RSA®CONFERENCE CHINA 2012

RSA信息安全大会2012

THE GREAT CIPHER

MIGHTIER THAN THE SWORD

伟大的密码胜于利剑

Testing Darwinism: The History and Evolution of Network Resiliency

Mike Hamilton

BreakingPoint

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012

Defining Resiliency

	How	Why
Performance	Application load, attacks, and impairments.	Measure and improve performance under high-stress conditions.
Security	Latest attacks, evasions, malware, and spam.	Identify and remediate vulnerabilities. Perform under DoS attack.
Stability	Impairments combined with application load.	Ensure reliable performance and availability.

RESILIENCY

Performance

	How	Why
Performance	Application load, attacks, and impairments.	Measure and improve performance under high-stress conditions.

Security

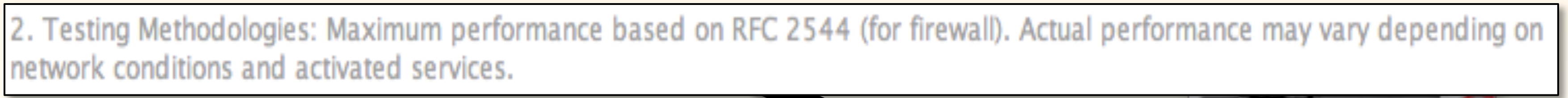
	How	Why
Performance	Application load, attacks, and impairments.	Measure and improve performance under high-stress conditions.
Security	Latest attacks, evasions, malware, and spam.	Identify and remediate vulnerabilities. Perform under DoS attack.

Stability

	How	Why
Performance	Application load, attacks, and impairments.	Measure and improve performance under high-stress conditions.
Security	Latest attacks, evasions, malware, and spam.	Identify and remediate vulnerabilities. Perform under DoS attack.
Stability	Impairments combined with application load.	Ensure reliable performance and availability.

RESILIENCY

Resiliency Testing: A History Lesson

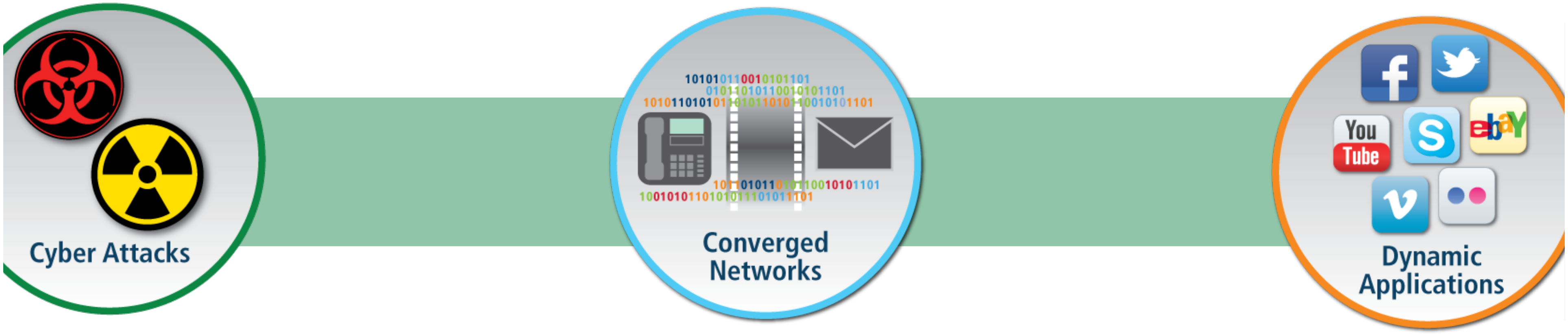


2. Testing Methodologies: Maximum performance based on RFC 2544 (for firewall). Actual performance may vary depending on network conditions and activated services.

