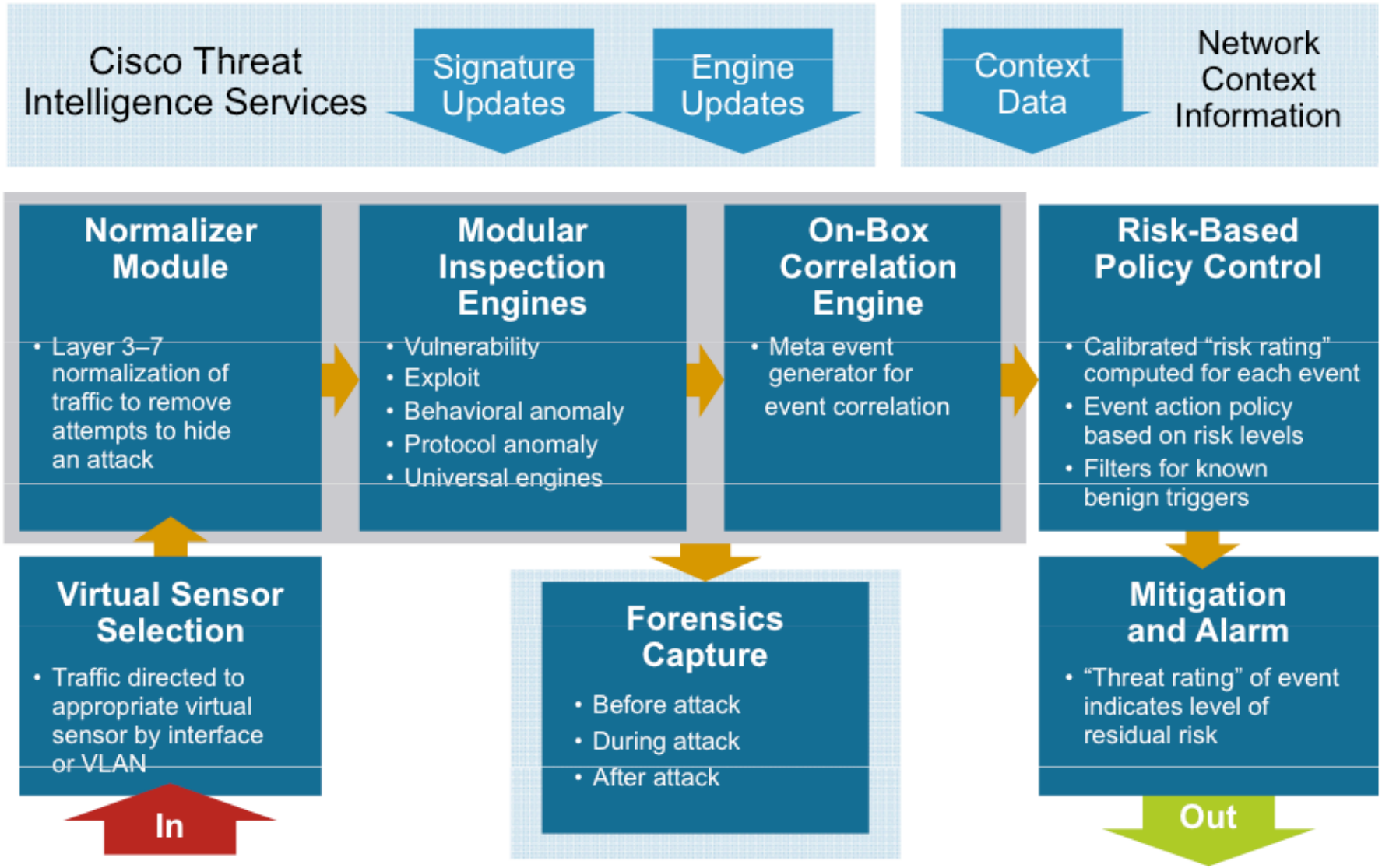
Cisco IPS Architecture

Intelligent Detection and Precision Response



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1 day of “crud” seen at ICSI (155K times)

