DIMITRIS GLYNOS (@dfunc) / dimitris @ census-labs.com
MOBILE APPS PANORAMA 2016

WELCOME TO THE JUNGLE (OF MOBILE APPS)

CENSUS
IT Security Works

ABOUT CENSUS S.A.

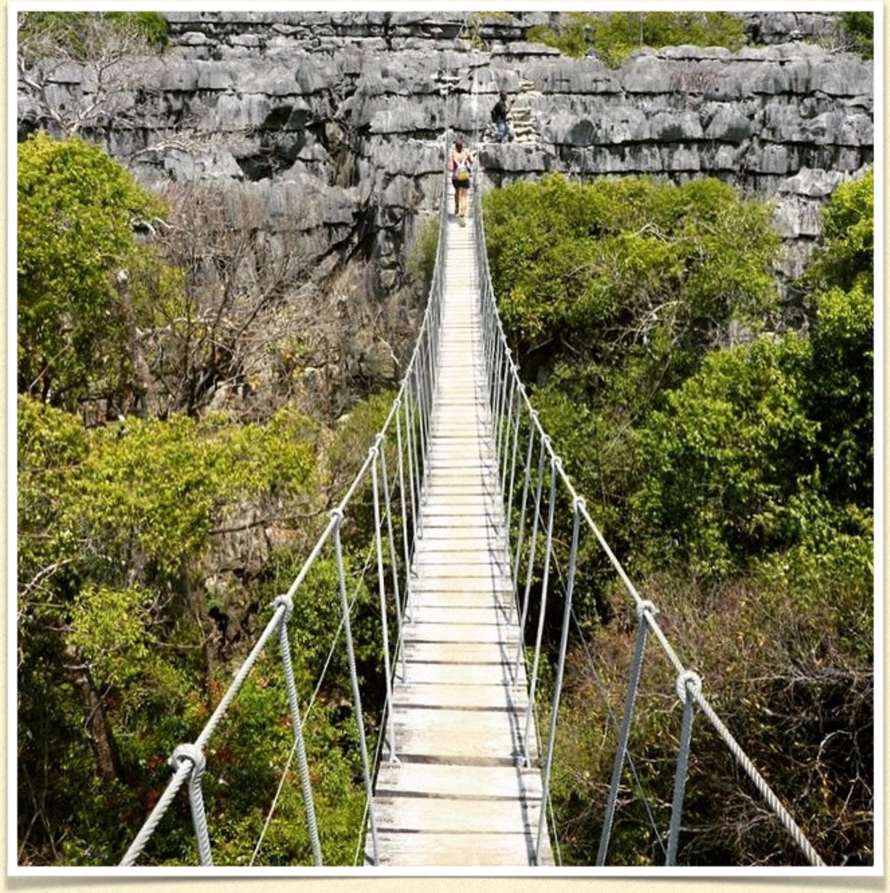
- We deliver security assessment services to customers worldwide
  - Including Mobile App Assessments for all major platforms
- We build on heavy-duty IT security research. Recent Android highlights include:
  - Five Android 6.x “stagefright" vulnerabilities (2016)
  - Multiple Android 5.x ART optimisation vulnerabilities (Hack-in-the-box Amsterdam 2015)
  - Android support for Google’s “honggfuzz” fuzzer (2015)
  - Many recent exploits for Android are based on our “jemalloc” exploitation work (Black Hat USA 2012)

WHERE THE WILD THINGS ARE (PART 1)

- Vulnerabilities in the App stack
  - App vulnerabilities
  - Framework / Third Party Component vulnerabilities
  - Platform vulnerabilities

WHERE THE WILD THINGS ARE (PART 2)

- Vulnerabilities in external services
  - Mobile Gateway / Web API vulnerabilities
  - Third party service (e.g. maps, app tracing etc.) vulnerabilities



THE WILD KINGDOM

Remote Attacker

- May perform attacks on the Web API
- May perform local attacks through malware
- May perform attacks requiring a specific position (man-in-the-middle, NFC etc.)

Thief

- Has physical access to the device for an extended period of time
- May collect unprotected (unencrypted) data from the device storage and memory
- May perform impersonation attacks

Valid User

- Has physical access to the device and rightful access to the app services
- May reverse engineer the app
- May run a modified version of the app

Third Party Service Provider

- May create a denial of service condition to the app
- May receive sensitive information from the app
- May sometimes be able to inject data / code to the app

EXAMPLE #1: A REMOTE ATTACKER THREAT

- Banking App allows overlays from other apps and uses SMS authorization (mTAN)
  - The ZitMo (2010) and Android.SpyAgent.SI (2016) malware target such mobile banking apps
  - They capture and forward all information needed to perform a successful bank transaction
    - user credentials
    - SMS token
  - NIST no longer recommends two factor authentication via SMS
  - Field experts can help in the quick identification and mitigation of such issues

EXAMPLE #2: A THIEF THREAT

- App framework uses the wrong API during TouchID authentication
  - An iOS mobile banking app uses the above framework to authenticate users
  - A thief could have exploited the above flaw to bypass authentication
  - An in-depth analysis of the application is required to identify such threats

EXAMPLE #3: A VALID USER THREAT

- A Game App performs business-critical actions on the device but employs no integrity protections
  - Users could modify and install an ad-free and/or cheating-friendly version of the game
  - This type of security issue is introduced at the *design* phase
  - If important logic must enter the app code then integrity protections must be applied

CHALLENGES IN HANDLING THREATS

- No time (“Traction now, security later!”)
  - Fixing a security issue after release comes with an increased cost / impact
- No budget (“Our clients don't mind!”)
  - Quality is the definitive attribute of leaders in competitive markets
- No expertise (“Is this really a threat?”)
  - Gain the needed insight through Security Consultancy services

SECURE SDLC

- Incorporates security checks by experts in all phases of the SDLC
- Early identification and mitigation of security risks
- Minimizes the security-related costs of projects

THANK YOU!

- Photo Material
  - *Slide 1 photo by Jon Olav Eikenes (Flickr ID "jonolave")*
  - *Slide 3 photo by "eclecctica" (Flickr ID "ecclectica")*
  - *Slide 4 photo by "frontierofficial" (Flickr ID "44634455@N08")*
  - *Slide 5 monkey photo by Steve Wilson (Flickr ID "pokerbrit")*
  - *Slide 5 hippopotamus photo by "oliver.dodd" (Flickr ID "oliverdodd")*
  - *Slide 5 lion photo by Angela N. (Flickr ID "aon")*
  - *Slide 5 eagle photo by Sinisa Djordje Majetic (Flickr ID "sinisadjordjemajetic")*

Follow us on Twitter!
@census_labs

CENSUS
IT Security Works