What Lies Beneath?
Analyzing Automated SSH Bruteforce Attacks

AbdelRahman Abdou, **David Barrera**, Paul van Oorschot

Carleton University

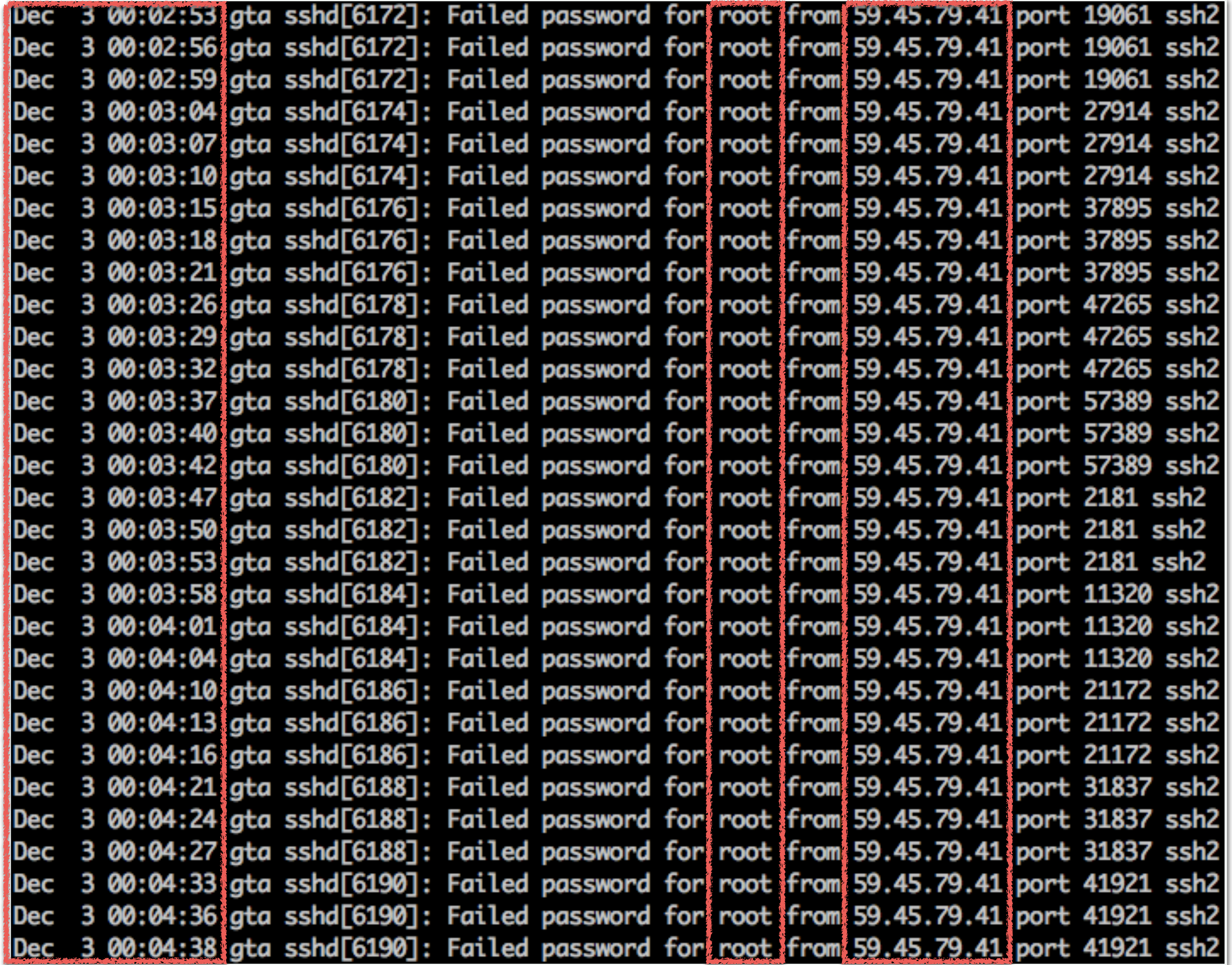
ETH Zürich

Secure Shell (SSH)

- Protocol to enable remote logins and network services over an unsecured network.
- Typically used for remote system administration
- Client/server implementations for all operating systems

Secure Shell (SSH)

- Setting up a server is easy
  - /etc/rc.d/sshd start or systemctl start ssh
- Sometimes enabled by default (e.g., routers, server distributions)
- Server listens on TCP port 22



```
Dec  3 00:02:53 gta sshd[6172]: Failed password for root from 59.45.79.41 port 19061 ssh2
Dec  3 00:02:56 gta sshd[6172]: Failed password for root from 59.45.79.41 port 19061 ssh2
Dec  3 00:02:59 gta sshd[6172]: Failed password for root from 59.45.79.41 port 19061 ssh2
Dec  3 00:03:04 gta sshd[6174]: Failed password for root from 59.45.79.41 port 27914 ssh2
Dec  3 00:03:07 gta sshd[6174]: Failed password for root from 59.45.79.41 port 27914 ssh2
Dec  3 00:03:10 gta sshd[6174]: Failed password for root from 59.45.79.41 port 27914 ssh2
Dec  3 00:03:15 gta sshd[6176]: Failed password for root from 59.45.79.41 port 37895 ssh2
Dec  3 00:03:18 gta sshd[6176]: Failed password for root from 59.45.79.41 port 37895 ssh2
Dec  3 00:03:21 gta sshd[6176]: Failed password for root from 59.45.79.41 port 37895 ssh2
Dec  3 00:03:26 gta sshd[6178]: Failed password for root from 59.45.79.41 port 47265 ssh2
Dec  3 00:03:29 gta sshd[6178]: Failed password for root from 59.45.79.41 port 47265 ssh2
Dec  3 00:03:32 gta sshd[6178]: Failed password for root from 59.45.79.41 port 47265 ssh2
Dec  3 00:03:37 gta sshd[6180]: Failed password for root from 59.45.79.41 port 57389 ssh2
Dec  3 00:03:40 gta sshd[6180]: Failed password for root from 59.45.79.41 port 57389 ssh2
Dec  3 00:03:42 gta sshd[6180]: Failed password for root from 59.45.79.41 port 57389 ssh2
Dec  3 00:03:47 gta sshd[6182]: Failed password for root from 59.45.79.41 port 2181 ssh2
Dec  3 00:03:50 gta sshd[6182]: Failed password for root from 59.45.79.41 port 2181 ssh2
Dec  3 00:03:53 gta sshd[6182]: Failed password for root from 59.45.79.41 port 2181 ssh2
Dec  3 00:03:58 gta sshd[6184]: Failed password for root from 59.45.79.41 port 11320 ssh2
Dec  3 00:04:01 gta sshd[6184]: Failed password for root from 59.45.79.41 port 11320 ssh2
Dec  3 00:04:04 gta sshd[6184]: Failed password for root from 59.45.79.41 port 11320 ssh2
Dec  3 00:04:10 gta sshd[6186]: Failed password for root from 59.45.79.41 port 21172 ssh2
Dec  3 00:04:13 gta sshd[6186]: Failed password for root from 59.45.79.41 port 21172 ssh2
Dec  3 00:04:16 gta sshd[6186]: Failed password for root from 59.45.79.41 port 21172 ssh2
Dec  3 00:04:21 gta sshd[6188]: Failed password for root from 59.45.79.41 port 31837 ssh2
Dec  3 00:04:24 gta sshd[6188]: Failed password for root from 59.45.79.41 port 31837 ssh2
Dec  3 00:04:27 gta sshd[6188]: Failed password for root from 59.45.79.41 port 31837 ssh2
Dec  3 00:04:33 gta sshd[6190]: Failed password for root from 59.45.79.41 port 41921 ssh2
Dec  3 00:04:36 gta sshd[6190]: Failed password for root from 59.45.79.41 port 41921 ssh2
Dec  3 00:04:38 gta sshd[6190]: Failed password for root from 59.45.79.41 port 41921 ssh2
```

