The Matter of Heartbleed

IMC 2014

Zakir Durumeric, Frank Li, James Kasten,
Johanna Amann, Jethro Beekman,
Mathias Payer, Nicholas Weaver,
David Adrian, Vern Paxson, Michael Bailey,
J. Alex Halderman

Heartbleed

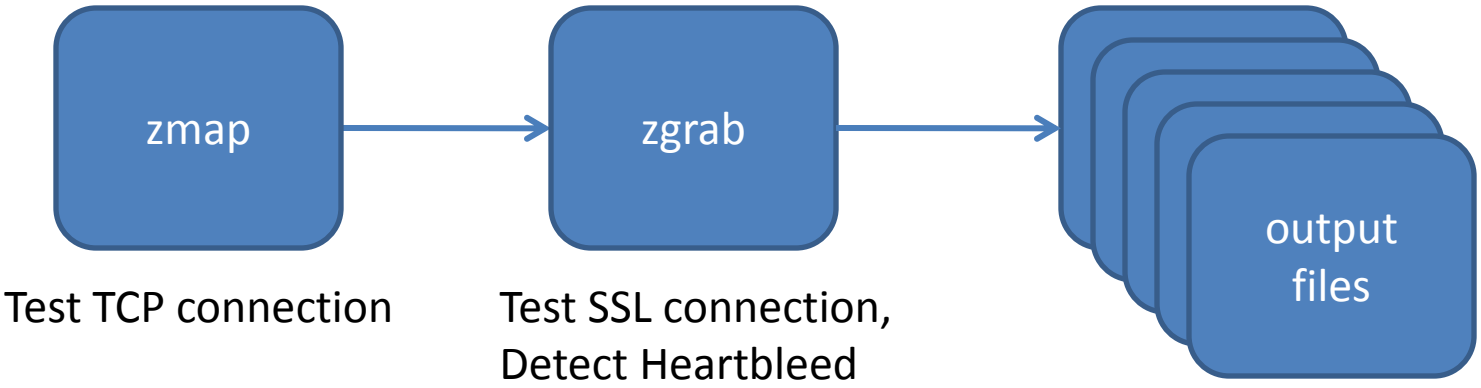
- 2014 catastrophic information disclosure vulnerability in OpenSSL
- Leakage of private data, encryption keys, etc.
- Many websites affected

This study: **measure global response**

Data overview

Data Source	Analysis	Size/Amount
Heartbleed ZMap scans	Estimate initial impact, patching rate, and notification reactions	43,142,864 datapoints=89GiB
Trustworthy Internet Movement's SSL Pulse	Estimate initial impact	200,000 HTTPS websites
Press releases, bug reports, security advisories	Estimate initial impact and vulnerable products	~60 documents
Michigan daily scans of the HTTPS ecosystem	Quantify certificate revocation and replacement	~3.5 billion scans= 250 GB
ICSI Certificate Notary	Quantify certificate replacement	3 million certificates
Network traces from ICSI, LBNL, NERSC, and an EC2 honeypot	Investigate pre-disclosure and postdisclosure wide-spread attacks	50+ TB of network traces
Debian weak keys vulnerability data [Yilek et al, 2008]	Compare Heartbleed with the Debian weak keys vulnerability	10,224,300 datapoints=500 MiB
Email exchanges with >4000 operator abuse contacts	Understand notification sentiment and measure responses	> 1000 emails

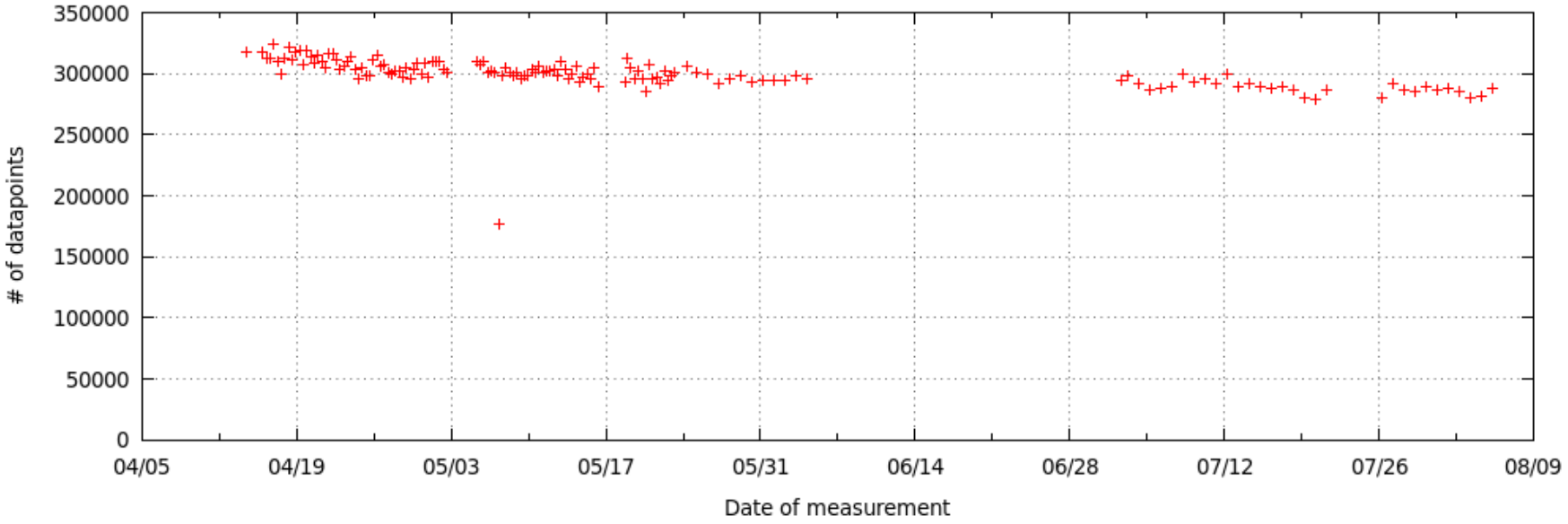
zmap: How was the data obtained?



