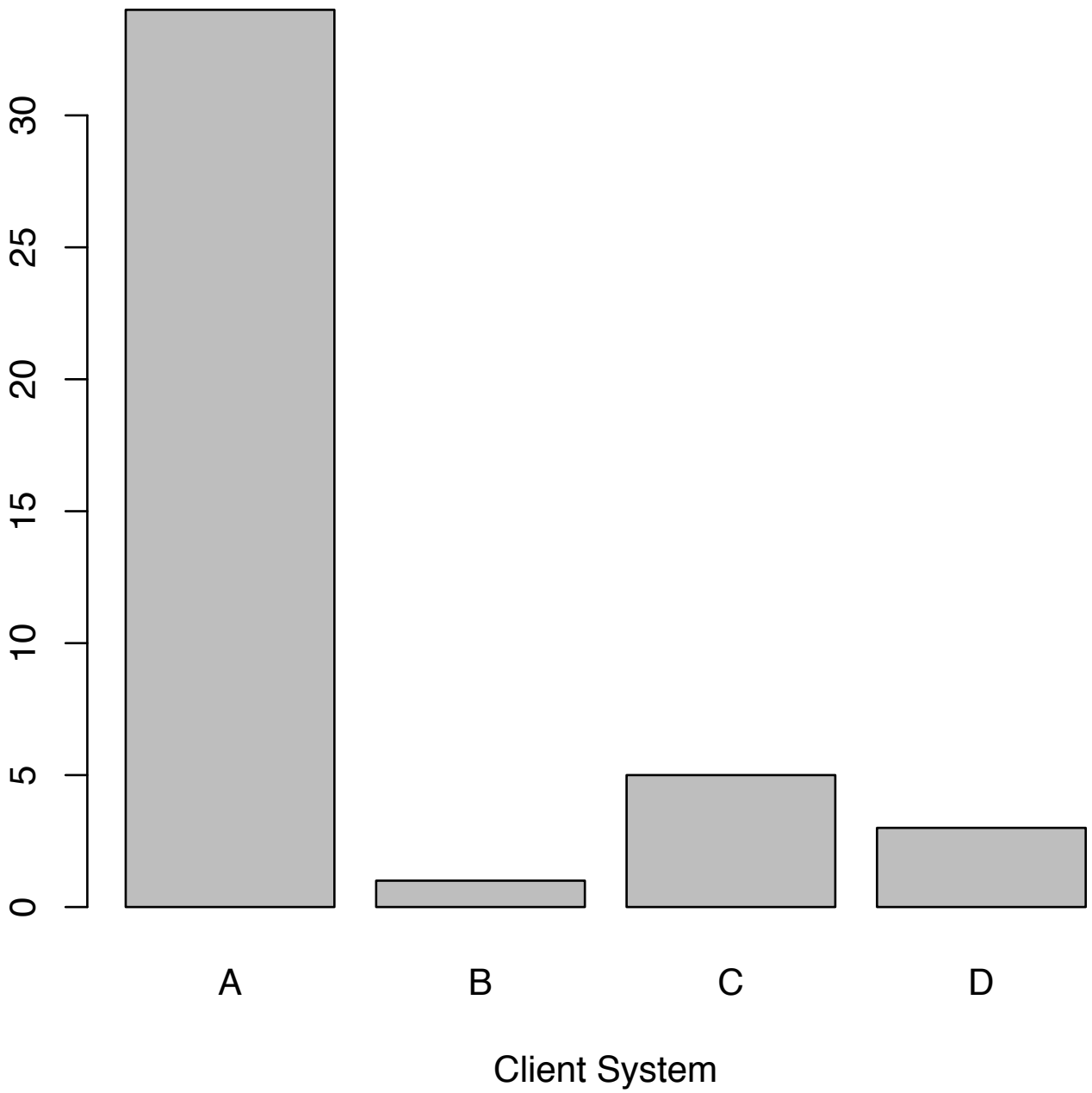
