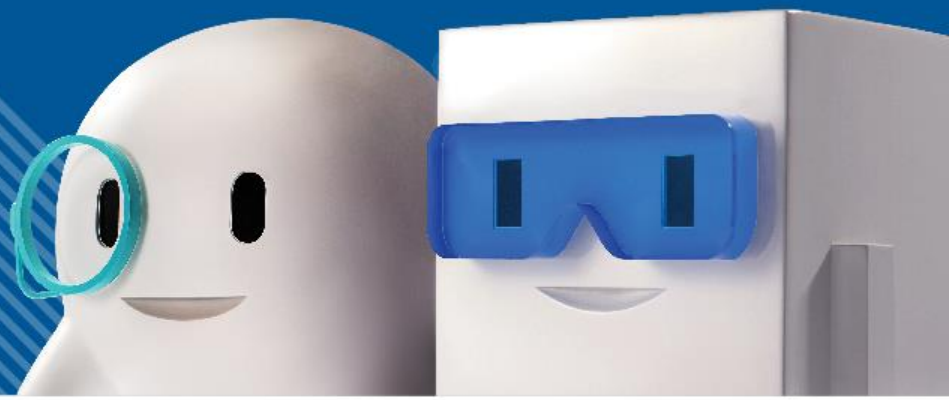
HKPC

HKCERT

Roland Cheung
Consultant, HKCERT

Security arrangement with mobile app development



All-round Productivity Partner
全方位企業伙伴

Agenda

- Introduction to HKCERT
- Security risks on mobile apps
- Security arrangements
  - 6 Highlights
- Conclusion

INTRODUCTION TO HKCERT

HKCERT 簡介

- Hong Kong
  Computer Emergency Response Team
  Coordination Centre
  香港電腦保安事故協調中心 (HKCERT)

- Established in 2001
- 100% funded by HK Gov
- Managed by HKPC

Introduction to HKCERT

- Services
  - Security Alerts & warnings
  - Incident handling & response
  - Publications & guidelines
  - Security awareness & education

- Coordination and collaboration with relevant parties on security preventive measures

Introduction to HKCERT

- Publications
  - Security Newsletter (monthly)
  - Google Play Store Apps Security Risk Report (monthly)
  - HK Security Watch Report (quarterly)
  - Botnet detection and cleanup
  - Security guidelines