zmap: How much data was obtained?

144 measurements between April 14 and August 5 2014

- 1% samples
- 3×/day, later 1×/day
- Each measurement about 300,000 datapoints
- 2KiB/datapoint (650MiB per measurement)
- 43,142,864 datapoints total (89GiB)



zmap: Data format

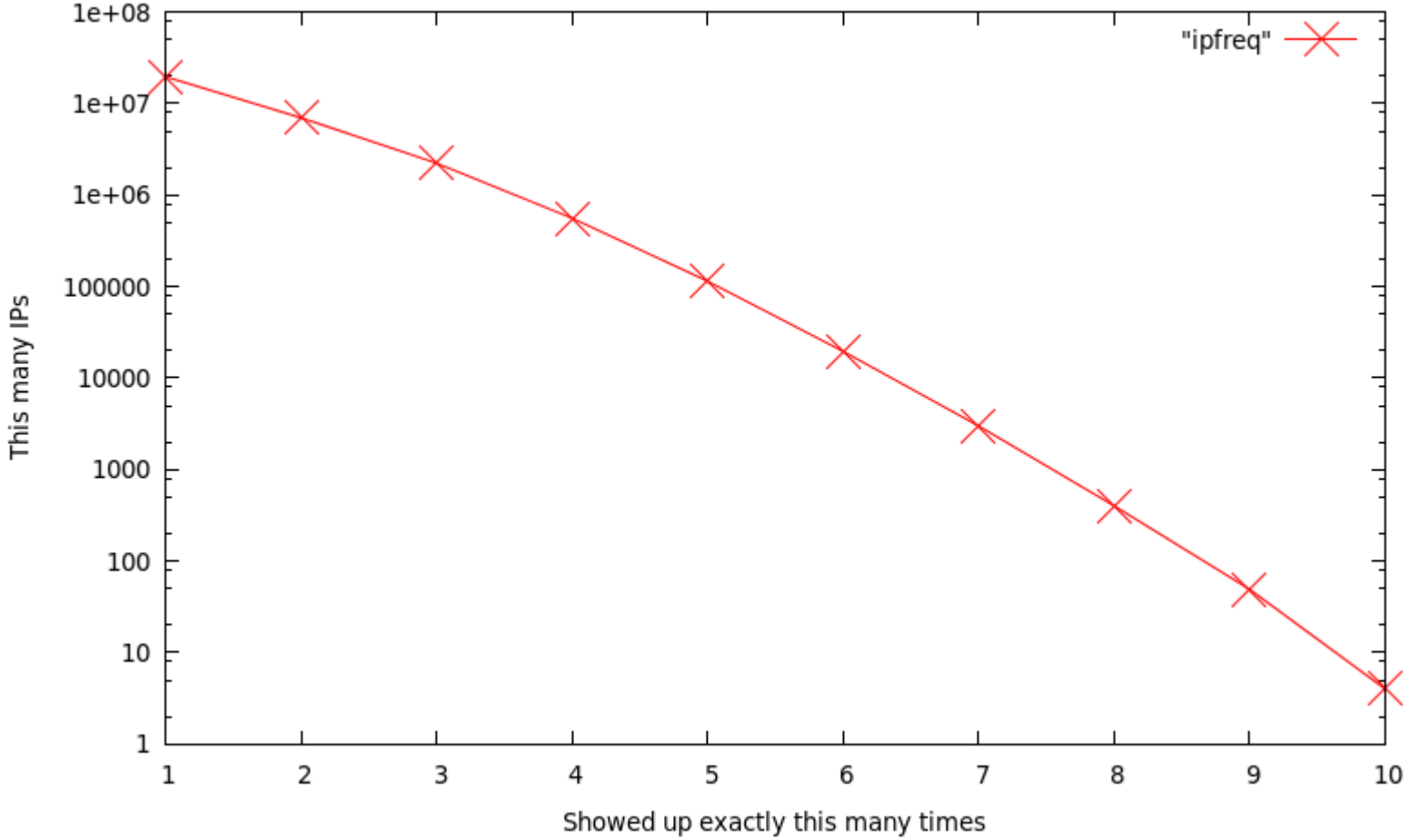
random.20140414T1144.json
random.20140415T2020.json
random.20140416T0635.json
random.20140416T1435.json
…

