Digital Payment Apps : Week 2

Shreejeet Golhait and Tushman Khalse

Tasks Completed

- **Collected Traffic from Payment Trannsactions of Various Apps**:We tried to collect network traffic for various applications using PCAPdroid and analysed the TLS and SNI of the payment transactions. We were only able to track HTTPS connections and were unable to find TLS transactions done by the digital payment app at the time of the trannsaction. It seems PCAPdroid is unable to observe the secure TLS transactions done by these digital payment apps. We were able to track TLS transactions from other sources like google messaging api, so it seems PCAPdroid can track other TLS handshakes but not of digital payment apps.

Proto	SrcIP	SrcPort	DstIp	DstPort	UID	App	Proto	Status	Info	BytesSent	BytesRcvd	PktsSent	PktsRcvd	FirstSeen	LastSeen
17	10.215.173.1	28285	10.215.173.2	53	10139	Google Play services	DNS	Closed	mtalk.google.com	62	107	1	1	2024-08-22T21:03:15.121+05:30	2024-08-22T21:0
6	10.215.173.1	47688	74.125.130.188	5228	10139	Google Play services	TLS	Closed	mtalk.google.com	1777	7186	15	15	2024-08-22T21:03:15.159+05:30	2024-08-22T21:0
17	10.215.173.1	21056	10.215.173.2	53	10139	Google Play services	DNS	Closed	playgateway-pa.googleapis.com	75	331	1	1	2024-08-22T21:03:31.876+05:30	2024-08-22T21:0
17	10.215.173.1	9599	10.215.173.2	53	10139	Google Play services	DNS	Closed	spot-pa.googleapis.com	68	324	1	1	2024-08-22T21:03:31.910+05:30	2024-08-22T21:0
17	10.215.173.1	37994	142.250.194.10	443	10139	Google Play services	QUIC	Closed	spot-pa.googleapis.com	4274	4320	9	11	2024-08-22T21:03:31.984+05:30	2024-08-22T21:0
17	10.215.173.1	50522	172.217.166.234	443	10139	Google Play services	QUIC	Closed	playgateway-pa.googleapis.com	2829	4371	8	11	2024-08-22T21:03:32.038+05:30	2024-08-22T21:0
17	10.215.173.1	42980	10.215.173.2	53	10264	GPay	DNS	Closed	firebaseinstallations.googleapis.com	82	338	1	1	2024-08-22T21:03:36.796+05:30	2024-08-22T21:0
6	10.215.173.1	47026	142.250.77.234	443	10264	GPay	HTTPS	Closed	firebaseinstallations.googleapis.com	1682	6297	7	7	2024-08-22T21:03:36.894+05:30	2024-08-22T21:0
17	10.215.173.1	7670	10.215.173.2	53	10264	GPay	DNS	Closed	india-paisa-pa.googleapis.com	75	91	1	1	2024-08-22T21:03:37.039+05:30	2024-08-22T21:0
6	10.215.173.1	56202	172.253.118.92	443	10264	GPay	HTTPS	Closed	india-paisa-pa.googleapis.com	63734	55570	213	208	2024-08-22T21:03:37.084+05:30	2024-08-22T21:0
17	10.215.173.1	49671	10.215.173.2	53	10139	Google Play services	DNS	Closed	voilatile-pa.googleapis.com	73	329	1	1	2024-08-22T21:03:37.896+05:30	2024-08-22T21:0
6	10.215.173.1	42096	142.250.193.202	443	10139	Google Play services	TLS	Closed	voilatile-pa.googleapis.com	1911	2143	11	12	2024-08-22T21:03:37.943+05:30	2024-08-22T21:0
17	10.215.173.1	55146	10.215.173.2	53	10264	GPay	DNS	Closed	paymentsincentives-pa.googleapis.com	82	338	1	1	2024-08-22T21:03:38.231+05:30	2024-08-22T21:0
17	10.215.173.1	52719	142.250.182.170	443	10264	GPay	QUIC	Closed	paymentsincentives-pa.googleapis.com	7256	26328	33	37	2024-08-22T21:03:38.332+05:30	2024-08-22T21:0
17	10.215.173.1	54685	10.215.173.2	53	10139	Google Play services	DNS	Closed	androidpay-users-pa.googleapis.com	80	96	1	1	2024-08-22T21:03:38.735+05:30	2024-08-22T21:0