active-connection-reuse	DNS-label-len-gt-pkt	HTTP-chunked-multipart	possible-split-routing
bad-Ident-reply	DNS-label-too-long	HTTP-version-mismatch	SYN-after-close
bad-RPC	DNS-RR-length-mismatch	illegal-%-at-end-of-URI	SYN-after-reset
bad-SYN-ack	DNS-RR-unknown-type	inappropriate-FIN	SYN-inside-connection
bad-TCP-header-len	DNS-truncated-answer	IRC-invalid-line	SYN-seq-jump
base64-illegal-encoding	DNS-len-lt-hdr-len	line-terminated-with-single-CR	truncated-NTP
connection-originator-SYN-ack	DNS-truncated-RR-rdlength	malformed-SSH-identification	unescaped-%-in-URI
data-after-reset	double-%-in-URI	no-login-prompt	unescaped-special-URI-char
data-before-established	excess-RPC	NUL-in-line	unmatched-HTTP-reply
too-many-DNS-queries	FIN-advanced-last-seq	POP3-server-sending-client-commands	window-recision
DNS-label-forward-compress-offset	fragment-with-DF		

Evasion At Higher Semantic Levels

- Consider the following attack URL:

  http://…./c/winnt/system32/cmd.exe?/c+dir

- Easy enough to scan for (e.g., “cmd.exe”), right?

- But what about

  http://…./c/winnt/system32/cm%64.exe?/c+dir

  - Okay, we need to handle % escapes. (%64=‘d’)