Secure Shell (SSH)

- Empirically, we know:
    - Password guessing attacks on SSH are annoyingly frequent
    - Root accounts are often targeted (probably the most rewarding account)
    - Source IP addresses of attacks are diverse
- Much advice online about how to deal with this problem (Fail2Ban, Denyhosts et al.)

Talk Outline

- Research objectives
- Methodology
- Timing stats
- Password composition and distribution
- Password sharing/reuse among attackers

Objective

Analyze **automated** SSH bruteforce attacks

Methodology

- Set up SSH servers with no valid accounts (not honeypots)
- Record guessing activity **including passwords**
- Analyze data
- Solve the SSH bruteforce attack problem

Methodology

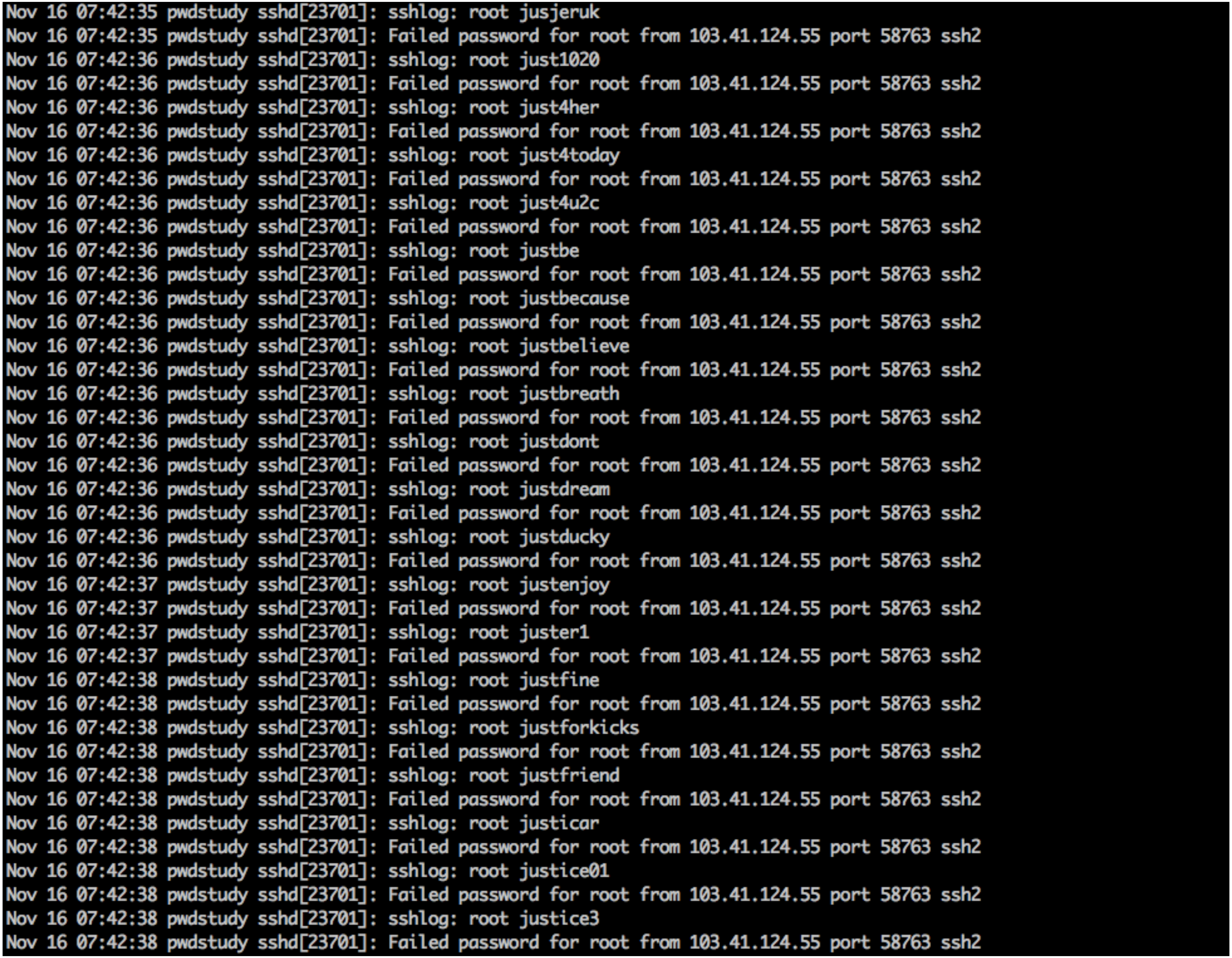
- Set up SSH servers with no valid accounts (not honeypots)
- Record guessing activity **including passwords**
- Analyze data
- ~~Solve the SSH bruteforce attack problem~~ Present findings at Passwords 2015

