CAMNEP: Multistage Collective Network Behavior Analysis System with Hardware Accelerated NetFlow Probes

Martin Rehak, Pavel Celeda, Michal Pechoucek, Jiri Novotny

CESNET, z. s. p. o.
Gerstner Laboratory - Agent Technology Center
Department of Cybernetics, Czech Technical University
Institute of Computer Science, Masaryk University

Supported by Czech Ministry of Education grants 6383917201 (CESNET), 1M0567, 6840770038 (CTU) and
CERDEC/ITC-A projects N62558-07-C-0001, W911NF-08-1-0250
Overview

- Network Intrusion Detection Systems
- Anomaly Detection Models
- Trust-Based Anomaly Integration
- Experimental Results
Network Intrusion Detection

- Identification of attacks against hosts or networks from the network traffic observation
  - **Signature based** - detects patterns in packet content
  - **Stateful protocol analysis** - anomalies in TCP protocol state sequences
  - **Network Behavior Analysis (NBA)** - identifies attacks from traffic statistics

- Current Challenges
  - **False positives** - legitimate traffic labeled as malicious
  - **False negatives** - malicious traffic classified as legitimate
  - **Performance** - high network speed, near-real-time results

- **Our Contribution**: Efficient algorithm for integration of NBA methods
  - Linear with traffic
  - Improves the classification rate by multi-layer combination
  - Based on extended trust modeling
System Architecture

Traffic Acquisition Layer
- **Preprocessing**
- **Collector**
  - FlowMon Probe
  - FlowMon Probe
  - FlowMon Probe

Operator Interface Layer
- Operator
- Security Incidents Up to 10 incidents/minute
- Requests for Additional Information
- Operator Interface displays the incidents
- Aggregated Flow Statistics: Up to 100k flows/minute
- Additional Flow Data
- Requests for Additional Flow Data

Detection Agents Layer
- Cooperative Threat Detection
  - Agent Platform
  - Agent
  - Agent

Visualisation Agent
- Detected Threats Up to 10k flows/minute
- Additional Flow Data Requests
- NetFlow Data: Up to 3800 new flows/s

Traffic Acquisition Layer provides the traffic statistics
High-Speed Network Traffic Acquisition

- **Probes** observe the traffic at the wire speed
- Each probe generates **NetFlow** traffic statistics
- Results are stored and preprocessed in **collector** servers
- **Hardware acceleration** necessary for high-speed networks
Hardware Accelerated FlowMon Probe

- **Requirements:**
  - traffic characteristics change heavily in time - network probes must behave reliably in all possible cases
  - capable of generating **NetFlow traffic statistics**
  - work at **wire speed** (1Gbits/sec - 10Gbits/sec)

- **FlowMon Probe:**
  - developed in Liberouter project
  - hardware accelerated network card based on COMBO hardware
  - high performance and accuracy
  - handles 1Gbits/sec and 10Gbits/sec traffic at line rate
  - exports acquired NetFlow data to different collectors
Traffic Acquisition Server Architecture

Cooperative Threat Detection

tasd

shared memory

cmd

data

nfdump

Traffic Acquisition Server

nfcapd

nfcapd

nfcapd

NetFlow Data v5,v9

FlowMon Probe

FlowMon Probe

FlowMon Probe

NetFlow Data v5,v9
Detection Process Overview

- Each agent based on one **anomaly detection** method
- **Input:** NetFlow statistics, same for all agents
- **Anomaly:** aggregated from individual agent’s anomalies
- **Update:** heterogenous trust model are updated, each has a **different structure**
- **Query:** all agents evaluate all flows, and aggregate the output
## Anomaly Detection Input (simplified)