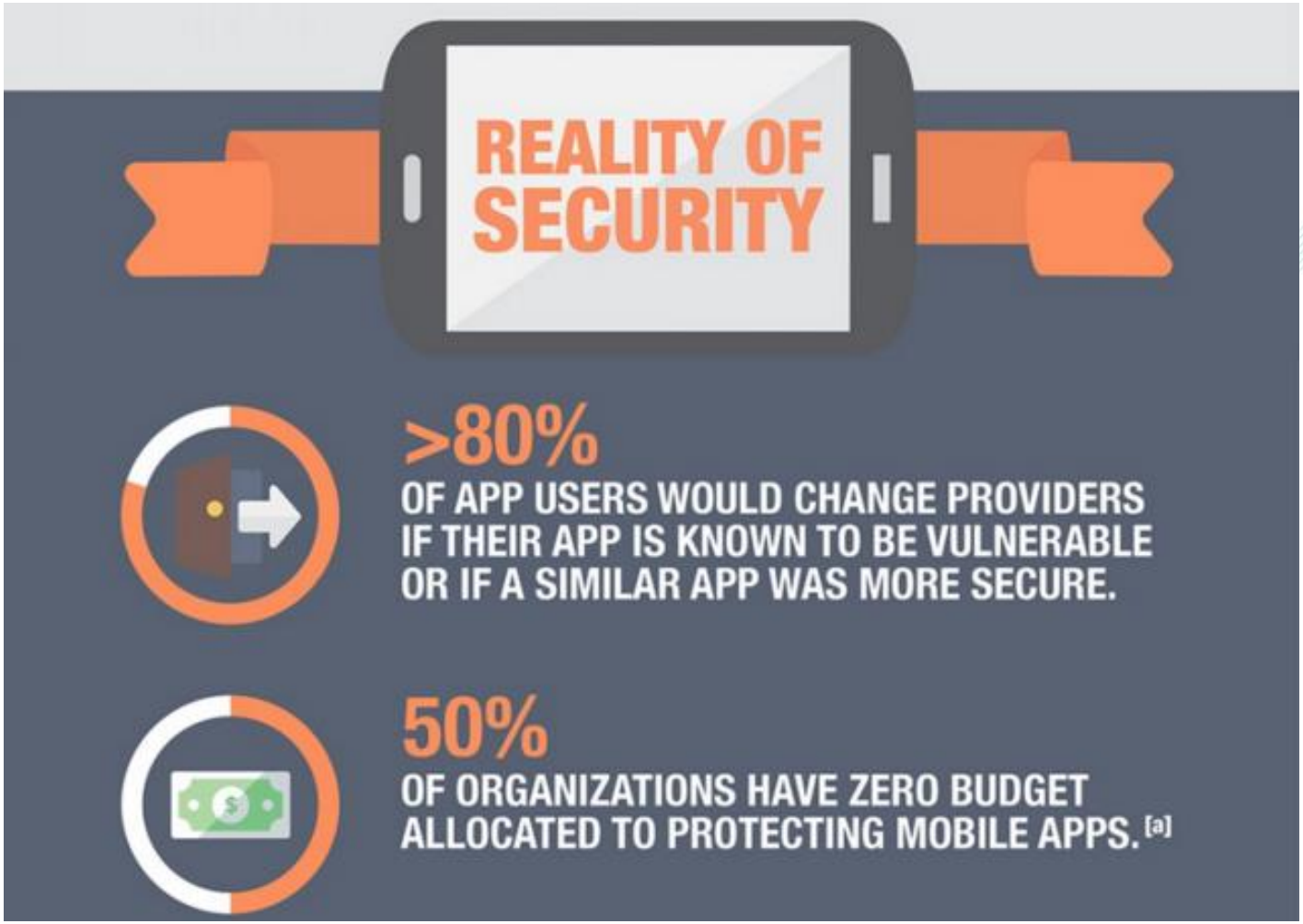
Security Alert Subscription

HKCERT Website : https://www.hkcert.org/

Subscription Page : https://www.hkcert.org/subscription

SECURITY RISKS ON MOBILE APPS

Security risks on mobile apps

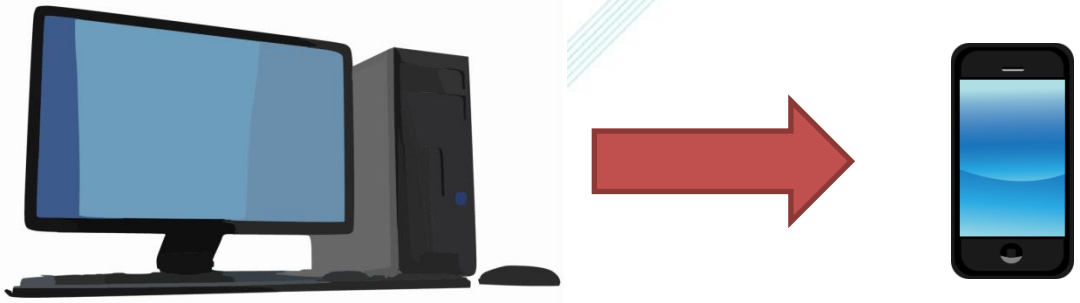


Source: http://betanews.com/2016/01/12/apps-are-far-less-secure-than-you-imagine/

Security risks on mobile apps

- Security risks
  - From Web security to Mobile ?

    The answer is NO
  - Mobile security is much more than traditional web application security
    - Identify insecure client-side vulnerabilities + traditional server-side vulnerabilities



Security risks on mobile apps

- There are several Top 10 mobile security risks
  - **OWASP** Mobile Top 10 

  - **Veracode** Mobile App Top 10 List 

  - **Cigital** Top 10 mobile risks 

Security risks on mobile apps

OWASP Mobile Security Top 10 2015

M1: Improper Platform Usage
M2: Insecure Data
M3: Insecure Communication
M4: Insecure Authentication
M5: Insufficient Cryptography
M6: Insecure Authorization
M7: Client Code Quality Issues
M8: Code Tampering
M9: Reverse Engineering
M10: Extraneous Functionality

https://goo.gl/UWXitO

Top 10 mobile risks

1. Weak server-side controls
2. Insecure data storage
3. Insufficient transport layer protection
4. Unintended data leakage
5. Poor authorization and authentication
6. Broken cryptography
7. Client-side injection
8. Security decisions via untrusted inputs
9. Improper session handling
10. Lack of binary protections

https://goo.gl/EGulkP

Security risks on mobile apps

- We have to consider the risks, but
  - Most developer are not trained to develop secure application
  - Most developers are new to creating mobile application

https://buildsecurityin.us-cert.gov/sites/default/files/DanCornell-MobileAppSecOverview.pdf

Security risks on mobile apps

DENIM GROUP

- Guidance for Developers
  - Overview of Application Development
  - Overview of Secure Development
  - Defeating Platform Environment Restrictions
  - Installing Applications
  - Application Permissions Model
  - Local Storage
  - Encryption APIs
  - Network Communications
  - Protecting Network Communications
  - Native Code Execution
  - Application Licensing and Payments
  - Browser URL Handling

http://www.denimgroup.com/media/pdfs/MobileDevReference.pdf

Security risks on mobile apps

- Summary of Guidance for Developers

1. **Understanding mobile platforms (e.g. iOS vs Android)**

– Development APIs and Security framework
– Application permissions model
– Bypassing way? Jailbroken / rooted device




