

## Android 執行檔注入與資料防護

thinker.li@gmail.com  
[http://www.codemud.net/~thinker/GinGin\\_CGI](http://www.codemud.net/~thinker/GinGin_CGI)

## Who Am I?

- 從事自由軟體創作的程式設計師
- 誼智科技
- 專注於工具的開發

## 主題

- **Android** 執行檔注入
- 資料防護

## 今日企業

佈置 **mobile service**



## Malware

沒有完全安全的系統

**Android** 也不例外

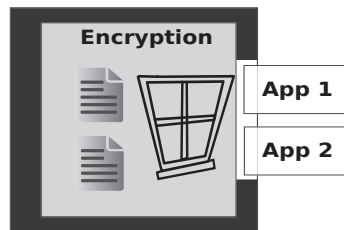
## Device 的安全

企業難以控制

- 軟體的安全
- 硬體周邊的安全
- 使用者的意圖

## Android 的 storage 加密

- 能防止移失造成的資料外洩
- 防止不了 **Malware**
- **root**
- **SD card**
- ...



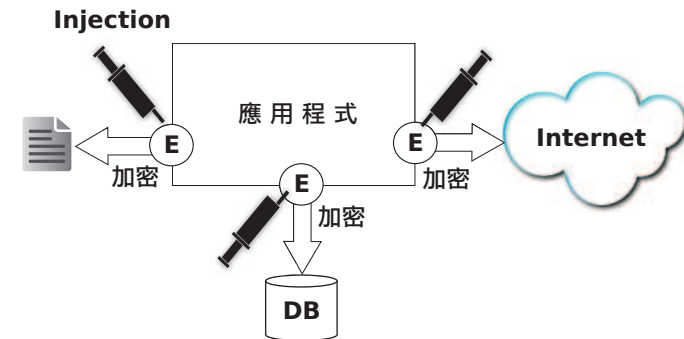
## 隔離企業資料

- 獨立的加密
- 限定程式讀取

## 客製化的應用程式

- 成本
- 不易取得

## 程式碼注入的途徑



## 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](mailto:thinker.li@gmail.com)
- [http://www.codemud.net/~thinker/GinGin\\_CGI.py](http://www.codemud.net/~thinker/GinGin_CGI.py)