Anomaly Extraction in Backbone Networks using Association Rules

Daniela Brauckhoff
Xenofontas (Fontas) Dimitropoulos
Arno Wagner
Kave Salamatian
Anomaly extraction

- **Problem statement:**
  - Given a large set of flows observed during a time interval labeled with an anomaly alert find and summarize the flows involved in the event(s) that triggered the alert.

- **Motivation:**
  - Root cause analysis
  - Attack mitigation
  - Anomaly modeling
Approach Overview (3 steps)

- **Detection:** Use a number of *histogram-based detectors*:
  - Identify affected bins and create set V of corresponding feature values
  - Use histogram cloning to reduce collisions and false positives
Approach Overview (3 steps)

- **Detection**: Use a number of histogram-based detectors:
  - Identify affected bins and create set $V$ of corresponding feature values
  - Use histogram cloning to reduce collisions and false positives
Approach Overview (3 steps)

- **Detection**: Use a number of histogram-based detectors:
  - Identify affected bins and create set V of corresponding feature values
  - Use histogram cloning to reduce collisions and false positives
Approach Overview (3 steps)

- **Detection**: Use a number of histogram-based detectors:
  - Identify affected bins and create set V of corresponding feature values
  - Use histogram cloning to reduce collisions and false positives
- **Filtering**: Filter flows that match union of meta-data provided by N detectors
  - Filtered flows are called “suspicious“ flows
- **Mining**: Use association rules to extract and summarize anomalous flows from the set of suspicious flows
Association Rule Mining

- Given a a number of itemsets, find frequent subsets which are common to at least a minimum number s of the itemsets.
- An itemset is a flow (7-tuple): {srcIP, dstIP, srcPort, dstPort, proto, #packets, #bytes}
- **Key intuition**: anomalies trigger a large number of flows with one or more common feature values, e.g., src IP addr, dst port, #packets.
- Use modified Apriori algorithm to find frequent subsets
- Example output:

<table>
<thead>
<tr>
<th>l</th>
<th>srcIP</th>
<th>dstIP</th>
<th>srcPort</th>
<th>dstPort</th>
<th>#packets</th>
<th>#bytes</th>
<th>support</th>
<th>what</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>2</td>
<td>*</td>
<td>10,407</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>25</td>
<td>*</td>
<td>22,659</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Host A</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>*</td>
<td>*</td>
<td>11,800</td>
<td>HTTP Proxy</td>
</tr>
<tr>
<td>2</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>*</td>
<td>6</td>
<td>*</td>
<td>35,475</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>80</td>
<td>*</td>
<td>*</td>
<td>14,477</td>
<td>HTTP Proxy</td>
</tr>
<tr>
<td>2</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>80</td>
<td>7</td>
<td>*</td>
<td>16,653</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Host C</td>
<td>*</td>
<td>80</td>
<td>*</td>
<td>5</td>
<td>*</td>
<td>15,230</td>
<td>HTTP Cache</td>
</tr>
<tr>
<td>2</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>80</td>
<td>5</td>
<td>*</td>
<td>58,304</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>1</td>
<td>46</td>
<td>17,212</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>*</td>
<td>1</td>
<td>48</td>
<td>11,833</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>80</td>
<td>1</td>
<td>1024</td>
<td>23,696</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>*</td>
<td>*</td>
<td>80</td>
<td>7000</td>
<td>1</td>
<td>48</td>
<td>12,672</td>
<td>Dist. Flooding</td>
</tr>
<tr>
<td>4</td>
<td>*</td>
<td>Host D</td>
<td>*</td>
<td>9022</td>
<td>1</td>
<td>48</td>
<td>22,573</td>
<td>Backscatter</td>
</tr>
<tr>
<td>5</td>
<td>*</td>
<td>Host E</td>
<td>54545</td>
<td>7000</td>
<td>1</td>
<td>48</td>
<td>23,799</td>
<td>Dist. Flooding</td>
</tr>
<tr>
<td>5</td>
<td>*</td>
<td>Host E</td>
<td>45454</td>
<td>7000</td>
<td>1</td>
<td>46</td>
<td>15,627</td>
<td>Dist. Flooding</td>
</tr>
</tbody>
</table>
**Accuracy**

- Use a two week NetFlow trace from SWITCH
- Manually classify generated itemsets as true/false positives
- Zero false positive itemsets for 21 anomalies (out of 31)
- False positive itemsets for remaining 10 anomalies →
- On average between 2 and 8.5 false positive itemsets
Conclusions

- Combination of histogram-based detectors and association rule mining works well for extracting anomalous flows

- Further reading: