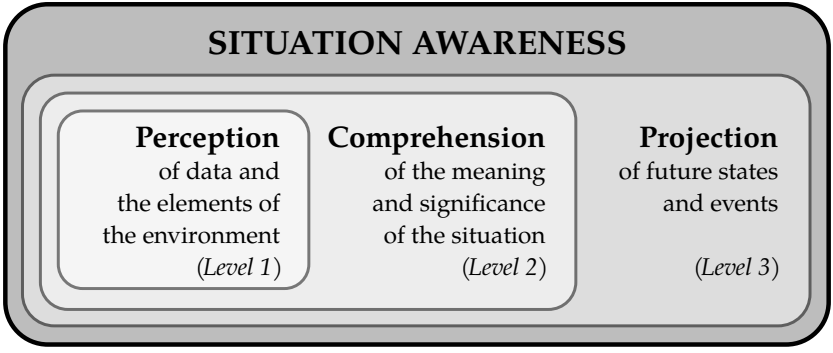
Motivation

- Large volumes of cybersecurity data are shared, only a small fraction of them is used
- Shift from reactive to proactive cybersecurity
- Achieving cyber situational awareness

Goals of the Work

- Explore and leverage the data shared among distributed heterogeneous sensors, networks, and organizations
- Describe and understand frequent attack patterns
- Predict cyberattacks and mitigate them preemptively

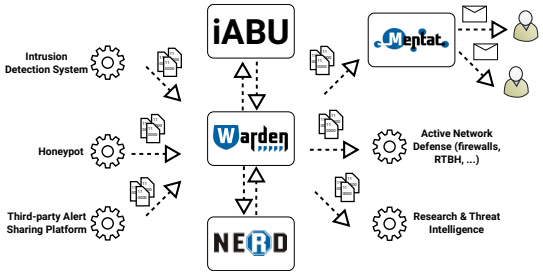
Cyber Situational Awareness



Mica R. Endsley. Toward a theory of situation awareness in dynamic systems. In: Human Factors. 1995. 37(1).

Collaboration and Information Sharing

- Overview of collaborative approaches in cybersecurity
- Illustrated on a case study of SABU alert sharing platform



- Technical issues – data formats, communication protocols, …
- Non-technical issues – policies, trust, privacy, impact of GDPR

Projection, Prediction, and Forecasting

Use cases and existing approaches

- Projection – What will the adversary do next?
- Intention Recognition – What is the adversary's goal?
- Prediction – What type of attack will happen, when, and where?
- Forecasting – How many attacks will we face?

Taxonomy of methods

- Discrete models (e.g., attack graph-based projection)
- Continuous models (e.g., time series forecasting)
- Methods supported by Machine Learning and Data Mining
- Other approaches

M. Husák et al. Survey of attack projection, prediction, and forecasting in cyber security. IEEE Communications Surveys & Tutorials. IEEE, 2018.

Part II

Perception

Sources of Alerts

Main sources of alerts (sensors):

- Network-based IDS – based on network flow monitoring
- Honeypots – server-side, low-interaction

(Strong bias towards network security and network attacks)

Goals of this phase:

- Adapting existing sensors for information exchange
- Observation and detection of attack patterns
- Leveraging sensors to detect particular attack phases

Network-based Intrusion Detection

Enhancements to network flow-based intrusion detection

- Use of extended flow monitoring – HTTP parsing
- Identification of security-relevant classes of HTTP traffic: application-level scanning, brute-forcing, web crawling
- Improved detection of users accessing phishing websites

Outcomes

- Fine-grained detection of particular attack phases
- Leveraging network monitoring to detect unconventional events

M. Husák et al. Security Monitoring of HTTP Traffic Using Extended Flows. In 10th International Conference on Availability, Reliability and Security. IEEE, 2015.

M. Husák and J. Čegan. PhiGARo: Automatic Phishing Detection and Incident Response Framework. In 9th International Conference on Availability, Reliability and Security. IEEE, 2014.

Honeypots

Flow-based monitoring of honeypots

- Combination of host-based and network-based monitoring
- Discussion of design and deployment considerations

Honeypots and Internet backscatter

- Case study of honeypot behavior during reflected DDoS attacks
- Reflections caused honeypots to report DDoS victims as scanners

M. Husák and M. Drašar. Flow-based Monitoring of Honeypots. In Security and Protection of Information 2013. University of Defence, 2013.

