**Volume 9, Issue 2**
October 2016
ISSN: 1946-1836

# JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

**In this issue:**

The **Journal of Information Systems Applied Research** (JISAR) is a double-blind peer-reviewed academic journal published by **ISCAP,** Information Systems and Computing Academic Professionals. Publishing frequency is currently quarterly. The first date of publication was December 1, 2008.

JISAR is published online (http://jisar.org) in connection with CONISAR, the Conference on Information Systems Applied Research, which is also double-blind peer reviewed. Our sister publication, the Proceedings of CONISAR, features all papers, panels, workshops, and presentations from the conference. (http://conisar.org)

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the conference. At that point papers are divided into award papers (top 15%), other journal papers (top 30%), unsettled papers, and non-journal papers. The unsettled papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the JISAR journal. Currently the target acceptance rate for the journal is about 40%.

Questions should be addressed to the editor at editor@jisar.org or the publisher at publisher@jisar.org. Special thanks to members of AITP-EDSIG who perform the editorial and review processes for JISAR.

# JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH

## Editors



## JISAR Editorial Board

# Leakage of Geolocation Data by Mobile Ad Networks

Christopher Snow
csnow@pace.edu

Darren Hayes
dhayes@pace.edu

Catherine Dwyer
cdwyer@pace.edu

Seidenberg School of Computer Science & Information Systems
Pace University
New York, NY

## Abstract

Mobile ad networks connect advertisers with mobile app publishers, to improve the suitability of ads shown to app users. These ad networks send metadata about mobile users and their devices to advertisers, who then use this metadata to select appropriate ads. This research demonstrates how mobile networks leak location data and other sensitive information from mobile phones by sending plaintext, unencrypted transmissions. It is therefore possible that geolocation information, associated with a user, could be captured by government and private sector entities, as well as by nefarious actors. An experiment was designed to discover how iPhone applications ("apps") transmit unencrypted geodata to identify a user's location. This research revealed that several popular mobile apps disclose the location of an iPhone by means of its UDID (serial number); this primarily occurred through mobile ad networks.

**Keywords:** Mobile Privacy, Mobile Advertisements, Geodata, iPhone Forensics, Edward Snowden, NSA

## 1. INTRODUCTION

Consider this: a person can no longer leave the country without a number of people, other than friends or family, knowing about it. It is only possible though if you pack-up, get in a car that is not wired to GPS, and leave your cellphone behind. Even then, some type of surveillance camera is monitoring and recording you. Sounds impossible, doesn't it? Mobile devices have completely taken away a user's sense of privacy, more specifically a user's sense of locational privacy. Modern smartphone owners have a subliminal sixth sense that "big brother" is always watching. From social media, to photos and mobile applications, there is always at least one person that a smart device user has never met who knows exactly where that smart device user is. Smart devices, such as the iPhone, the Microsoft Surface Tablet, and even a car's navigation system are always collecting, storing, analyzing, and sending data about the user's location in the form of longitude and latitude metadata, otherwise known as geodata.

Documents released by Edward Snowden in 2015 describe Operation BADASS – a U.S. government program that included the retrieval of metadata transmitted by mobile ad networks, including user location information from mobile devices and computers. The National Security Agency and Department of Defense allegedly captured

geodata from these devices via Wi-Fi, iPhone UDID, and electronic paper trails (SPIEGEL ONLINE, 2013).

Unbeknownst to many, U.S. government agencies, like the National Security Agency (NSA) or the Department of Justice (DOJ), are silently intercepting foreign and domestic communications from mobile devices and subsequently analyzing these communications. The United States is not the only country performing these covert operations. India, France, and Saudi Arabia all perform similar, if not more invasive, surveillance on their citizens. According to documents leaked by whistleblower Edward Snowden and other anonymous sources, government agencies are collecting electronic data at unfathomable speeds and quantities (Bamford, 2012; MacAskill, 2013).

A leaked presentation from the British intelligence agency Government Communications Headquarters (GCHQ) titled "Mobile Apps Doubleheader: BADASS Angry Birds" shows that government agencies are capturing data collected from private sector communications, typically mobile advertisements, using a program under the codename 'BADASS' (Lee, 2015). The research presented in this paper shows data collection from mobile advertisements is quite possible, demonstrating how insecure mobile advertisement transmissions can be.

