


Jbeil: Temporal Graph-Based Inductive Learning to Infer Lateral Movement in Evolving Enterprise Networks

Elias Bou-Harb, Ph.D., CISSP








computer emergency response team
for the EU institutions, bodies and agencies

CERT-EU Security Whitepaper 17-002

Detecting Lateral Movements in Windows Infrastructure



UNIVERSITY OF TWENTE.

Faculty of Electrical Engineering,
Mathematics & Computer Science

Detecting Lateral Movement Attacks through SMB using BRO




MITRE | FiGHT™ v2.0.0

MESCAL: Malicious Login Detection Based on Heterogeneous Graph Embedding with Supervised Contrastive Learning

Weiqing Huang^{1,2}, Yangyang Zong^{1,2*}, Zhixin Shi¹, Puzhuo Liu^{1,2}

¹ Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
² School of Cyber Security, University of Chinese Academy of Sciences, Beijing, China
{huangweiqing, zongyangyang, shizhixin, liupuzhuo}@ie.ac.cn



Japan Computer Emergency Response Team Coordination Center

電子署名者: Japan Computer Emergency Response Team Coordination Center
日付: 2017.06.12 13:45:12 +09'00'

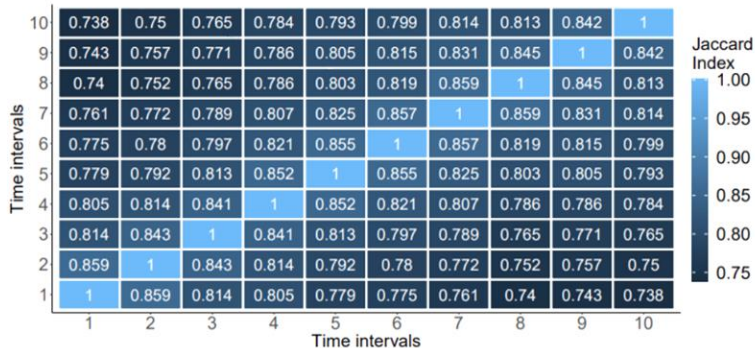
Ikram Ullah
Master Thesis
November 2016



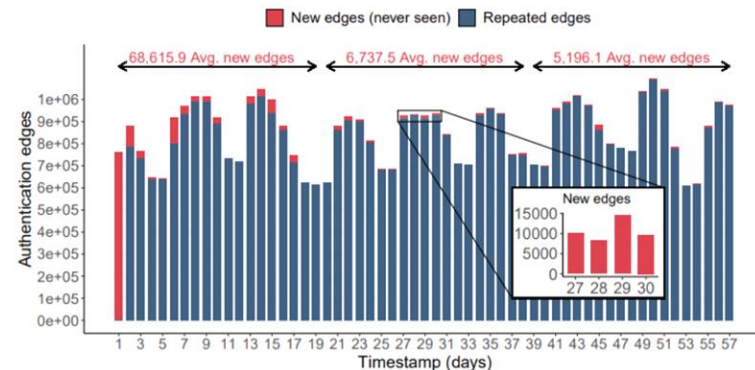
NDG Ethical Hacking v2

Detecting Lateral Movement through Tracking Event Logs

- Lack of visibility
- Absence of contextual relationships between different elements
- Constant evolving nature of networks



(a) **Evolution of nodes:** Jaccard similarity matrix showing the drop of node similarities over time in the network; an approximate 26% drop in node similarity between the first and last time interval.



(b) **Evolution of edges:** Depicting the number of new edges (never seen before) over time. An average of 5,196.1 new edges emerged between days 39 and 57.

- Obscured empirical data (to leverage) to address the LM problem
- Deficiency in appropriately modeling network behaviors and interactions
- Shortcoming of models that can anticipate the evolving nature of networks

Hopper (USENIX '21) constructs a graph of logins, introduces an inference algorithm to identify the broader paths of movements, and applies a new anomaly scoring algorithm.