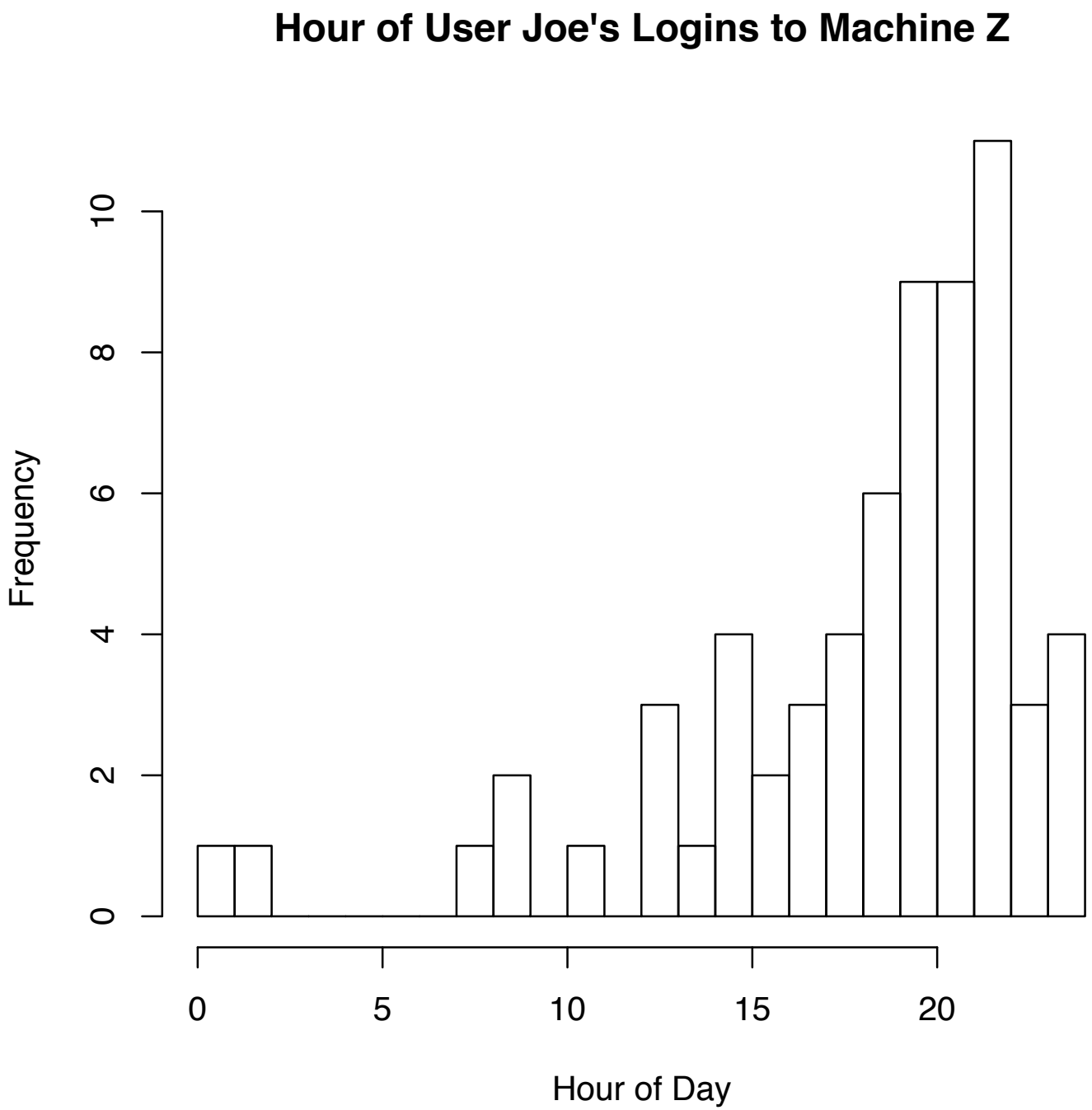

