Real-time Protocol
Shepherds

Raytheon BBN technologies
Ron Watro

17 September 2013
Raytheon BBN Technologies

BGP Routing Security

First Internet router

Acquired by Raytheon in 2010

First deployment of Quantum Key Distribution

Route Origin Authorization (ROA)

<table>
<thead>
<tr>
<th>Origin ASN:</th>
<th>17771</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not valid Before:</td>
<td>2010-12-07 00:00:00</td>
</tr>
<tr>
<td>Not valid After:</td>
<td>2011-12-07 23:59:59</td>
</tr>
<tr>
<td>Prefixes:</td>
<td>2405:1e00::/32 (max length /48)</td>
</tr>
<tr>
<td></td>
<td>202.63.96.0/19 (max length /24)</td>
</tr>
<tr>
<td></td>
<td>49.238.32.0/19 (max length /32)</td>
</tr>
</tbody>
</table>

National Technology Medal

Current programs: PlanX, ICAS, VET, CSFV, APAC, CRASH, CyberGenome, PROCEED, SAFER, MilNetP, ...
Customers need automated, faster-than-human, response to sophisticated attacks.

Attacks are commonly novel enough to bypass conventional signature checking.

Advanced Persistent Threat (APT) does not announce itself; rather, it...
- Penetrates an enclave
- Remains resident and exfiltrates data
- Damage can be long lasting

...without costing too much!!!
Approach

• RePS uses “inherent anomaly detection” as a basis for finding zero-day attacks
  – “Inherent” implies no training required
  – Based on detectors developed by BBN on the DARPA Scalable Network Monitoring (SNM) program
  – Deploying the sensors into existing open source programs
• Using a signature creation algorithm to create polymorphic signatures for the detected attacks
• Integrating Suricata (in-line mode) and Bro to deploy the tool
# Sensors Deployed

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  ICMP</td>
<td>The ICMP monitor checks for unreasonable packet lengths, strange/illegal IP headers, and use of unused or deprecated packet types and codes. The monitor checks for signs of a covert data channel (traffic tunneled over ICMP). It also checks for misuse of ICMP Redirects and ICMP Destination Unreachable (DU).</td>
</tr>
<tr>
<td>2  DNS</td>
<td>New sensors to support detection of DNS churning, poisoning, Kaminsky-style attacks, Akamai-like redirection/load-balancing, and detection evasion attempts</td>
</tr>
<tr>
<td>3  Flow Analysis</td>
<td>Detects long-term flows, traffic rates, “fat” flows, wrong-way traffic (out greater than in for client), overall traffic rates</td>
</tr>
<tr>
<td>4  Host Peering Characteristics</td>
<td>Sensors for sudden wide peering changes, half-peering, long-term peers.</td>
</tr>
<tr>
<td>5  Host / Ext Address Block Characterization</td>
<td>Tracks connection aspects of internal hosts and external host blocks. Estimate coarse-granularity traffic flow rates inbound and outbound.</td>
</tr>
<tr>
<td>6  Replicated Content Detection</td>
<td>Generates a signature from a set of suspected attack packets. This capability supports detection of polymorphic attacks by using a signature scheme that recognized specific small patterns (called n-grams) in varying locations in the attack.</td>
</tr>
<tr>
<td>7  Detection Correlations</td>
<td>A capability to combine the basic detections (1-5) into a range of required detection sequences, in order to obtain higher confidence in the results.</td>
</tr>
</tbody>
</table>
• Polymorphic/Metamorphic malware changes between instances of an infection to avoid detection
• Worms make heavy use of this behavior
• Attack invariants – some portions of packet content that are used before the unpacker can have some of their content changed, but some elements are unchanged (e.g. required for the exploit)
Signature Generation Architecture

- **Bro**
  - Host Peering sensor added to Bro and writes detections to Bro log
- **Signature Extractor**
  - Trigger on new Bro log event
  - Start collecting packets from suspicious host
  - Cluster packets
  - Generate signature for each cluster
  - Load rules into Suricata by calling script
- **Suricata**
  - Rules dynamically added
  - Rules loaded and inline packet blocking is enabled
Dendrogram Clustering

- Technique borrowed from DARPA DECODE program
- Start with clusters of size one
- Distance metric is local alignment edit distance
- Find closest cluster and merge
- Distance between multi-element clusters is shortest between any two
- Cluster is broken off when next merge involves big jump
Signature Extraction

- Extract all Local Alignment (LA) pairs for a cluster and add to String of Interest (SI) list
- Apply recursive Longest Common Substring (LCS) algorithm to find all string sequence chunks common to all SI elements
- Signature consists of string chunks in sequence
Sample Results for FTP attack

X-axis is number of packets used for signature generation
Benefits

• What is the value that your solution provides?
  – Adds new detection capacity to Suricata and Bro
  – Provides ability to generate highly accurate attack signatures in an automated manner
  – Fits well into an open source approach
  – Is expandable and works well with other approaches
## Competition

<table>
<thead>
<tr>
<th>Coverage</th>
<th>Signature</th>
<th>Anomaly</th>
<th>RePS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known signatures</td>
<td>√</td>
<td></td>
<td>N/A</td>
</tr>
<tr>
<td>Deviations from trained</td>
<td>N/A</td>
<td>√</td>
<td>N/A</td>
</tr>
<tr>
<td>Deviations from normal</td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Encrypted attacks</td>
<td></td>
<td>Some</td>
<td>Some</td>
</tr>
<tr>
<td>Extensible</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Scales w/ population</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Scales w/ traffic</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Scales w/ attack type</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Detection score</td>
<td></td>
<td>Tunable</td>
<td></td>
</tr>
<tr>
<td>High Bandwidth</td>
<td>Costly</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Zero Day Attacks</td>
<td>Few</td>
<td>Some</td>
<td>More!</td>
</tr>
<tr>
<td>Identify Attack</td>
<td>Specific</td>
<td>General</td>
<td>General</td>
</tr>
<tr>
<td>Determine Attack Success</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Current Status

• Prototype capability has been developed
• Additional testing is underway
• Current work ends in November
• Follow-on opportunities being pursued
Next Steps

• What are your plans for the remainder of the effort?
  – Complete testing

• Technology Transition Activities?
  – Coordinate with Suricata and Bro
  – Reach out to commercial partners
  – Work the ideas inside Raytheon
Contact Information

• Ron Watro, rwatro@bbn.com
• Dan Wyschogrod, dwyschog@bbn.com
• David Mandelberg, dmandelb@bbn.com