Pros

- Develops a practical detection system for LM attacks
- Uses graph-based modeling to identify paths for each login

Cons

- Scalability will induce reduced performance
- Does not explicitly address 0-days/new techniques

Euler (NDSS '22) proposes a discrete-time dynamic graph techniques that adopts a transductive reasoning to improve the detection of anomalous activity in a network.



Pros

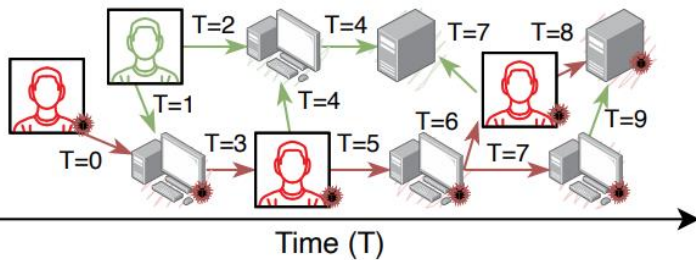
- Uses GNN models with node embeddings for authentication logs

Cons

- Does not generalize to unseen authentication entities
- Discrete-time dynamic graphs do not model the evolving nature of events

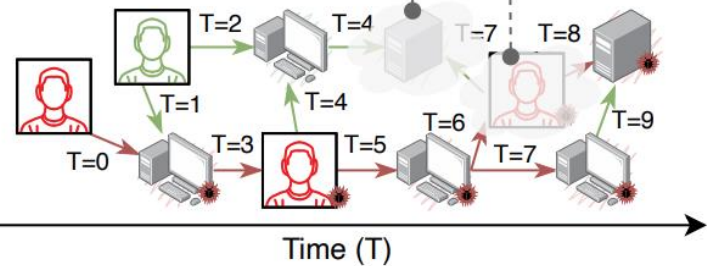
- Continuous-time dynamic graphs
- Inductive learning in temporal GNNs
- Threat sample augmentation

Legend:  Compromised user, machine, server  Benign user, machine, server



Full Intelligence (Transductive Reasoning)

Unprocessed Intelligence (entities and events)
- never seen before or due to resource constraints



Limited Intelligence (Inductive Reasoning)

Authentication Graph Construction

- Nodes representing diverse entities (hosts, users, virtualized environments, applications)
- Edges define authentication events, capturing interactions within the enterprise network

Dynamic Graph Feature Extraction

- Extracts graph features to grasp the dynamic nature of the enterprise network
- Focuses on evolving nodes' connectivity over time to capture the changing relationships between authenticating entities

Self-Supervised Temporal Node Embedding

- Implements a self-supervised temporal node embedding technique
- Computes latent representations for each node at every time, updating dynamic states during events and aggregating memory from neighboring nodes

LM Link Prediction

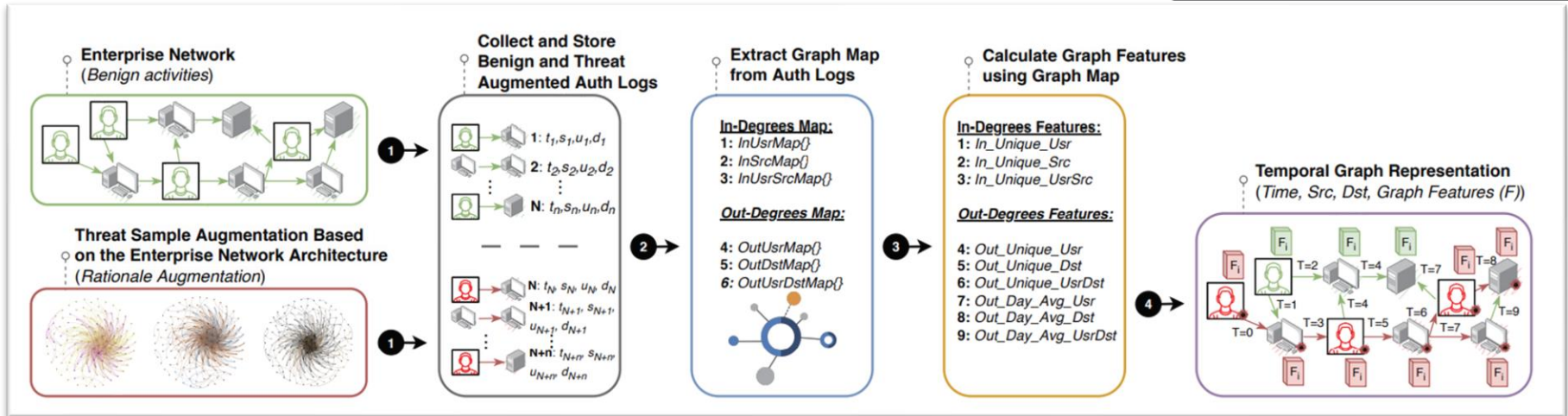
- Utilizes a decoder to calculate edge probabilities and perform LM link prediction
- Captures the temporal order of edges to enhance the understanding of evolving network behaviors