## 2. BACKGROUND

One must analyze U.S. law to understand how the U.S. government has the legal authority to collect metadata from smartphone users. Section 216 of the PATRIOT Act states that the U.S. government has the ability to collect "data without content" under pen register. Thus, data such as IP addresses, geolocation, phone numbers, and URLs can be collected with a court order rather than meeting the higher standards needed to obtain a warrant. Of course, this data can be used to determine more invasive information by performing a search for a URL or using the coordinates on a map (Doyle, 2001). However, analyzing this data superficially does not provide sensitive information about an individual.

Section 216's definition of pen register allows the NSA to legally perform operations, like Operation BADASS, to collect content-less data in large quantities. Operation BADASS indicates that governments can collect personal information from private sector activities and communications. Figure A1 shows what information is collected through mobile advertising provider Mobclix, now named Axonix. The slide, which is derived from the previously mentioned leaked GCHQ presentation, identifies the fields within the mobile advertiser's HTTP requests. The most important fields noted in the presentation include "&ll" and "&u." The "&ll" field is described in the slide as the field containing longitude and latitude coordinates. While the "&u" field in the request is noted as containing an "IMEI." An IMEI number uniquely identifies a user's cellphone on a GSM network (Lee, 2015). Both of these combined elements allow a user profile to be developed and track movements. A query could be made on Mobclix/Axonix's database for a specific IMEI sequence to display the HTTP requests made by that specific user. This would allow a map to be generated based on the locations where a specific user has made HTTP requests while being served an advertisement. This map could ultimately lead to someone's true identity being revealed based on the patterns of their movement.

A bill introduced in the U.S. House of Representatives on July 8, 2015, titled "The Consumer Privacy Protection Act", would require companies to notify their customers within 30 days if hackers obtained "sensitive information". This bill expands the definition of "sensitive information" to include geolocation data (Davis, 2015). Treating geolocation as "sensitive information" could set a precedent for future legislation to include geolocation as personal information. The bill also seeks to encourage higher security procedures, including the minimization of "sensitive personally identifiable information" stored by companies.

## 3. RELATED WORK

A report titled "Taming the Android AppStore: Lightweight Characterization of Android Applications" from the networking and security department at EURECOM, a graduate school in France, described research on the Android platform (Vigneri, Chandrashekar, Pefkianakis, & Heen, 2015). Their research sought to analyze network connections when Android applications are launched. The goal of EURECOM's research was to categorize the types of communication connections and develop an application for users to calculate the privacy of an application. They sought to provide users with information about how apps collect personal information. They tracked a smart device's network connections, through apps, to verify whether these connections were safe. The researchers routed all traffic from these Android applications through a virtual private network (VPN).

EURECOM's research uncovered that AdMob and Flurry, which are two popular advertisement companies, made the top 20 list of servers receiving communications from Android applications. From the analyzed requests, EURECOM researchers were able to develop a suspicion algorithm that is used to identify how suspicious an application is. They used factors such as the webutation.com ranking to decide how safe or malicious the HTTP request made by the application was and how many times HTTP requests are made. Their research concluded that many Android applications on the *Google Play Store* make undesirable communications unbeknownst to the user. Additionally, the research concluded that a number of high-ranking applications made excessive requests to advertising companies.

A report released by Zscaler Inc. in early 2014 documented how the Angry Birds app was divulging personal information to third parties. After the accusation, Rovio, the developers of Angry Birds, attributed blame to mobile advertisers (Robertson, 2014). Their privacy policy exclusively states Rovio "may collect and process your location data to provide location related services and advertisements." Additionally, Rovio states they "reserve the right to use and disclose the collected, non-personal data for purposes of advertising by Rovio" (Rovio, 2013). This accusation coincided with the GCHQ presentation of Operation BADASS and it is not hard to surmise that user location data has been leaked since the Angry Birds application does use advertising extensively. The study conducted by Zscaler Inc. looked at 30,000 Android applications and found that 38% leaked a smartphone's unique IMEI/MEID number and 15% of these apps divulged the user's phone number (Robertson, 2014).

## 4. EXPERIMENTAL RESEARCH

The experimental research documented in this paper sought to discover how a user could be profiled by means of mobile advertisements directed through iPhone apps. Related work has shown that Android applications regularly divulge personal data. With 1.2 million applications available in Apple's App Store, it is hard to believe that all of them are secure when dealing with a user's personal information (Perez, 2014). Additionally, this research seeks to investigate mobile advertisement security through ad networks.

### *Experimental Design*

Our experimental research simulated Operation BADASS, where application data is captured and recorded.

