IETF BMWG
Security Effectiveness Benchmarking

Kenneth Green

82nd IETF

Taipei, 13-18 Nov 2011

Critical Functions of Content Aware Devices

Content-aware security devices perform the following key functions:

1. Categorise traffic as either legal or illegal
2. Log/notify about illegal traffic (in-band/out-of-band)
3. Block illegal traffic (in-band)
4. Forward legal traffic (in-band)

All devices must implement categorisation as it is fundamental to the other functions.

Distinguishing Performance and Effectiveness

- **Security Performance** = how well a content-aware device forwards good traffic with security features enabled and in the presence of illegal traffic.

  This has begun to be addressed by:
  `draft-hamilton-bmwg-ca-bench_xxx`

- **Security Effectiveness** = how well the device categorises traffic.

  - No false negatives = accurately identifies all evil traffic
  - No false positives = never flags good traffic as evil

  This is not currently addressed.

The Proposed Drafts

Two drafts: Terminology and methodology for Security Effectiveness benchmarking

- **Terminology** draft will cover items specific to Security Effectiveness testing
  - Legal traffic, Illegal traffic (taking RFC2647 as a starting point)
  - Vulnerability, Malware, Virus, Trojan, Rootkit …
  - False positive, false negative …
  - Wildlist
  - Others TBD (as required by the Methodology draft)

The Proposed Drafts (cont.)

Methodology draft will provide general information on test setups and test results, then describe the specific benchmark metrics and tests

- Maximum Attack Blocking Rate
- Useful Attack Blocking Rate
- Attack Blocking Effectiveness
- Others TBD

- Results to include details of all attacks and identify those blocked and those not blocked.

Why Do We Need To Do This?

- The nature of this testing is orthogonal to that of performance testing and is not covered by existing RFCs or IDs.
  - A security device with high forwarding performance is of little use if it misses malicious traffic.
  - Currently there is no standard way to validate effectiveness of security solutions and hence no mechanism exists for realistic apples-to-apples comparisons of the breadth and currency of competing solutions.
- The range of security challenges grows exponentially
  - Existing exploits and malware remain a risk and effectiveness against them must be validated for both new and updated products.
  - New exploits and malware appear all the time requiring re-validation of the effectiveness of existing devices and solution updates.

Next steps

- Continue to solicit comments, feedback, and support

- Submit initial drafts based on comments and input received

Initial methodology draft: **`draft-green-bmwg-seceff-bench-meth-00.txt`**

Comments?