Methodology

- SSH servers were instrumented to **log guessed passwords** in addition to all standard logged properties

```
*WARNING*

This OpenSSH server has been modified to STORE
USERNAMES AND PASSWORDS. This server does not
have any valid user accounts, so no attempted
logins will succeed. The sole purpose of this
server is to collect (for research purposes)
login information used in automated SSH brute-
force attacks. If you are human, you should
not attempt to log in to this server.
```

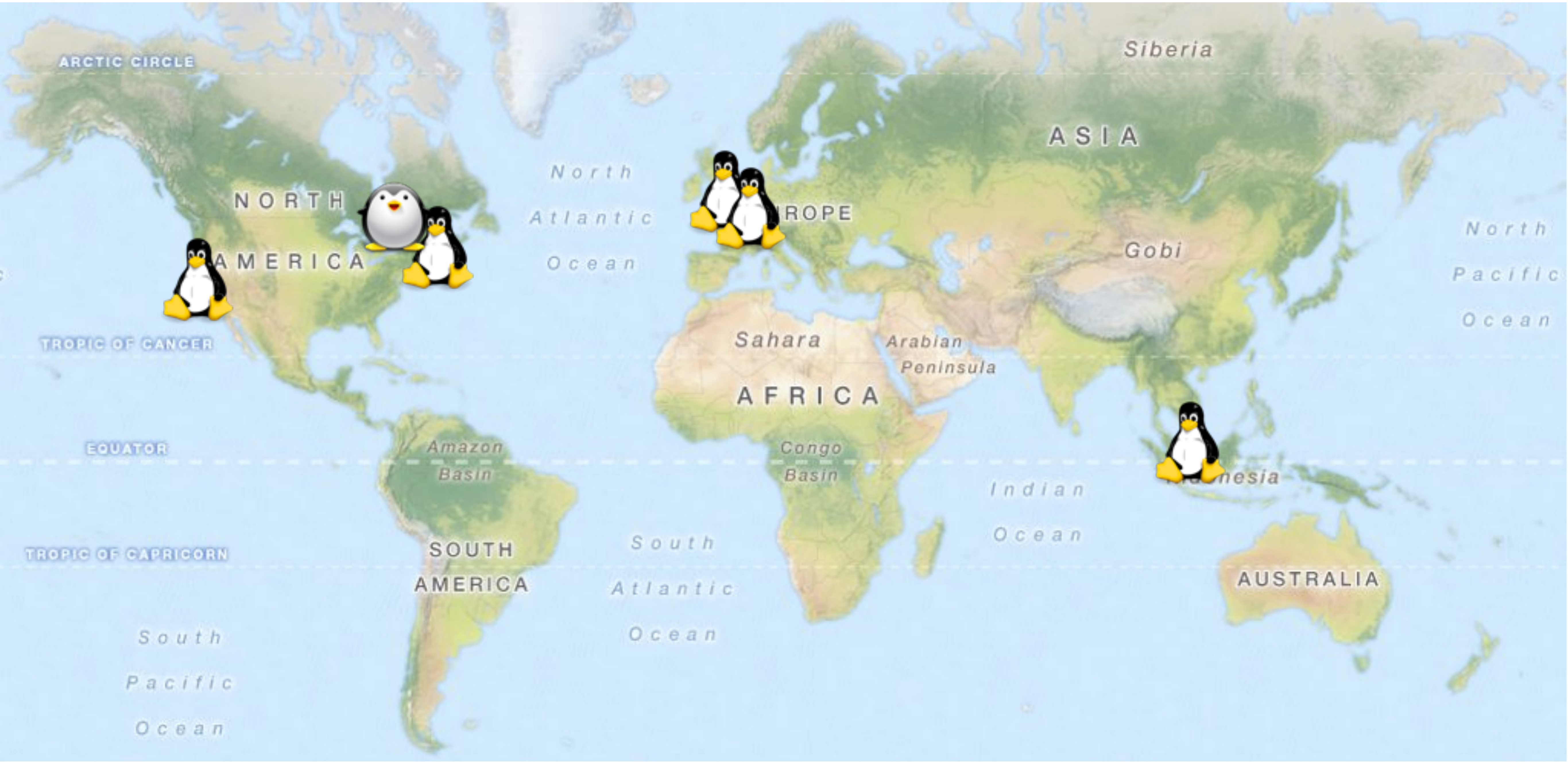


```
Nov 16 07:42:35 pwdstudy sshd[23701]: sshlog: root jusjeruk
Nov 16 07:42:35 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root just1020
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root just4her
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root just4today
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root just4u2c
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justbe
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justbecause
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justbelieve
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justbreath
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justdont
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justdream
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:36 pwdstudy sshd[23701]: sshlog: root justducky
Nov 16 07:42:36 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:37 pwdstudy sshd[23701]: sshlog: root justenjoy
Nov 16 07:42:37 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:37 pwdstudy sshd[23701]: sshlog: root juster1
Nov 16 07:42:37 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justfine
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justforkicks
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justfriend
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justicar
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justice01
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
Nov 16 07:42:38 pwdstudy sshd[23701]: sshlog: root justice3
Nov 16 07:42:38 pwdstudy sshd[23701]: Failed password for root from 103.41.124.55 port 58763 ssh2
```

Methodology

- Long-term: 1 VM started March 1, 2014 for 373 days
- Short-term: 5 VMs started Jan 4, 2015 for 66 days

Methodology



Results Overview

- Total guessing **attempts**: 17,217,676
- Total source **IPs**: 6,297
    - From 1,235 ASs in 112 countries
- Distinct **usernames**: 27,855
- Distinct **passwords** 1,449,146

