Android Executable Files Injection & Data Protection

Android 執行檔注入與資料防護

thinker.li@gmail.com
http://www.codemud.net/~thinker/GinGin_CGI

Who Am I?

A programmer that develops free software

- 從事自由軟體創作的程式設計師
- 誼智科技 Allwitz.com
- 專注於工具的開發 Concentrate on tool developing

主題 Topic

Android executable files injection

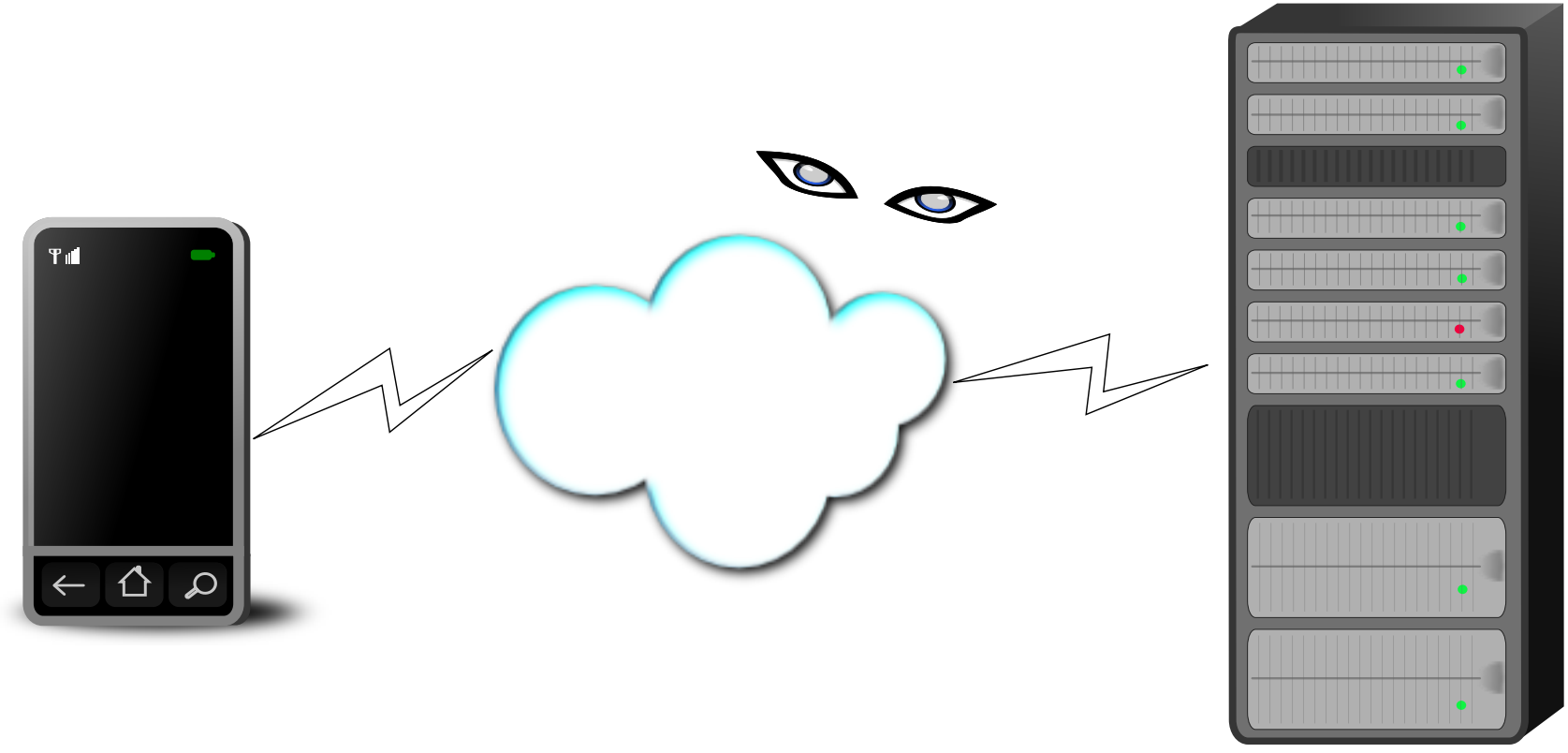
- **Android 執行檔注入**

- **資料防護** Data Protection

今日企業 Business nowadays

Mobile Service Deployment

佈置 mobile service



Malware

There is NO 100% safe system

沒有完全安全的系統

Android 也不例外

Android is no exception

Device 的安全 Device Security

企業難以控制 Corporations have difficulty of controlling

- 軟體的安全 Software Security
- 硬體周邊的安全 Hardware Peripheral Security
- 使用者的意圖 User's Intention

