Universal mobile sniffer

Ideas and PoC
@ONsec_lab @d0znpp

DCG#7812, Saint-Petersburg, 27th March 2013

Sniffers: basics

- All that can listen are also can sniff
- Classic sniffers:
  - Wi-Fi (promisc. mode, injections)
  - Bluetooth (hi-jacking, abusing pairing)
  - Geolocation (GPS, wi-fi, GSM APs)
  - Camera (photo, video)
  - Microphone (sounds)

Sniffers: basics

- All that can listen are are can sniff
- Non-classic sniffers - **vibrations**:
  - Accelerometer
  - Gyroscope
  - Microphone (sound vibrations)
  - Camera's picture deviations to determine vibrations? (stabilization system problem)

Vibrations? WTF?

- Classic example:
  - count steps while walking
- Non-classic example:
  - count keystrokes (password length)
  - determine keys (password content)

What algo can be used?

- Statistical algo of course!
- Frequency statistic
  - long text
  - typing language
- Training procedure
  - attack scenario?

Is it possible? #1

- Lets watch at nice video!
- «Working iPhone 5 paper keyboard»
- Florian Krautli, University of London

Is it possible? #2

- Plaid CTF 2012
  - Traitor quest
  - Hard to solve but possible
  - Long text
  - Frequency analysis
  - http://int3pids.blogspot.ru/2012/05/plaidctf-2012-traitor-200-pts.html

What's new?

- Combine gyroscope and microphone as independent sources
- Suggests nice attack scenario to collect train set
- Some measurements to determine max possible distance between keyboard and phone to vibrosniff

Data from accelerometer and gyroscope

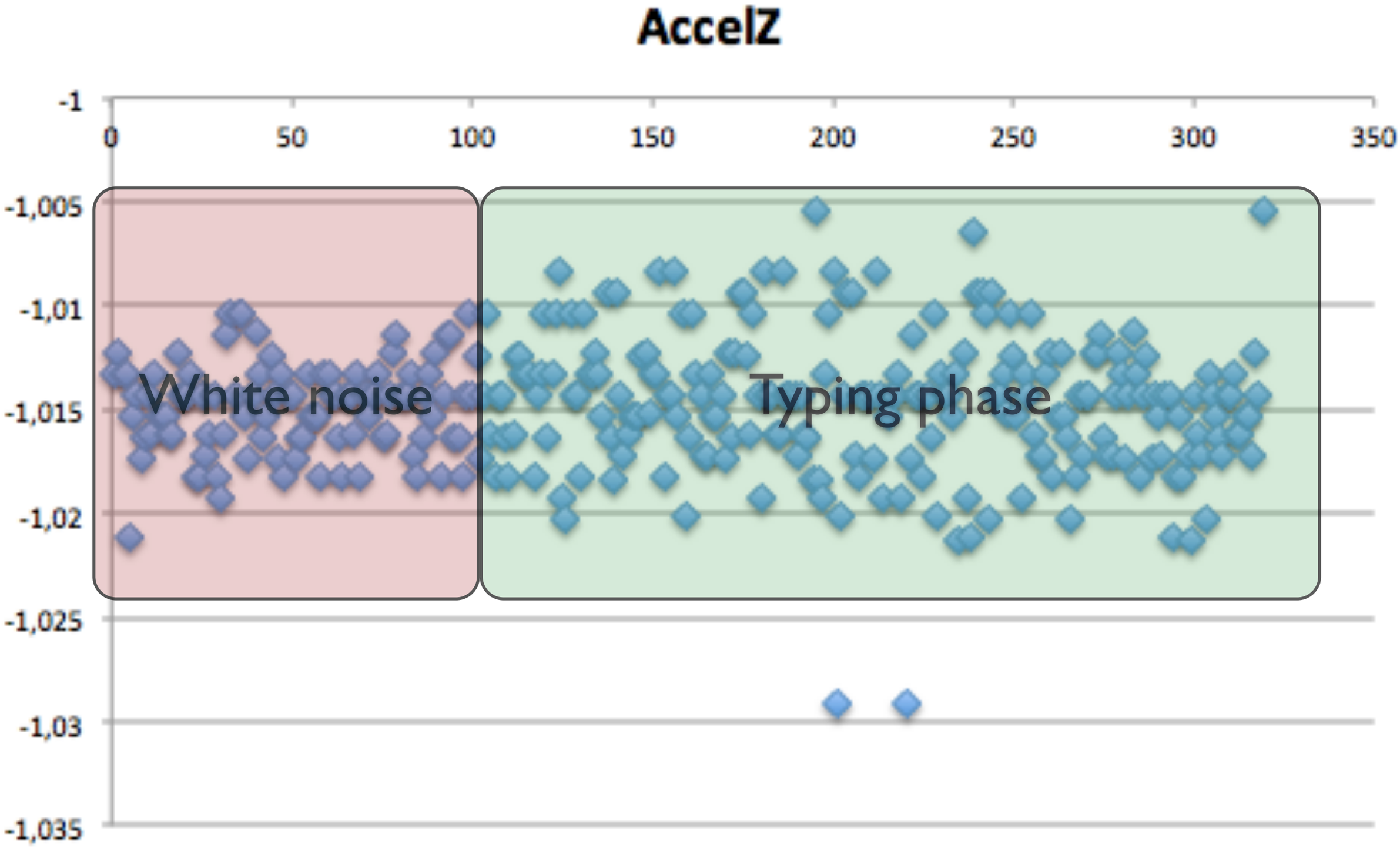
- Acceleration by axis: X, Y, Z
- Heading by axis: X, Y,Z
- Rotation by axis: X, Y,Z
- MotionYaw, MotionRoll, MotionPitch
- MotionRate by axis: X, Y,Z
- MotionUserAcceleration by axis: X, Y,Z

Measurements

- Simple way is using SensorLog for iOS
  - Free software
  - Log data to CSV, export via email

C	D	E	F	G	H	I	J	K
recordtime	acceleration	acceleration	acceleration	Heading	Heading	HeadingZ	RotationX	RotationY
0,05	-0,00821	0,01181	-1,01328	4,636	12,867	-56,63016	-0,007167365	-0,004892759
0,1	-0,00815	0,01474	-1,01233	4,797	12,598	-56,35013	-0,01442927	-0,001365935
0,15	-0,00912	0,013748	-1,01331	4,636	12,652	-57,19025	-0,004728709	-0,007272028
0,2	-0,01303	0,01268	-1,01335	4,475	12,706	-57,13422	-0,007183345	-9,11E-005
0,25	-0,011	0,013687	-1,02119	4,314	12,867	-57,41428	-0,01079938	-0,009725598
0,3	-0,00812	0,015717	-1,01527	4,475	11,74	-57,13419	-0,009487778	-0,007339672
0,35	-0,00919	0,010803	-1,01428	4,851	12,437	-56,63007	-0,01801149	-0,005011803
0,4	-0,01006	0,014679	-1,01729	4,744	12,545	-57,30215	-0,007088003	-0,008510131
0,45	-0,01097	0,016617	-1,01631	4,261	12,813	-57,69418	-0,009598299	-0,01211073
0,5	-0,00726	0,009857	-1,01424	3,939	12,491	-57,47015	-0,004703143	-0,007278153
0,55	-0,01016	0,009811	-1,01625	3,992	12,652	-56,96609	-0,00962493	-0,01090485
0,6	-0,01018	0,010788	-1,01331	4,207	12,867	-57,19012	-0,009598299	-0,01211073
0,65	-0,00916	0,011795	-1,01526	4,851	13,296	-57,75021	-0,0120026	-0,004941761
0,7	-0,00818	0,012772	-1,01526	4,69	13,028	-57,35818	-0,005962019	-0,0120761
0,75	-0,00916	0,011795	-1,01526	4,583	12,491	-56,91013	-0,009430519	0,001042095
0,8	-0,00917	0,010803	-1,01625	4,636	12,545	-57,30222	-0,01809591	-0,0109882
0,85	-0,00917	0,010803	-1,01625	4,583	12,92	-57,58221	-0,008377239	-0,007303453
0,9	-0,00922	0,009842	-1,0123	4,851	12,545	-57,63818	-0,01317439	-0,007362043
0,95	-0,00824	0,009842	-1,01425	5,173	12,223	-56,7421	-0,007127152	-0,007301323
1	-0,00819	0,01181	-1,01427	5,173	12,759	-56,74207	-0,01198795	-0,007344199
1,05	-0,0092	0,009827	-1,01427	4,261	13,564	-57,13409	-0,005938583	-0,009682721
1,1	-0,00917	0,011795	-1,01329	4,153	13,135	-56,57401	-0,01070564	-0,01574567
1,15	-0,01295	0,013657	-1,01828	4,583	12,92	-57,24606	-0,007187073	-0,01208463
1,2	-0,0081	0,014709	-1,01823	4,368	12,706	-57,24606	-0,01322339	-0,009748767
1,25	-0,01207	0,011734	-1,01431	4,529	12,545	-57,63809	-0,01070458	-0,01694543
1,3	-0,01108	0,011734	-1,01726	4,422	12,759	-57,30203	0,006162821	-0,002367018
1,35	-0,00914	0,011795	-1,01625	4,046	12,813	-57,35803	-0,005896771	-0,01449079

Measurements



Measurements

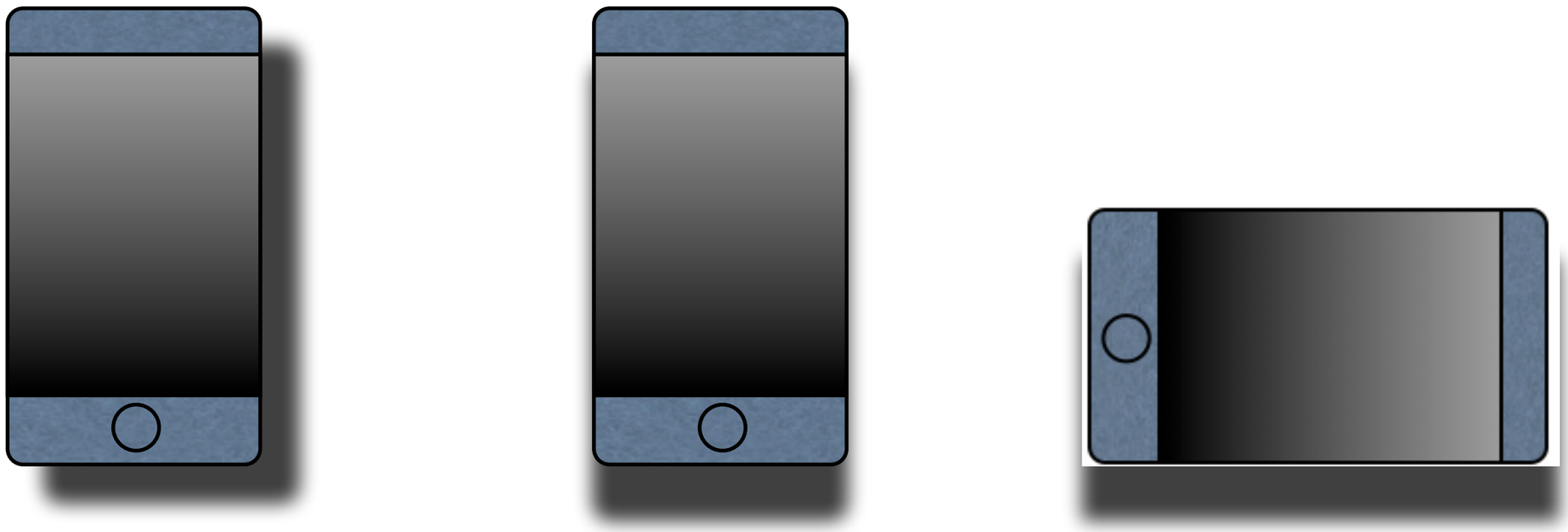
- Determination of possible distance between laptop and phone to sniff
  - Macbook Air
  - iPhone 4S
  - 0-20cm per each 5cm
  - Wooden table (made in USSR)

Measurements

- Determination of possible distance between laptop and phone to sniff
  - 0 cm with touching - OK
  - 0 cm w/o touching - OK
  - 5 cm - OK
  - 10 cm - OK
  - 15 cm - NO

Measurements

- Lets try to cheat!
- Increasing accuracy by rotation!
- Why? Backside from glass - amorphous
- Full-metal case is more sensitive



Measurements

- Determination of possible distance between laptop and phone to sniff
  - 5 cm - OK
  - 10 cm - OK
  - 15 cm - OK
  - 20 cm - OK
  - 25 cm - NO

w/o training set

- Determine character sets in password:
  - Upper cases: ~90%
  - Special chars: ~90%
- Password length: ~95%
- Password input fact determination: ~65%
  - After login input (second word criteria)
  - 6-12 bytes typically

w/o training set

- Example for password: asv^y%73tFYG
  - Sniffing results:
    - 12 bytes total
      - 1-3, 5, 7-9 bytes are a-z, 0-9 or .,-=/\][;’
      - 4, 6, 10, 11, 12 bytes are A-Z or spec.chars (with «Shift» key)
  - 92^12 basic entropy ~ 3.7*10^23
  - 46^12 after sniff ;) ~9*10^18

w/o training set

- Combine with wireless traffic sniffing
- Determine SSL sessions time
- Correct passwords input facts
- Combine with target service passwords policy

Attack scenario

- Place your phone to victim's table
- Send message to victim via Skype/Jabber
- Use victim's answer as training set ;)))

Conclusion

- It's possible
- Want to find enthusiasts for do it
- Contact us: @ONsec_lab, @d0znpp

- Questions?