17	10.215.173.1	57215	142.251.175.92	443	10139	Google Play services	QUIC	Closed	androidpay-users-pa.googleapis.com	6390	0	5	0	2024-08-22T21:03:38.831+05:30	2024-08-22T21:0
6	10.215.173.1	53098	142.251.175.92	443	10139	Google Play services	HTTPS	Closed	androidpay-users-pa.googleapis.com	4112	4267	19	22	2024-08-22T21:03:38.833+05:30	2024-08-22T21:0
17	10.215.173.1	48847	172.253.118.92	443	10264	GPay	QUIC	Closed	india-paisa-pa.googleapis.com	6390	0	5	0	2024-08-22T21:03:41.968+05:30	2024-08-22T21:0
17	10.215.173.1	14561	10.215.173.2	53	10264	GPay	DNS	Closed	paisafs-pa.googleapis.com	71	327	1	1	2024-08-22T21:03:42.380+05:30	2024-08-22T21:0
17	10.215.173.1	42114	10.215.173.2	53	10139	Google Play services	DNS	Closed	app-measurement.com	65	81	1	1	2024-08-22T21:03:47.007+05:30	2024-08-22T21:0
6	10.215.173.1	58600	142.250.194.174	443	10139	Google Play services	HTTPS	Closed	app-measurement.com	2987	814	7	7	2024-08-22T21:03:47.146+05:30	2024-08-22T21:0
17	10.215.173.1	36408	10.215.173.2	53	10264	GPay	DNS	Closed	lh3.googleusercontent.com	71	116	1	1	2024-08-22T21:03:47.248+05:30	2024-08-22T21:0
17	10.215.173.1	42081	10.215.173.2	53	10264	GPay	DNS	Closed	lh3.googleusercontent.com	71	128	1	1	2024-08-22T21:03:47.277+05:30	2024-08-22T21:0
6	10.215.173.1	56216	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1311	12179	13	14	2024-08-22T21:03:47.313+05:30	2024-08-22T21:0
6	10.215.173.1	56226	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1150	12279	9	11	2024-08-22T21:03:47.315+05:30	2024-08-22T21:0
6	10.215.173.1	56230	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1310	12173	13	13	2024-08-22T21:03:47.317+05:30	2024-08-22T21:0
6	10.215.173.1	56244	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1195	17132	10	10	2024-08-22T21:03:47.318+05:30	2024-08-22T21:0
6	10.215.173.1	56248	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1458	19302	11	12	2024-08-22T21:03:47.319+05:30	2024-08-22T21:0
6	10.215.173.1	56258	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1702	39136	18	18	2024-08-22T21:03:47.321+05:30	2024-08-22T21:0
6	10.215.173.1	56266	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1634	26187	15	15	2024-08-22T21:03:47.323+05:30	2024-08-22T21:0
6	10.215.173.1	56282	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1150	12552	9	10	2024-08-22T21:03:47.326+05:30	2024-08-22T21:0
6	10.215.173.1	56288	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1193	19495	10	10	2024-08-22T21:03:47.327+05:30	2024-08-22T21:0
6	10.215.173.1	56292	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1193	14391	10	10	2024-08-22T21:03:47.328+05:30	2024-08-22T21:0
6	10.215.173.1	43276	216.58.200.193	443	10264	GPay	HTTPS	Closed	lh3.googleusercontent.com	1145	15240	9	8	2024-08-22T21:03:48.310+05:30	2024-08-22T21:0
17	10.215.173.1	58972	10.215.173.2	53	10139	Google Play services	DNS	Closed	android.apis.google.com	69	109	1	1	2024-08-22T21:03:57.030+05:30	2024-08-22T21:0
17	10.215.173.1	57714	142.250.195.14	443	10139	Google Play services	QUIC	Closed	android.apis.google.com	7867	5681	14	12	2024-08-22T21:03:57.079+05:30	2024-08-22T21:0
17	10.215.173.1	48809	10.215.173.2	53	10139	Google Play services	DNS	Closed	app-measurement.com	65	81	1	1	2024-08-22T21:05:21.352+05:30	2024-08-22T21:0