# Logins by User Joe to Machine Z
0
5
10
15
20
25
30
A
B
C
D
Client System


Hour of User Joe's Logins to Machine Z
Frequency
0
2
4
6
8
10
0
5
10
15
20
Hour of Day

# 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 |

**Joe Stewart**
@joestewart71

Follow

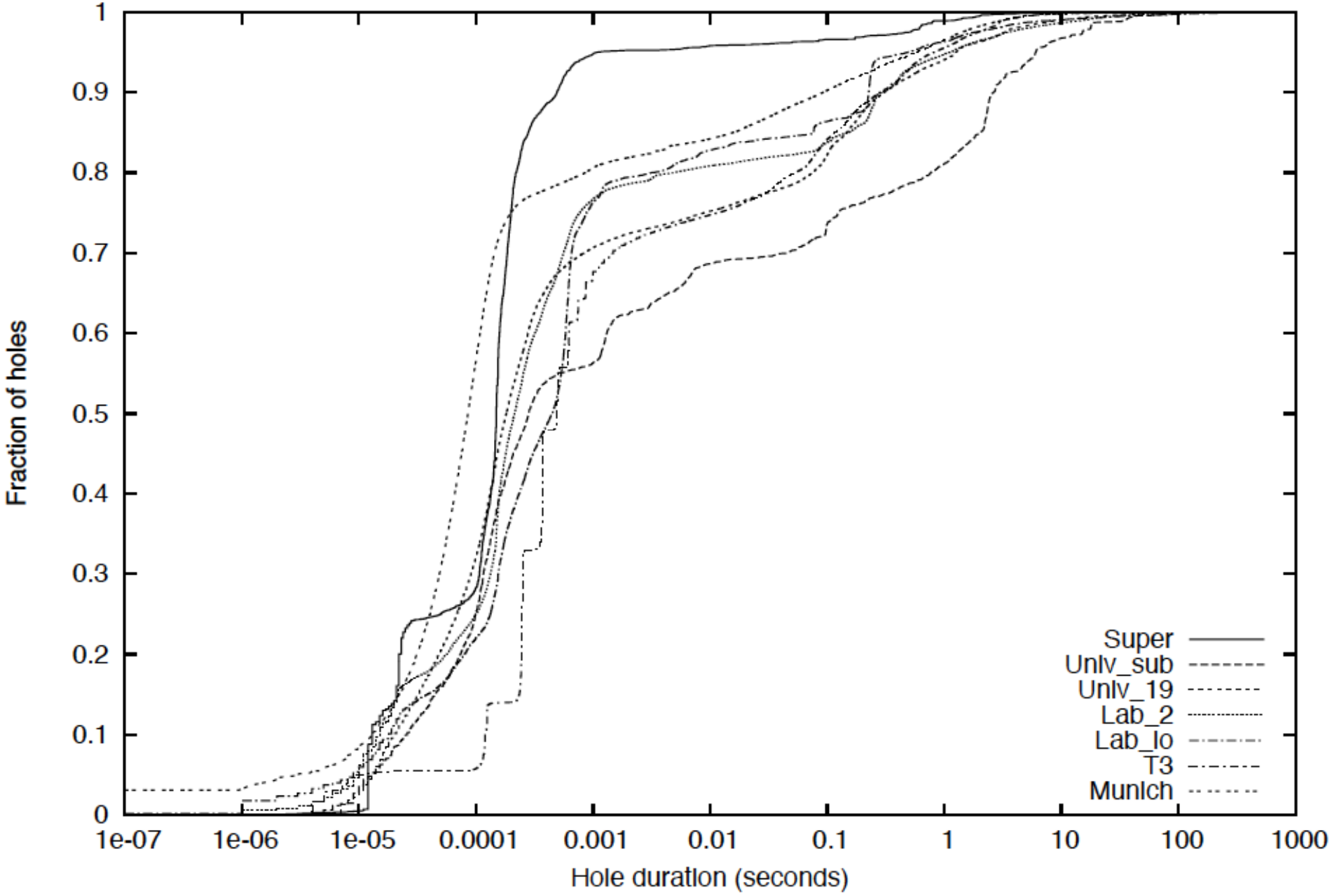
Future of host IDS: Just a Bitcoin wallet with small amount of BTC. When emptied it means time to wipe/reinstall + change all your PWs.