{"host":"50.97.227.237","error":null,"tls_handshake":{"ServerHelloMsg":{"version":771,"random":"U0wCVfr6qytUEGrvGlHyt7lkaOaKzOheRRMYjcRuudY=","session_id":"UFdf9Mk5i4rjja+odAlhyToDD+lEr6Wx54EQummqm/Y=","cipher_suite":49199,"compression_method":0,"next_protocol_negotiation":false,"next_protocols":null,"ocsp_stapling":false,"ticket_supported":false,"heartbeat_supported":true,"heartbleed_vulnerable":true},"ServerCertificatesMsg":{"certificates":["*2KB_base64_blob*","*2KB_base64_blob*","*2KB_base64_blob*"]},"ServerKeyExchangeMsg":{"key":"*1KB_key_blob*"},"ServerFinishedMsg":{"verify_data":"wtirjakJwhuUNSwG"}},"encoding":"string","data":""}

zmap: Data format

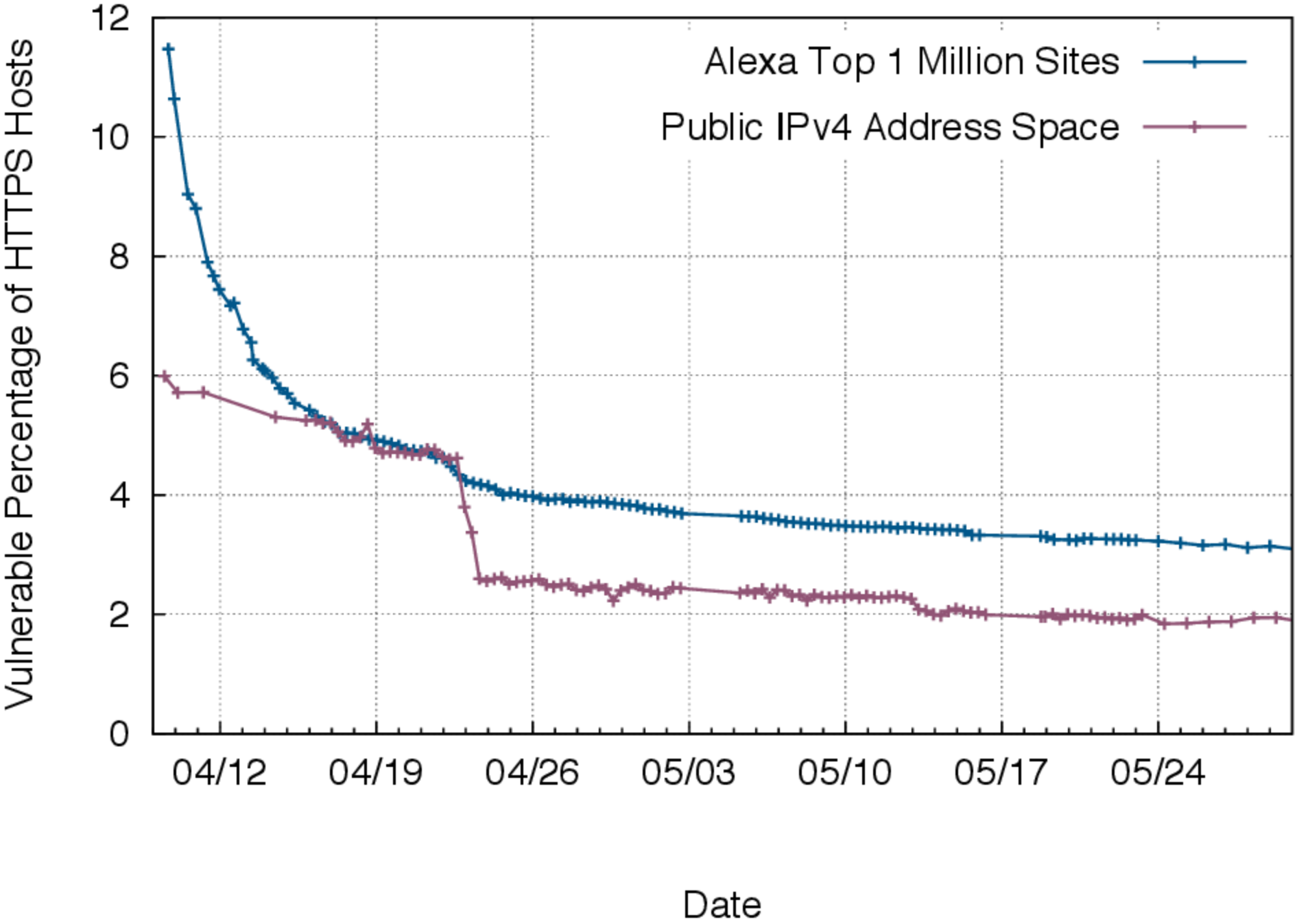

```
{
  "host": "50.97.227.237",
  "error": null,
  "tls_handshake": {
    "ServerHelloMsg": {
      "version": 771,
      "random": "U0wCVfr6qytUEGrvGlHyt7lkaOaKzOheRRMYjcRuudY=",
      "session_id": "UFdf9Mk5i4rjja+odAlhyToDD+lEr6Wx54EQummqm/Y=",
      "cipher_suite": 49199,
      "compression_method": 0,
      "next_protocol_negotiation": false,
      "next_protocols": null,
      "ocsp_stapling": false,
      "ticket_supported": false,
      "heartbeat_supported": true,
      "heartbleed_vulnerable": true
    },
    "ServerCertificatesMsg": {
      "certificates": [
        "2KB_base64_blob",
        "2KB_base64_blob",
        "2KB_base64_blob"
      ]
    },
    "ServerKeyExchangeMsg": {
      "key": "1KB_key_blob"
    },
    "ServerFinishedMsg": {
      "verify_data": "wtirjakJwhuUNSwG"
    }
  },
  "encoding": "string",
  "data": ""
}
```

