THE GEORGE WASHINGTON UNIVERSITY

WASHINGTON, DC

Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI

Benjamin Bowman   Craig Laprade   Yuede Ji   H. Howie Huang

George Washington University

Graph Lab

Overview

1. Lateral Movement & The Lifecycle of a Cyber Attack
2. Machine Learning on Graphs & Unsupervised Graph AI
3. Detecting Lateral Movement with Unsupervised Graph AI
4. Evaluations and Results
5. Conclusion

Overview

1 **Lateral Movement & The Lifecycle of a Cyber Attack**

2 Machine Learning on Graphs & Unsupervised Graph AI

3 Detecting Lateral Movement with Unsupervised Graph AI

4 Evaluations and Results

5 Conclusion

Lifecycle of a Cyber Attack

- Advanced Persistent Threats (APTs) are stealthy and sophisticated threat actors

- Attacks waged by APTs are complex, multi-stage campaigns that can span long periods of time

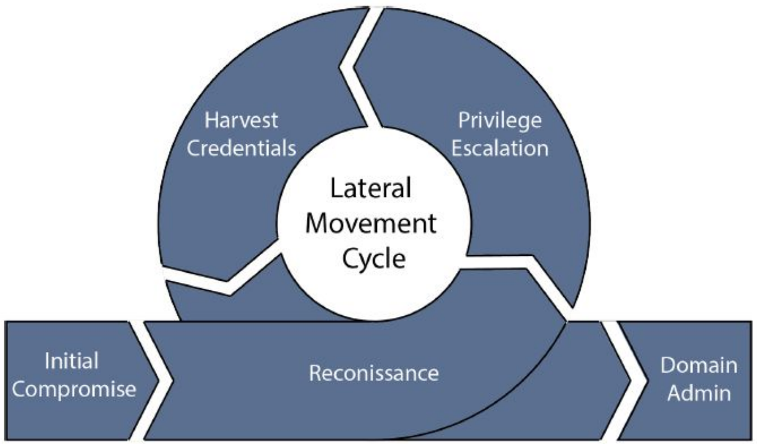


Figure 2: An APT-style campaign showing the cycle of lateral movement after initial compromise and prior to full domain ownership.

Lifecycle of a Cyber Attack

- Initial compromise typically occurs on low-privilege systems as these users are typically more susceptible to low-level attacks
    - Phishing
    - Credential stuffing
    - Bad passwords

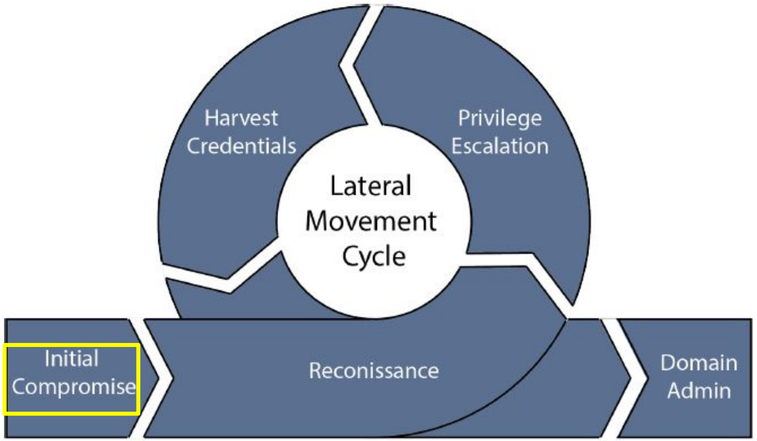


Figure 2: An APT-style campaign showing the cycle of lateral movement after initial compromise and prior to full domain ownership.

Lifecycle of a Cyber Attack

- The adversary then must move laterally through the network to gain access to systems necessary to accomplish their mission
  - Reconnaissance to identify accessible systems and services
  - Privilege escalation either on the local machine or by moving to a machine where the user has more privileges
  - Credential harvesting from memory or files

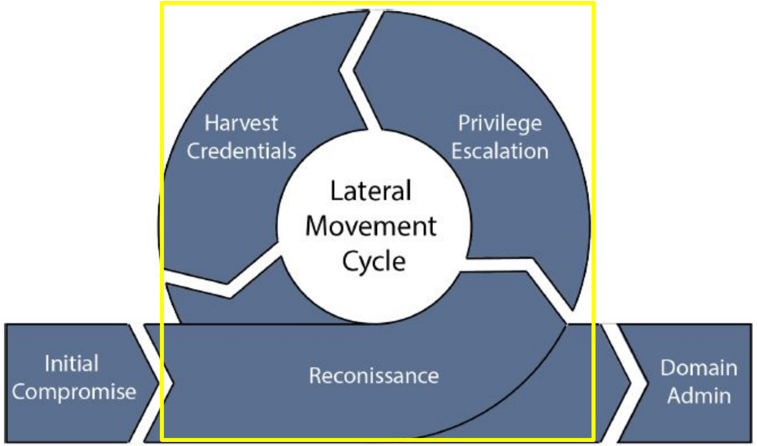


Figure 2: An APT-style campaign showing the cycle of lateral movement after initial compromise and prior to full domain ownership.