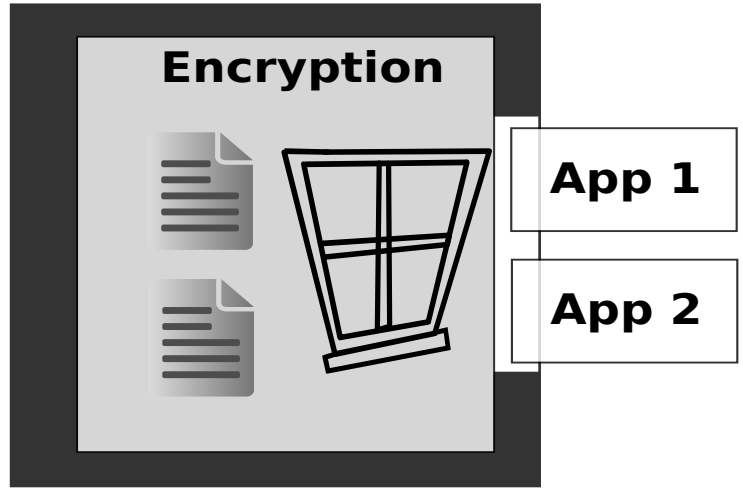
Android 的 storage 加密

Can prevent data leakage caused by losing

- 能防止移失造成的資料外洩

But unable to prevent from

- 防止不了 **Malware**
  - **root**
  - **SD card**
  - **...**



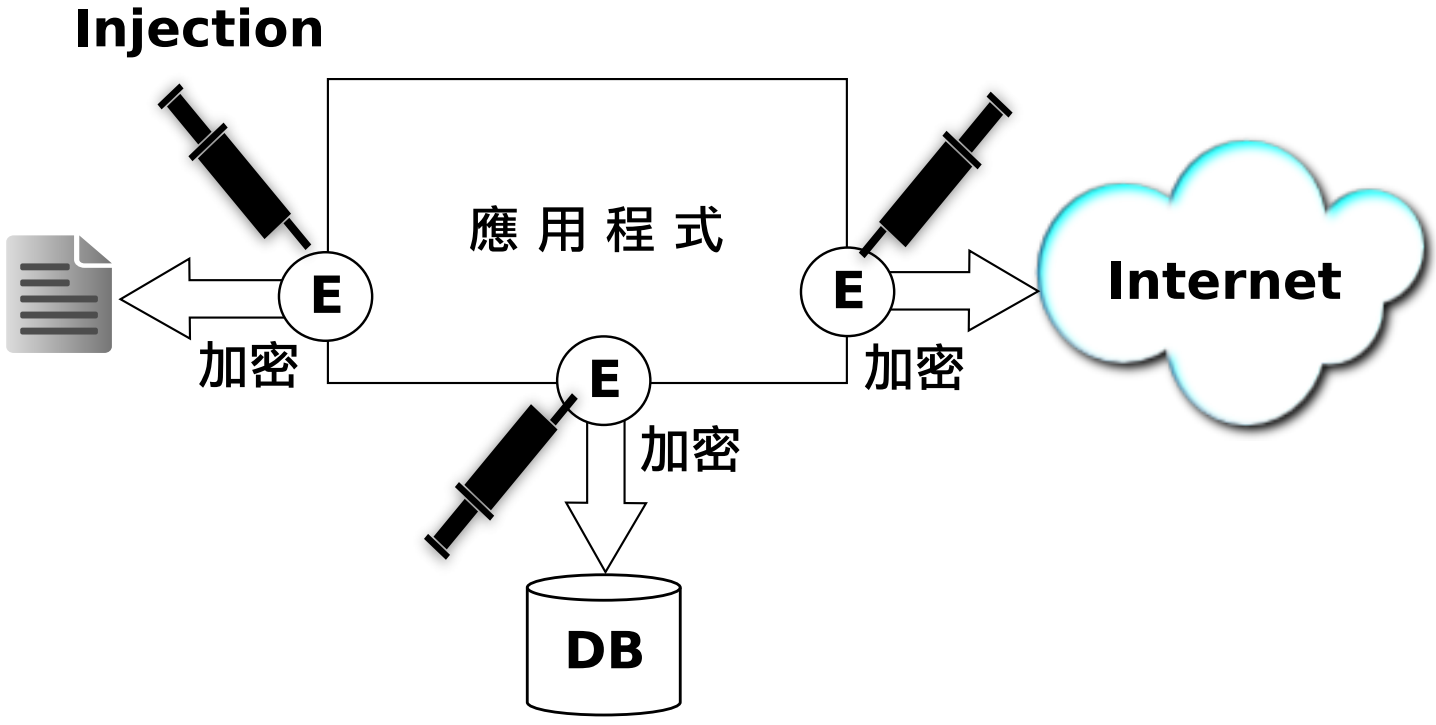
隔離企業資料 Quarantine Business Data

- 獨立的加密 Independent Encryption
- 限定程式讀取 Limited Program Access

客製化的應用程式 Customized Applications

- 成本 Cost
- 不易取得 Difficult to obtain

程式碼注入的途徑 Code injection paths



Android 執行檔

- DEX
- Bytecode

執行檔格式 (format)

$(ANDROID_TOP)/

dalvik/libdex/DexFile.h

Header

T.B.D.

Class List

T.B.D.

String List

T.B.D.

Redirect Method/Function Calls

T.B.D.

Add/Inject New Classe

T.B.D.

Working On

T.B.D.

Example Code

T.B.D.

Contact Me

- thinker.li@gmail.com
- http://www.codemud.net/~thinker/GinGin_CGI.py