Figure A2 graphically reflects the communications identified in this experiment. This experiment displays the "Middlemen Servers" used to capture the HTTP and HTTPS requests between the smartphone application and the application server (or advertising agency). The figure also shows metadata being shared between the application and the advertising agency. Essentially, an advertising agency, like Mobclix, could use information loaded into an application by the user, such as age or location, to learn more about the user in order to serve targeted, or more suitable, ads. Typically, communications between the application and an application server are encrypted. However, communications between the application and an advertising agency are not encrypted (Lee, 2015). This means that data gathered about a user, by an advertisement may be leaked and collected by "middlemen," such as the NSA.

Our experiments sought to identify what data on an iPhone is transmitted from applications via insecure HTTP requests. With our framework, multiple iPhone applications are used casually and authentically while a program, called Debookee, analyzes and captures the Internet traffic flowing through a wireless router. This data captured from Internet requests is then analyzed to see if any personal information, specifically data related to location, is recorded.

To test this framework, the following tools were used:

- Debookee by iwaxx
- iPhone loaded with various applications (travel, gaming, dating, shopping, etc.)
- Wireless Internet router
- Internet connected computer running Mac OS X

### *Experiment*

The data for this experiment was obtained in April 2015. First, a controlled environment had to be established before any HTTP requests from the target smartphone were captured. To do this, a wireless router was connected to an Ethernet port to facilitate the connection of mobile devices to the Internet. Subsequently, all wireless devices connected to the wireless router were documented. Debookee offers a LAN scan to display all connected devices and also a basic description of these devices. Figure A3 and Figure

A4 show how the target used is correct by matching the IP addresses (i.e., 192.168.1.103).

With the target identified, the HTTP traffic transmitted by the phone can be captured. The traffic from about 40 applications was analyzed. Three yielded the most useful data and were chosen for further analysis. They included Transit, BestBuy, and Kick the Buddy.

***Transit***

Transit operates as a NYC subway navigator. The application allows a user to input a starting destination, often their current location, and an end point. The application then shows the user the best subway to take to get from point A to point B. This application was used at 100 Henry Street, Brooklyn, NY, and a request was made for transit directions to downtown Manhattan. The Transit app sends requests to a server with fields matching a user's search terms. Debookee was able to capture the following unencrypted HTTP request when this search was performed:

http://us-east-planner1.thetransitapp.com/opentripplanner-api-webapp/ws/plan?routerId=10&showIntermediateStops=true&walkReluctance=3.75&**toPlace=40.711016,- 74.004845&fromPlace=40.697740,-73.993262&time=16:40&date=04/18/2015**

**Figure 1: Unencrypted HTTP request from Transit App.**

The important fields are bolded, namely "**toPlace**," "**fromPlace**," and "**time**." The "toPlace" and "fromPlace" are easy to distinguish; they are the starting and end coordinates of the query. Figure A5 and Figure A6 show that the coordinates, provided by gps-coordinates.net, in the "toPlace" and "fromPlace" fields match this search. Additionally, time shows the exact military time when the search was performed, as well as the date.

If intercepted, this locational data could easily determine that a student performed the search. A quick search with the term "100 Henry Street" on Google will reveal that the building is used as student housing. Someone intercepting this communication could easily conclude that the search was performed a student in the building. However, identifying the exact student would be difficult because the capture request did not contain any identifying ID or token. Nevertheless, this data shows that these types of navigational searches on Transit are insecure and could be read by someone unbeknownst to the user.

***BestBuy***

BestBuy, unlike Transit, does not provide users with navigational information. It does, however, utilize a user's information to locate BestBuy retailers in the area. What was surprising about the data captured from the BestBuy app was that it remembered previous locations. The request in Figure A7 was made after the application was loaded. An interesting "area" field appears in the second line of the request (portions are redacted for privacy). Using gps-coordinates.net, the coordinates pointed to a residence on Long Island. The residence in question happened to be the user's actual permanent address and it also happens to be the last place where the application was run. It is unclear why this request was made, but it appears the application may have been pulling saved data from the application's last use.

A more interesting part of this request is the "cookie" field that also appears in Figure A7 on the fifth line. This cookie field ties back to previous research, specifically operation BADASS. BestBuy appears to be using a cookie to store personal data, which can communicate data to and from the application for advertising and marketing purposes. Therefore, BestBuy presumably has a database where specific cookie tokens could be used in a query in order to see where and when someone has used their app. In this case, it would be easy to tie this specific request back to someone who lives at the residence based on the accurate coordinates the user's phone provided them.