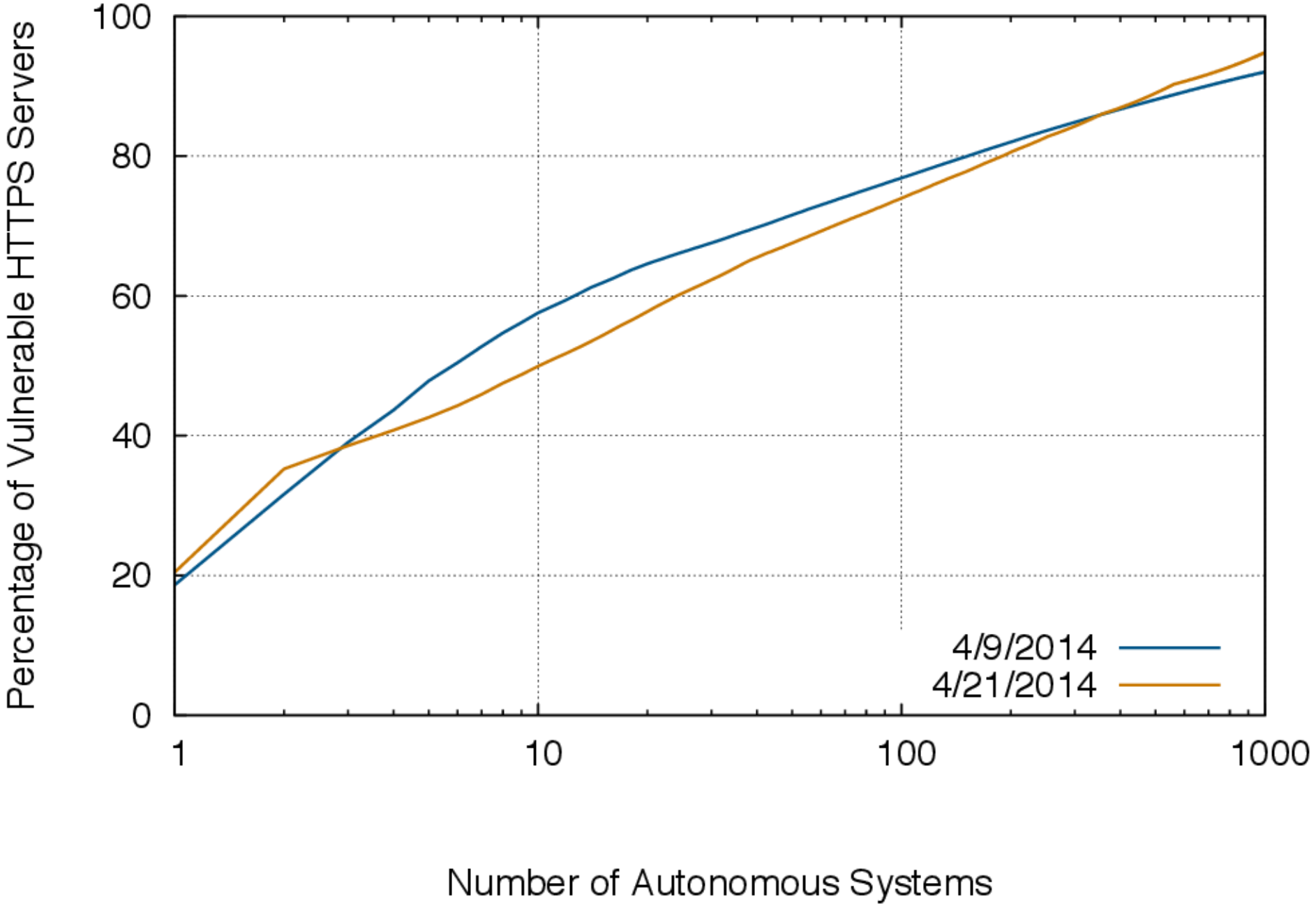
zmap: How often did we see a certain host?