Lifecycle of a Cyber Attack

- The last phase are the actual actions on objectives
  - Domain Admin
  - Data Exfiltration
  - Data Destruction
  - Ransomware

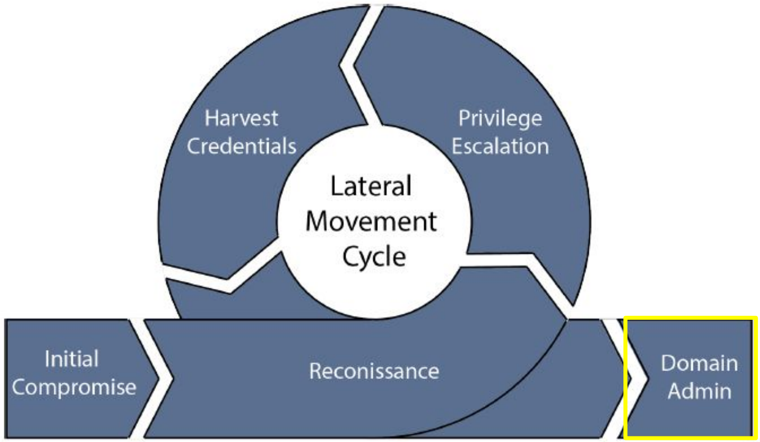


Figure 2: An APT-style campaign showing the cycle of lateral movement after initial compromise and prior to full domain ownership.

Lateral Movement

- Key stage of the attack lifecycle that allows the adversary to achieve their actions on objectives

- Challenging to detect as often adversaries will use *legitimate credentials, services, and authentication channels*
  - WMI, WinRM, RDP, SMB, etc

We need a technique capable of learning from past authentication behavior, that will allow us to detect anomalous authentication events that may be indicative of lateral movement.

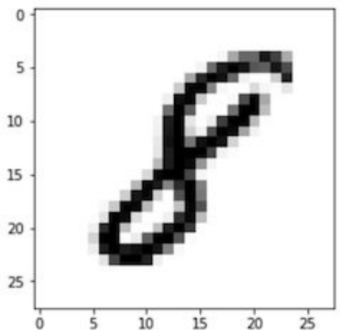
Overview

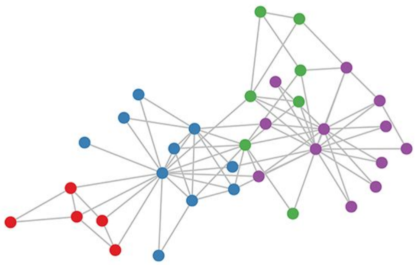
1. Lateral Movement & The Lifecycle of a Cyber Attack
2. **Machine Learning on Graphs & Unsupervised Graph AI**
3. Detecting Lateral Movement with Unsupervised Graph AI
4. Evaluations and Results
5. Conclusion

Machine Learning on Graphs

- Graph data structures consisting of a set of nodes and edges are extremely powerful for representing heterogeneous relational data (social networks, computer networks, knowledge graphs, etc)

- Applying ML to graphs is non-trivial due to non-euclidian nature of the data



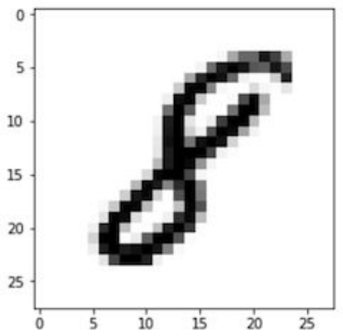


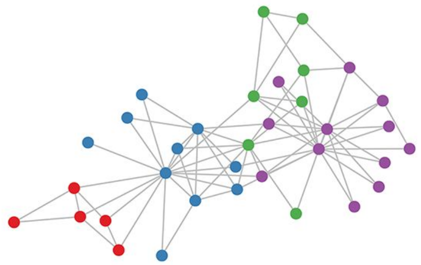
Machine Learning on Graphs

- Graph data structures consisting of a set of nodes and edges are extremely powerful for representing heterogeneous relational data (social networks, computer networks, knowledge graphs, etc)

- Applying ML to graphs is non-trivial due to non-euclidian nature of the data

Location & order
is meaningful!