***Kick the Buddy***

Crazylion Studios Limited has produced multiple free games that appear on the Apple App Store top charts, including Kick the Buddy. Free games frequently feature more mobile advertisements. Mobile ads are an effective way to make money while keeping the application free for users to download (Hof, 2014). Kick the Buddy features multiple advertisements, as seen in Figure A8 and Figure A9. These advertisements have made Kick the Buddy the perfect candidate to explore further in this controlled experiment.

As expected, multiple requests were made to advertising services that transmit advertisements to the user. The following unencrypted HTTP request stood out:

http://ads/m/imp?appid=&cid=c666ac880b044f8cac90a19fdc099893&**city=Brooklyn**[…]&**dev=iPhone7**%2C2&[…]http%3A%2F%2Fcpp-test.imp.mpx.**mopub.com**%2Fclick%[…]%26app_name%3D**kick%2520the%2520Buddy%253A%2520Second%2520Kick%2520Free**%

[…]&**udid=**ifa%3A**90E*****CC9-4**C-B7B8-6D24*****B54**

**Figure 2: Unencrypted HTTP request from Kick the Buddy Mobile Game.**

The ad was identified as Kick the Buddy: A Second Kick Free, the full name of the application where the ad was found. It is important to note that no advertisements were opened in this experiment; these requests came only from the advertisement found in the application being used. The advertisement was able to determine the correct general location of the user in Brooklyn. Though, perhaps the most valuable piece of information to come from this request is the UDID number, **90E*****CC9-4**C-B7B8-6D24*****B54** (portions of the UDID number have been omitted for privacy).

The UDID is the token assigned to the user specifically. It is used so that Mopub can pull the information they have already collected about the user and subsequently transmit the user with more targeted marketing materials based on like one's gender, age, and/or location. With this UDID number that potentially identified the user, a query was made to Debookee using the discovered UDID to find any other requests that were made by Mopub. Debookee returned with 45 HTTP requests made by Mopub from other applications to serve advertisements to the user. A majority of the requests contained the same information as the Kick the Buddy request, many with less information. Though, there was one alarming result:

**http://ads.mopub.com**/m/ad?v=8&**udid**=ifa:**90E*****CC9-4**C-B7B8-6D24*****B54**&id=agltb3B1Yi1pbmNyDAsSBFNpdGUYorkhDA&nv=1.17.2.0&**q=m_gender:m,m_age:21**&o=p&sc=2.0&z=0400&**ll=40.697700885046903,-73.99321115040379**&lla=65&mr=1&ct=2&av=2.2.2&cn=Verizon&iso=us&mnc=480&mcc=311&dn=iPhone7%2C2

**Figure 3: Unencrypted HTTP request from MoPub ad network.**

As one can see, the UDID highlighted in bold matches the UDID from the Kick the Buddy HTTP request. There is also gender and age information being transmitted. This information matches the first author, whose phone was used to collect this data. The advertisement is also identified to come from Mopub. Unfortunately, the HTTP request does not exclusively provide what application generated the ad. But, the information that is stored within this request is extremely personal. Recalling Figure A1, there are similar fields in this request that GCHQ pointed out in their presentation; specifically the "ll=" field for longitude and latitude. The "ll=" field provides the same coordinates from Figure A6, the Transit results. However, it can be inferred that this advertisement request did not come from Transit because the Transit application does not transmit ads to their users. It could, however, have come from another advertisement within Kick the Buddy because the game transmits multiple advertisements. It is unclear how the advertisement was able to identify the user's gender and age as both fields were never provided to any of the applications we researched. It is also important to note that Facebook was not a part of this experiment and the application was not loaded onto the subject smartphone at the time of experimentation.

## 5. EXPERIMENTAL CONCLUSIONS

This experiment showed that not only mobile advertisers, but also location-aware applications, disclose geodata from mobile phones. The experiment showed applications, like Transit, knowingly using location are sending unencrypted requests. Therefore, it is plausible that the NSA, or any other interested parties, have the ability to gain intelligence regarding location through the interception of mobile advertising transmissions. It is important to note that this was a very small-scale experiment. Imagine if this collection was performed on the entire city of New York by tapping into all of the unencrypted, or open, Wi-Fi hotspots. Unencrypted HTTP requests could theoretically be collected by thousands of people at once. Then requests with the same UDID can be identified as the same people to start building different profiles. The experiment showed identification of targets is possible; 45 other queries were found using the Mopub UDID that was assigned to the first author.