Inductive Learning for Continuous-Time Dynamics

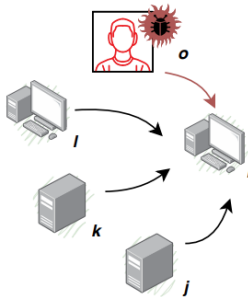
- Trains Jbeil as an inductive learning model, adapting to the continuous-time dynamic nature of the data
- Training involves both benign and malicious authentication events

Augmenting threat data using “lateral-movement-simulator”

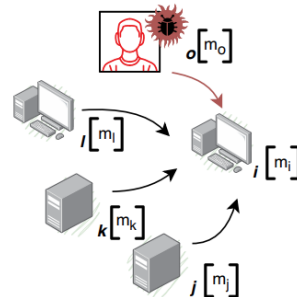
Make Jbeil open source on GitHub



1. Interaction events between source nodes j, k, l, o and destination node i at time t



2. Calculate the memory m for each interaction node at time t using previous memories m at time $t-1$

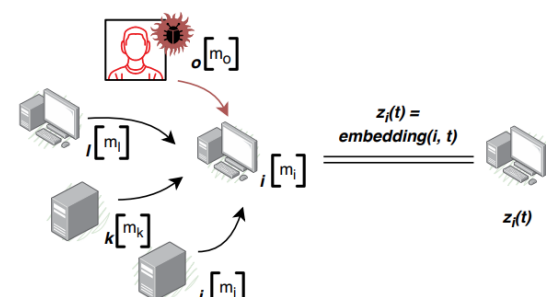


$$m_{src} = msg_{src}(m_{src}(t-1), m_{dst}(t-1), t) \quad (1)$$

$$m_{dst} = msg_{dst}(m_{src}(t-1), m_{dst}(t-1), t) \quad (2)$$

For every interaction event occurring at time t

3. Compute the final temporal embedding for each node using the graph at any time t



$$z_i(t) = \text{embedding}(i, t)$$

$$z_i(t) = \text{embedding}(i, t) = \sum_{j \in J(\{0, t\})} h(m_i(t), m_j(t), v_i(t), v_j(t)) \quad (3)$$

Calculate embedding of node i at any time t

| Dataset | Nodes | Edges | Type | Duration |
|---------------|--------|------------|-----------------|----------|
| LANL [70] | 15,610 | 49,341,300 | Net. Auth. logs | 58 Days |
| Pivoting [29] | 1,015 | 74,551,643 | Network flows | 1 Day |

