Resilience of Deployed TCP to Blink Attack

Paper written by

Matthew Luckie
University of Waikato
mjl@wand.net.nz

Robert Beverly
Naval Postgraduate School
rbeverly@nps.edu

Tiange Wu
CAIDA / UC San Diego
tiangewu@caida.org

Mark Allman
ICSI
mallman@icir.org

Kc Claffy
CAIDA / UC San Diego
kc@caida.org

Presented by:
Victor Aguboshim
03679101

Content

- Motivation
- Methodology
  - Active Measured Methods
  - Vantage Points
- Conducted Tests
  - Result of Tests
- Conclusions

Motivation

- To determine how a TCP connection will react to an attack from a unrevealed false IP address such that the attacker does not intend to receive traffic from the attack.
  - Does this attack cause a TCP connection reset?
  - Is it accepted, Challenged or just ignored?
- Understand what TCP features enhance its resistance to Blind attacks

Methodology

- Active Measured Methods
  - Blind Reset and SYN Test
  - Blind Data Test
  - Fingerprinting Test

Methodology

- Vantage Points of Measurement:
  - cld-us, hosted by CAIDA (San Diego, USA)
  - hlz-nz, hosted by the University of Waikato (Waikato, New zealand)
  - Hosted by Massachusetts Institute of Technology (MIT), Cambridge.

Conducted Tests and Results

❖Webserver Vulnerability

Result	Blind reset		Blind SYN		Blind data	
	in	out	in	out	behind	ahead
Accepted	3.4%	0.4%	-	-	29.6%	5.4%
Reset (ack-blind)	-	-	17.1%	0.0%	0.6%	0.6%
Reset (dup-ack)	18.8%	0.6%	5.3%	1.2%	0.1%	0.2%
Vulnerable	22.2%	1.0%	22.4%	1.2%	30.3%	6.2%
Challenge ACK	71.4%	1.1%	37.7%	57.0%	37.1%	8.1%
Ignored	5.1%	91.8%	35.9%	38.3%	29.3%	81.3%
Not Vulnerable	76.5%	93.0%	73.6%	95.3%	66.4%	89.4%
Parallel TCP	-	-	1.1%	1.1%	-	-
Early FIN	0.3%	3.3%	1.5%	1.6%	3.2%	3.7%
No Result	1.0%	2.7%	1.3%	0.9%	0.1%	0.7%
Other	1.3%	6.0%	4.0%	3.6%	3.3%	4.4%

Fig1: Overview of Results from the cld-us VP

	cld-us	MIT	hlz-nz
Blind reset (in):			
Vulnerable	22.2%	22.1%	21.9%
Not Vulnerable	76.5%	76.0%	76.5%
Other	1.3%	1.9%	1.6%
Blind SYN (in):			
Vulnerable	22.4%	22.2%	0.3%
Not Vulnerable	73.6%	73.2%	94.2%
Other	4.0%	4.6%	5.5%
Blind data (behind):			
Vulnerable	30.3%	30.3%	30.3%
Not Vulnerable	66.4%	66.5%	66.2%
Other	3.3%	3.3%	4.5%

Fig 2: Overview of the Results based on VPs

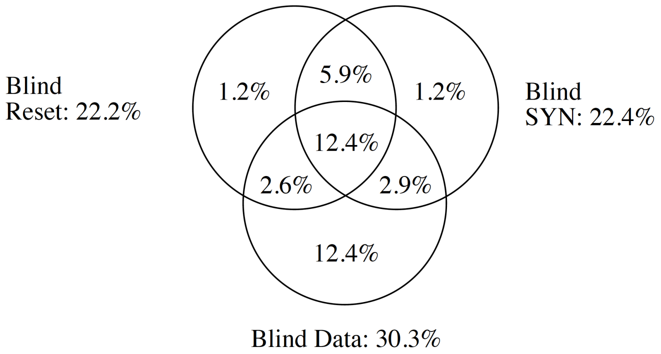

Fig 3: Overlap of results from the cld-us VP

Conducted Tests and Results

❖Infrastructure Vulnerability

Device	OS date	Blind reset in	Blind reset out	Blind SYN in	Blind SYN out	Blind data behind	Blind data ahead	Port range
Cisco 2610 12.1(13)	2002-01	× (A)	✓ (I)	× (R)	✓ (C)	× (A)	✓ (C)	seq.
Cisco 2610 12.2(7)	2002-01	× (A)	✓ (I)	× (R)	✓ (C)	× (A)	✓ (C)	seq.
Cisco 2650 12.3(15b)	2005-08	✓ (C)	✓ (I)	✓ (C)	✓ (C)	× (A)	✓ (C)	40785
Cisco 7206 12.4(20)	2008-07	✓ (C)	✓ (I)	✓ (C)	✓ (C)	× (A)	✓ (C)	54167
Cisco 2811 15.0(1)	2010-10	✓ (C)	✓ (I)	✓ (C)	✓ (C)	× (A)	✓ (C)	46166
Cisco 2911 15.1(4)	2012-03	✓ (C)	✓ (I)	✓ (C)	✓ (C)	× (A)	✓ (C)	39422
Juniper M7i 8.2R1.7	2007-01	× (A)	✓ (I)	× (R)	✓ (I)	× (A)	✓ (C)	181
Juniper EX9208 14.1R1.10	2014-06	✓ (C)	✓ (I)	✓ (C)	✓ (I)	× (A)	✓ (C)	13769
Juniper MX960 13.3	2015-05	✓ (I)	✓ (I)	✓ (C)	✓ (I)	× (A)	✓ (C)	13033
Juniper J2350 12.1X46-D35.1	2015-05	✓ (I)	✓ (I)	✓ (C)	✓ (I)	× (A)	✓ (C)	12481
HP 2920 WB.15.16.0006	2015-01	✓ (C)	✓ (C)	✓ (C)	✓ (C)	✓ (I)	✓ (I)	14273
HP e3500 K.15.16.0007	2015-06	× (A)	✓ (I)	× (R)	✓ (C)	✓ (I)	✓ (I)	15611
Brocade MLX-4 5.7.0bT177	2014-10	✓ (I)	✓ (I)	✓ (C)	✓ (C)	✓ (C)	✓ (C)	const.
Pica8 Pronto3290 v2.6	2015-05	× (A)	✓ (I)	× (R)	✓ (C)	× (A)	× (A)	HBPS

