Estudi del tapjacking
en Android

Autor: Alejandro García Rodríguez
Consultor: Carlos Ares Angulo

Estudi del *tapjacking* en Android

- Objectius del projecte
  - Anàlisi d'una vulnerabilitat : el *tapjacking* en Android
    - Quin és el seu origen.
    - El seu funcionament
    - La solució proposada per Google
  - Presentació d'una prova de concepte
    - Prova de concepte en forma d'aplicació: ANDROID HUNT
  - Desenvolupar una solució alternativa
    - Estudi de la plataforma Android
    - Posible solució en forma d'aplicació: MIST

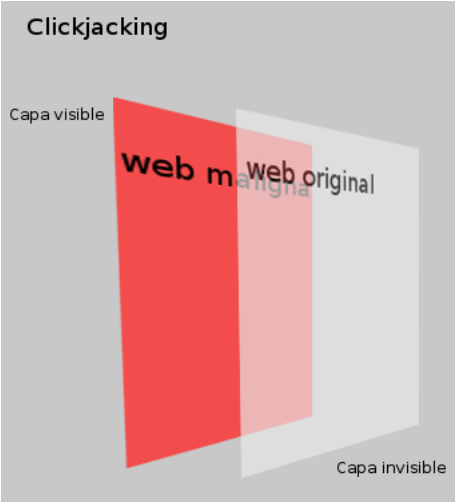
Estudi del *tapjacking* en Android

- Origen del *tapjacking*
  - *Clickjacking* a Internet
    - Conegut com a "segrest de clic"
    - Presentat per Jeremiah Grossman i

    Robert Hansen l'any 2008
  - ¿Com actua?
    - Dues capes:
      - Un capa visible i opaca vista per l'usuari.

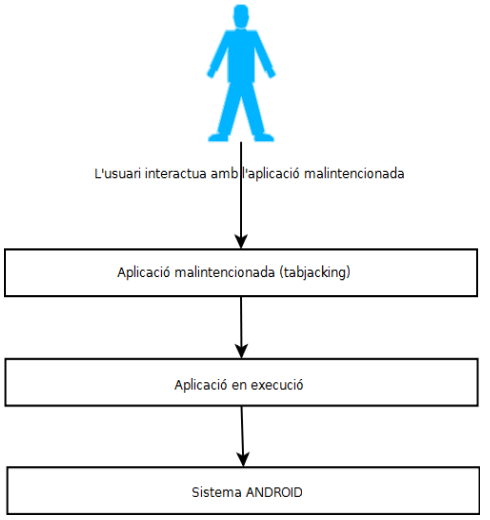
      Acostuma a ser un *iframe.*
      - Una capa invisible que es troba per sota de la capa visible.

      Aquesta capa rebria tots els events (pulsacions, clics, etc..) fets en la capa visible.



Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android
  - Es coneix com *tapjacking*
  - Afecta a les versions **1.5, 1.6, 2.0/2.1 i 2.2 de Android**
  - ¿Perquè aquesta tècnica?
    - Evitar el sistema de permisos d'Android.
    - Executar



Estudi del *tapjacking* en Android

- Anàlisi del *Tapjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- Solució proposada per Google
  - Google va solucionar el tapjacking poc abans d'alliberar la versió 2.3 GingerBread
  - Els desenvolupados poden fer servir:
    - Codi Java
      - setFilterTouchesWhenObscured(boolean)
    - Fitxer .xml
      - <elementGrafic android:filterTouchesWhenObscured="true" />

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android

Estudi del *tapjacking* en Android

- *Clickjacking* a la plataforma Android