Although the results from this experiment are quite specific, one must consider broader implications of linking data to other data. The information from, for example, one Mopub advertisement may only have information about the user's gender. But, since all Mopub advertisements are linked to one person with UDID, a user's profile can be expanded. Now, not only does Mopub know a user's gender from application "x" they also now know the same user's location from application "y." Now that a user's coordinate location is known, an analyst can query that location against the HTTP capture database to see if navigation applications like Transit were used to see where the same user traveled.

Another issue that this experiment has unexpectedly uncovered is the question of who is responsible for the data being leaked. It is completely up to the discretion of the app developer and/or advertising companies to ensure the HTTP requests to and from served ads are secure, not the phone manufacturer or wireless router. As seen in Figure A10, HopStop, another subway navigation application like Transit, secures all HTTP requests under HTTPS. This means that any search and serving of data travels through a safer port so man-in-the-middle applications, such as Debookee and WireShark, cannot intercept wireless data.

Google has brought HTTPS encryption to all of their services, including AdMob, its mobile advertising service. In June 2015, a "vast majority" of AdMob's connections were moved over to HTTPS encryption (Google, 2015). In addition, Apple added App Transport Security (ATS) in September 2015 to the iOS 9 operating system. ATS is a framework that imposes network security best practices, for example requiring HTTPS for all network requests, and the use of Transport Layer Security (TLS) 1.2 or higher (Jacobs, 2015).

## 6. IMPORTANCE OF RESEARCH

This research was able to reproduce how easy it is to collect geodata leaked by mobile apps. These findings validate the leaked Snowden documents from GCHQ.

This research shows government agencies could use the private sector for data collection. The experiment shows that the data displayed in *Figure A1* is accurate. It is not hard to imagine that the American government, or any government, could be collecting the unencrypted data detailed in this paper's findings. The claimed operations of the NSA, outlined by Edward Snowden, are perhaps valid. The private sector is an interesting sector to investigate since companies like Apple and Microsoft are adamant about not facilitating government investigations. But, downloaded applications on smart devices, including the iPhone, are leaking personal data that people would rather not share with law enforcement.

The conclusions drawn from this paper's research also show a defining shift in intelligence gathering. Before the widespread use of smartphones, an important source of information about people and/or their location was through public records or hacking. However, now, there is a plethora of unencrypted personal data flowing through the Internet for anyone to intercept. With that in mind, the key stakeholders in all of this data collection are definitely the mobile advertisers. Mobile advertisement providers like AdMob and Mopub essentially can build entire profiles on a person by correlating all of the information they have on a person. This is one of the most important takeaways from the research conducted in this paper.

## 7. FUTURE EXPERIMENTS

A future experiment could be to label each incoming transmission, and identify which app it came from. When the HTTP requests were compiled and exported for analysis, it proved difficult to distinguish which apps generated them. Most requests contained the name of the application inside the HTTP requests but some did not.

It may be useful to create multiple applications using different advertising companies, like AdMob or Mopub, to see how much a developer can control the data that can be captured and how easy it is to secure these transmissions. Aside from advertisers, it may prove helpful to also create applications that make HTTP requests back to a self-operated webserver. Transit and BestBuy, for example, both use unsecure HTTP requests back to servers they own. A future experiment might examine how easy it is to secure data transmissions where the app and the hosted server are both self-operated. This could help decide who is responsible for leaking data when encryption is not enabled on transmissions.

A future experiment could also have two participants, one "agent" and one "criminal," both connected to a controlled public wireless router with casual innocent users. In this experiment the designated agent would be capturing the wireless router's unencrypted HTTP requests in an attempt to identify the designated criminal the designated agent has been tracking. This experiment would both look at the possibility of detecting a target on an unencrypted wireless router as well as how much accidental data could be collected from innocent users in a real operation.

## 8. CONCLUSION

The conclusions drawn from the data presented in literature research and experimental research shows that the U.S. government, along with any other interested parties, does have the ability to target a person and track them through their mobile geodata.

An important finding is that mobile devices are emitting more personal data about the user than

the user may realize. Wireless unencrypted personal data is free for anyone to use, whether it is government, a business, or a criminal. In this wireless day and age a hacker no longer has to know a username and password to get personal data, they just essentially have to eavesdrop on the personal data that a user is unintentionally sending. Along the same lines, a business can simply use a tool to analyze social media chatter to find where people are discussing their product instead of sending out an old-fashioned survey. Both cases use the free available location data on Internet that users are willingly sharing, whether or not they know it.