1	19,579,439	6	19,576
2	6,972,753	7	2,984
3	2,223,616	8	401
4	558,182	9	49
5	114,462	10	4

Total: 29,471,466 unique hosts


Alexa Top 1 Million Sites
Public IPv4 Address Space
Vulnerable Percentage of HTTPS Hosts
12
10
8
6
4
2
0
04/12
04/19
04/26
05/03
05/10
05/17
05/24
Date


Percentage of Vulnerable HTTPS Servers
100
80
60
40
20
0
1
10
100
1000
4/9/2014
4/21/2014
Number of Autonomous Systems

Debian PRNG bug data

2008 catastrophic key generation bug

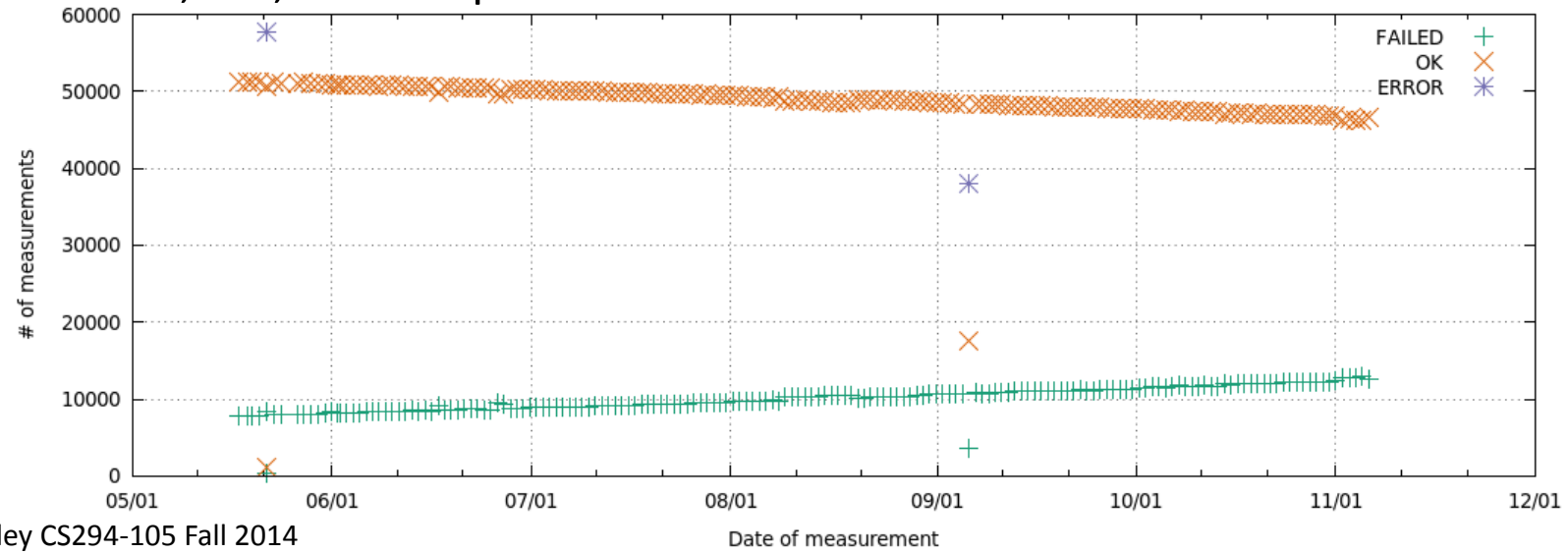
- Debian version of OpenSSL
- SSL Certificates issued with weak keys

Yilek et al. study: measure response of popular websites

How much data was obtained?

