

UNIVERSITÀ TOR VERGATA

CORSO DI LAUREA DI INGEGNERIA INFORMATICA

A.A. 2016-2017

Mobile Sniffing Tool

Progetto di Sicurezza Informatica e Internet

Autori:

Paolo SALOMÉ

Stefano AGOSTINI

Supervisori:

Prof. Giuseppe ITALIANO

Dr. Marco QUERINI

January 11, 2017

Contents

1	Introduzione	2
2	Descrizione dell'Applicazione	2
2.1	Tcpdump	2
2.2	Struttura APK	4
2.2.1	Subsubsection 1	4
3	Conclusion	6

1 Introduzione

Nella società odierna vi é un larga diffusione di applicazioni mobile di messaggistica che espongono implicitamente gli utenti a problematiche riguardanti la privacy. Infatti fino a qualche mese fa i dati in transito di Whatsapp (e.g.) erano in chiaro e quindi accedibili facilmente da chiunque utilizzasse una qualsiasi applicazione per lo sniffing (e.g. Whireshark). Tuttavia attualmente molte delle applicazioni di messaggistica hanno rimediato interamente o parzialmente utilizzando tecniche di crittografia end-to-end. L'obiettivo del nostro progetto é la realizzazione di una applicazione per sistemi mobile Android che all'interno di una certa rete wifi catturi i dati in transito e li filtri in base ad un flag. In tal modo ci preponiamo l'obiettivo di isolare i pacchetti dati per ogni applicazione di messaggistica presa in considerazione e analizzarli.

2 Descrizione dell'Applicazione

Per realizzare uno *sniffer Android* c'erano due strade alternative da poter seguire: sfruttare le *Android VPN* oppure utilizzare l'eseguibile *C tcpdump*. L'approccio *Android VPN* consiste nella creazione di un'interfaccia *VPNService*, gestita da una applicazione in *userspace*, che una volta attivata forza tutto il traffico del *device* ad attraversarla. Tuttavia questo approccio non permette la cattura di pacchetti appartenenti a dispositivi diversi da quello ospitante l'applicazione. Per utilizzare il secondo approccio é necessario che il dispositivo abbia i permessi di *root* in quanto verrà eseguito uno *script bash tcpdump*, il quale si occuperá di catturare i pacchetti. Inoltre questa libreria permette di sfruttare la scheda di rete in uso in varie modalità (e.g. *promiscuous mode*, *monitor mode*) qualora il dispositivo lo consenta. La possibilità di sfruttare a pieno le potenzialità della scheda di rete ci ha indotto a scegliere *tcpdump*.

2.1 Tcpdump

Il comando *bash* dell'eseguibile *tcpdump* permette l'inserimento di alcuni parametri che permettono la visualizzazione dei pacchetti in vari formati. Nel caso della nostra applicazione utilizziamo i seguenti parametri:

- **-i** : seguito dal nome dell'interfaccia, per specificare dove porsi in ascolto (e.g. wlan0)
- **-XX** in alternativa a **-A**: il primo stampa l'header di ogni pacchetto e i dati in esadecimale e *ASCII* mentre il secondo non stampa l'esadecimale
- **-tttt**: stampa la data corrente davanti l'header di ogni pacchetto in formato *YYYY-MM-DD hh:mm:ss:dddddd*

Di seguito inseriamo un pacchetto di esempio stampato da bash come risultato del comando `sudo tcpdump -i wlan0 -XX -tttt` (figure 1) e del comando `sudo tcpdump -i wlan0 -A -tttt` (figure 2).

```
2017-01-11 17:22:59.118063 IP 192.168.1.107.42883 > 74.125.143.127.19305: UDP, length 122
0x0000: 001e e594 eb56 18f4 6ac1 f394 0800 4500 .....V..j.....E.
0x0010: 0096 1ec5 4000 4011 7f82 c0a8 016b 4a7d ....@.@.....kJ}
0x0020: 8f7f a783 4b69 0082 e2b6 906f 7a48 0392 ....Ki.....ozH...section
0x0030: d930 2a8d 9dfd bede 0002 1094 323e ccd9 .0*.....2>..
0x0040: 0000 493a 5b44 98d7 4469 b75a 9dcd e0c7 ..I:[D..Di.Z...
0x0050: 0c5f 5630 d811 794b e8c5 886d 671a 75ed ._V0..yK...mg.u.
0x0060: 1cf0 426a cccb 62fd ac76 67da bfe1 8ce6 ..Bj..b..vg....
0x0070: 136e bb7f 34a3 8380 a83a 2c52 f910 9029 .n..4.....:R...)
0x0080: 1513 f195 4a84 e9e8 a270 2162 7bad b473 ....J....p!b{..s
0x0090: c645 65ea dba6 930a 2149 7654 fe71 b4d3 .Ee.....!IVT.q..
0x00a0: 7b02 efe4 {...
```

Figure 1: Con opzione -XX

```
2017-01-11 17:35:03.273751 IP 192.168.1.107.42883 > 74.125.143.127.19305: UDP, length 1203
E....v@.@.....kJ}....Ki...@.d.....{IV.H....2.lM...q.9....      ;...-i_...|.UU5P.....=....
...a;<=.....$...-e.....f[V]K.<...-;VW-LiXd.@`_.....0....^N!?W...qb'...1J.....f0
.Mt..+/n[...g....Y.F....q.o.....l.../. ...^..2....F7....N<.7d.>.....}|...      c0.
....V.$5..m..U..~.6_..i,0
..D...T...;`.y.3.0.p[.....[*...+.....N5....V....l2.z.6..er0.LtE..S..=. ....R.7....
..C...L~K9./.....#.e.`.%8s...8a.oNc.\...70....8~...."..^L...b.%W...~.'.'0U3X.-...v`.. "-.-o
.Ch.f..lu.....jx.l.`..qP.&...3.....q.<...w...e...Z..q.....%n..U.R.Wl.#&y../
...*.0....v!B.....'<.->.....`.8....1s.o1Ha..|..".f.F.....T...[.....f5.....;.....
...].u.....}. ....K_b..6y.....4..%..).7V.:.....SF./^.....{"..GZ)..h.[B....g+.G.p..
```