Timing Analysis

Timing Analysis

Daily

- No days with 0 attempts on any VM
  - Min of 180 attempts/day. Max 273,120/day

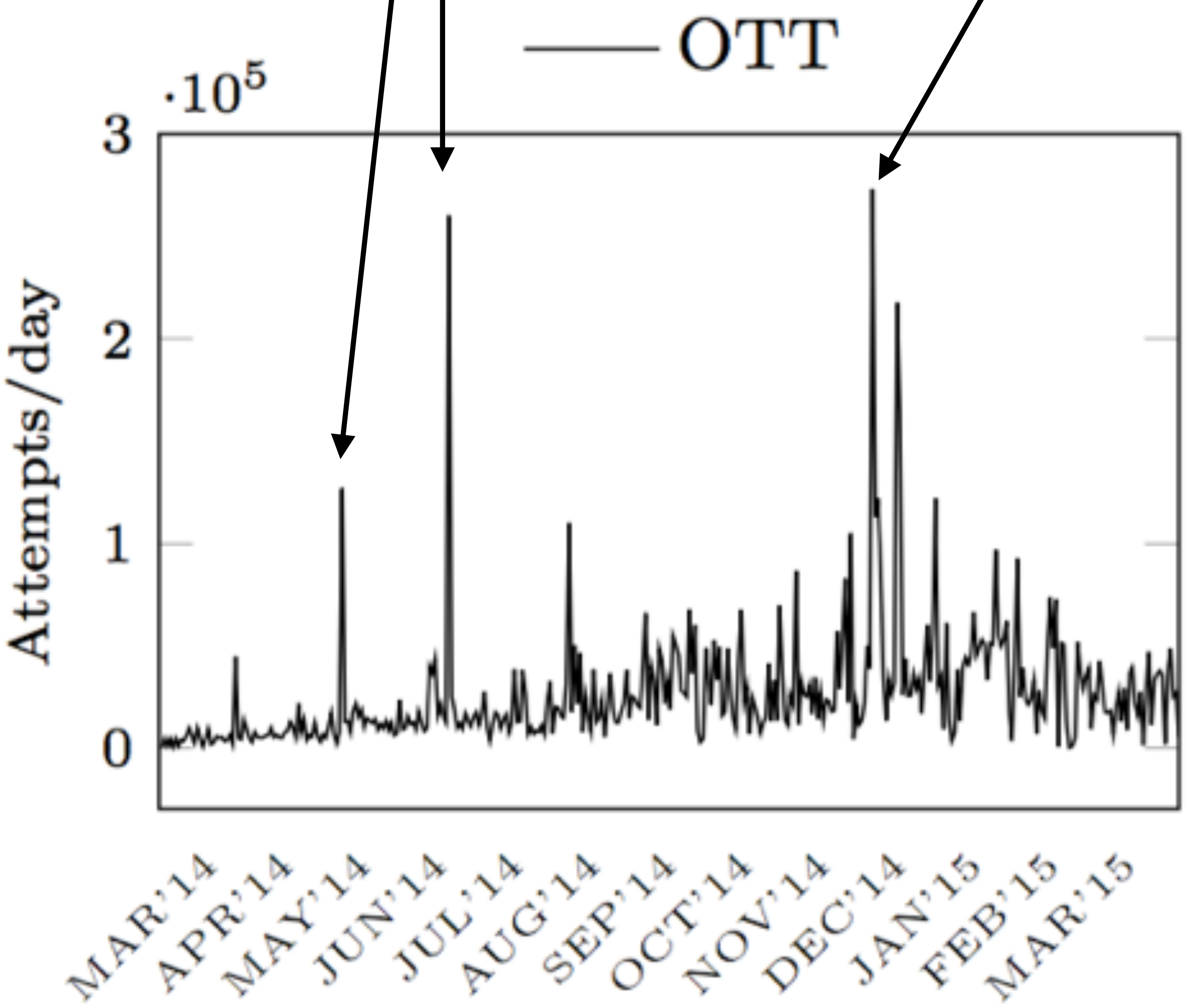
Hourly

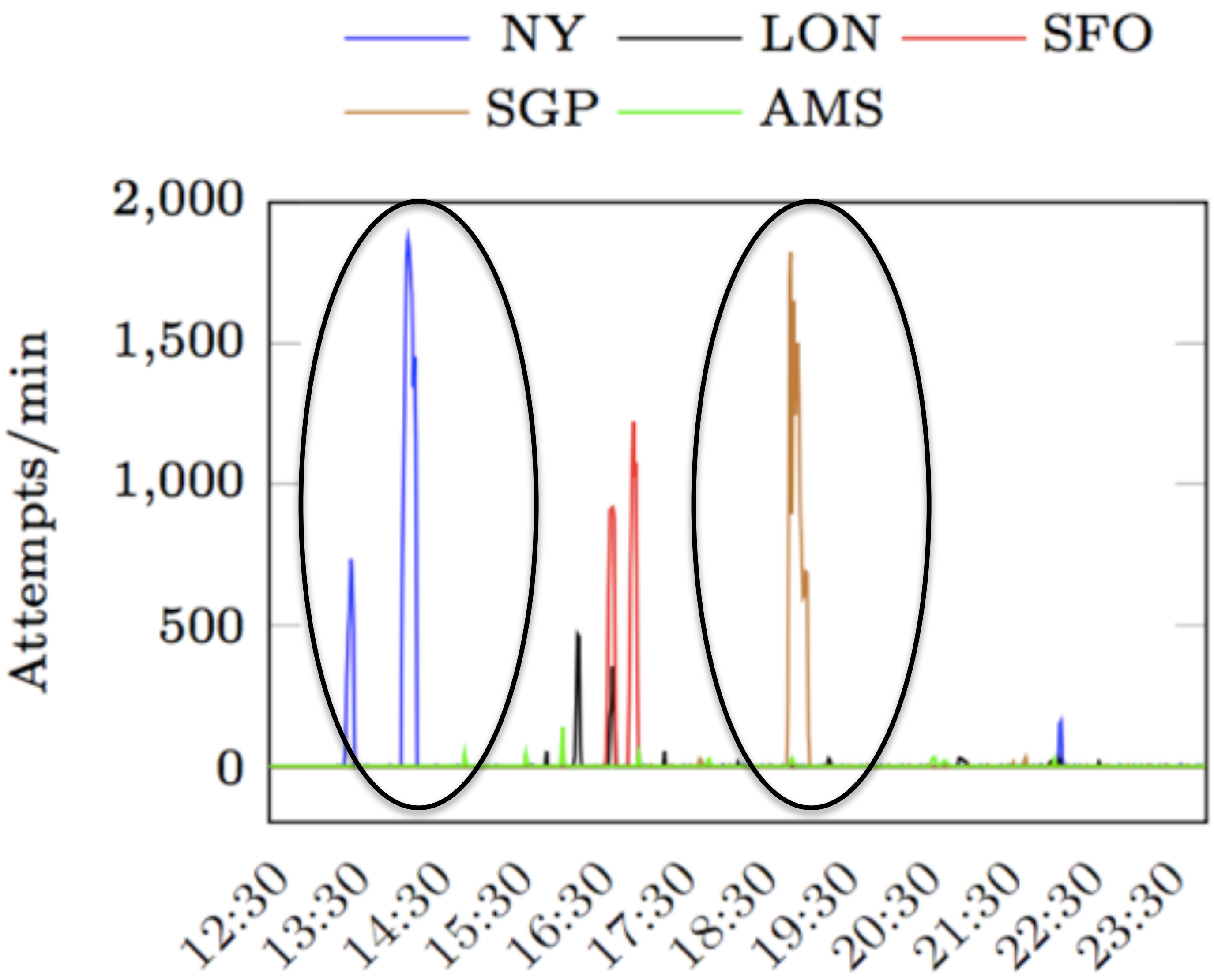
- Ottawa VM received 85,770 in one hour on June 14 (24/s!)