173 measurements between May 17 and November 6 2008

- Each measurement 59,100 dataponts
- 10,224,300 datapoints total



Debian comparison

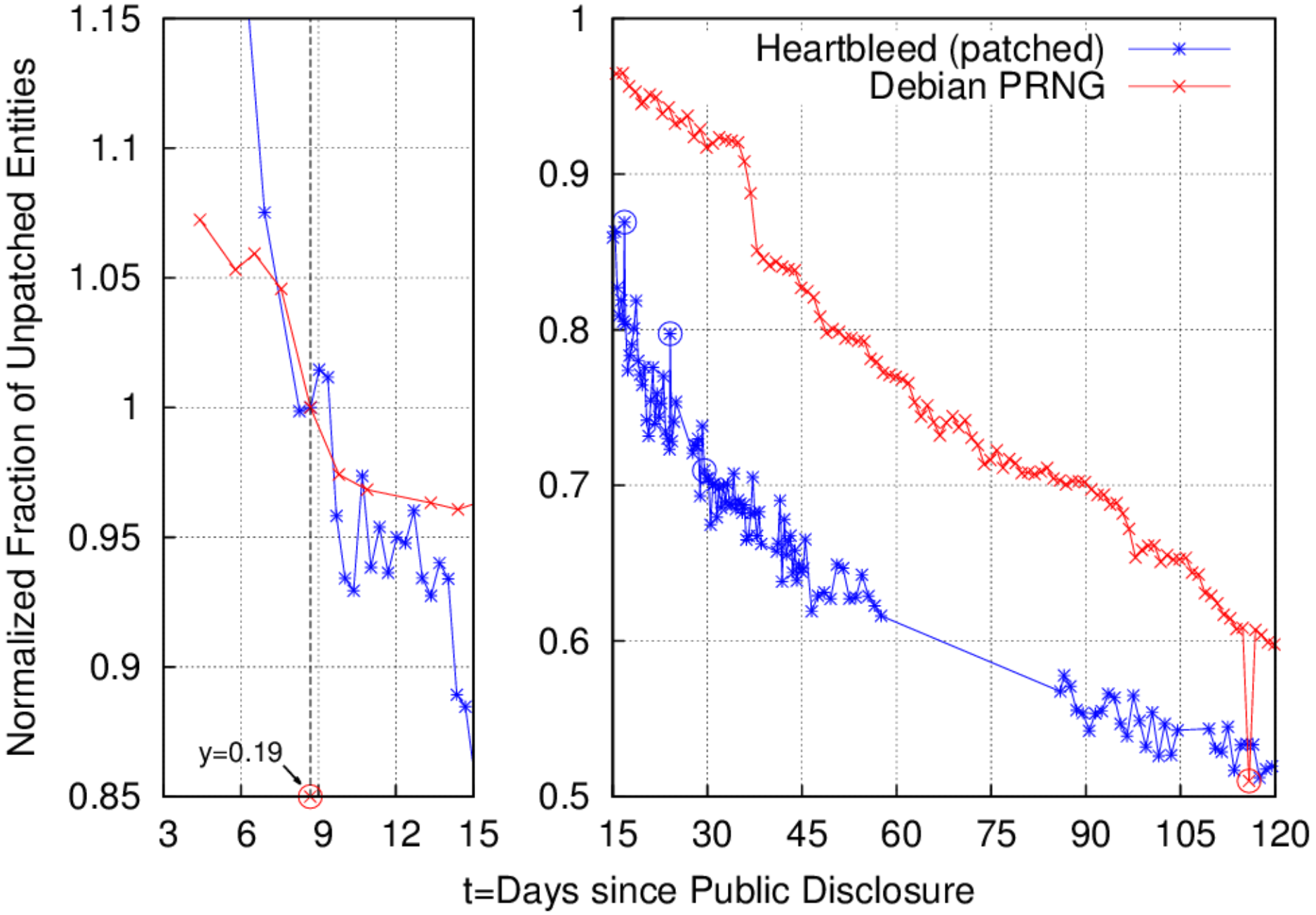
"apples-to-apples" comparison? => compare "entities"

Entity: group of servers that all present the same certificate during a particular measurement

zmap: First full measurement – April 11 10:05 UTC
2651838 entities
- 180049 not patched (6.8%)

zmap: First sampled measurement – April 14 15:44 UTC
108592 entities
- 6422 not patched (5.9%)

Debian: First meaurement – May 17 21:59 UTC
43132 entities
- 468 not patched (11%)