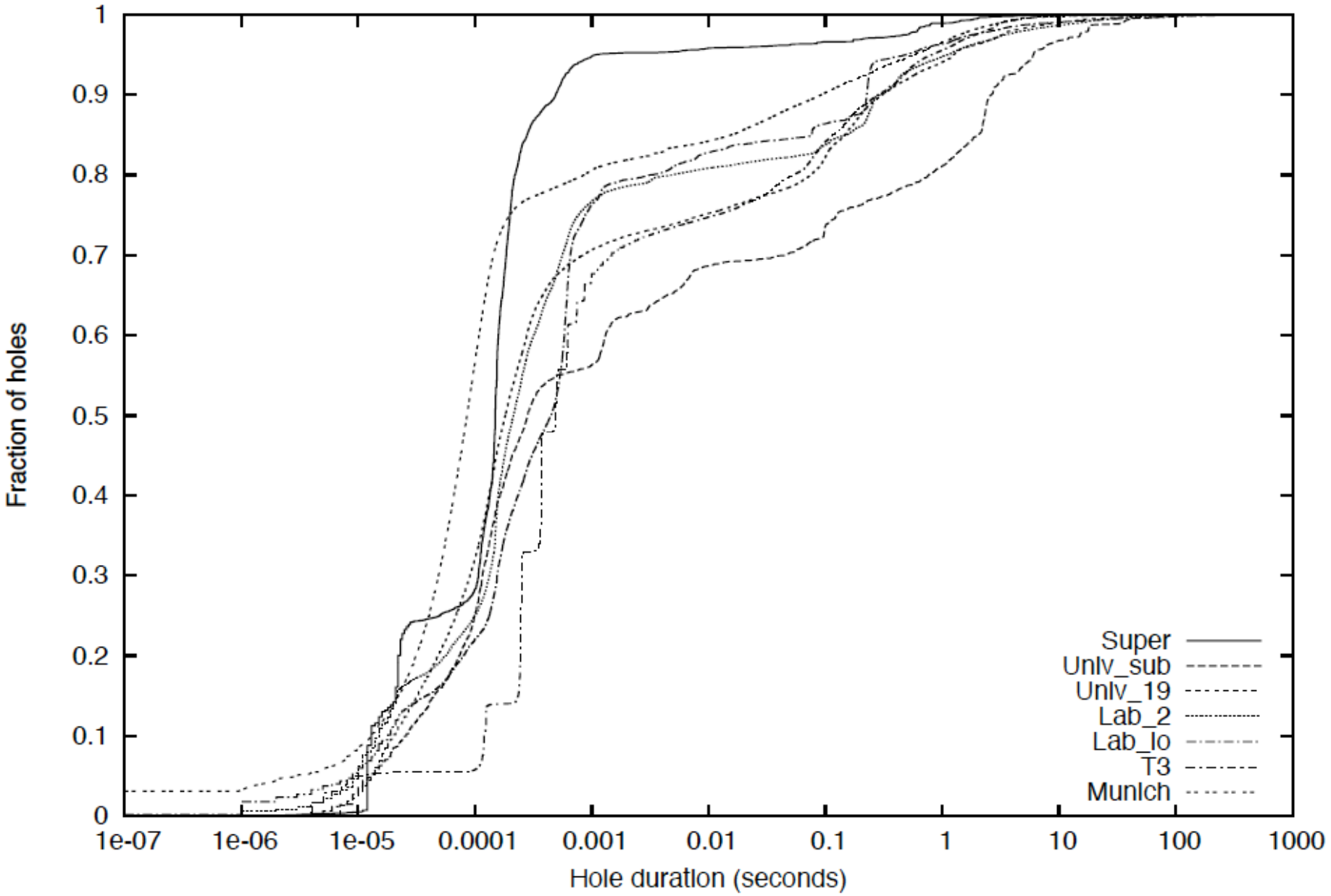
- But what about

  http://…./c/winnt/system32/cm%25%36%34.exe?/c+dir

  - Oops. Will server double-expand escapes … or not?
    - %25=‘%’ %36=‘6’ %34=‘4’