Timing Analysis

Single sources

273k guesses

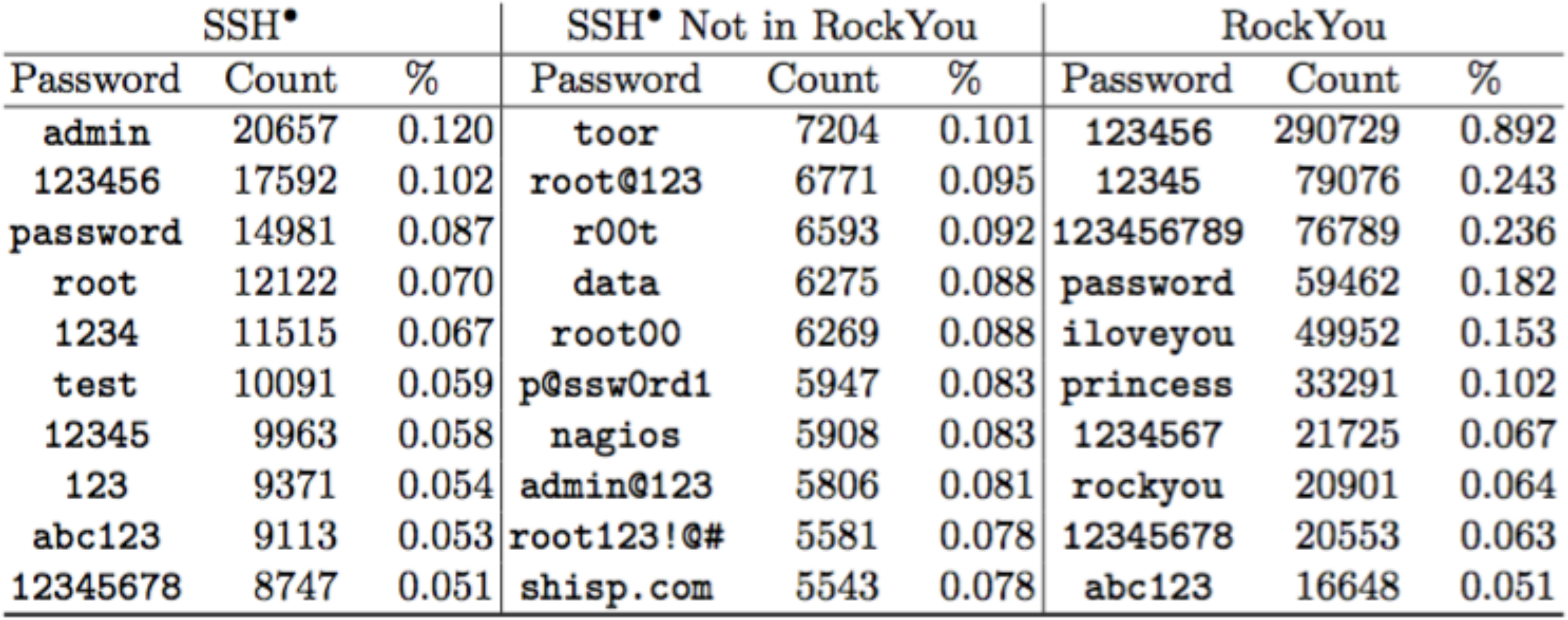




90% chance a new server will see between 6k and 24k daily attempts

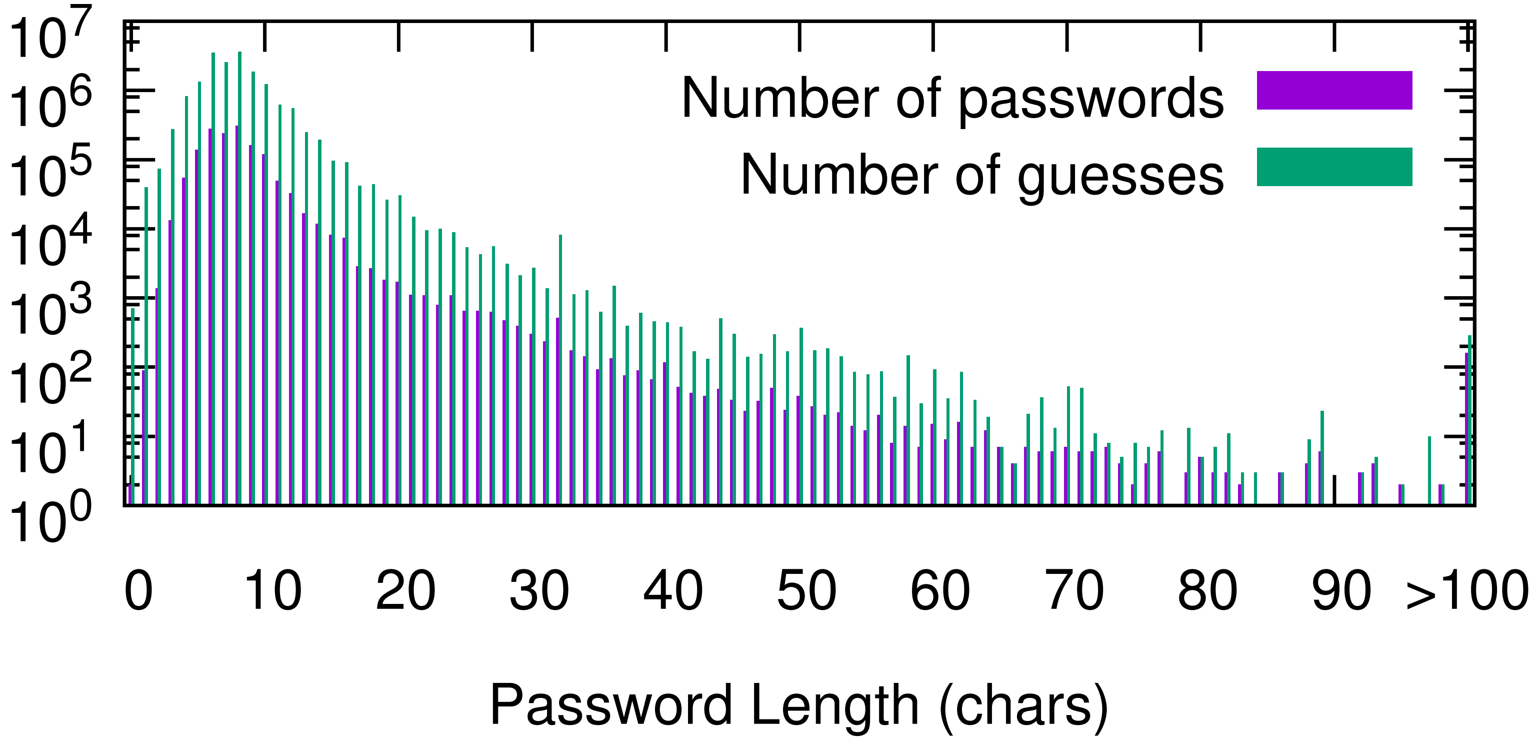
Password Analysis

Top Passwords Used in SSH Bruteforce Attacks



SSH•			SSH• Not in RockYou			RockYou		
Password	Count	%	Password	Count	%	Password	Count	%
admin	20657	0.120	toor	7204	0.101	123456	290729	0.892
123456	17592	0.102	root@123	6771	0.095	12345	79076	0.243
password	14981	0.087	r00t	6593	0.092	123456789	76789	0.236
root	12122	0.070	data	6275	0.088	password	59462	0.182