RETWEETS
31

FAVORITES
9

12:10 PM - 21 Nov 2013

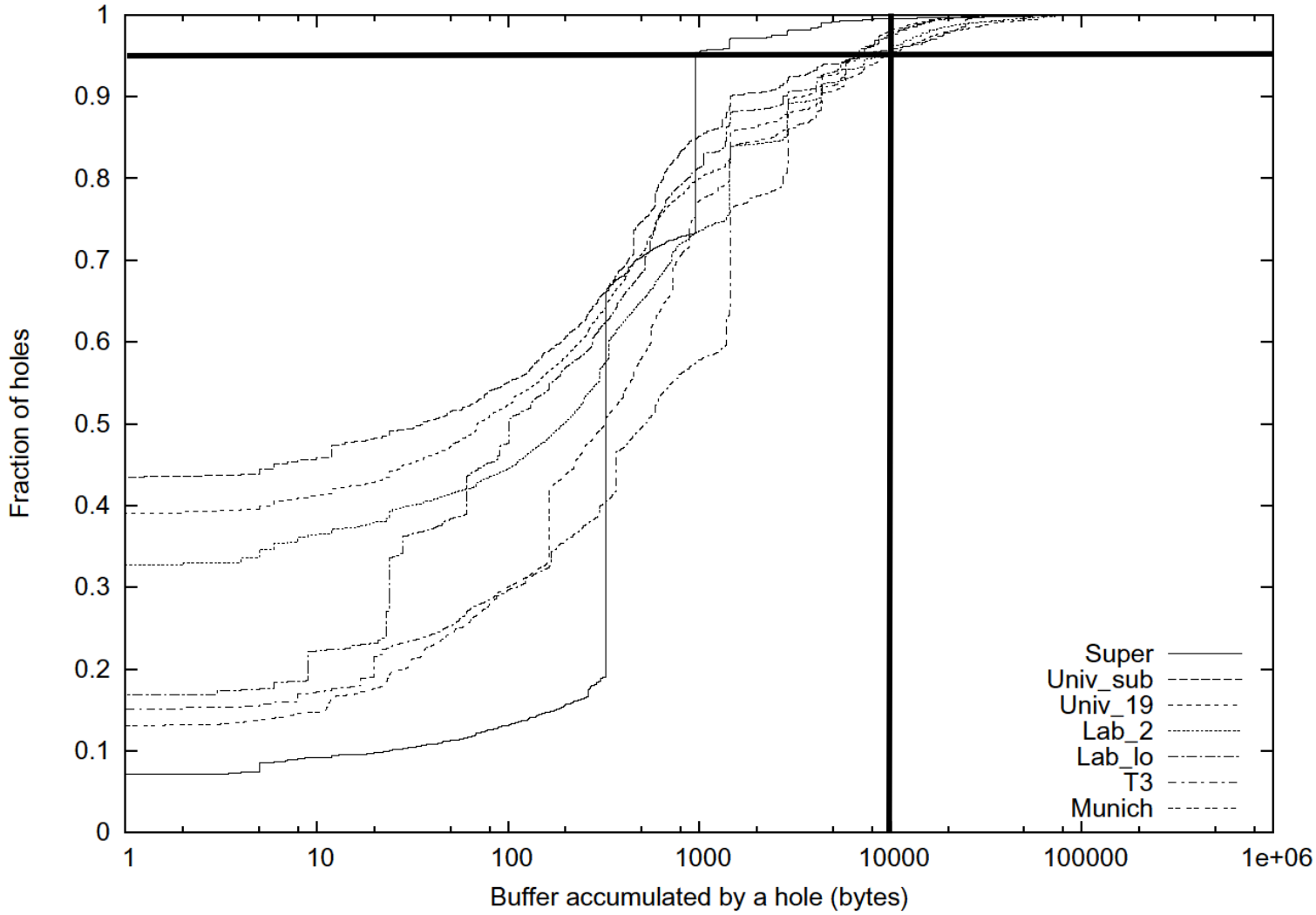
| | $Univ_{sub}$ | $Univ_{19}$ | $Lab_{lo}$ | $Lab_2$ | *Super* | *T3* | *Munich* |
|---|---|---|---|---|---|---|---|
| Trace duration (seconds) | 303 | 5,697 / 300* | 3,602 | 3,604 | 3,606 | 10,800 | 6,167 |
| Total packets | 1.25M | 6.2M | 1.5M | 14.1M | 3.5M | 36M | 220M |
| Total connections | 53K | 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 *external* host (§ 5.1) | 0.5% | 0.02% | 0.06% | 0.06% | 0% | 0.46% | 0.02% |