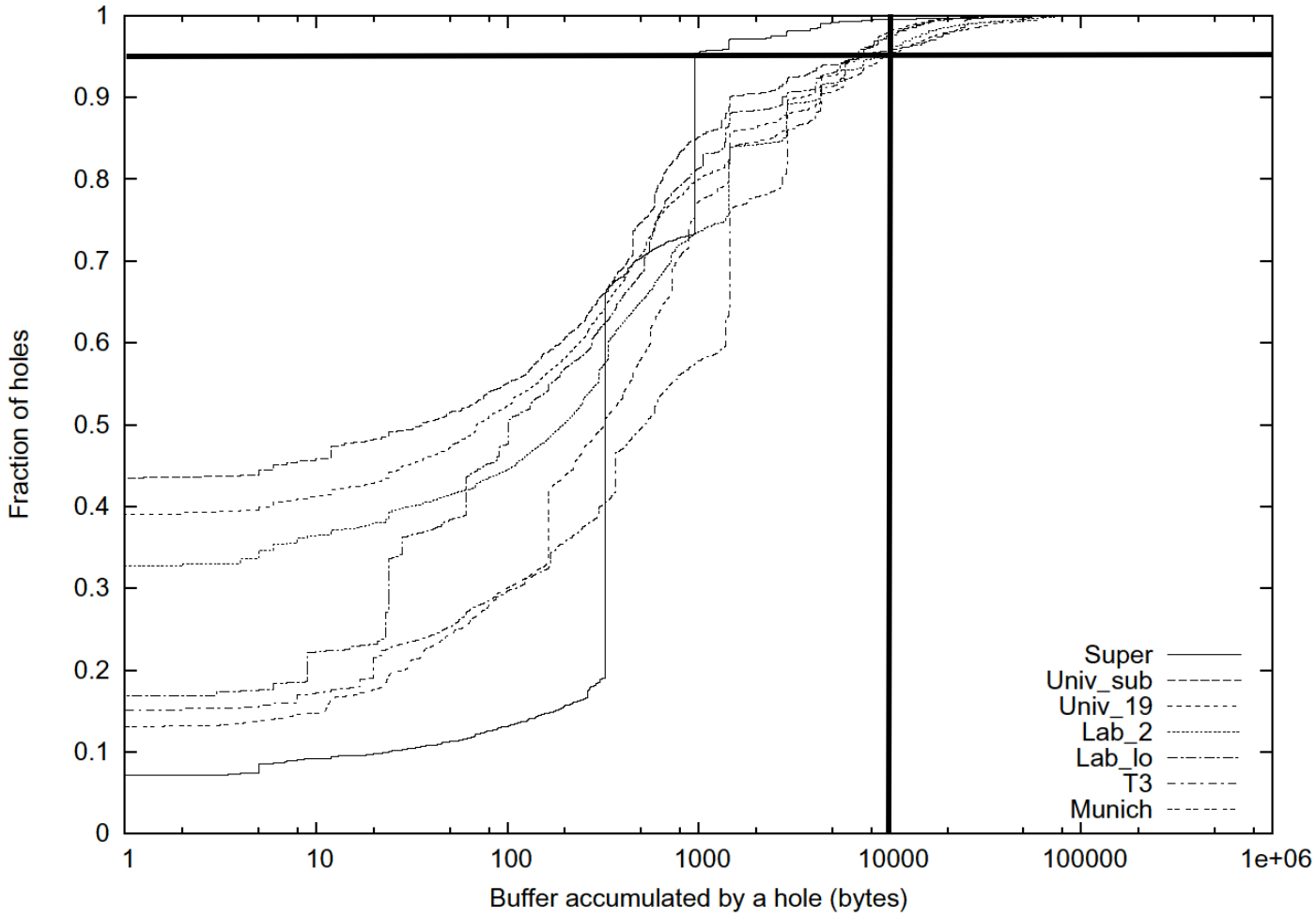
	$Univ_{sub}$	$Univ_{19}$	Lab_{lo}	Lab_2	*Super*	*T3*	*Munich*
Trace duration (seconds)	303	5,697 / 300*	3,602	3,604	3,606	10,800	6,167
Total packets	1.25M	6.2M	1.5M	14.1M	3.5M	36M	220M
Total connections	53K	237K	50K	215K	21K	1.04M	5.62M
Connections with holes	1,146	17,476	4,469	41,611	598	174,687	714,953
Total holes	2,048	29,003	8,848	79,321	4,088	575K	1.88M
Max buffer required (bytes)	128 KB	91 KB	68 KB	253K	269 KB	202 KB	560KB
Avg buffer required (bytes)	5,943	2,227	3,111	13,392	122	28,707	178KB
Max simultaneous holes	15	13	9	39	6	94	114
Max simultaneous holes in single connection	9	16	6	16	6	85	61
Fraction of holes with < 3 packets in buffer	90%	87%	90%	87%	97%	85%	87%
Fraction of connections with single concurrent hole	96%	98%	96%	97%	97%	95%	97%
Fraction of holes that overlap hole on another connection of same *external* host (§ 5.1)	0.5%	0.02%	0.06%	0.06%	0%	0.46%	0.02%

- Many connections have holes, but little buffer required


Fraction of holes
Hole duration (seconds)
1
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0
1e-07
1e-06
1e-05
0.0001
0.001
0.01
0.1
1
10
100
1000
Super
Unlv_sub
Unlv_19
Lab_2
Lab_Io
T3
Munich

Adversary can fill the entire buffer with just a single connection!

Policy 1: Restrict per-connection buffer to threshold (10KB)



- Adversary can create *multiple* connections to overflow the buffer!

- ***Policy 2:*** Do not allow a single host to create two connections with holes