Security risks on mobile apps

- Summary of Guidance for Developers

2. **Local Storage**

  - File system
    - e.g. Any data write on external storage (Android)?
  - Data management and data storage
    - Shared data? Protected data?
    - e.g. Can sensitive data stored in Property List *plist* (iOS) or *SharedPreferences* (Android)?
    - e.g. How sensitive data stored in storage or SQLite

Security risks on mobile apps

- Summary of Guidance for Developers

3. Encryption APIs

- Native device vs. 3rd parties encryption libraries
- Certificate, Key and Trust services
- For more detail:
  - (iOS) ***CryptoExercise***
    https://developer.apple.com/library/ios/samplecode/CryptoExercise/Introduction/Intro.html
  - (Android) ***javax.crypto***
    http://developer.android.com/reference/javax/crypto/package-summary.html

Security risks on mobile apps

- Summary of Guidance for Developers

4. **Protecting Network Communications**

  - SSL sockets / HTTPS requests required
  - For more detail:
    - (iOS) ***Secure Transport***
      https://developer.apple.com/library/ios/documentation/Security/Reference/secureTransportRef/index.html
    - (Android) ***android.net.SSLCertificatSocketFactory***
      http://developer.android.com/reference/android/net/SSLCertificateSocketFactory.html

Security risks on mobile apps

- Summary of Guidance for Developers

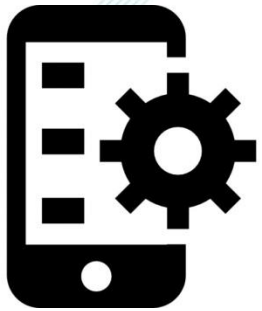
5. Mobile Browser / WebView

– Application run on WebView (WebApp)
– Does the Framework secure?
– What browser (WebKit) run on mobile platform?
– Any vulnerabilities exist?

Security risks on mobile apps

- Summary of Guidance for Developers

6. URI protocol handling



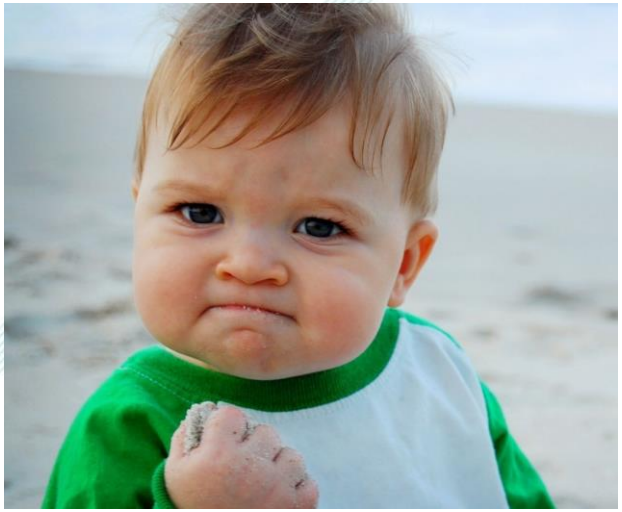
– Allow external app to call your app?
– Any parameters?
– Does your app filter and handle it well?

Conclusion

Image: http://searchfactory.com.au/

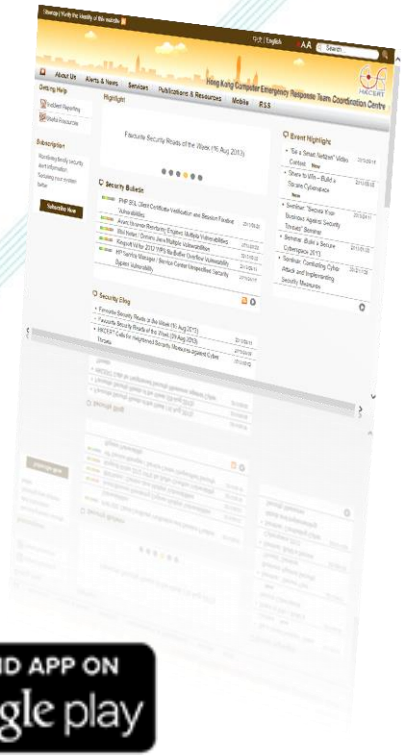
Conclusion

- I believe that there is **NO 100% bug free** application
  - Security review
  - Security assessment
  - Patch management
- Be a responsible developer



HKCERT Channels

- Security Alert
  - https://www.hkcert.org/security-bulletin
- Security Guidelines
  - https://www.hkcert.org/security-guideline
- Security Tools
  - https://www.hkcert.org/security-tools
- HKCERT Mobile App
  - Search：HKCERT



Available on the App Store

ANDROID APP ON Google play

Security Alert Subscription

Thank you

HKCERT

www.hkcert.org