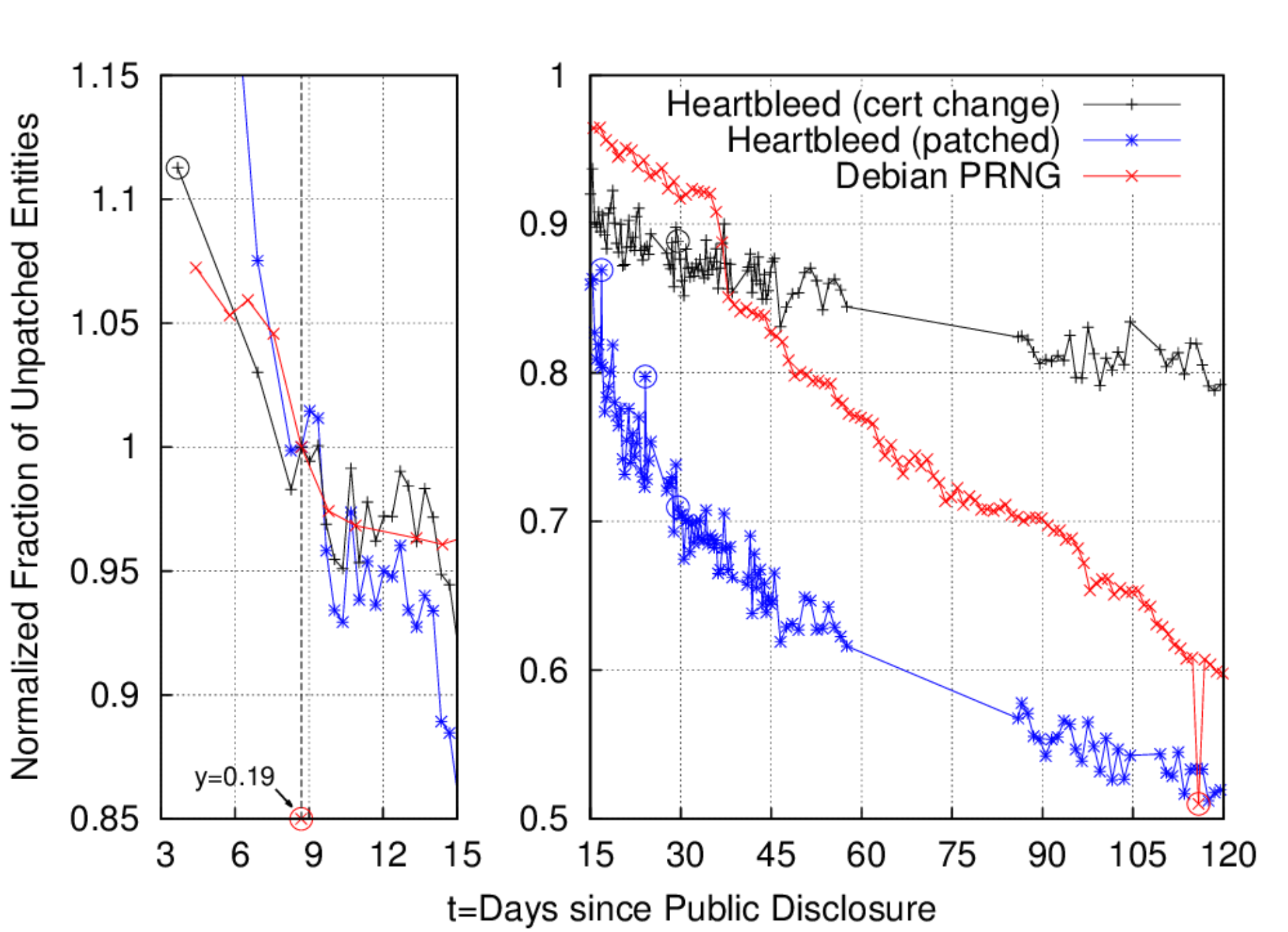

Heartbleed (patched)
Debian PRNG
Normalized Fraction of Unpatched Entities
t=Days since Public Disclosure
y=0.19
1.15
1.1
1.05
1
0.95
0.9
0.85
3
6
9
12
15
1
0.9
0.8
0.7
0.6
0.5
15
30
45
60
75
90
105
120