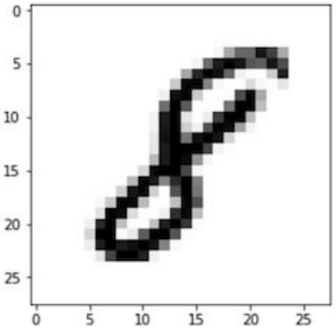


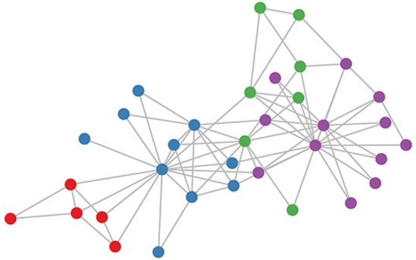
Machine Learning on Graphs

- Graph data structures consisting of a set of nodes and edges are extremely powerful for representing heterogeneous relational data (social networks, computer networks, knowledge graphs, etc)

- Applying ML to graphs is non-trivial due to non-euclidian nature of the data

Location & order
is meaningful!

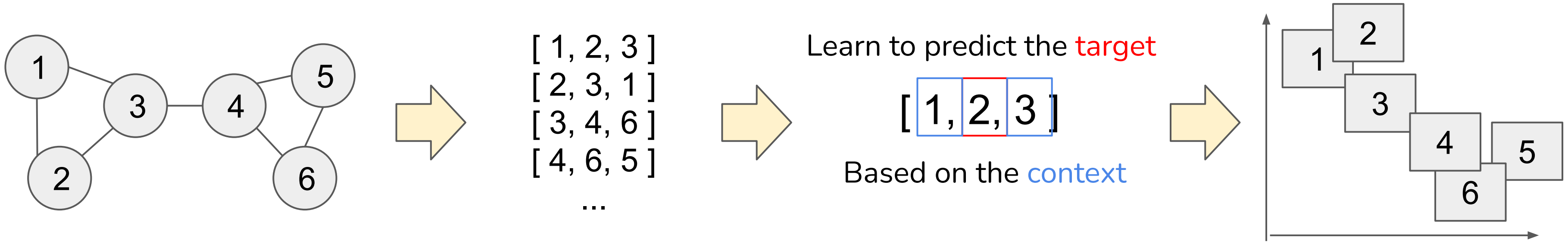




No location!
No order!

Unsupervised Graph AI

- Graphs can be sampled to form fixed-length sequences of nodes which can be used in conjunction with traditional data mining techniques from NLP (popularized by works such as DeepWalk and node2vec)



Input Graph **Random Walk Sampling** **CBOW Embedding** **Tuned Embeddings**

Grover, Aditya, and Jure Leskovec. "node2vec: Scalable feature learning for networks." *SIGKDD* 2016.
Perozzi, Bryan, Rami Al-Rfou, and Steven Skiena. "Deepwalk: Online learning of social representations." *SIGKDD* 2014.

