1. **Abstract**

Riassunto in poche righe di tutto ciò che segue

1. **Introduction**
   1. **Sensitive data** (non mi piace questo titolo)

Mobile apps and social networks are now part of our daily life and we often record on them sensitive and private data bla bla bla

Mobile apps are used for a variety of applications, from accessing services, communication chats, navigation, banking and economic transactions, …. Bba bla bla

Checking the robustness and data protection is therefore mandatory bla bla bla

* 1. **Goals**

Goal of the study in this thesis is checking if software features expose it to the risk of providing more information than planned ….

The study was conducted by examining case studies on Android bla bla bla devices and analyzing different mobile apps belonging to three area of interests

* General apps without user authentication
* Apps with authentication, apps that manage geographical information have been specifically studied
* IM appa (solo se facciamo Fb)
  1. **Methodologies**

Apps have been investigated starting from an analysis of the network traffic and then passing, where necessary, to an examination of the code …. estendere

* 1. **Collaboration with IPS**

Questa ci vuole, andrebbe

Semplicemente ringraziato o

elencati possibili risvolti per il nostro mercato o i nostri prodotti

da ripensare

1. **Fundamental**

Qui mettere un breve descrizione di tutti gli argomenti teorici che ritieni di dove “precisare” prima di affrontare il lavoro vero e proprio. Se lungo separare in sotto-paragrafi

SSL

App decoding

Unpin

…….

1. **Testing environment**

Descrivere versioni specifiche dei telefoni

Emulatori

Strumenti e tool utilizzati

1. **Use Case METEO.it**

(potrebbero tutti far parte di un unico paragrafo ?? decidere)

* 1. **General description**

Cosa fa, come comunica, come lavora l’app ……

* 1. **Study detail**

Descrizione di cosa hai dovuto fare esempio

- non funzionava toolkit passato a Burp

- ho dovuto decompilare

- è stato ritenuto utile / necessario provare l’app in stati differenti

- necessario unpint

….

* 1. **Sensitive data**

Dati sensibili rilevati.

Essere precisi, usare tabelle riepilogative

* 1. **Other vulnerabilities**

Es the app is vulnerable to impersonation attempts because the reuse of the header ....

1. **Use Case Pacer**
2. **Use Case Waze**
3. **Use case ……..**
4. **Conclusion**

Questo è importante . E’ quello che insieme ad Abstract (e forse Introduction) si leggeranno il 90% delle persone a cui capiterà la tua tesi. Una volta redatto riporta i concetti ed i risultati base anche nell’abstact

The studied apps are obviously a minority in the vast world of mobile applications, but the study demonstrated how, even commonly used software, can be exposed to attacks and consequently detect sensitive information bla bla bla

The identified vulnerabilities and personal data can be categorized into THREE major macro topics:

* Exposure of personal data of the APP user

Despite the widespread use of TLS, sensitive data encodings and transmissions are detectable within it …

Mettere tabella chiara in cui per ciascun app si chiariscono i termini dell’esposizione

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | TLS | Certificate  Pinning | Comm  Protocol | attackable with MITM ?? |  |  |
| Meteo.it | Yes |  |  |  |  |  |
| Pacer |  |  |  |  |  |  |
|  |  | Yes | Protobuf |  |  |  |

It should be noted that together with the strictly personal data of the user (id, username, email, photo, ..) it was sometimes possible to trace information on contacts (agenda) bla bla bla

* Behavior monitoring

The study, in particular of Waze, revealed the possibility of tracing third parties in the neighborhood and therefore potentially creating a map of users that over time approach a specific location.

Geofencing applications (tracing of the user during the tasting) and behavior analysis (e.g. frequency of access to roads, toll booths, shops) could be imagined.

* Impersonation

The most serious vulnerability was the possibility, for an attacker, to act on behalf of a victim user and ...