SUMMARY FINDINGS FROM SINGAPORE'S FIRST PRIVACY SURVEY COVERING MOBILE APPLICATIONS - 2015

Objectives of Survey

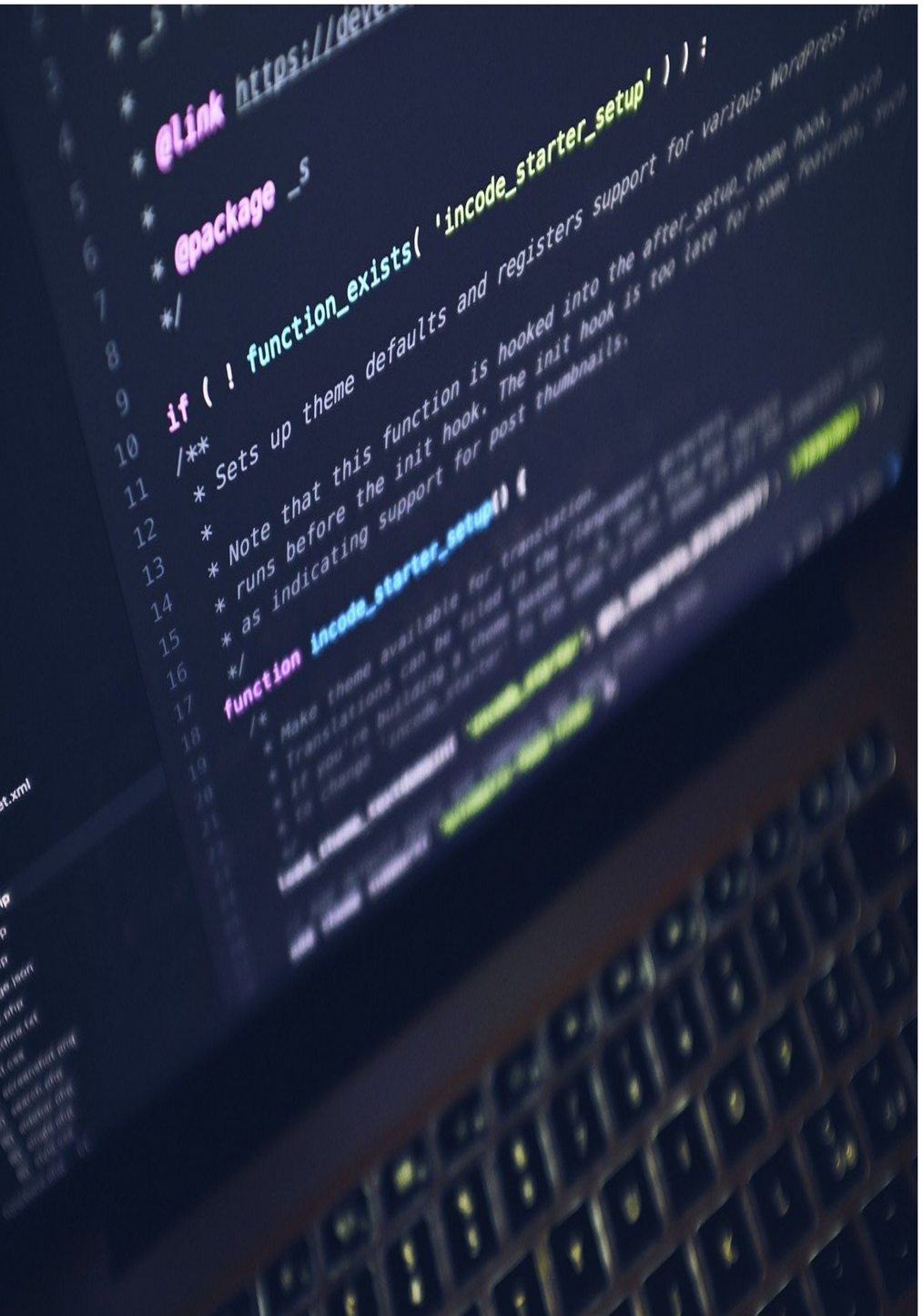
- Assess Data Protection / Privacy practices for mobile apps

- Scan mobile apps for privacy risks (conducted between. Aug – Sep 2015)

The survey is benchmarked against a similar survey done by the Global Privacy Enforcement Network (GPEN).