Overview

1 Lateral Movement & The Lifecycle of a Cyber Attack

2 Machine Learning on Graphs & Unsupervised Graph AI

3 **Detecting Lateral Movement with Unsupervised Graph AI**

4 Evaluations and Results

5 Conclusion

Method

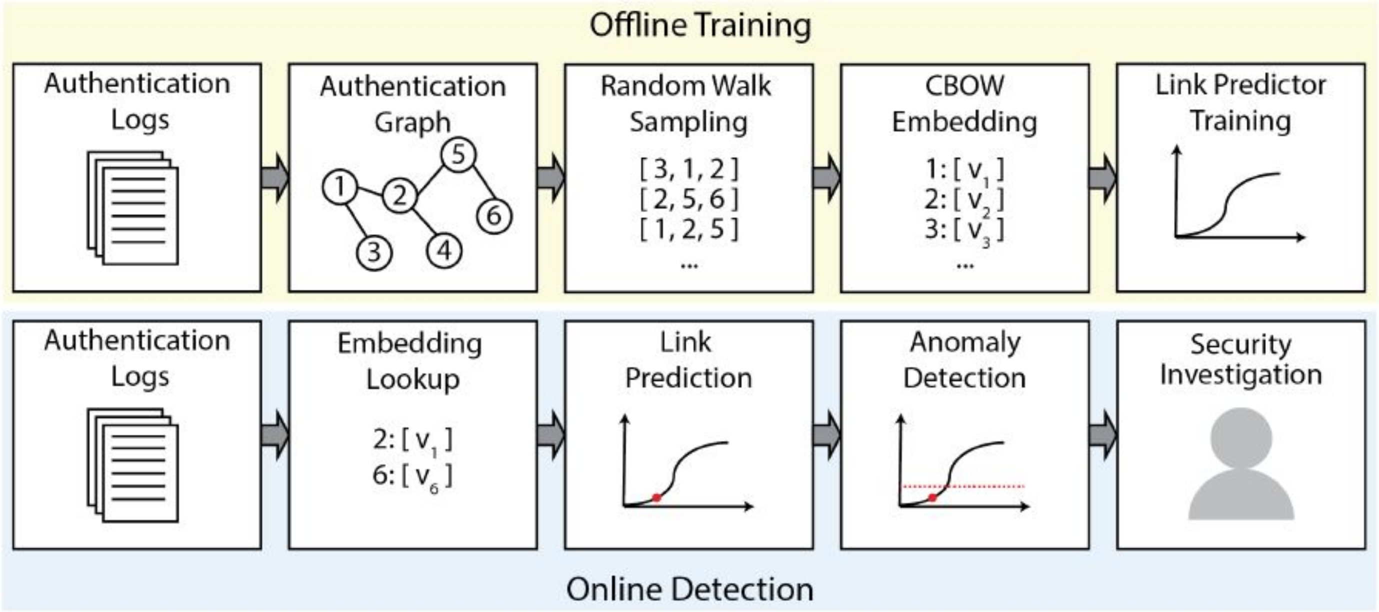


Figure 3: Full algorithm pipeline including offline training of node embeddings and logistic regression link predictor, as well as online detection via an embedding lookup, link prediction, and threshold-based anomaly detection.

Method

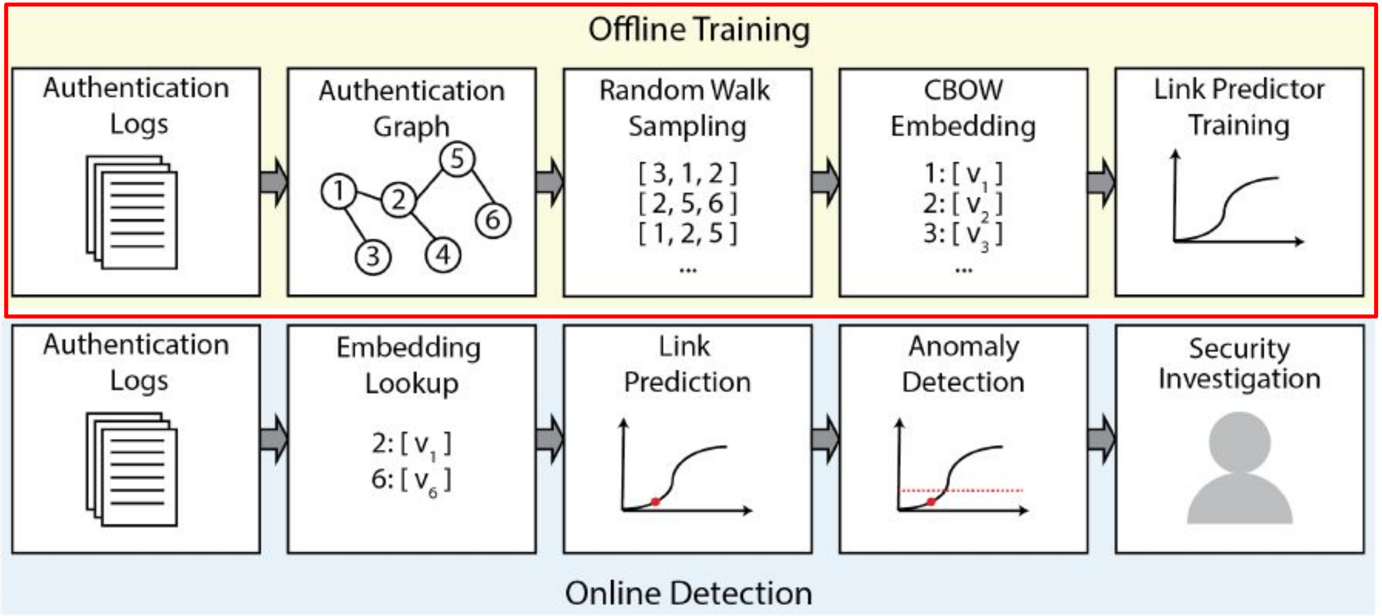


Figure 3: Full algorithm pipeline including offline training of node embeddings and logistic regression link predictor, as well as online detection via an embedding lookup, link prediction, and threshold-based anomaly detection.

Method

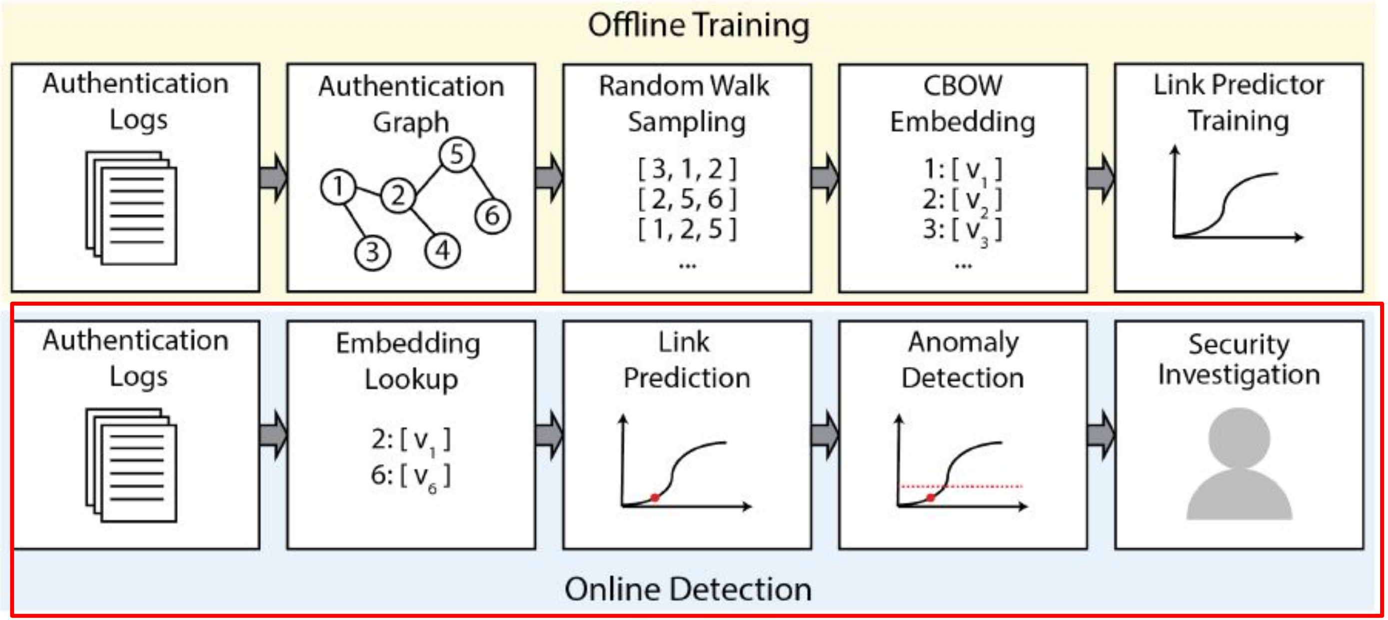


Figure 3: Full algorithm pipeline including offline training of node embeddings and logistic regression link predictor, as well as online detection via an embedding lookup, link prediction, and threshold-based anomaly detection.

Authentication Graph Generation

- Parse industry standard Kerberos logs to build an Authentication Graph
- Kerberos is a network authentication protocol - does not require host logs
- Extracted fields:
  - Client & Service Principals
  - IP Addresses
- “Who is authenticating to what, from where”

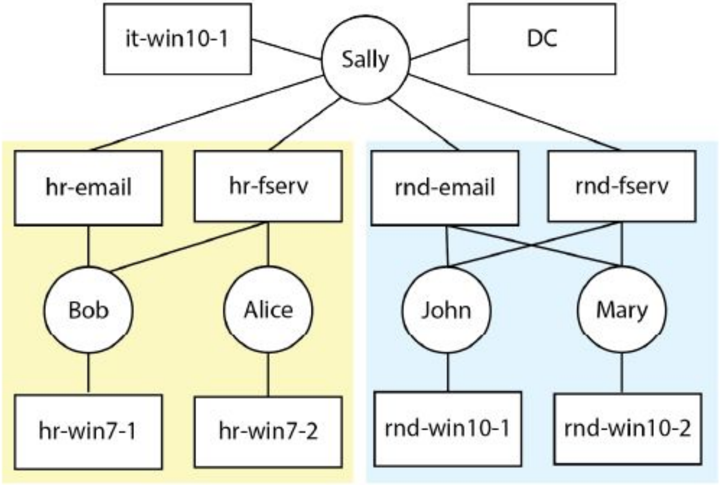


Figure 1: Example of an authentication graph for a small simulated network.

Node Embedding

- Embedding process based on node2vec
- Random walks generate sequences of nodes
- CBOW is used to learn node embeddings