<table>
<thead>
<tr>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Pack.</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.195.164:1086</td>
<td>192.168.10.12:445</td>
<td>.A....</td>
<td>2</td>
<td>84</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>62.97.162.208:3417</td>
<td>192.168.192.83:1172</td>
<td>.AP...</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.077</td>
<td>TCP</td>
<td>192.168.195.132:2544</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.076</td>
<td>TCP</td>
<td>192.168.195.132:2545</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.19.247:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.19.247:53</td>
<td>192.168.60.31:4021</td>
<td>......</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.60.1:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4020</td>
<td>192.43.244.18:123</td>
<td>......</td>
<td>1</td>
<td>72</td>
</tr>
<tr>
<td>30.276</td>
<td>TCP</td>
<td>192.168.192.170:61158</td>
<td>71.33.170.53:1358</td>
<td>.AP...</td>
<td>307</td>
<td>368627</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>24.28.89.160:63319</td>
<td>192.168.192.83:58359</td>
<td>......</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>63.208.197.21:443</td>
<td>192.168.192.106:1031</td>
<td>.AP...</td>
<td>1</td>
<td>73</td>
</tr>
<tr>
<td>0.093</td>
<td>TCP</td>
<td>192.168.193.58:1302</td>
<td>192.168.192.5:110</td>
<td>.AP.SF</td>
<td>8</td>
<td>356</td>
</tr>
<tr>
<td>0.093</td>
<td>TCP</td>
<td>192.168.192.5:110</td>
<td>192.168.193.58:1302</td>
<td>.AP.SF</td>
<td>8</td>
<td>440</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>85.160.81.10:6766</td>
<td>192.168.192.217:11084</td>
<td>......</td>
<td>1</td>
<td>45</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.192.217:11084</td>
<td>85.160.81.10:6766</td>
<td>......</td>
<td>1</td>
<td>45</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.19.247:1723</td>
<td>192.168.60.19:1042</td>
<td>.AP...</td>
<td>1</td>
<td>56</td>
</tr>
</tbody>
</table>
Anomaly Detection Methods: MINDS

- **Features:** Flow counts from/to important IP/port combinations.
- **Classification:** Comparison with windowed average of past values, different from original MINDS.
Anomaly Detection Methods: Xu et al.

- **Features:** Determines the entropies of dstIP, dstPrt and srcPrt on the set of all flows from each source IP.
- **Classification:** Classifies the traffic with a set of static rules.
- All flows from the same source share the classification features and result.
Uses Principal Component Analysis to predict the volume of traffic from individual sources.

**Features:** Ratio of predicted/observed numbers of bytes, packets and flows.

**Classification:** Anomaly is derived from the ratio of prediction and observation, for all flows from the same source.
Anomaly Detection Methods: Entropy Prediction, Lakhina et al.

- Uses Principal Component Analysis to predict the entropies of features on the flows from each source IP.

- **Features:** Difference between the predicted and observed entropies of dstIP, dstPrt and srcPrt on the set of all flows from each source IP.

- **Classification:** Anomaly is derived from the difference between the prediction and observation, defined by the source only.
Extended Trust Modeling

- Agents describe each flow using its **identity** and **context**.
- **Identity** - defined by the features measured on the flow
- **Context** - uses the features from the AD model, measured on other flows
- Metric **feature space**, metrics determines similarity
- Trustfulness is determined for cluster **centroids** in the feature space
## Extended Trust Modeling: Identity/Context Example

<table>
<thead>
<tr>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Pack.</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.195.164:1086</td>
<td>192.168.10.12:445</td>
<td>.A....</td>
<td></td>
<td>84</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>62.97.162.208:3417</td>
<td>192.168.192.83:1172</td>
<td>.AP...</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.195.164:2544</td>
<td>194.228.32.3:80</td>
<td>.AP...</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.576</td>
<td>TCP</td>
<td>192.168.195.132:2545</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.19.247:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.195.164:1087</td>
<td>192.168.60.31:445</td>
<td>......</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.60.1:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4020</td>
<td>192.43.244.18:123</td>
<td>......</td>
<td>1</td>
<td>72</td>
</tr>
</tbody>
</table>