M. Husák and M. Vizváry. POSTER: Reflected attacks abusing honeypots. In Proceedings of the 2013 ACM SIGSAC conference on Computer & Communications Security. ACM, 2013.

Preliminary Attack Patterns

Example observed via flow-based intrusion detection:

1. Horizontal scan on port 80
2. HTTP request on all responding hosts with */wp/admin.php*
3. Brute-force password attack on found WordPress instances

Example observed during honeypot deployment:

1. Honeypot reports scanning attempt
2. Network-based IDS reports scanning of the whole network
3. Honeypot reports brute-forcing

? Can we expect brute-forcing of other hosts in the network?

Part III

Comprehension

Data Mining

Task

- Finding sequences of alerts – patterns of attackers' behavior
- Selecting the most frequent and explanatory patterns

Approach

- Sequential pattern mining
- Extracted information: sensor, event type, destination port
- Sequences of alerts with the same source IP address (attacker)

Pattern example

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

M. Husák et al. On the Sequential Pattern and Rule Mining in the Analysis of Cyber Security Alerts. In 12th International Conference on Availability, Reliability and Security. ACM, 2017.

Towards Prediction

Sequential pattern and rule mining

- Sequential pattern describes the behavior of an attacker
- Sequential rule suggest the next action of an attacker

Confidence value

- Portion of sequences conforming to the rule
- Can be interpreted as a probability of future events

Rule example

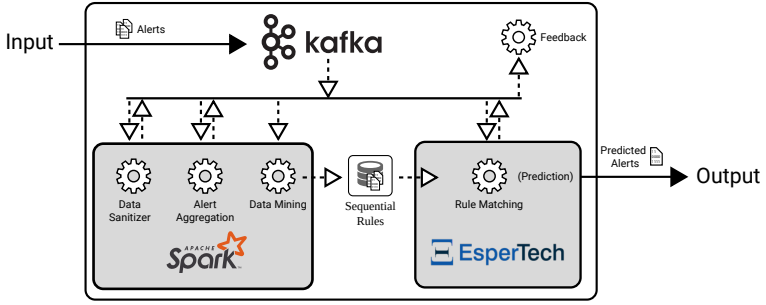
- *{IDS1, Scan, 22}, {IDS2, Scan, 22}* => *{IDS3, Scan, 22}*; *#CONF 0.8*

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

Part IV

Prediction

AIDA Framework



- If the first part of a rule is matched, the remainder is predicted
- Rule Matching component inspired by Complex Event Processing

M. Husák and J. Kašpar. AIDA Framework: Real-Time Correlation and Prediction of Intrusion Detection Alerts. In 14th International Conference on Availability, Reliability and Security. ACM, 2019.

Evaluation

Evaluation issues

- Not repeatable in a live environment
- No information about incident response and mitigation
- Very hard to evaluate in a laboratory setting
- Existing datasets are often old and unreliable

Dataset

- Dataset of alerts from SABU
- Anonymized, cleansed, published
- Allows reproduction of the experiments

M. Husák et al. Dataset of intrusion detection alerts from a sharing platform, Mendeley Data, http://dx.doi.org/10.17632/p6tym3fghz.1

Results

Experiment results

- Top-10 rules mined every day
- Rule confidence up to 0.9
- Most of the predictions leave at least 5 minutes for a response

Predictive blacklisting

- Straightforward utilization of predictions
- Generating blacklists from predicted events
- 65 % hit rate

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

M. Husák and J. Kašpar. AIDA Framework: Real-Time Correlation and Prediction of Intrusion Detection Alerts. In 14th International Conference on Availability, Reliability and Security. ACM, 2019.

Part V

Summary

Summary

1. Perception – alert sharing
   - Alert sharing is beneficial and allows achieving CSA
   - Suitable granularity of events is required to observe patterns

2. Comprehension – pattern extraction
   - Sequential pattern/rule mining allow for unsupervised mining
   - Alert aggregation and other preprocessing is imperative

3. Projection – attack prediction
   - Proposed approached implemented in the AIDA framework
   - Dataset created to allow for reproduction of the experiments

MUNI
C4E

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

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

C4E.CZ