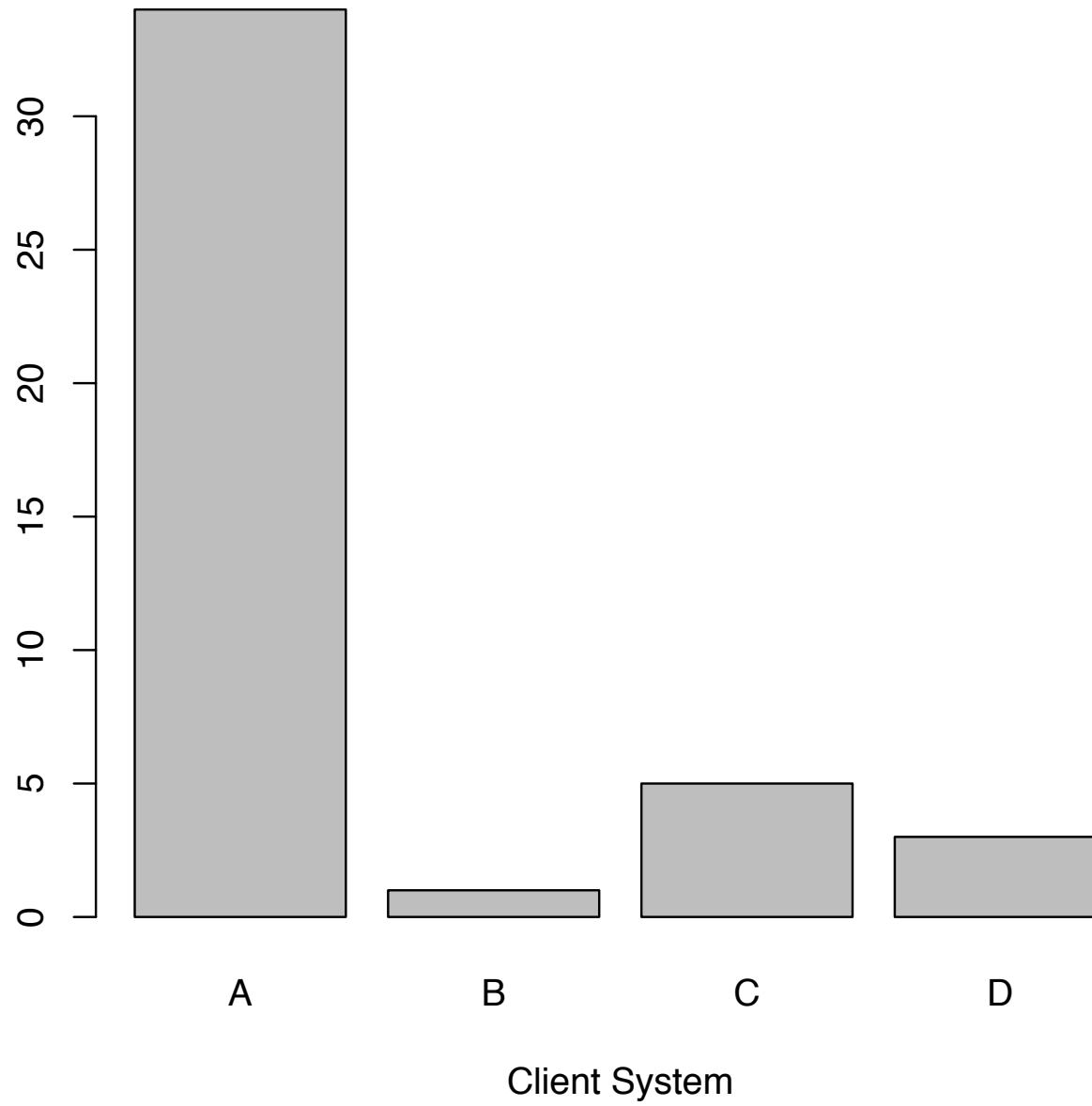