### Identity
- srcIP: 192.168.195.164
- dstIP: 192.168.10.12
- srcPrt: 1086
- dstPrt: 445
- protocol: TCP
- bytes: 84
- packets: 2

### Context (MINDS)
- count-srcIP: 3
- count-dstIP: 1
- count-srcIP-dstPrt: 2
- count-dstIP-srcPrt: 1
## Extended Trust Modeling: Identity/Context Example

<table>
<thead>
<tr>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Pack.</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.195.164:1086</td>
<td>192.168.10.12:445</td>
<td>.A...</td>
<td>2</td>
<td>84</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>62.97.162.208:3417</td>
<td>192.168.192.83:1172</td>
<td>.A.P...</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.577</td>
<td>TCP</td>
<td>192.168.195.164:2544</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.576</td>
<td>TCP</td>
<td>192.168.195.132:2545</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.19.247:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.195.164:1087</td>
<td>192.168.60.31:445</td>
<td>......</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.60.1:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4020</td>
<td>192.43.244.18:123</td>
<td>......</td>
<td>1</td>
<td>72</td>
</tr>
</tbody>
</table>

### Identity
- srcIP: 192.168.195.164
- dstIP: 192.168.10.12
- srcPrt: 1086
- dstPrt: 445
- protocol: TCP
- bytes: 84
- packets: 2

### Context (MINDS)
- count-srcIP: 3
- count-dstIP: 1
- count-srcIP-dstPrt: 2
- count-dstIP-srcPrt: 1
# Extended Trust Modeling: Identity/Context Example

<table>
<thead>
<tr>
<th>Duration</th>
<th>Proto</th>
<th>Src IP Addr:Port</th>
<th>Dst IP Addr:Port</th>
<th>Flags</th>
<th>Pack.</th>
<th>Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>192.168.195.164:1086</td>
<td>192.168.10.12:445</td>
<td>.A....</td>
<td>2</td>
<td>84</td>
</tr>
<tr>
<td>0.000</td>
<td>TCP</td>
<td>62.97.162.208:3417</td>
<td>192.168.192.83:1172</td>
<td>.A....</td>
<td>1</td>
<td>42</td>
</tr>
<tr>
<td>0.577</td>
<td>TCP</td>
<td>192.168.195.164:2544</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.576</td>
<td>TCP</td>
<td>192.168.195.132:2545</td>
<td>194.228.32.3:80</td>
<td>.A.R..</td>
<td>3</td>
<td>126</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.19.247:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.195.164:1087</td>
<td>192.168.60.31:445</td>
<td>......</td>
<td>1</td>
<td>149</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4021</td>
<td>192.168.60.1:53</td>
<td>......</td>
<td>1</td>
<td>55</td>
</tr>
<tr>
<td>0.000</td>
<td>UDP</td>
<td>192.168.60.31:4020</td>
<td>192.43.244.18:123</td>
<td>......</td>
<td>1</td>
<td>72</td>
</tr>
</tbody>
</table>

**Identity**
- **srcIP:** 192.168.195.164
- **dstIP:** 192.168.10.12
- **srcPrt:** 1086
- **dstPrt:** 445
- **protocol:** TCP
- **bytes:** 84
- **packets:** 2

**Context (MINDS)**
- **count-srcIP:** 3
- **count-dstIP:** 1
- **count-srcIP-dstPrt:** 2
- **count-dstIP-srcPrt:** 1
Extended Trust Modeling

- Agents describe each flow using its **identity** and **context**.
- **Identity** - defined by the features measured on the flow
- **Context** - uses the features from the AD model, measured on other flows
- Metric **feature space**, metrics determines similarity
- Trustfulness is determined for cluster **centroids** in the feature space
Trust Update and Query

- Trustfulness update:
  1. Find relevant centroids
  2. Determine the update weight for each centroid
  3. Update the trustfulness of centroid using a given weight

- Trustfulness query:
  1. Find relevant centroids
  2. Determine the weight for each centroid
  3. Aggregate the trustfulness from centroid, with respective weights
Multi-Source Trustfulness Integration

- Effectiveness improved by:
- **Aggregated anomaly value** reduces the effect of singular anomaly peaks
- Similarity between flows varies between the agents e.g. trustfulness is based on anomaly aggregated over the agent-specific clusters
- Normalized individual **trustfulness** is re-aggregated into the common value
Agent Specific Clusters

Attack data (as identified by other agent) are concentrated in a single centroid.