Fig 4: Overview of Response Laboratory testing of blind TCP attacks against BGP-speaking router and OpenFlow-speaking switches

Conducted Tests and Results

❖Ports Selection Predictability

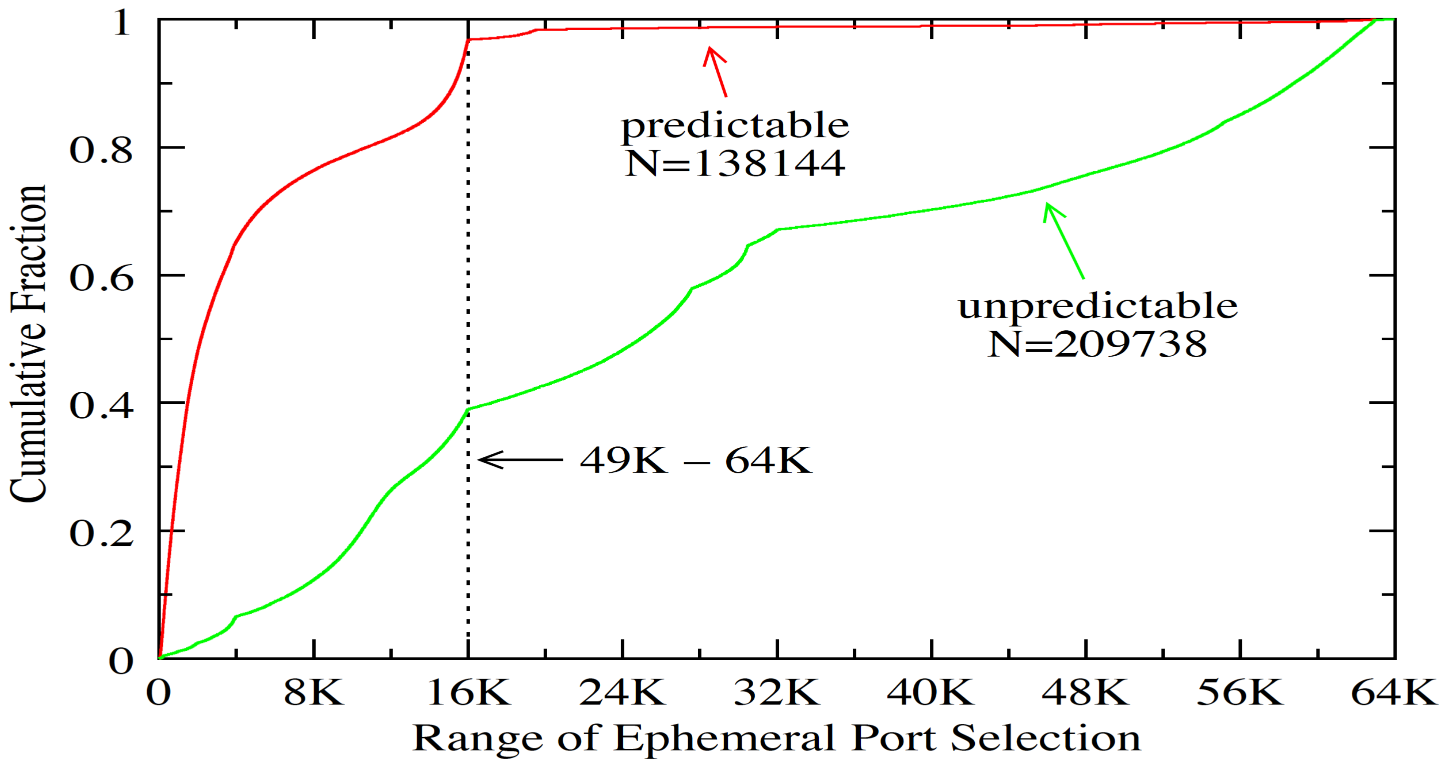

Fig 5: Overview of the predictability of the observed ports

Conclusion

- TCP is an important protocol with huge traffic and so the need for constant security and performance improvements.
- 22% of connections are vulnerable to SYN and rest packets
- 30% vulnerable to in-window data packets
- 38.4% vulnerable to at least one of the three tested in-window attacks tested

References

- Alexa. Top 1,000,000 sites. http://www.alexa.com/topsites.

- Cisco. TCP Vulnerabilities in Multiple IOS-Based Cisco Products,2004.http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20040420-tcp-ios.

- M. Zalewski. p0f v3 (version3.08b).http://lcamtuf.coredump.cx/p0f3/.

- M. Luckie. Scamper: a scalable and extensible packet prober for active measurement of the Internet. In IMC, pages 239–245, Nov. 2010.

Thank you for your time

Questions?