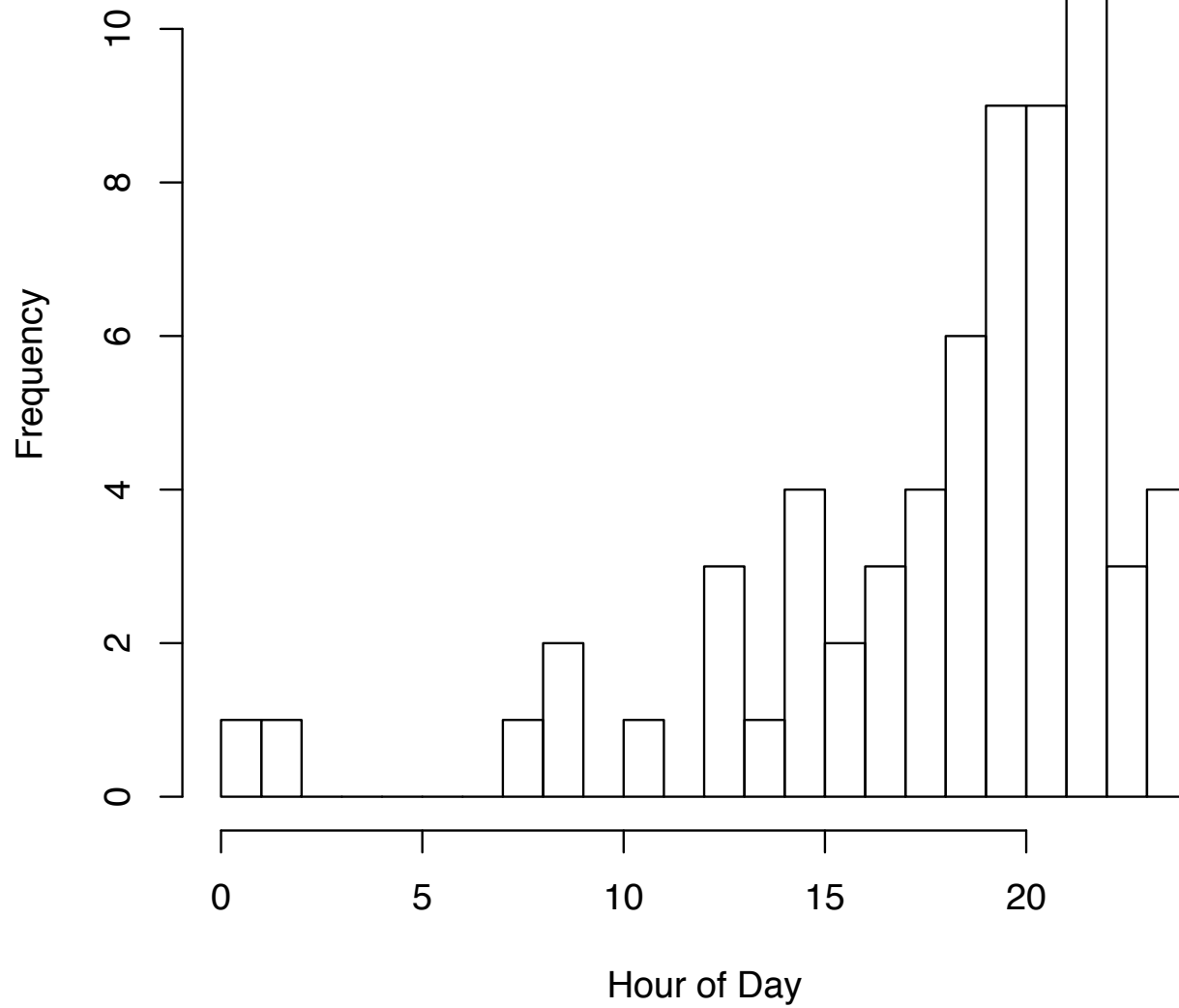