1234	11515	0.067	root00	6269	0.088	iloveyou	49952	0.153
test	10091	0.059	p@ssw0rd1	5947	0.083	princess	33291	0.102
12345	9963	0.058	nagios	5908	0.083	1234567	21725	0.067
123	9371	0.054	admin@123	5806	0.081	rockyou	20901	0.064
abc123	9113	0.053	root123!@#	5581	0.078	12345678	20553	0.063
12345678	8747	0.051	shisp.com	5543	0.078	abc123	16648	0.051

Password Length

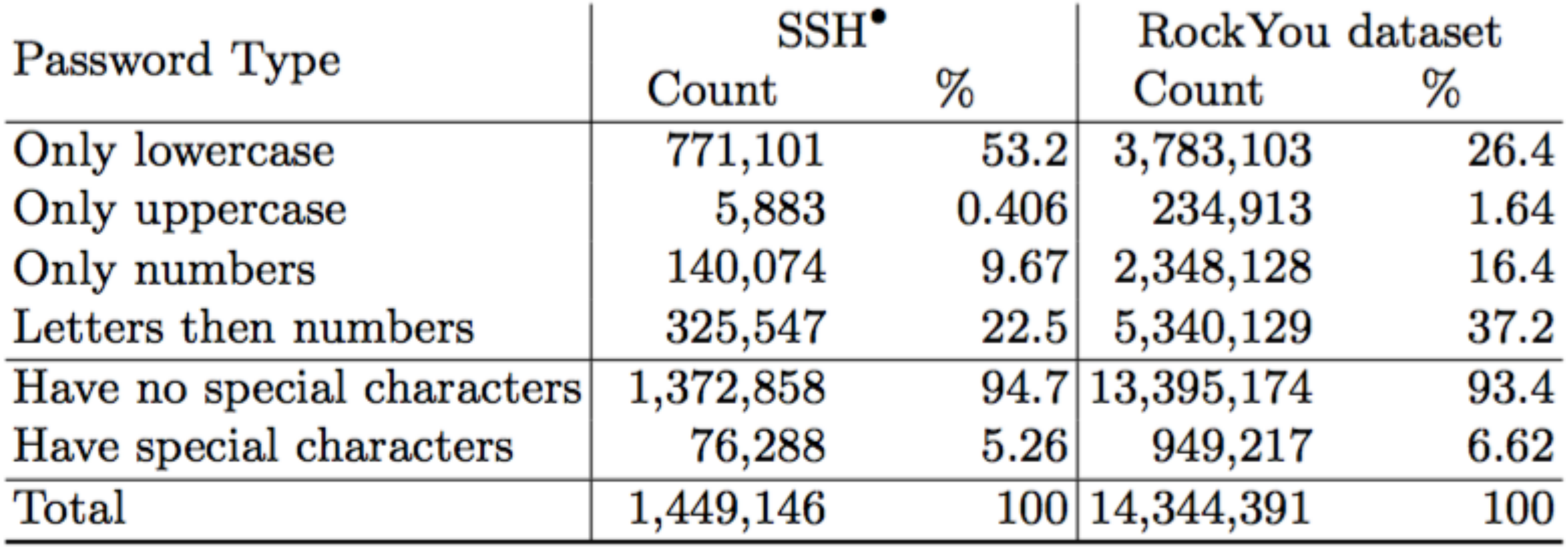


falconfallacyfalliblefallofffalltofamefamilyfaminefamousfanaticfancifulfangfangfangfanghuoqiangfangh…

energenerategenerousgeneticggeniegenregentlygenusgeologygeorge1geraldgermgermanygerrygertrudegestur