17	10.215.173.1	51804	10.215.173.2	53	10291	Paytm	DNS	Closed	securegw-online.paytm.in	70	192	1	1	2024-08-22T20:38:08.834+05
17	10.215.173.1	19902	10.215.173.2	53	10291	Paytm	DNS	Closed	trust.paytmbank.com	65	162	1	1	2024-08-22T20:38:08.836+05
17	10.215.173.1	28197	10.215.173.2	53	10291	Paytm	DNS	Closed	crashlyticsreports-pa.googleapis.com	82	98	1	1	2024-08-22T20:38:08.904+05
17	10.215.173.1	45466	10.215.173.2	53	10291	Paytm	DNS	Closed	accounts.paytm.com	64	164	1	1	2024-08-22T20:38:09.066+05
6	10.215.173.1	52520	23.41.202.38	443	10291	Paytm	HTTPS	Closed	kyc.paytmbank.com	2559	8443	15	16	2024-08-22T20:38:09.121+05
17	10.215.173.1	48726	14.139.60.107	123	10291	Paytm	NTP	Closed	time.nplindia.org	76	76	1	1	2024-08-22T20:38:09.137+05
6	10.215.173.1	42836	23.44.236.219	443	10291	Paytm	HTTPS	Closed	securegw-online.paytm.in	1724	5237	12	13	2024-08-22T20:38:09.194+05
6	10.215.173.1	52532	23.41.202.38	443	10291	Paytm	HTTPS	Closed	trust.paytmbank.com	1239	4475	12	12	2024-08-22T20:38:09.204+05
6	10.215.173.1	46860	142.250.193.3	443	10291	Paytm	HTTPS	Closed	crashlyticsreports-pa.googleapis.com	6879	6577	10	9	2024-08-22T20:38:09.215+05
17	10.215.173.1	64438	10.215.173.2	53	10291	Paytm	DNS	Closed	push-registry.paytm.com	69	171	1	1	2024-08-22T20:38:09.318+05
17	10.215.173.1	20499	10.215.173.2	53	10291	Paytm	DNS	Closed	ws-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	98	169	1	1	2024-08-22T20:38:09.372+05
6	10.215.173.1	57992	3.109.20.208	443	10291	Paytm	HTTPS	Closed	ws-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	2555	19642	23	26	2024-08-22T20:38:09.641+05
17	10.215.173.1	40174	10.215.173.2	53	10291	Paytm	DNS	Closed	assetscdn1.paytm.com	66	162	1	1	2024-08-22T20:38:09.663+05
17	10.215.173.1	43450	10.215.173.2	53	10291	Paytm	DNS	Closed	push-signal.paytm.com	67	167	1	1	2024-08-22T20:38:09.904+05
6	10.215.173.1	43862	118.215.153.218	443	10291	Paytm	HTTPS	Closed	assetscdn1.paytm.com	4280	76963	76	78	2024-08-22T20:38:09.940+05
17	10.215.173.1	64598	10.215.173.2	53	10291	Paytm	DNS	Closed	api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	99	171	1	1	2024-08-22T20:38:10.517+05
6	10.215.173.1	54350	13.202.14.203	443	10291	Paytm	HTTPS	Closed	api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	3653	11264	22	23	2024-08-22T20:38:10.744+05
6	10.215.173.1	54352	13.202.14.203	443	10291	Paytm	HTTPS	Closed	api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	1199	4370	11	11	2024-08-22T20:38:10.749+05
6	10.215.173.1	54368	13.202.14.203	443	10291	Paytm	HTTPS	Error	api-7cc3e8d0-d35b-4685-b603-135df578e7de.sendbird.com	1159	3525	10	9	2024-08-22T20:38:10.754+05
17	10.215.173.1	14766	10.215.173.2	53	10291	Paytm	DNS	Closed	appmanager.paytm.com	66	165	1	1	2024-08-22T20:38:12.139+05
17	10.215.173.1	59238	10.215.173.2	53	10291	Paytm	DNS	Closed	graph.facebook.com	64	104	1	1	2024-08-22T20:38:23.778+05
6	10.215.173.1	59926	163.70.143.15	443	10291	Paytm	HTTPS	Closed	graph.facebook.com	1735	4688	9	9	2024-08-22T20:38:24.035+05
17	10.215.173.1	25708	10.215.173.2	53	10133	Google Play Store	DNS	Closed	play.googleapis.com	65	129	1	1	2024-08-22T20:38:25.690+05
17	10.215.173.1	38162	10.215.173.2	53	10291	Paytm	DNS	Closed	sig.paytm.com	59	238	1	1	2024-08-22T20:38:25.713+05