Results of the 2014 GPEN Privacy Sweep Global Trends and Canada (Office of Privacy Commission).

Source: https://www.priv.gc.ca/media/nr-c/2014/bg_140910_e.asp



Methodology

1) Assess Data Privacy Practices

1. Only Android Applications were chosen for consistency

2. Reference site: https://play.google.com/

3. Searched the most popular applications, as well as those representative of several categories

Methodology

4. In each search, the following were collated:
   - App/Company Name
   - Developer (Is it internal or outsourced, individual; app development company?)
   - Privacy policy (Does it cover mobile apps?)
   - Website
   - Review (indication of quality)

5. Analysis of 103 mobile applications plus 10 apps relating to financial advisors/real estate agents

2) Use of Scan technology from AppKnox
Analyzed APK binary file from play.google.com

Code Analysis

Code analysis covers basic coding practices, data flow and metrics which include OWASP configurations. The Open Web Application Security Project (OWASP) is an online community dedicated to web application security.

Attacker's Approach

Going a step further and using an attacker's approach to analyze mobile Network and Product's security.

Summary findings for mobile apps privacy practices

	GLOBAL APPS	OPC APPS	SG APPS
Total # apps examined	1211	151	103
Permissions (Indicator 2)			
Apps requesting ≥ 1 permissions	75%	70%	89%

Permission Requested	GLOBAL APPS	OPC APPS	SG APPS
Location	32%	22%	70%
Contacts	9%	10%	7%
Calendar	2%	2%	8%
Microphone	5%	7%	4%
Camera	10%	8%	29%

Permission Requested	GLOBAL APPS	OPC APPS	SG APPS
Device ID	16%	13%	52%
Access to other accounts	15%	23%	49%
SMS	4%	6%	12%
Call Log	7%	11%	2%

Privacy Communications	GLOBAL APPS	OPC APPS	SG APPS
Apps with concerns regarding pre-installation privacy communications	59%	42%	65%
Apps with excessive permission based on sweeper's understanding of app's functionality	31%	28%	58%
Apps with privacy communications not well tailored to small screen	43%	31%	Not Assessed

Overall Privacy Marks	GLOBAL APPS	OPC APPS	SG APPS
0 = No privacy information other than permissions	30%	11%	18%
1 = Privacy information not adequate; sweeper does not know how information will be collected, used and disclosed	24%	15%	55%

Overall Privacy Marks	GLOBAL APPS	OPC APPS	SG APPS
2 = Privacy information somewhat explains the app's collection, use and disclosure of personal information. However, sweeper still had questions about certain permissions	31%	46%	17%
3 = Privacy information clearly explains how app collects/uses/discloses personal information; sweeper is confident in his/her knowledge of app's practices	15%	28%	10%

Conclusion on Findings for Mobile Apps with Privacy/ Security Concerns

Top 3 privacy/security concerns

69% – Javascript-interface: This gives privilege to hacker to execute or run any code and perform unexpected results or action on behalf of the user remotely without even touching the device physically.

61% – Misconfiguration in SSL: This can lead to attacks which compromises user details. Simply means any hacker can intercept the internet connection. This can lead to Man in the middle attack.

52% – Poor Encryption: This can be misused to get access to user's personal data by hackers. Easily decrypted information is like keeping user's keys in open for any thief to steal their data.

Mobile application developers are advised to get their mobile apps scanned for privacy and security vulnerabilities.

High Risk Vulnerabilities	% of Overall Mobile Apps Grand Total
Broken Trust Mgr for SSL (High Risk)	61%
Broken Host Name Verifier for SSL	45%
Host name Verifier Allow All Host Names	31%
Remote code execution through Java Script Interface	69%
Insufficient Transport Layer Protection	28%
Derived Crypton Keys	52%
Appliction Log (Medium risks)	45%

To get the complete report and findings, as well as the individual security report of the mobile application covered, please contact sales@straitsinteractive.com.

Thank you

https://www.straitsinteractive.com

16 March 2020