| Experiments | Experiment 1 | | Experiment 2 | | Experiment 3 | |
|----------------|--------------|-----------|--------------|-----------|--------------|-----------|
| Training nodes | 9,886 | | 8,423 | | 6,943 | |
| Reasoning | Transductive | Inductive | Transductive | Inductive | Transductive | Inductive |
| Nodes # | 1,041 | 4,683 | 943 | 6,244 | 862 | 7,805 |
| Precision (%) | 98.93 | 98.48 | 97.65 | 97.52 | 67.85 | 66.83 |
| Recall (%) | 99.22 | 99.25 | 91.47 | 91.23 | 97.58 | 97.76 |
| AP (%) | 99.80 | 99.63 | 93.72 | 93.49 | 67.45 | 66.49 |
| AUC (%) | 99.82 | 99.73 | 94.76 | 94.59 | 75.62 | 74.55 |

| Network Flows | Training nodes | 1,015 | |
|------------------|----------------|--------------|-----------|
| | Reasoning | Transductive | Inductive |
| | Nodes # | 609 | 406 |
| Pivoting dataset | Precision (%) | 99.12 | 99.09 |
| | Recall (%) | 97.09 | 97.42 |
| | AP (%) | 97.72 | 97.84 |
| | AUC (%) | 98.12 | 98.26 |

Scenario 1 - Limited Knowledge Attack

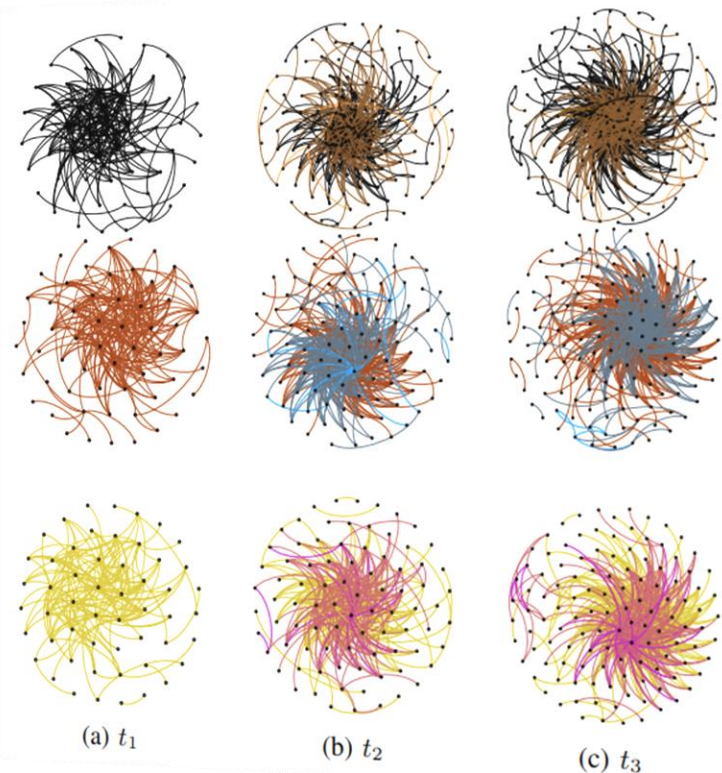
- Attacker only leverages knowledge of previously accessed machines.
- Attack stops generating new logins upon acquiring access to a system not accessible to the initial victim.

