Enriching IDS events using traffic monitoring data

Ralph Koning
Universiteit van Amsterdam

Nick Buraglio (ESnet), Paola Grosso (UvA), Cees de Laat (UvA)
Motivation

To effectively block attacks, the information from an IDS is not always sufficient.

When an event triggers, the security team has to manually collect additional data from different sources to enrich the event to create context and understanding of the event. Only then appropriate action can be taken.
ESnet

ENERGY SCIENCES NETWORK

- Ames: Ames Laboratory (Ames, IA)
- ANL: Argonne National Laboratory (Argonne, IL)
- BNL: Brookhaven National Laboratory (Upton, NY)
- FNAL: Fermi National Accelerator Laboratory (Batavia, IL)
- JLAB: Thomas Jefferson National Accelerator Facility (Newport News, VA)
- LBNL: Lawrence Berkeley National Laboratory (Berkeley, CA)
- ORNL: Oak Ridge National Laboratory (Oak Ridge, TN)
- PNPL: Pacific Northwest National Laboratory (Richland, WA)
- PPPL: Princeton Plasma Physics Laboratory (Princeton, NJ)
- SLAC: SLAC National Accelerator Laboratory (Menlo Park, CA)
Carrier networks are different

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Enterprise/Campus</th>
<th>Carrier/Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>network capacity</td>
<td>small: one organization</td>
<td>huge: accommodates many institutions</td>
</tr>
<tr>
<td>external connectivity</td>
<td>limited (single or redundant uplink)</td>
<td>many connected networks</td>
</tr>
<tr>
<td>application security</td>
<td>security can be tailored to application</td>
<td>need to allow everything</td>
</tr>
<tr>
<td>restrictions and policies</td>
<td>can be applied anywhere</td>
<td>subject net neutrality laws</td>
</tr>
<tr>
<td>impact of countermeasure</td>
<td>may affect users of a host or system accommodates</td>
<td>can affect many users and other networks</td>
</tr>
</tbody>
</table>
Research questions

Can we correlate data from these different sources?

Can we build a poc system that does live correlation of the events on a carrier network?

Do we gain new options and information from enriching the information?
CoreFlow

- Input: Bro events
- Enricher: Packet Design Route Analyzer
- Enricher: netflow data
- Output: Enriched Events
ESnet implementation
CoreFlow execution

1. **Start**
   - `event_id` from `bro` event
   - `create()` from `assign event_id or EOF`

2. **Read Bro Events**
   - `event_id, bro_alert`

3. **Assign Event ID or EOF**
   - `assign event_id or EOF`

4. **Search Flows**
   - `poolsize = 20`

5. **Map Netflow to Events**
   - `event_id, flow`

6. **Extract Flow Data**
   - `event_id`

7. **Add Flow Data to Event**
   - `event_id` [netflow, ...]

8. **Estimate Route**

9. **Export Results**

10. **Stop**

Application: traffic spoofing
Route Estimation

Algorithm 1 route estimation algorithm
1: $\text{topology} \leftarrow$ topology graph of the network
2: $\text{depth} \leftarrow$ max search depth
3: $D \leftarrow$ detected routers in the path
4: **procedure** $\text{ESTIMATE\_PATH}(D)$
5: \hspace{2em} $\text{start} \leftarrow D[0]$
6: \hspace{2em} $P \leftarrow$ all paths up to $\text{depth}$ from $\text{start}$ in $\text{topology}$
7: \hspace{2em} for each $p \in P$ do
8: \hspace{3em} $R \leftarrow$ add reverse$(\text{path})$
9: \hspace{2em} end for
10: \hspace{2em} for each $p \in P$ do
11: \hspace{3em} for each $r \in R$ do
12: \hspace{4em} $A \leftarrow$ add $r + p[1:]$
13: \hspace{3em} end for
14: \hspace{2em} end for
15: \hspace{2em} for each $p \in A$ do
16: \hspace{3em} if $D \subseteq p$ then
17: \hspace{4em} $F \leftarrow$ add $p$
18: \hspace{3em} end if
19: \hspace{2em} end for
20: \hspace{2em} for each $p \in F$ do
21: \hspace{3em} $O \leftarrow \min(\text{lenght}(p))$
22: \hspace{3em} end for
23: \hspace{2em} return $O$
24: **end procedure**
Route Estimation: Example
Conclusion

Enriching IDS data with NetFlow information gives a better view of an attack.

The enriched information can be used to set up and automate more advanced countermeasures.
Future work

<table>
<thead>
<tr>
<th>Aspect</th>
<th>Enterprise/Campus</th>
<th>Carrier/Transit</th>
</tr>
</thead>
<tbody>
<tr>
<td>external connectivity</td>
<td>limited (single or redundant uplink) security can be</td>
<td>many connected networks</td>
</tr>
<tr>
<td>application security</td>
<td>tailored to application</td>
<td>need to allow everything</td>
</tr>
<tr>
<td>restrictions and policies</td>
<td>can be applied anywhere</td>
<td>subject net neutrality laws</td>
</tr>
<tr>
<td>impact of countermeasure</td>
<td>may affect users of a host or system accommodates</td>
<td>can affect many users and other networks</td>
</tr>
<tr>
<td>network capacity</td>
<td>one organization</td>
<td>accommodates many institutions</td>
</tr>
</tbody>
</table>
EOF

Contact:

Ralph Koning (UvA / ESnet)
r.koning _at_ uva.nl
https://staff.fnwi.uva.nl/r.koning/