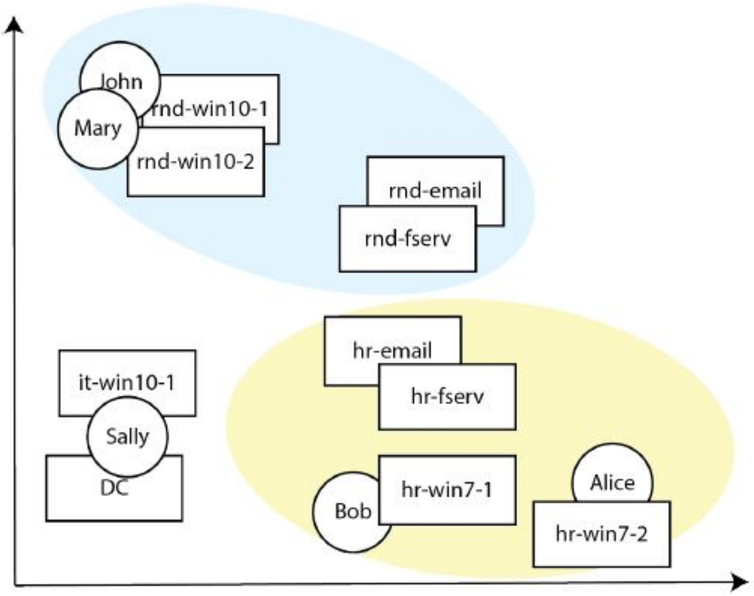
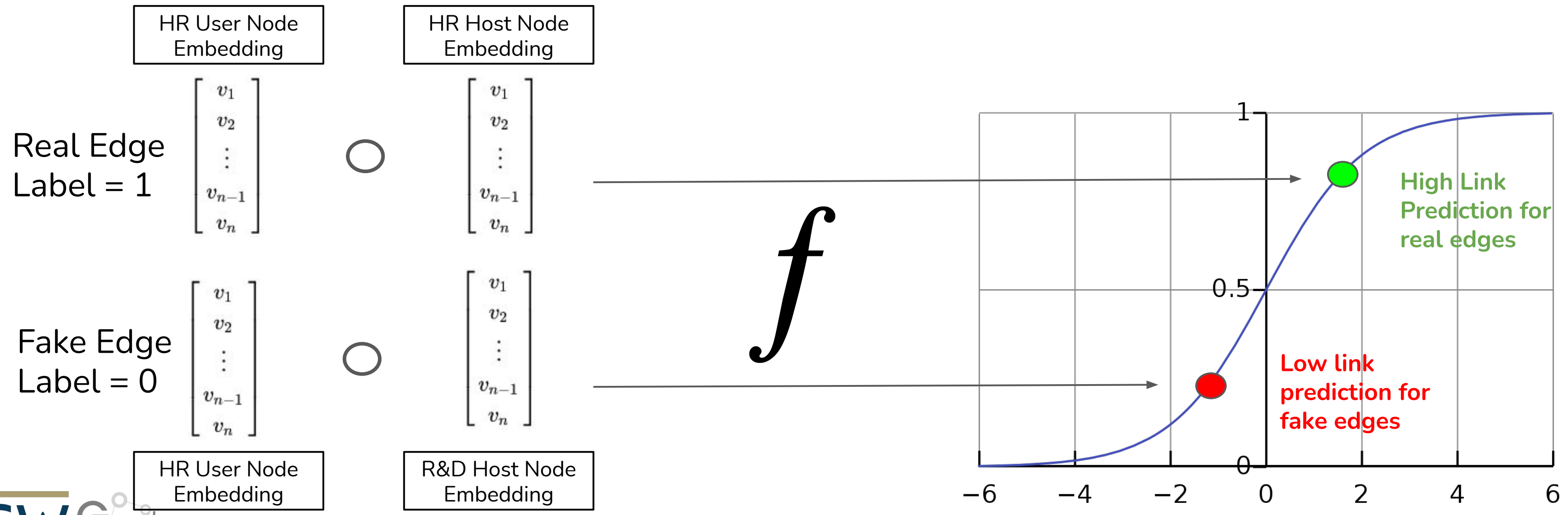


Figure 4: Example embedding space generated from a random-walk based node-embedding process.

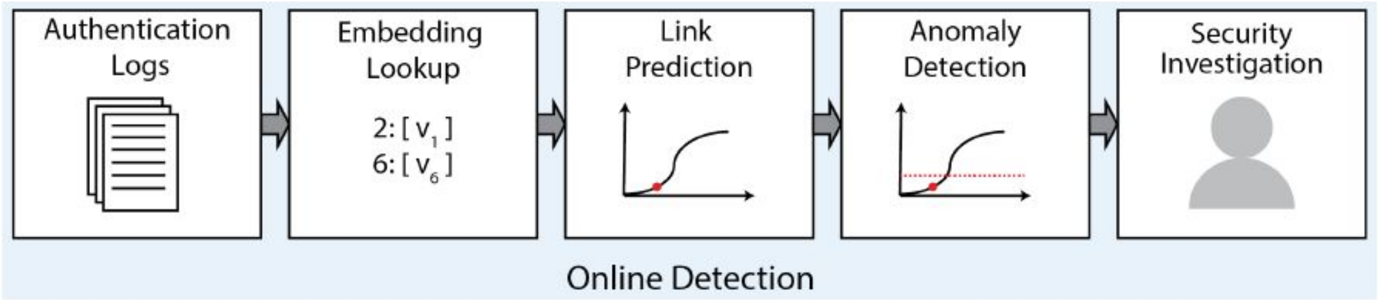
Grover, Aditya, and Jure Leskovec. "node2vec: Scalable feature learning for networks." *SIGKDD* 2016.

