Hopper: Modeling and Detecting Lateral Movement

Grant Ho*, Mayank Dhiman, Devdata Akhawe, Vern Paxson, Geoffrey M. Voelker, Stefan Savage, David Wagner

UC San Diego*, UC Berkeley*, Dropbox*, Figma, ICSI
How can we thwart attackers after they breach an enterprise’s internal network?
Enterprise attackers often need to move beyond their initial point of compromise
Enterprise attackers often need to move beyond their initial point of compromise.
Lateral Movement:
Attacker movement *between* **internal** machines
**The Problem:** Detecting Lateral Movement

**Threat model:** attacker has successfully compromised an internal *Machine A* and wants to get to some target *Machine Z*

**Goal:** detect malicious movement b/t internal machines w/ low false positives

**Prior work:** *anomalous* movement activity = an attack

- “Authentication graphs: Analyzing user behavior within an enterprise network”. A Kent et al. 2015
- “Detecting Structurally Anomalous Logins Within Enterprise Networks”. H Siadati, N Memon. 2017
- “Latte: Large-Scale Lateral Movement Detection”. Q Liu et al. 2018
- “Log2vec: A Heterogeneous Graph Embedding Based Approach for Detecting Cyber Threats within Enterprise”. Liu et al. 2019
- “Detecting Lateral Movement in Enterprise Computer Networks with Unsupervised Graph AI”. B Bowman et al. 2020
- ...
The Problem: Detecting Lateral Movement

**Goal:** detect malicious movement between internal machines with *low false positives*

**Prior work:** anomalous movement activity = an attack

**Key Limitation:** Prior state-of-the-art generates *too many FPs* (\(\geq 100\)’s per day)

- Deluge of anomalous-but-benign activity in modern enterprises
**Our work:** Detecting Lateral Movement

**Hopper:** detects malicious movement between internal machines

- Detects > 94% attacks with < 9 FP per day
- Evaluated on 15 months of data at Dropbox
- No labeled data needed

**Key insight:** look for movement that is *suspicious* and not just statistically anomalous
Movement between machines (ssh, RDP, Kerberos, etc.) produces “login” records

Standard login information
- session start time \((t_1)\),
- username (Alice),
- source machine (A),
- dest machine (Y)
Detection

• **Training:** Build a graph from historical logins
Detection setup: Find suspicious login paths

Detection

• **Training**: Build a graph from historical logins

• **Test**: Given a new set of logins, do any form a *suspicious* path?

Key Question
What does it mean for a login path to be “suspicious”?
What is a suspicious path?
Decomposing Lateral Movement
What is a suspicious path?
Decomposing Lateral Movement
What is a suspicious path?
Decomposing Lateral Movement
What is a suspicious path?
Decomposing Lateral Movement

Bob lacks access to the target machine
What is a suspicious path?
Decomposing Lateral Movement

Attack Step 1:
Move laterally to steal additional (privileged) credentials from new machines
What is a suspicious path? Decomposing Lateral Movement

Attack Step 2:
Use new, privileged credentials to access target machine
Property #1: path contains 1+ login that uses a new or unexpected set of credentials
Property #2: path accesses a machine that the initial user does not have legitimate access to
Property #1: path has a login that uses an unexpected set of credentials
Property #2: path accesses a machine that the initial user could not access
Correctly identifying which set of logins form paths “caused” by same user

- Which inbound login forms a path with login L_4?
  - Real-world authentication logs don’t provide causality information
Overview: Key sub-problems + our solutions

Correctly identifying which set of logins form paths “caused” by same user
  • Methods to infer login causality using enterprise domain knowledge

Handling gaps & ambiguity in path inference
  • Conservatively infer multiple potential paths
  • Specification-based anomaly detection:
    reduce FP by selectively applying anomaly detection
    only to paths that potentially contain both suspicious properties
15 months of data from Dropbox’s internal corp network: 700M+ logins

- 1 red-team attack + 326 simulated attacks:
  - various goals (e.g., ransomware & targeted compromise) + stealthiness

### Evaluation

<table>
<thead>
<tr>
<th></th>
<th>Hopper</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Positives</td>
<td>309 / 327</td>
</tr>
<tr>
<td>(Detection Rate)</td>
<td></td>
</tr>
<tr>
<td>False Positives</td>
<td>3,560</td>
</tr>
<tr>
<td>Avg Daily Alerts</td>
<td>9 alerts / day</td>
</tr>
</tbody>
</table>
15 months of data from Dropbox’s internal corp network: 700M+ logins

- 1 red-team attack + 326 simulated attacks:
  - various goals (e.g., ransomware & targeted compromise) + stealthiness

### Evaluation

<table>
<thead>
<tr>
<th></th>
<th>Hopper</th>
<th>SAL (CCS 2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>True Positives</strong></td>
<td>309 / 327</td>
<td>309 / 327</td>
</tr>
<tr>
<td>(Detection Rate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>False Positives</strong></td>
<td>3,560</td>
<td>27,927</td>
</tr>
<tr>
<td><strong>Avg Daily Alerts</strong></td>
<td>9 alerts / day</td>
<td>71 alerts / day</td>
</tr>
</tbody>
</table>

- Equal Detection
15 months of data from Dropbox’s internal corp network: 700M+ logins

- 1 red-team attack + 326 simulated attacks:
  various goals (e.g., ransomware & targeted compromise) + stealthiness

### Evaluation

<table>
<thead>
<tr>
<th></th>
<th>Hopper</th>
<th>SAL (CCS 2017)</th>
</tr>
</thead>
<tbody>
<tr>
<td>True Positives</td>
<td>309 / 327</td>
<td>309 / 327</td>
</tr>
<tr>
<td>(Detection Rate)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>False Positives</td>
<td>3,560</td>
<td>27,927</td>
</tr>
<tr>
<td>Avg Daily Alerts</td>
<td>9 alerts / day</td>
<td>71 alerts / day</td>
</tr>
</tbody>
</table>

Our Work (Hopper)

- **8x** improvement over state-of-the-art (traditional anomaly detection)
- Key improvement = look for paths with suspicious structure, rather than just statistical anomalies
• Analyzing network movement between *internal machines* can help mitigate enterprise attacks

• Enterprises have lots of anomalous-but-benign activity: need to combine anomaly detection w/ *suspicious structure* for practical detection

• Identifying *causally-related movement* is challenging, but provides a powerful detection paradigm

• Hopper, an approach built on these ideas, detected > 94% of lateral movement scenarios with < 9 FP / day across 15 months at Dropbox