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_lo
T3
Munich

| | *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% |

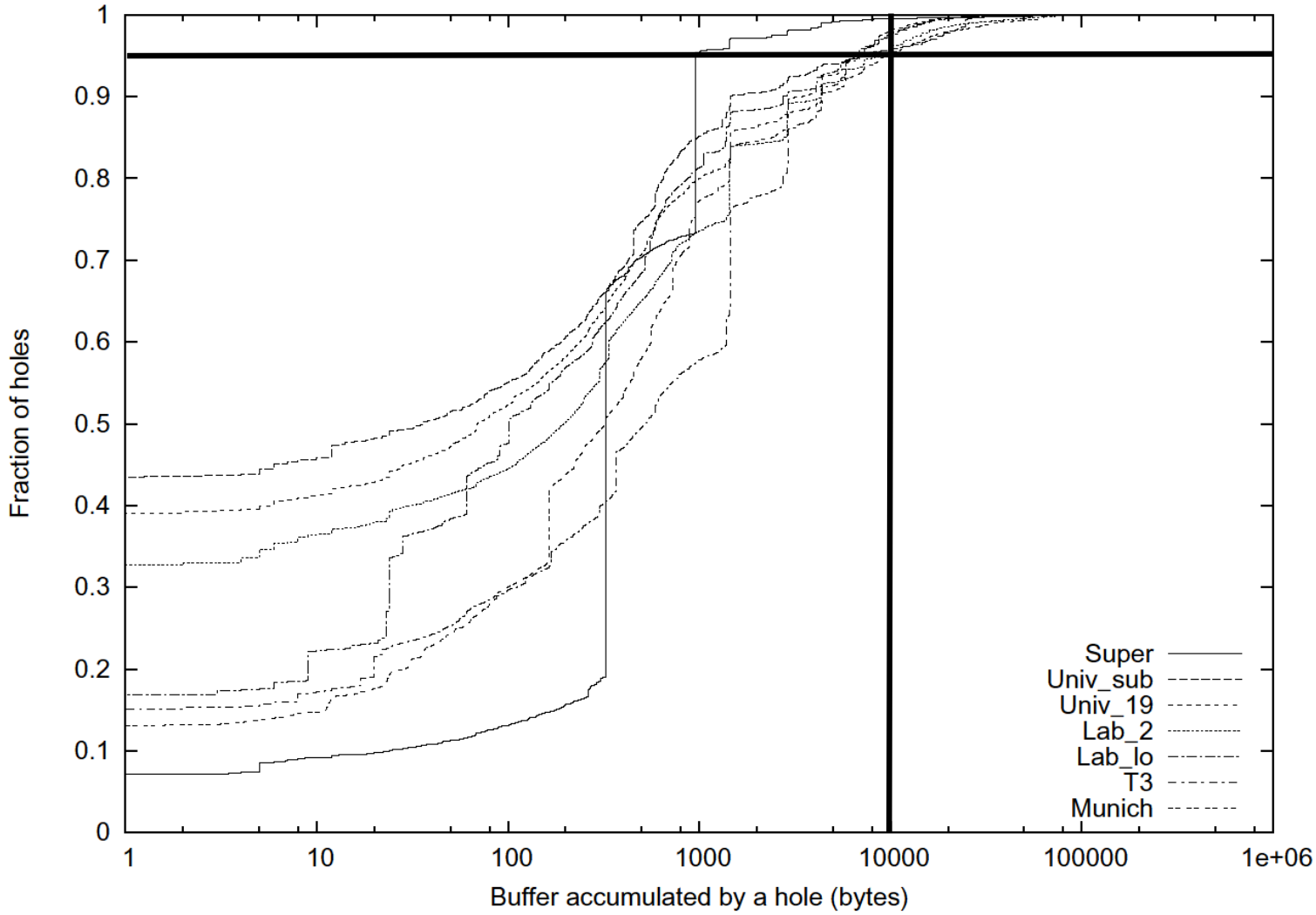
Adversary can fill the entire buffer with just a single connection!