$6$4aOmWdpJ$kyPOik9rR0kSLyABIYNXggUqlWX3c1eIaovOLWphShTGXmuUAMq6iu9DrcQqlVUw3Pirizns4u27w3Ugvb6.:1

Password Composition



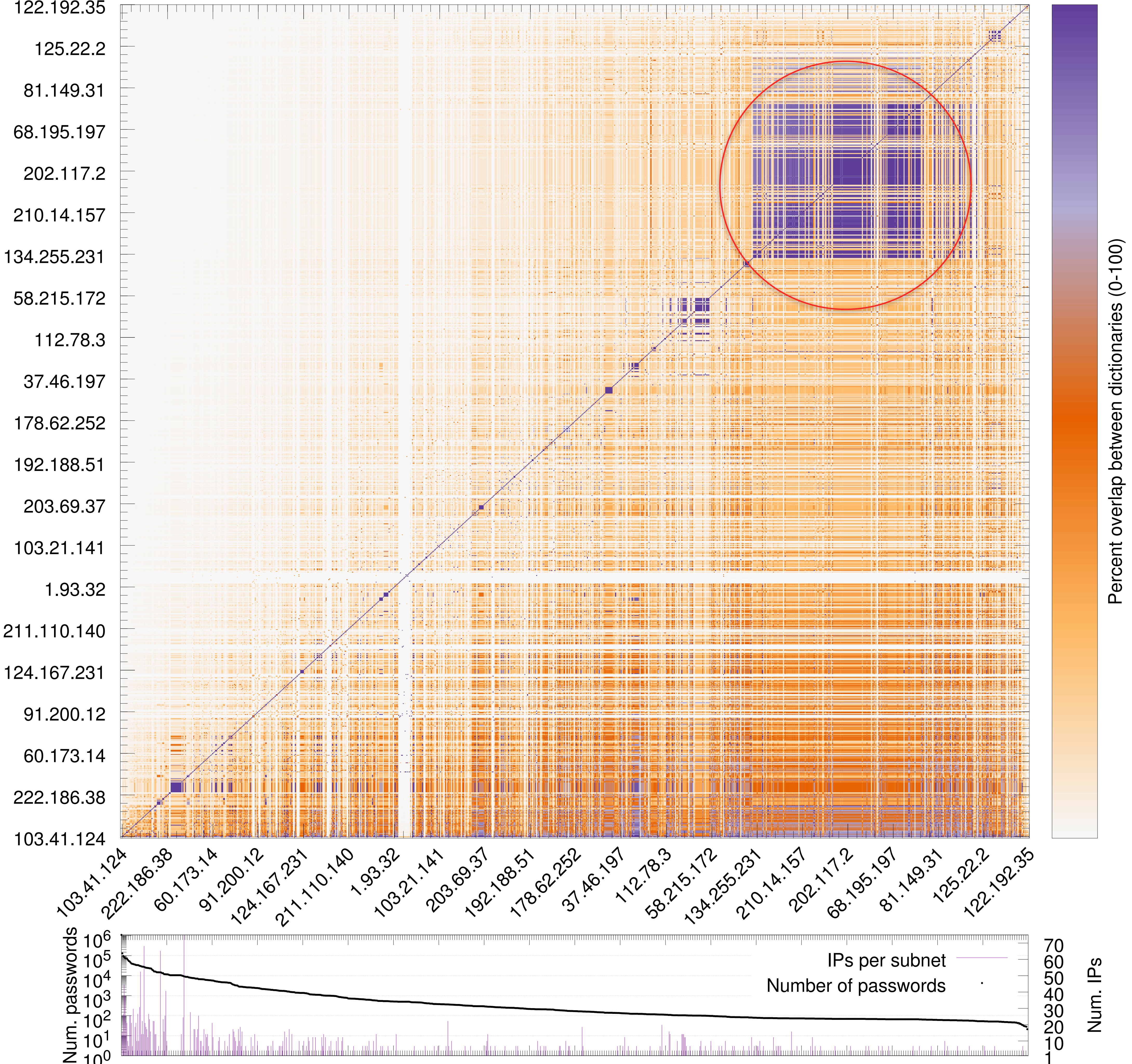
Password Type	SSH•		RockYou dataset	
	Count	%	Count	%
Only lowercase	771,101	53.2	3,783,103	26.4
Only uppercase	5,883	0.406	234,913	1.64
Only numbers	140,074	9.67	2,348,128	16.4
Letters then numbers	325,547	22.5	5,340,129	37.2
Have no special characters	1,372,858	94.7	13,395,174	93.4
Have special characters	76,288	5.26	949,217	6.62
Total	1,449,146	100	14,344,391	100

Open questions:

- Passwords in the form of URLs (123.com, nowtop.net)
- No evidence of overlap with leaked dictionaries (Rockyou, Yahoo, Sony, etc)

Password List Sharing

- Owens and Matthews (2008) observed several sources attempting the same set of username/password pairs
    - Defined sharing as 2 or more username+password guesses from distinct sources in the same order
- We wanted to see if this happened in our data



122.192.35
125.22.2
81.149.31
68.195.197
202.117.2
210.14.157
134.255.231
58.215.172
112.78.3
37.46.197
178.62.252
192.188.51
203.69.37
103.21.141
1.93.32
211.110.140
124.167.231
91.200.12
60.173.14
222.186.38
103.41.124
103.41.124
222.186.38
60.173.14
91.200.12
124.167.231
211.110.140
1.93.32
103.21.141
203.69.37
192.188.51
178.62.252
37.46.197
112.78.3
58.215.172
134.255.231
210.14.157
202.117.2
68.195.197
81.149.31
125.22.2
122.192.35
Percent overlap between dictionaries (0-100)
Num. passwords
10^6
10^5
10^4
10^3
10^2
10^1
10^0
IPs per subnet
Number of passwords
70
60
50
40
30
20
10
1
Num. IPs

Usernames+Passwords

- 98% of all guesses tried **`root`** or **`admin`**
- 37% of all sources never targeted **`root`** or **`admin`**
- 50% of non-root and non-admin usernames saw guesses with username=password
- 27% of usernames were only tried with a single password

(Re-)Guessing Passwords

- Odd behaviour: 1/3 of all sources tried the same username/password pair on the same VM more than once.