- Internet Growth Leads to Technology Standards
- IETF Testing Standards
  - RFC 1944
  - RFC 2544
  - RFC 3511

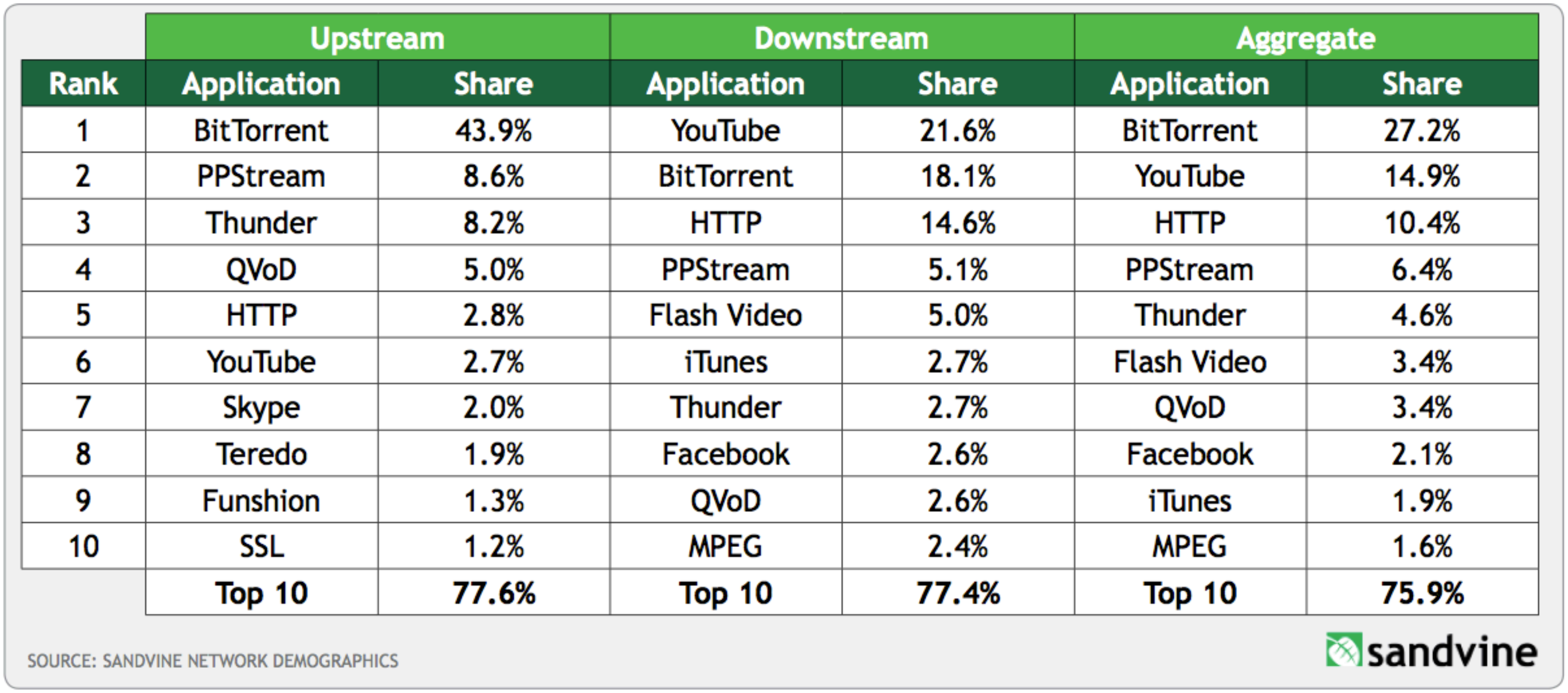
RFC 2544: Right Standard, Wrong Time

- Original Goal
  - Create Vendor-Agnostic Comparisons
- 18 years later (Today)
  - Industry continues to apply RFC 2544 to next-generation and content aware devices



RFC 3511: False Sense of Security?