Logins by User Joe to Machine Z



Hour of User Joe's Logins to Machine Z



1 day of “crud” seen at ICSI (110K times)

above-hole-data-without-any-acks	double-%-in-URI	line-terminated-with-single-CR	SYN-with-data
active-connection-reuse	excessively-small-fragment	malformed-ssh-identification	TCP-ack-underflow-or-misorder
bad-TCP-header-len	excessive-data-without-further-acks	non-ip-packet-in-egre	Teredo-bubble-with-payload
base64-illegal-encoding	FIN-advanced-last-seq	NUL-in-line	truncated-GRE
could-not-parse-X509-certificate	fragment-with-DF	possible-split-routing	truncated-header-in-tunnel
data-before-established	HTTP-chunked-transfer-for-multipart-message	premature-connection-reuse	unescaped-%-in-URI
dnp3-header-lacks-magic	HTTP-version-mismatch	RST-storm	unescaped-special-URI-char
DNS-conn-count-too-large	illegal-%-at-end-of-URI	SYN-after-close	unknown-HTTP-method
DNS-RR-length-mismatch	inappropriate-FIN	SYN-after-reset	unknown-routing-type-14
DNS-truncated-len-lt-hdr-len	inflate-failed	SYN-inside-connection	unmatched-HTTP-reply
dns-unmatched-query-id-quantity	irc-invalid-line	SYN-seq-jump	window-recision

This copy is for your personal, noncommercial use only. You can order presentation-ready copies for distribution to your colleagues, clients or customers, please [click here](#) or use the "Reprints" tool that appears next to any article. Visit www.nytreprints.com for samples and additional information. [Order a reprint of this article now.](#) »

December 16, 2010

Ohio State Says Hackers Breached Data on 760,000

By [TAMAR LEWIN](#)

[Ohio State University](#) is notifying about 760,000 people whose personal information was stored in the university's computer server that a data breach could put them at risk for identity theft.

The university, located in Columbus, began sending letters on Wednesday to current and former faculty and staff members, students and applicants, telling them that hackers had broken into the server that stored their names, [Social Security](#) numbers, dates of birth and addresses.

The university said that although there was no evidence that the information had been used for identity theft, it was nonetheless offering a year of free credit protection to everyone whose data was on the server.

"We regret that this has occurred and are exercising an abundance of caution in choosing to notify those affected," Joseph A. Alutto, the university provost, said in a news release.



Joe Stewart

@joestewart71

 Follow

Future of host IDS: Just a Bitcoin wallet with small amount of BTC. When emptied it means time to wipe/reinstall + change all your PWs.