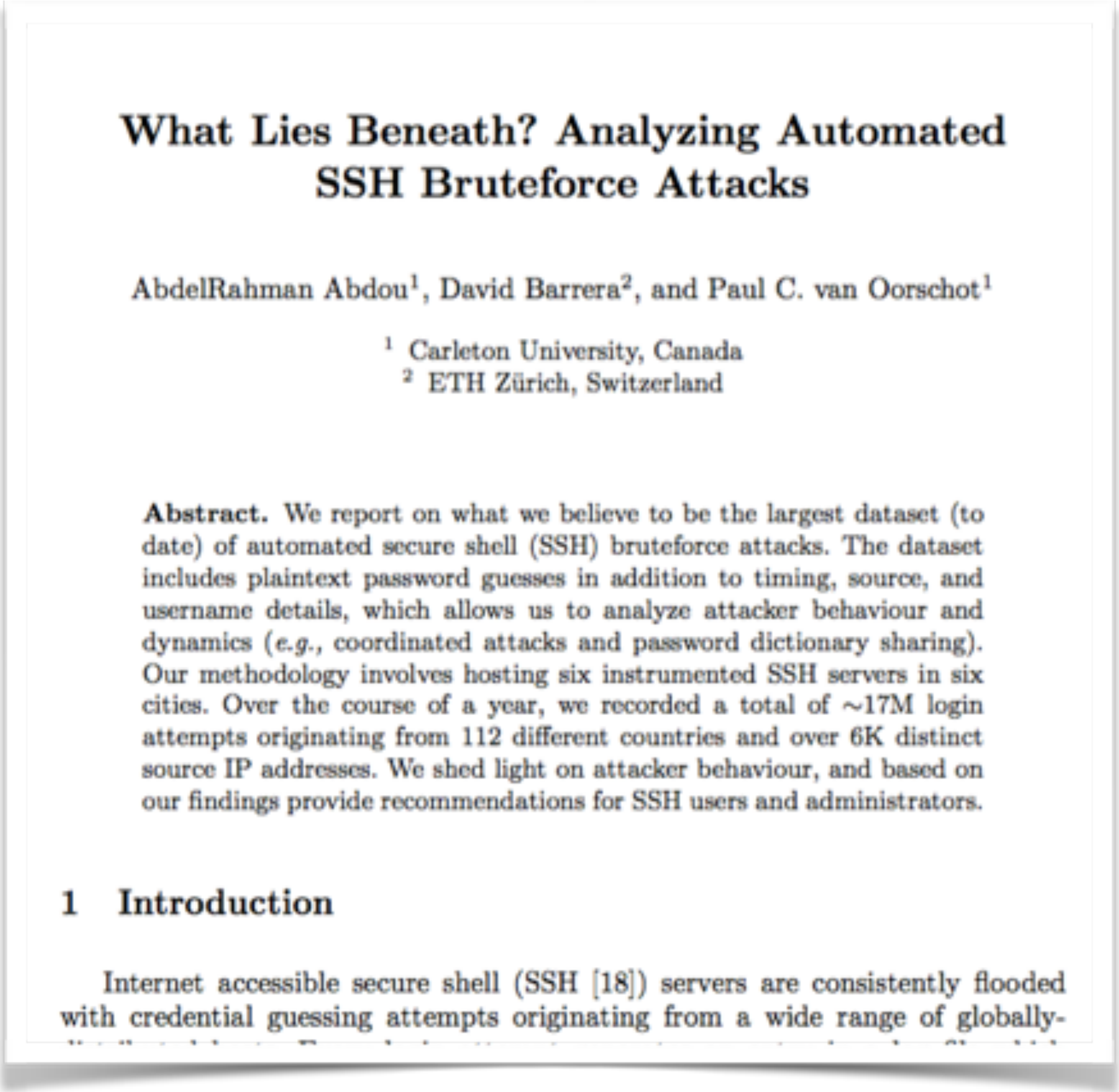
- 25% of all guesses (4.3M) were repeated guesses

- Time between repeats varies from <1s to 11 months

  - One source tried **`root:\\001`** 1220 times on the same VM in 19 minutes

For more details

- Username analysis
- Distribution of IPs per subnet
- IP addresses as a ratio of total IP allocation per country
- Changing SSH daemon to non-standard port
- Another heatmap
- Recommendations



What Lies Beneath? Analyzing Automated SSH Bruteforce Attacks

AbdelRahman Abdou[1], David Barrera[2], and Paul C. van Oorschot[1]

[1] Carleton University, Canada
[2] ETH Zürich, Switzerland

Abstract. We report on what we believe to be the largest dataset (to date) of automated secure shell (SSH) bruteforce attacks. The dataset includes plaintext password guesses in addition to timing, source, and username details, which allows us to analyze attacker behaviour and dynamics (*e.g.,* coordinated attacks and password dictionary sharing). Our methodology involves hosting six instrumented SSH servers in six cities. Over the course of a year, we recorded a total of ∼17M login attempts originating from 112 different countries and over 6K distinct source IP addresses. We shed light on attacker behaviour, and based on our findings provide recommendations for SSH users and administrators.

1 Introduction

Internet accessible secure shell (SSH [18]) servers are consistently flooded with credential guessing attempts originating from a wide range of globally-

Thank you

@davidbb
david.barrera@inf.ethz.ch
abdou@sce.carleton.ca