Scenario 2 - Informed Network Topology Attack

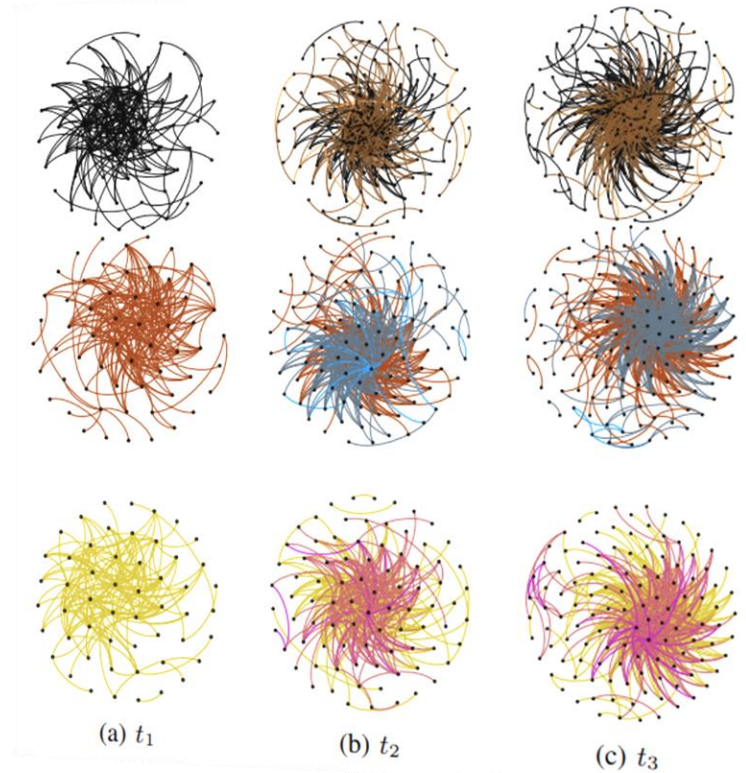
- Attacker possesses knowledge of the entire network topology.
- Attack terminates after accessing 50 devices or logging into every reachable machine with the final credential set.
- Logins only traverse edges previously traversed by valid users.

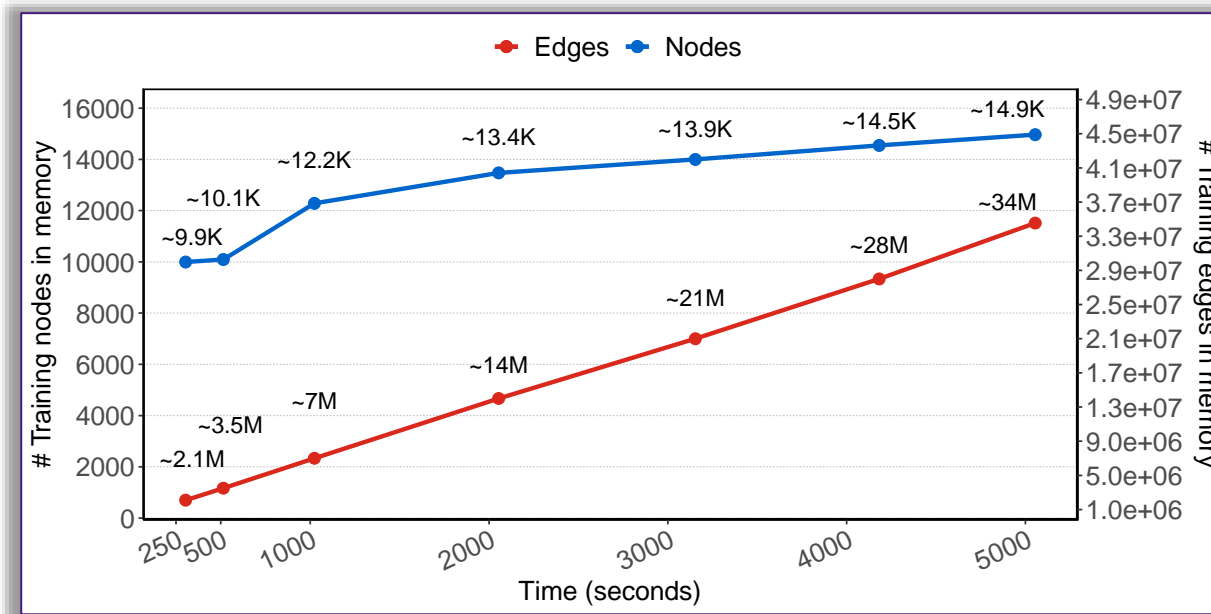
Scenario 3 - Targeted High-Value Server Attack

- Attacker is knowledgeable about the entire network topology.
- Performs multiple logins until access is gained to a high-value server.
- Logins follow edges traversed by valid users and use credentials if the authorized user recently logged into the source machine.