RETWEETS

31

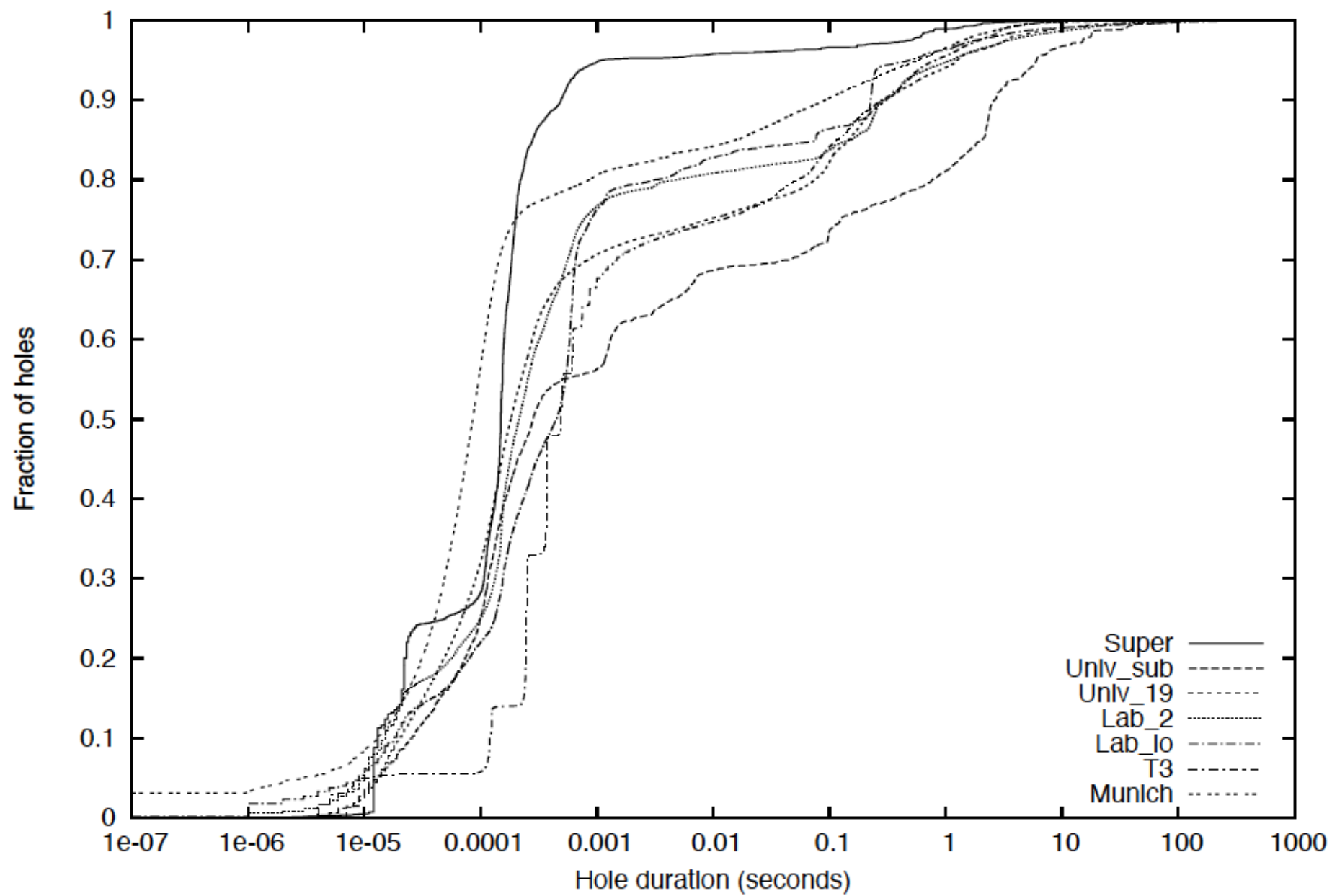
FAVORITES

9



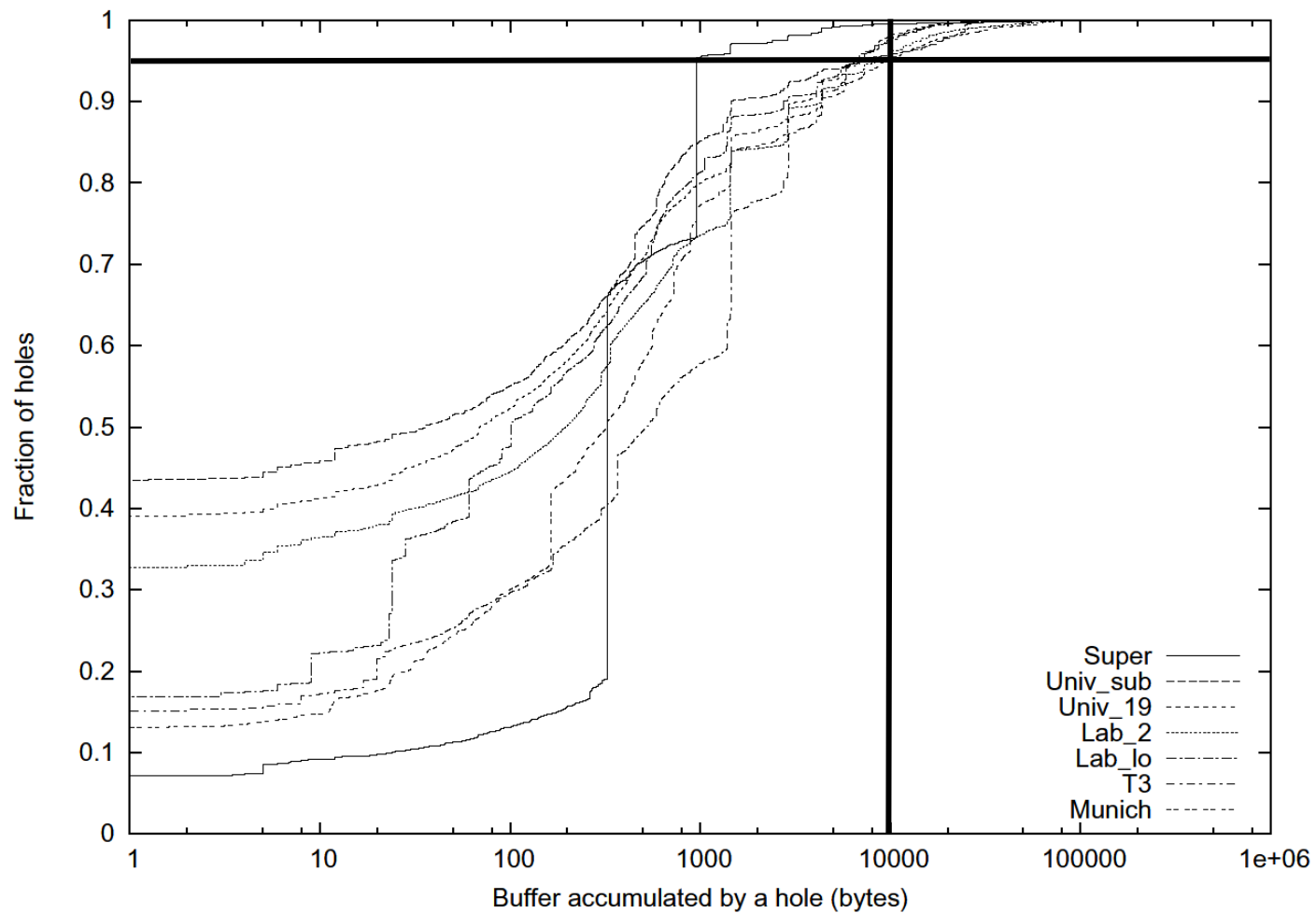
12:10 PM - 21 Nov 2013

	$Univ_{sub}$	$Univ_{19}$	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 <i>external</i> host (§ 5.1)	0.5%	0.02%	0.06%	0.06%	0%	0.46%	0.02%