Link Predictor

- A logistic regression classifier is trained on node embeddings from real & fake edges in the graph



Detection



- Anomalous link detection can be achieved by alerting on links with a probability less than a user-defined threshold $\boldsymbol{\delta}$

$$A(h_a, h_b) = \begin{cases} 1, & if\ f(h_a \circ h_b) < \delta \\ 0, & otherwise \end{cases}$$

Overview

1. Lateral Movement & The Lifecycle of a Cyber Attack
2. Machine Learning on Graphs & Unsupervised Graph AI
3. Detecting Lateral Movement with Unsupervised Graph AI
4. **Evaluations and Results**
5. Conclusion

Datasets

- PicoDomain Dataset
  - Custom dataset we built in-house https://github.com/iHeartGraph/PicoDomain
  - Characterized by its small size, but full visibility into a cyber attack that spans the killchain
- LANL 2015 Dataset
  - Real-world, enterprise network from
  - Characterized by its large size, but highly anonymized data, with very little detail on malicious activity

Table 1: Dataset Details

	PicoDomain	LANL
Duration in Days	3	58
Days with Attacks	2	18
Total Records	4686	1.05 B
Total Attack Records	129	749
User and Machine Accounts	86	99968
Computers	6	17666

Comparison Techniques

Graph ML

Graph-Learning **Local-View** (GLGV): **small** node embedding context window

Graph-Learning **Global-View** (GLGV): **large** node embedding context window

Traditional ML: 1-hot encoded authentication feature vector per-entity

Local Outlier Factor (LOF) - local density-based outliers

Isolation Forest (IF) - decision-tree-based anomaly detector

Rule-Based

Unknown Authentication (UA) - alert on authentications not previously observed

Failed Authentication (FA) - alert on failed authentication attempts

Results on PicoDomain

- UA detects the most malicious activity
- ML detects some malicious events but FPR too high
- GL achieves 80% TPR at 0% FPR

Table 2: Anomaly Detection Results on PicoDomain Dataset

Algorithm	**TP**	**FP**	**TPR (%)**	**FPR (%)**
UA	**129**	11	**100**	1.5
FL	1	15	0.8	2.0
LOF	41	19	32	2.5
IF	34	62	26	8.3
GL-LV	102	**0**	80	**0.0**
GL-GV	102	**0**	80	**0.0**

Results on LANL Dataset

- UA still detects most of malicious activity but at expense of FPs
- ML techniques are noisy and don't detect much activity
- GL-GV has best TPR and least FPR

Table 3: Anomaly Detection Results on LANL Dataset

Algorithm	TP	FP	TPR (%)	FPR (%)
UA	542	530082	72	4.4
FL	31	116600	4	1.0
LOF	87	169460	12	9.6
IF	65	299737	9	16.9
GL-LV	503	146285	67	1.2
GL-GV	**635**	**107960**	**85**	**0.9**

Reducing False Positives

- False positives are bad, waste time, and are a serious problem in cyber

- What can we learn from the data to help reduce the number of FPs?

Observation 1: The malicious authentication events are predominantly first authentication events.

Observation 2: The malicious authentication events are predominantly based on user interactions.

Observation 3: The malicious authentication events are predominantly related to a few specific user accounts and systems.