6	10.215.173.1	33496	216.239.34.223	443	10133	Google Play Store	HTTPS	Closed	play.googleapis.com	2974	2176	8	7	2024-08-22T20:38:25.943+05
6	10.215.173.1	33690	13.234.214.227	443	10291	Paytm	HTTPS	Closed	sig.paytm.com	40014	11703	57	57	2024-08-22T20:38:25.955+05
17	10.215.173.1	6413	10.215.173.2	53	10291	Paytm	DNS	Closed	digital-search.paytm.com	70	173	1	1	2024-08-22T20:38:29.422+05
17	10.215.173.1	51375	10.215.173.2	53	10291	Paytm	DNS	Closed	upi.paytm.com	59	151	1	1	2024-08-22T20:38:32.971+05
17	10.215.173.1	59115	10.215.173.2	53	10139	Google Play services	DNS	Closed	people-pa.googleapis.com	70	326	1	1	2024-08-22T20:38:53.640+05
6	10.215.173.1	33774	142.250.192.234	443	10139	Google Play services	TLS	Closed	people-pa.googleapis.com	2905	6442	14	16	2024-08-22T20:38:53.883+05
17	10.215.173.1	18741	10.215.173.2	53	10291	Paytm	DNS	Closed	firebaselogging.googleapis.com	76	332	1	1	2024-08-22T20:39:02.489+05
6	10.215.173.1	33578	142.250.195.10	443	10291	Paytm	HTTPS	Closed	firebaselogging.googleapis.com	1863	6062	8	8	2024-08-22T20:39:03.039+05
17	10.215.173.1	37626	10.215.173.2	53	10291	Paytm	DNS	Closed	firebaselogging-pa.googleapis.com	79	335	1	1	2024-08-22T20:39:04.135+05
6	10.215.173.1	35478	142.250.194.202	443	10291	Paytm	HTTPS	Closed	firebaselogging-pa.googleapis.com	2414	6120	7	6	2024-08-22T20:39:04.464+05
6	10.215.173.1	51634	172.217.166.202	443	10291	Paytm	HTTPS	Closed	firebaseremoteconfigrealtime.googleapis.com	1579	4709	6	5	2024-08-22T20:39:10.362+05
6	10.215.173.1	32902	74.125.68.188	5228	10139	Google Play services	TLS	Closed	mtalk.google.com	1462	2890	9	9	2024-08-22T20:39:15.380+05
17	10.215.173.1	49948	10.215.173.2	53	10532	Instagram	DNS	Closed	i.instagram.com	61	106	1	1	2024-08-22T20:39:25.728+05
17	10.215.173.1	55095	163.70.143.63	443	10532	Instagram	QUIC	Closed	i.instagram.com	5127	15096	9	23	2024-08-22T20:39:25.732+05

- **Analyzed the collected data from PCAPdroid and plotted graphs of when TLS handshakes**: We wrote a python script which uses dpkt library and matpotlib to plot TLS transactions and the transaction's SNI. We used this script and also manually went through the pcap file by converting it to a csv file but in both cases were unable to find TLS transactions done by the digital payment app.

- **Using apk-mitm we rebuild PayTM, Mobiqwick, PhonePe, Google Pay, BHIM, Bharat Pe**: We patched apks of these apps using apk-mitm. After installing the patched apks, we tried running them. A few of them opened but we were unable to proceed from the login page. A few apps crashed after being patched(PhonePe). As these apps use advanced security measures like certificate pinning we could not perform any transaction using the patched apks.

Conclusion

We analysed the logs from PCAPdroid for multiple digital payment apps and searched for TLS handshakes. We used a python script which used dpkt to plot the logs. We were unable to find TLS handshakes corresponding to the payment transaction. We also used apk-mitm to patch many digital payment apps and monitored them. We were unable to do a transaction using these patched apks but some of them opened till the login page.