False positive data are spread across the whole feature space of other agent.
System Output
Known Attacks, Regardless of Type

![Graph showing the trustfulness of malicious flows over the number of malicious flows. The graph includes various markers and symbols representing different types of attacks and their trustfulness values.](https://via.placeholder.com/150)

- **θ_M** MINDS
- **θ_X** Xu
- **θ_V** Volume pred
- **θ_E** Entropy pred
- **θ_A** Aggreg found
- **θ_A** Aggreg not found
# Third Party Attacks Results

<table>
<thead>
<tr>
<th></th>
<th>Anomalous</th>
<th>Untrusted</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$A_M$</td>
<td>$A_X$</td>
</tr>
<tr>
<td></td>
<td>$\Theta_M$</td>
<td>$\Theta_X$</td>
</tr>
<tr>
<td><strong># flows</strong></td>
<td>detected</td>
<td>6653</td>
</tr>
<tr>
<td></td>
<td>TP</td>
<td>35</td>
</tr>
<tr>
<td></td>
<td>FP</td>
<td>6618</td>
</tr>
<tr>
<td></td>
<td>FP[%] all traffic</td>
<td>15.9 %</td>
</tr>
<tr>
<td><strong># srcIP</strong></td>
<td>detected</td>
<td>72.5</td>
</tr>
<tr>
<td></td>
<td>TP</td>
<td>1.7</td>
</tr>
<tr>
<td></td>
<td>FP</td>
<td>70.8</td>
</tr>
<tr>
<td></td>
<td>FP[%] all traffic</td>
<td>1.52 %</td>
</tr>
</tbody>
</table>
Trustfulness Histogram - Flows

θ⁻¹ Aggregator
SSH Brute Force Attack

0 0.1 0.2 0.3 0.4 0.5 0.6 0.7 0.8 0.9 1
0 500 1000 1500 2000 2500
Trustfulness
Number of Flows
Impact of Collaboration 2

Trustfulness Histogram - Flows

θ Entropy pred collective
SSH Brute Force Attack
avg avg - σ avg - 1.5σ

θ Xu collective
SSH Brute Force Attack
avg avg - σ avg - 1.5σ

θ Xu alone
SSH Brute Force Attack
avg avg - σ avg - 1.5σ
Reporting

Traffic Acquisition Server

Agent A  Agent B  Agent C

Trust Aggregation

Events

IT-A1  IT-A2  IT-A3

Incident reporting

FlowMon Probe

Attack

Text report

Analyzer: ConepeM-4
Create Time: 2007-12-27T14:13:01.012+0100
Classification: port_sena_vertical
Sources:
Nodes: 147.251.192.59
Ports: 0.22, 32059, 56064, 56066
Protocol: UDP, ICMP, TCP

Targets:
Nodes: 147.32.94.185 147.251.50.156 147.251.192.1
Protocol: UDP, ICMP, TCP
Conclusions

- Collaborative trust mechanism reduces the error rate of existing anomaly detection approaches.

- The error rate reduction is achieved by:
  - Aggregation of anomaly values
  - Specific trust models of individual agents, each providing different insight into the flow data
  - Trustfulness aggregation re-integrates the opinions from the various trust models, each using different perspective

- Agent-based trust techniques can be used under high-performance constraints.

- A-Globe multi-agent platform has negligible computational overhead, architecture naturally scales to multiprocessor environments.
Thank You For Your Attention