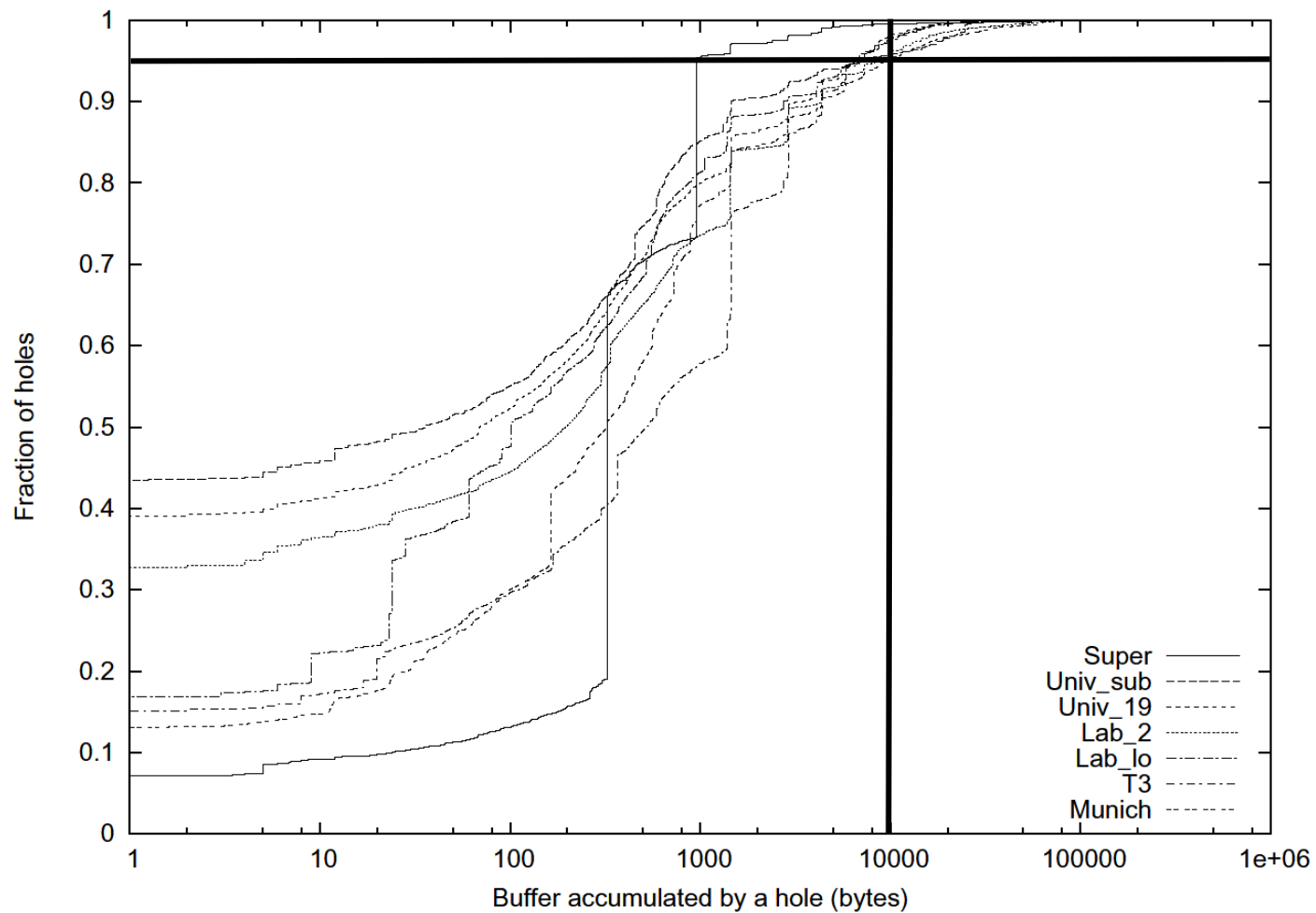
	$Univ_{sub}$	$Univ_{19}$	Lab_{lo}	Lab_2	$Super$	$T3$	$Munich$
Trace duration (seconds)	303	5,697 / 300*	3,602	3,604	3,606	10,800	6,167
Total packets	1.25M	6.2M	1.5M	14.1M	3.5M	36M	220M
Total connections	53K	237K	50K	215K	21K	1.04M	5.62M
Connections with holes	1,146	17,476	4,469	41,611	598	174,687	714,953
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 <i>external</i> host (§ 5.1)	0.5%	0.02%	0.06%	0.06%	0%	0.46%	0.02%

Policy 1: Restrict per-connection buffer to threshold (= ?)



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

Policy 1: Restrict per-connection buffer to threshold (say 20KB)