- HTTP is NOT an Application



	Upstream		Downstream		Aggregate	
Rank	Application	Share	Application	Share	Application	Share
1	BitTorrent	43.9%	YouTube	21.6%	BitTorrent	27.2%
2	PPStream	8.6%	BitTorrent	18.1%	YouTube	14.9%
3	Thunder	8.2%	HTTP	14.6%	HTTP	10.4%
4	QVoD	5.0%	PPStream	5.1%	PPStream	6.4%
5	HTTP	2.8%	Flash Video	5.0%	Thunder	4.6%
6	YouTube	2.7%	iTunes	2.7%	Flash Video	3.4%
7	Skype	2.0%	Thunder	2.7%	QVoD	3.4%
8	Teredo	1.9%	Facebook	2.6%	Facebook	2.1%
9	Funshion	1.3%	QVoD	2.6%	iTunes	1.9%
10	SSL	1.2%	MPEG	2.4%	MPEG	1.6%
	Top 10	77.6%	Top 10	77.4%	Top 10	75.9%

SOURCE: SANDVINE NETWORK DEMOGRAPHICS

sandvine

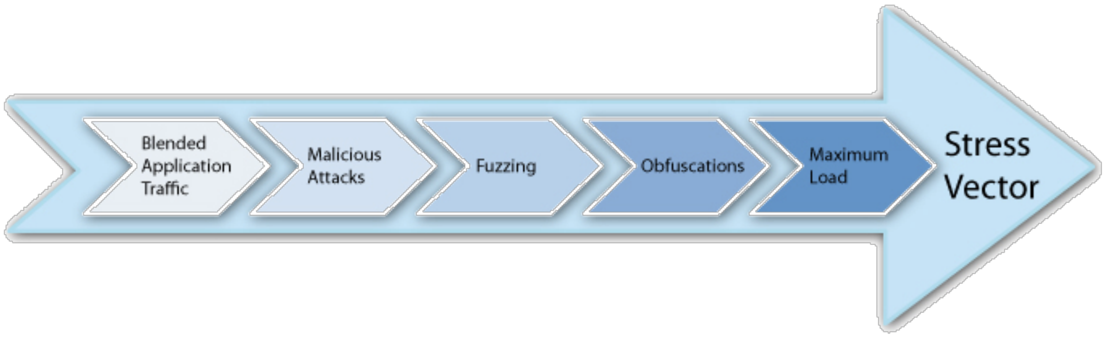
Table 4: Top Peak Period Applications by Bytes - Asia-Pacific, Fixed Access

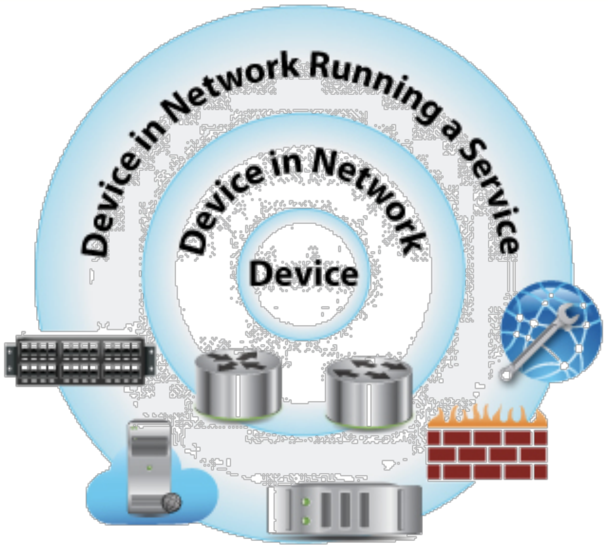
Moving Ahead: Evolving Testing Standards

- IETF
  - Benchmarking Working Group
  - Content-aware device methodology
- Industry consortiums
  - DPIbench

Resiliency = Battle-Tested

- Apply emerging standards today
  - Download the most recent work
- Understand your network traffic
  - Enterprise, service provider, government, etc.
- Know thy attacker





Wrap Up: Questions To Ask Your Vendors

- Ask your vendor*:
  1. Are you keeping up with emerging testing standards?
  2. What application mixes and weights do you use during testing?
  3. Do you combine applications and high-stress user load during testing?
  4. What have the results been when you have tested using malformed traffic?
  5. How does the device perform against application-layer attacks?
  6. Can I test your product with my unique network, application, and user conditions?

*Vendors, ask yourself the same questions.

Questions?

- Contact information:
  - Mike Hamilton
  - Director of Global Systems Engineering
  - BreakingPoint Systems
  - mhamilton@breakingpoint.com

Thank You

RSA CONFERENCE
CHINA 2012
RSA信息安全大会2012