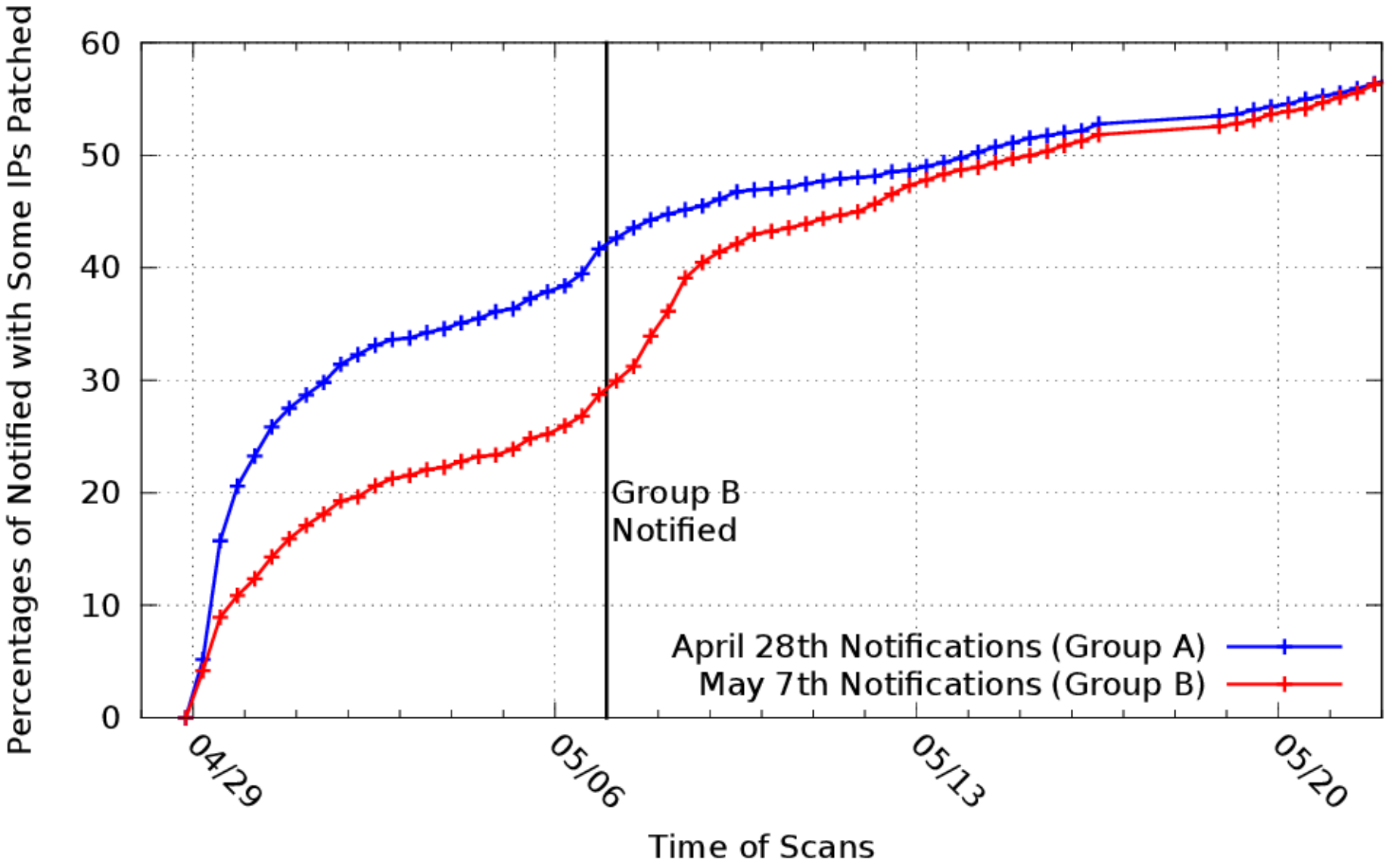
Debian comparison

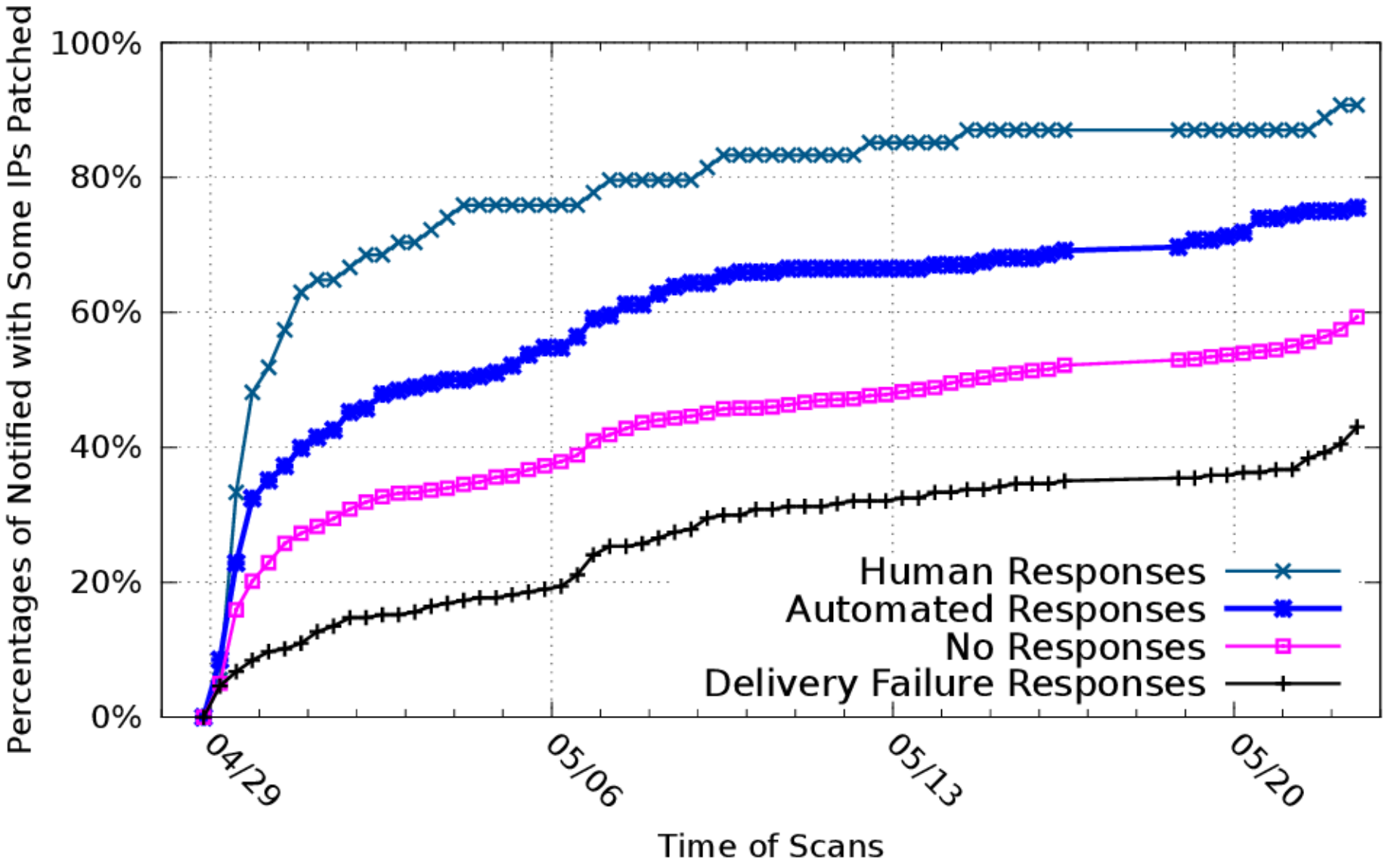
"apples-to-apples" comparison? => compare "entities"

Debian measured certificate change,
we just measured software upgrade
=> certificate change recommended

new entity: group of servers that all present the same certificate during **both a particular measurement and all previous measurements**


Heartbleed (cert change)
Heartbleed (patched)
Debian PRNG
Normalized Fraction of Unpatched Entities
t=Days since Public Disclosure
y=0.19
1.15
1.1
1.05
1
0.95
0.9
0.85
3
6
9
12
15
1
0.9
0.8
0.7
0.6
0.5
15
30
45
60
75
90
105
120


Percentages of Notified with Some IPs Patched
60
50
40
30
20
10
0
04/29
05/06
05/13
05/20
Time of Scans
Group B
Notified
April 28th Notifications (Group A)
May 7th Notifications (Group B)


Percentages of Notified with Some IPs Patched
100%
80%
60%
40%
20%
0%
04/29
05/06
05/13
05/20
Time of Scans
Human Responses
Automated Responses
No Responses
Delivery Failure Responses