**Method Principle**

**Collection**
- **INPUT:** Traffic descriptors (source and destination addresses, ports, protocols, entropy, etc.).
- **SOURCE:** Switches, routers, network probes, etc.
- **ALTERNATE SOURCE:** With proper preprocessing even the output of other methods.

**Decomposition**
- Creation of so-called **ASPECTS**.
- **ASPECT:** A vector field generated by a vector which elements are a subset of available traffic descriptors.
- **EXAMPLE 1:** Traffic volume (generated by time and byte count).
- **EXAMPLE 2:** Service usage (generated by time, port, byte count and eventually host).

**Analysis**
- **ASPECT:** n-dimensional array, filled gradually and analyzed for deviations in given time intervals.
- **METHODS:** Arbitrary. Best suited for linear and non-linear filtering.
- **NON-LINEAR FILTERS:** Detect static deviations (the number of connected computers rises over certain threshold).
- **LINEAR FILTERS:** Tackle dynamic aspects of traffic. Identify deviations in trends.

**Recomposition**
- **MOTIVATION:** Analyzed aspects rarely identify attack (false positive).
- **CORRELATION** of findings in each aspect.
- Aspects are **COMPOSED** into vector field with dimensions equal to all employed traffic descriptors.
- **DEVIATIONS** of different aspects influence each other, even in dimensions they are not defined for.

**Example Detection**

**Discovering the Chuck Norris botnet** [1].

**Collection phase**
- **TRAFFIC DESCRIPTORS:** Source and destination IPs and ports, byte count, TCP flags, timestamp
- **TIME FRAME:** 5 minutes

**Decomposition phase**
- **4 ASPECTS** selected for analysis.

1) **Overall Traffic volume for each port**
2) **Traffic volume for each host and port**
3) **SYN flag only host communication**
4) **Distinct connections for each host**

**Analytic phase**

- **LINEAR** Sobel operator (LSO) applied on the **PC** reveals spikes in port 23 usage.
- A thresholding **NON-LINEAR** operator (TNO) applied on the **PC** shows high **TRAFFIC** on a port that should not be used.
- **LSO** applied on the **PC** reveals **SPIKES** in port 23 usage. **RAPID BURSTS** of packets.
- **TNO** applied on the **PC** shows that host tries to connect to too many other hosts. Possible **SCANNING**.
- **TNO** applied on the **PC** reveals hosts that communicate with **TOO MANY** other hosts.

**Recomposition and attack identification**
- **DEVIATION IN MORE ASPECTS:** Likely to be part of the botnet.
- Deviations combined cross certain threshold.

**Conclusion**

- On a simple example, we have shown how the aspect-based detection can reveal botnet zombies in a network.
- Using more aspects or other filters, different attacks can be discovered, even those previously unknown.

<table>
<thead>
<tr>
<th>Safe subspace</th>
<th>Suspicious subspace</th>
<th>Attack subspace</th>
</tr>
</thead>
</table>

**Reference**


**Acknowledgment**

This material is based upon work supported by the Czech Ministry of Defence under Contract No. SMC00288PR880-OVMSUN20801.