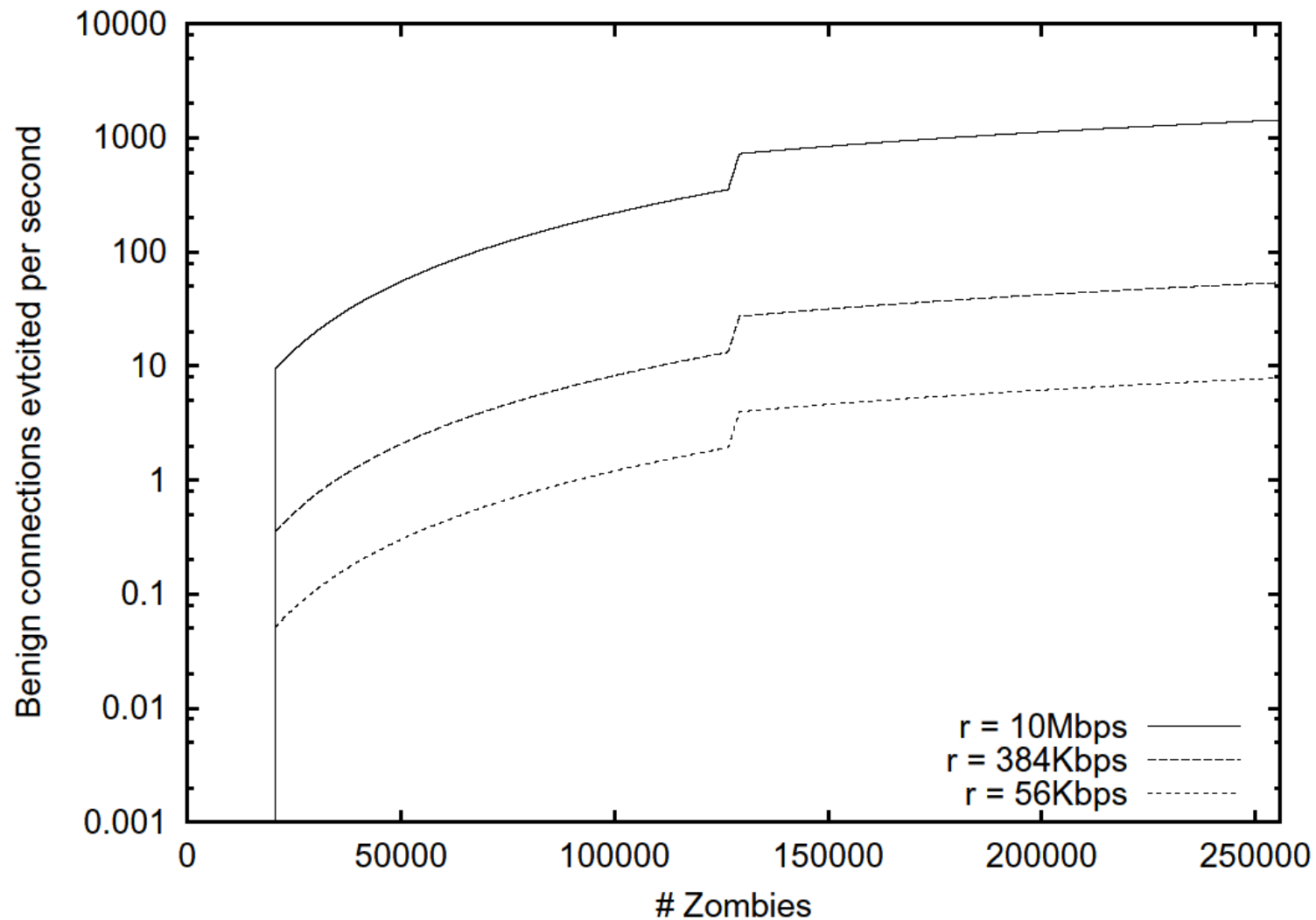


- Adversary can create *multiple* connections to exhaust the buffer!
- **Policy 2:** Do not allow a single host to create two connections with holes

	<i>Univ_{sub}</i>	<i>Univ₁₉</i>	<i>Lab_{lo}</i>	<i>Lab₂</i>	<i>Super</i>	<i>T3</i>	<i>Munich</i>
Fraction of holes that overlap hole on another connection of same <i>external</i> 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 exhaustion ...
 - ... Evict one buffer **page** *randomly* and reallocate it to new packet
 - **Kill** the connection of the evicted page (mod details)
 - And recover *all* of its pages
- 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

Cisco IPS Architecture

Intelligent Detection and Precision Response