False Positive Filters

Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

False Positive Filters

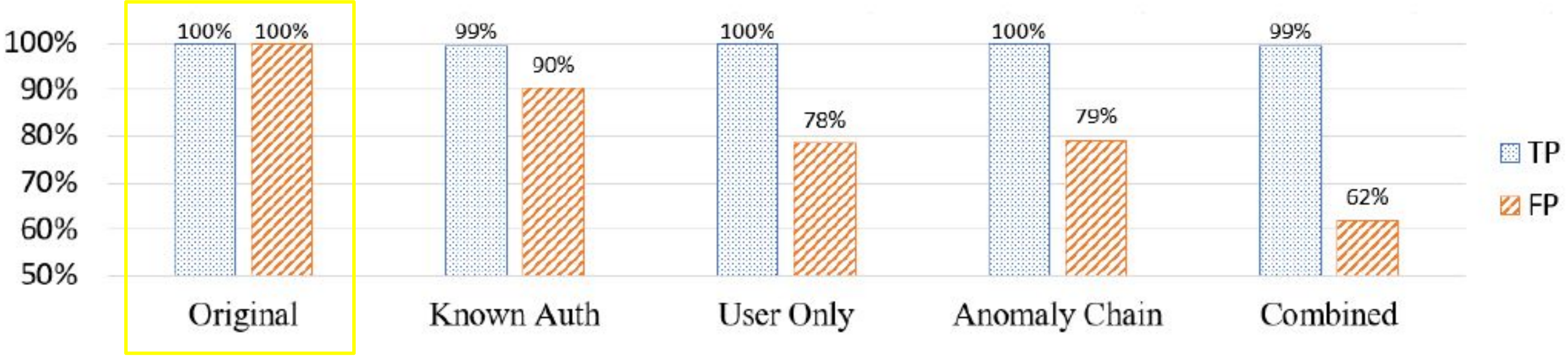


Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

Original results on the LANL dataset presented previously

False Positive Filters

Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

Filter out anomalies from authentications seen during training

False Positive Filters

Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

Filter out anomalies that don’t involve a user account

False Positive Filters

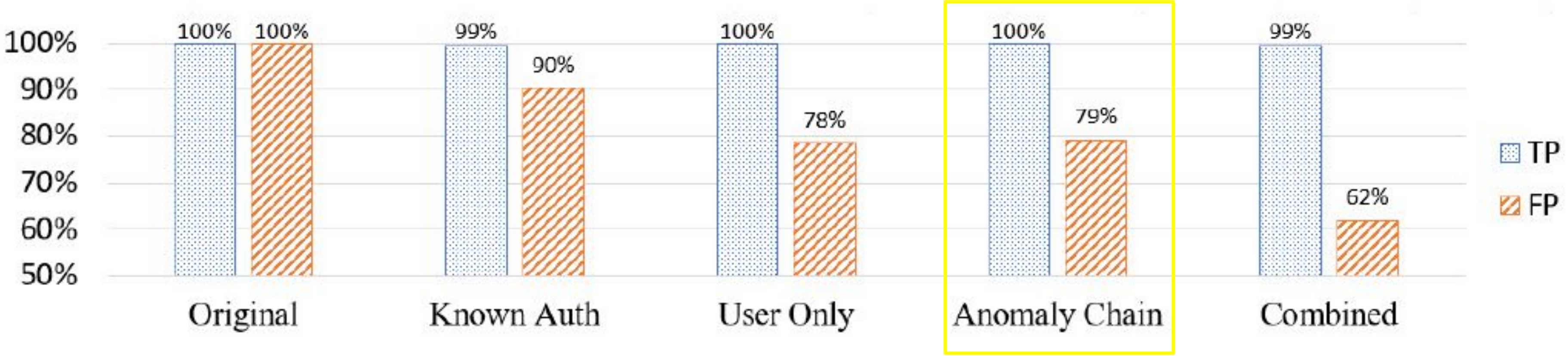


Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

Filter out anomalies singletons

False Positive Filters

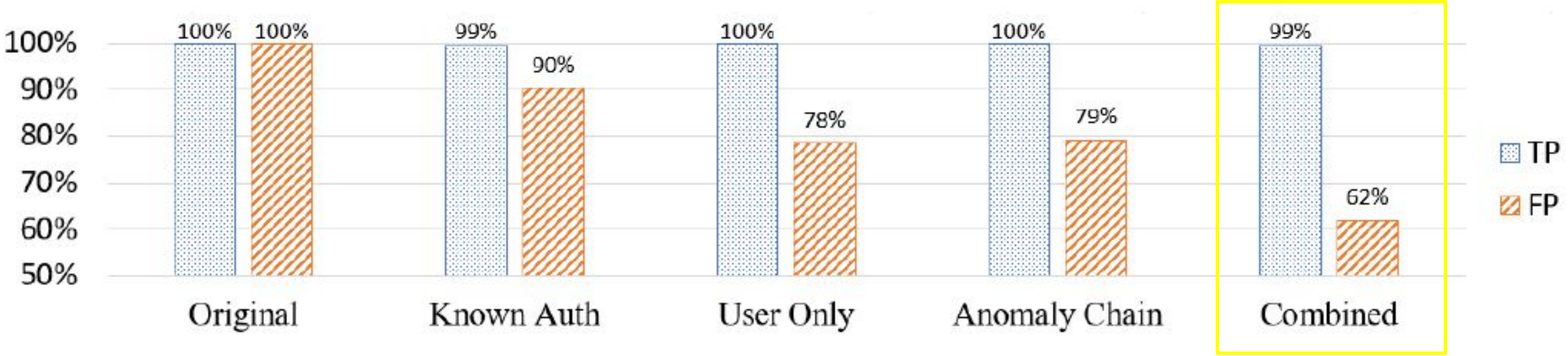


Figure 5: Impact of various approaches in reducing the number of false positives returned on the LANL dataset.

Combining all filters together

Overview

1. Lateral Movement & The Lifecycle of a Cyber Attack
2. Machine Learning on Graphs & Unsupervised Graph AI
3. Detecting Lateral Movement with Unsupervised Graph AI
4. Evaluations and Results
5. **Conclusion**

Conclusion

- Lateral movement is a critical phase of APT cyber attack campaigns that is very challenging to detect
- Using an authentication graph data structure, and unsupervised Graph AI, we can learn patterns of authentication activity of different classes of users
- We can use these learned patterns to detect malicious lateral movement with improved accuracy over several baseline detection algorithms
- With some simple post-processing filters we can reduce the number of false positives by nearly 40%.

Thanks!

Benjamin Bowman
bbowman410@gwu.edu
George Washington University