Figure 2: Con opzione -A

2.2 Struttura APK

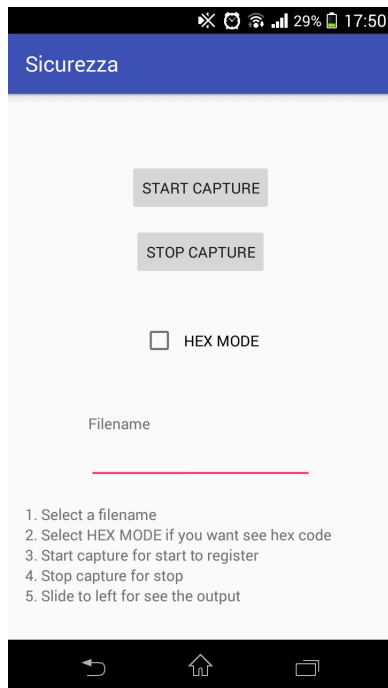
La nostra *APK* si compone di due *Activity* e due *Service*:

- L'*Activity* di cattura espone un'interfaccia semplice per impostare la modalità di cattura (specificare il *flag hex mode*). Successivamente l'utente può specificare il nome del file sul quale vuole che vengano salvati i pacchetti. Infine possibile attivare il servizio di cattura.
- L'*Activity* di filtraggio si occupa di fornire all'utente un elenco dei file contenenti i pacchetti, salvati dall'applicazione stessa nelle precedenti catture. Selezionato il file da elenco possibile inserire la parola chiave di ricerca. Mediante il servizio di filtraggio é vengono scanditi i pacchetti e visualizzati in una lista soltanto quelli contenenti la parola desiderata.
- Il *Service* di cattura si occupa dell'invocazione del comando *tcpdump* con le opzioni e il nome del file passati dall'*Activity* di cattura, redirezionando l'output su quest'ultimo. Quando questo servizio viene interrotto si esegue il comando bash *pkill tcpdump* per terminare il comando dello *sniffer*.
- Il *Service* di filtraggio agisce sul file selezionato esaminando ogni pacchetto e inserendolo in una lista visualizzata a schermo solo se contiene la *keyword* fornita, all'interno dell'*header* o del *body*.

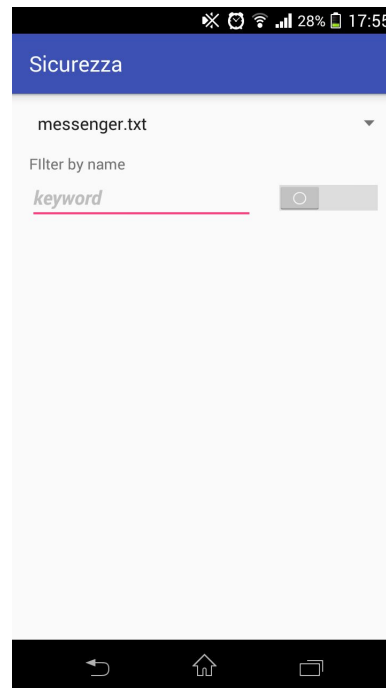
Di seguito inseriamo degli *screen* dell'applicazione appena descritta (figure 3).

2.2.1 Subsubsection 1

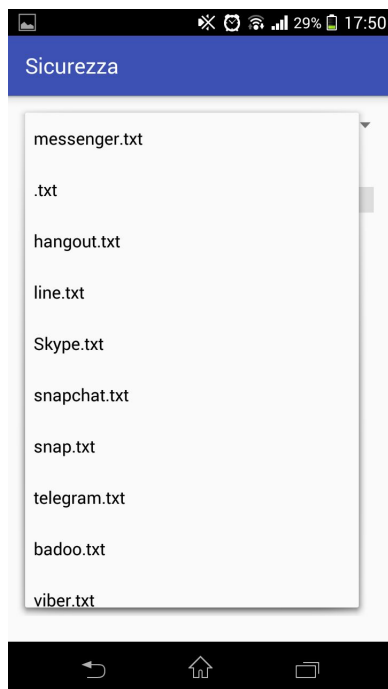
Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.



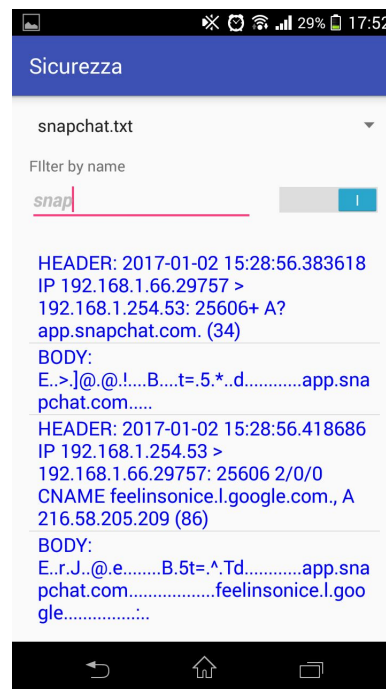
(a) Activity di cattura



(b) Activity di filtraggio



(c) Lista di file



(d) Pacchetti filtrati

Figure 3: Pagine dell'applicazione

3 Conclusion

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetur tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

References

- [Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.