URL Logger

Mobile http Request Tracking

Technical Document

MITCHELL ETZEL(PO), DARIUS SAKHAPOUR(SM), AUSTIN SHELTON, CEDRIC LINARES

Product Name:	URL Logger
Release Name:	Alpha
Release Date:	02/2/2017
Revision Number:	2
Revision Date:	02/2/2017

PRODUCED BY: CEDRIC LINARES

Why http requests/urls recovered without rooting or using a proxy on Android cannot be done:

What a 3rd party app can do without root access:

-Send requests to certain APIs and listen for a response. The response may contain data or nothing.

-Access people's location and media (photos, music, certain files on the phone[can see only if you have permission], ect.).

-Open another app. You cannot return back to the original app unless the user does it manually.

-Send/Recover data to/from a database

Why we need root access without a proxy

- A 3rd party application is unable to monitor the activity of another 3rd party app such as google.

-This is done for security reasons

-Secondly web based apps encrypt the https requests to prevent people from using packet sniffing

-However, there does exist an app that can sniff packets and decrypt them.

-Unfortunately to gain access to the saved packet log files we would need root access.

-Root access is an Android requirement to view 3rd party app data -Without root access, a simple user does not have the privileges to view that data.

-With considerable effort our team may be able to develop a packet sniffing application

-However, designing and coding decryption software is completely out of our scope.

Why we need a proxy without root access

-If rooting a device is out of the question the only other known option is to set up a proxy

-The http requests would then be routed and tracked by the users PC instead of the phone. We would then track the urls through the PC.

-Downside is that users will have to set up the proxies themselves and be using the same LAN as their PC

Good News!

-Google browser history is accessible cross-platform.

-This means that if a user is signed into their google account on their phone and used the browser, our extension could track that history if the user is logged into the same account on their PC when we collect urls.

Sources

http://stackoverflow.com/questions/12525009/log-url-visits-in-android

http://android.stackexchange.com/questions/43444/listen-which-urls-an-app-tries-to-connect

http://stackoverflow.com/questions/22353717/list-http-requests-from-android-phone

http://stackoverflow.com/questions/17684936/android-capturing-http-requests-with-non-rooted-android-device

http://stackoverflow.com/questions/22338898/getting-device-network-urls-calls

https://www.mspy.com/blog/how-to-track-android-device-without-rooting-cell-phone/