***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

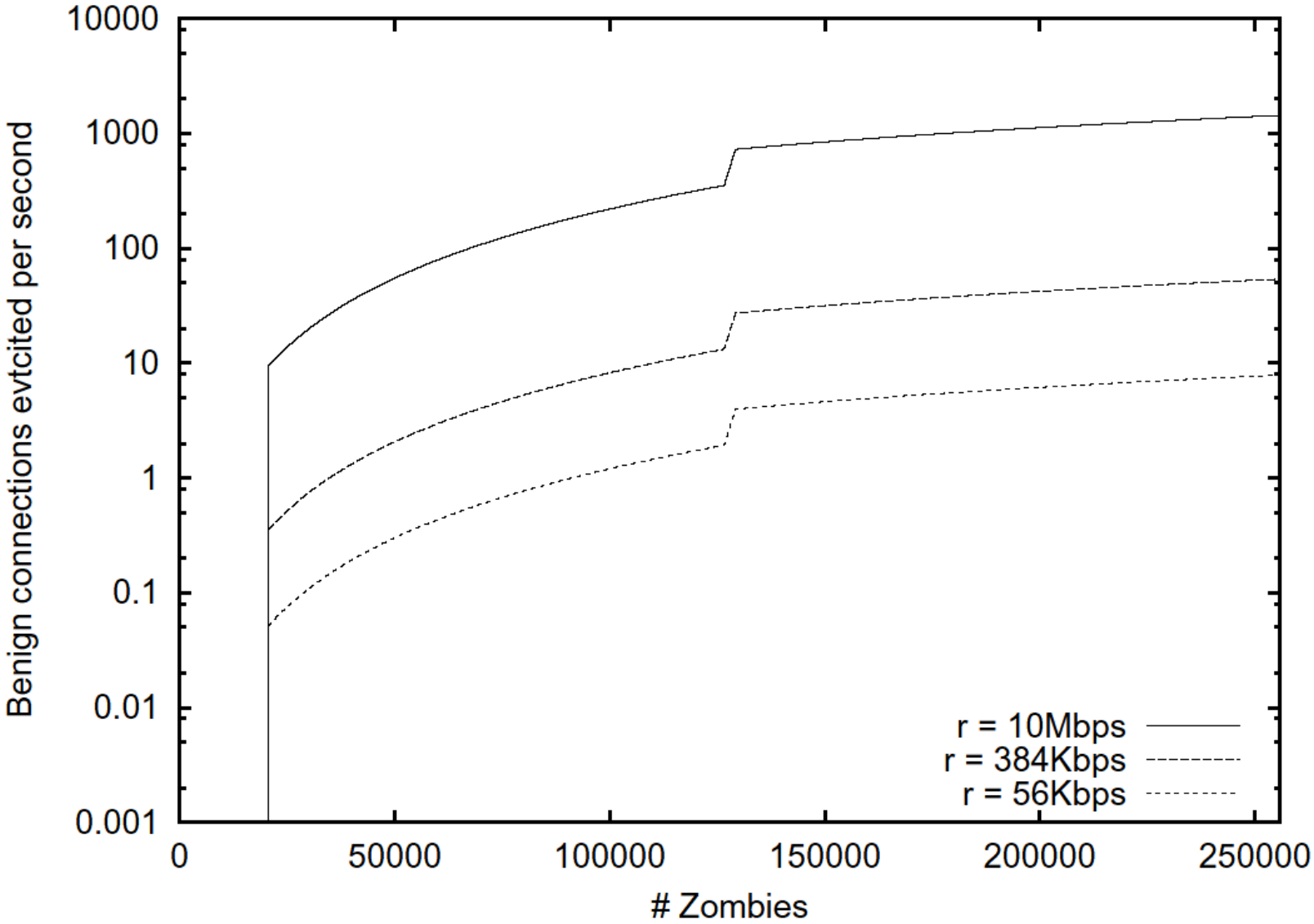
| | $Univ_{sub}$ | $Univ_{19}$ | $Lab_{lo}$ | $Lab_2$ | *Super* | *T3* | *Munich* |
|---|---|---|---|---|---|---|---|
| Fraction of holes that overlap hole on another connection of same *external* host | 0.5% | 0.02% | 0.06% | 0.06% | 0% | 0.46% | 0.02% |

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

- ***Policy 3:*** Upon buffer 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