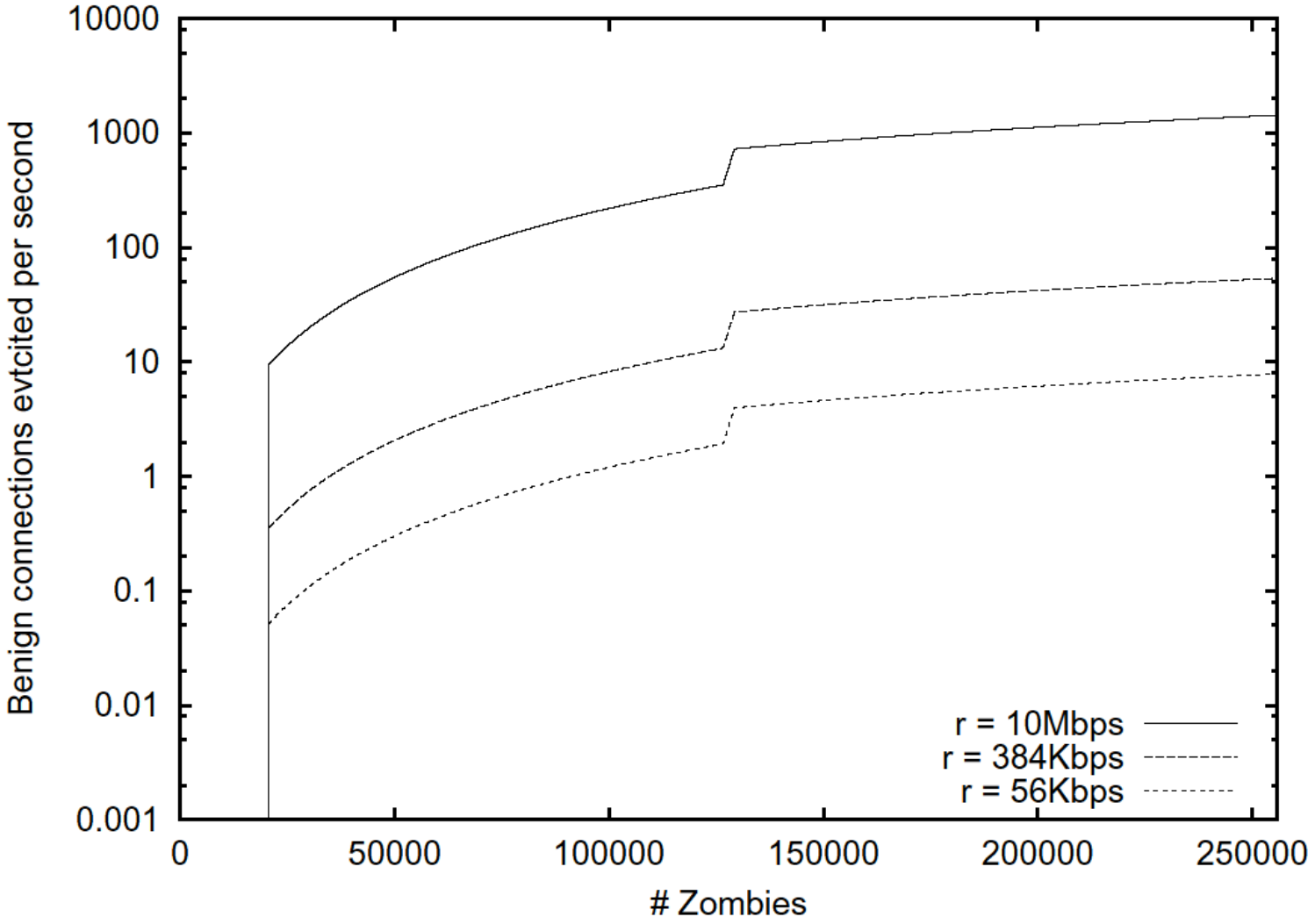
	$Univ_{sub}$	$Univ_{19}$	Lab_{lo}	Lab_2	*Super*	*T3*	*Munich*
Fraction of holes that overlap hole on another connection of same *external* host	0.5%	0.02%	0.06%	0.06%	0%	0.46%	0.02%

- Adversary attacks from distributed hosts! (*zombies*)
  - No connection can be isolated as adversary's… all of them look good

- ***Policy 3:*** Upon buffer overflow …
  - … Evict one buffer page randomly and reallocate it to new packet
  - Kill the connection of the evicted page (mod details)

- If the buffer is **large**, then *most evicted connections belong to the adversary*
  - They fight an uphill battle!

- Suppose total 512 MB, 2KB page, 25KB/conn



Avg. Legitimate Buffer = 30 KB