| Authentication attacks | Training nodes | 9,886 | |
|------------------------|-------------------|--------------|-----------|
| | Reasoning Nodes # | Transductive | Inductive |
| LANL - scenario 1 | Precision | 99.21 | 99.31 |
| | Recall | 98.17 | 98.84 |
| | AP | 99.67 | 99.49 |
| | AUC | 99.66 | 99.61 |
| LANL - scenario 2 | Precision | 99.38 | 99.31 |
| | Recall | 98.24 | 99.08 |
| | AP | 99.61 | 99.44 |
| | AUC | 99.54 | 99.60 |
| LANL - scenario 3 | Precision | 99.17 | 99.27 |
| | Recall | 97.95 | 98.83 |
| | AP | 99.59 | 99.36 |
| | AUC | 99.54 | 99.54 |





- In the transductive case when the number of nodes is 14.9K and the number of edges is 34M, the training time complexity is very high
- Inference time ranges from 12 seconds for a graph with 1 million edges, to ~6 minutes for a graph with 30 million edges

Assistant, Associate or Full Professor



Apply

Pay Grade:
Academic

Job Description:

[Faculty Positions - Cluster Hire \(Multiple positions available\)](#)
(Tenure-Track/Tenured)
School of Electrical Engineering and Computer Science
Louisiana State University

The Division of Computer Science and Engineering within the School of Electrical Engineering and Computer Science at Louisiana State University (LSU) in Baton Rouge is thrilled to announce a cluster hiring initiative for multiple faculty positions at the forefront of cybersecurity. This cluster hiring effort is a crucial component of the university's strategic plan to establish itself as a leader in defense and cybersecurity (

<https://www.lsu.edu/strategic-plan/planning/direction.php>). We invite applications for tenure-track Assistant Professors, with the possibility of considering exceptionally qualified candidates for positions at the Associate and Full Professor ranks with tenure. These roles are set to commence in August 2024 or earlier. At LSU, we are deeply committed to fostering diversity and inclusivity, and we strongly encourage women and minorities to apply. We are particularly interested in candidates with expertise in a range of areas, including but not limited to:

- System security (including fuzzing and TEEs)
- ML/AI safety & security
- Differential privacy
- Applied cryptography (including post-quantum cryptography)
- HCI & cybersecurity; usable security
- Cloud, web, and network security
- Cyber-physical and critical infrastructure security
- AI-driven cyber analytics
- Operational cybersecurity
- Hardware security
- Cyber forensics (defensive and offensive)
- Cyber threat intelligence

Assistant Professor



Apply

Job Description:

Assistant Professor (Tenure-Track)
School of Electrical Engineering and Computer Science
Louisiana State University

The School of Electrical Engineering and Computer Science (EECS) at Louisiana State University (LSU), Baton Rouge invites applications for a tenure-track Assistant Professor position starting August 2024. The EECS School consists of the Electrical and Computer Engineering (ECE), and the Computer Science and Engineering (CSE) divisions.

We seek candidates with expertise that complement and add to the current cybersecurity focus of the school, particularly in the areas of hardware security and trust, and security aspects of cyber-physical systems, IoT, and industrial control systems. Candidates in other areas of cybersecurity, including trustworthy AI and machine learning, AI-driven cyber-analytics, cyber-forensics, security in distributed systems, network security, and cloud and web security are also encouraged to apply.

LSU is Louisiana's flagship university and is committed to expanding its cybersecurity research and education presence. The EECS school has a strong track record in research and graduate training, with active research projects in various electrical engineering, and computer science and engineering fields. LSU is an NSA-designated Center of Academic Excellence in Cyber Operations (CAE-CO). The ECE Division offers ABET-Accredited programs in Electrical Engineering and Computer Engineering. The CSE Division offers concentrations in Software Engineering, Cybersecurity, Cloud Computing, and Data Science at the undergraduate level.