## 9. REFERENCES

Bamford, J. (2012, March 15). The NSA is building the country's biggest spy center (watch what you say). Retrieved from http://www.wired.com/2012/03/ff_nsadatacenter/

Doyle, C. (2001, December). Terrorism: section by section analysis of the USA PATRIOT act. Congressional Research Service, the Library of Congress.

Davis, W. (2015, July 8). New data breach bill covers photos, geolocation data, other 'sensitive' information. Retrieved July 14, 2015, from http://www.mediapost.com/publications/article/253573/new-data-breach-bill-covers-photos-geolocation-da.html?utm_source=newsletter&utm_medium=email&utm_content=headline&utm_campaign=84298

Google. (2015, April 17). Inside adwords: ads take a step towards "HTTPS everywhere". Retrieved July 10, 2015, from http://adwords.blogspot.com/2015/04/ads-take-step-towards-https-everywhere.html

Hof, R. (2014, August 27). Study: mobile ads actually do work - especially in apps. Retrieved from http://www.forbes.com/sites/roberthof/2014/08/27/study-mobile-ads-actually-do-work-especially-in-apps/

Jacobs, B. (2015). Apple Tightens Security With App Transport Security. *Code Tutorials*. http://code.tutsplus.com/articles/apple-tightens-security-with-app-transport-security--cms-24420 Retrieved from http://code.tutsplus.com/articles/apple-tightens-security-with-app-transport-security--cms-24420

Lee, M. (2015, January 26). Secret 'BADASS' intelligence program spied on smartphones. *First Look Media*. Retrieved May 4, 2015, from https://firstlook.org/theintercept/2015/01/26/secret-badass-spy-program/

MacAskill, E. (2013, August 23). NSA paid millions to cover PRISM compliance costs for tech companies. Retrieved from http://www.theguardian.com/world/2013/aug/23/nsprism-costs-tech-companies-paid

Perez, S. (2014, June 2). iTunes app store now has 1.2 million apps, has seen 75 billion downloads to date. Retrieved April 15, 2015, from http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/

Robertson, J. (2014, Jan 29). Leaked docs: NSA uses 'candy crush,' 'angry birds' to spy. *SFGate*. Retrieved April 11, 2015, from http://www.sfgate.com/technology/article/Leaked-docs-NSA-uses-Candy-Crush-Angry-5186801.php

Rovio. (2013, October). Privacy policy - rovio entertainment ltd. Retrieved from http://www.rovio.com/Privacy

SPIEGEL ONLINE. (2013, December 30). Interactive graphic: the NSA's spy catalog. Retrieved from http://www.spiegel.de/international/world/941262.html

Vigneri, L., Chandrashekar, J., Pefkianakis, I., & Heen, O. (2015). Taming the android appStore: lightweight characterization of Android applications. *arXiv preprint arXiv:1504.06093*.

# Appendix

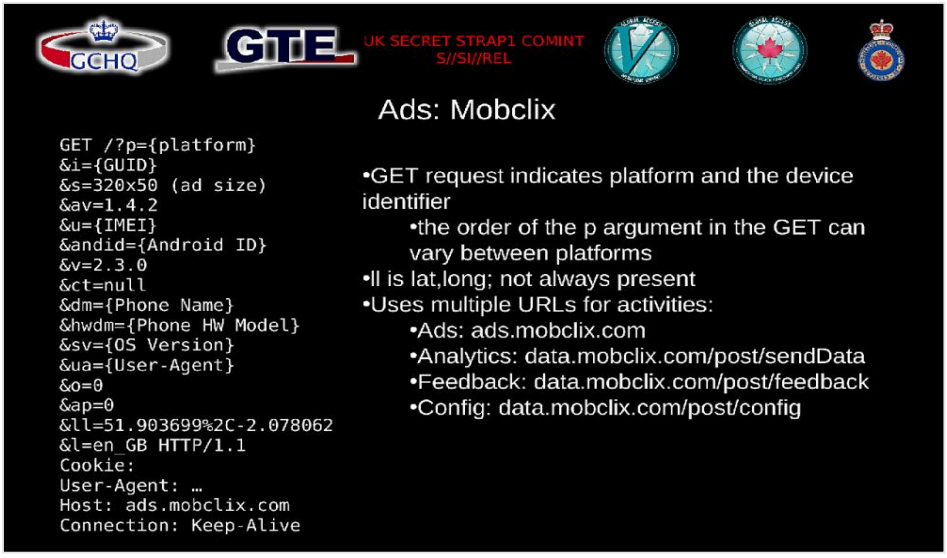
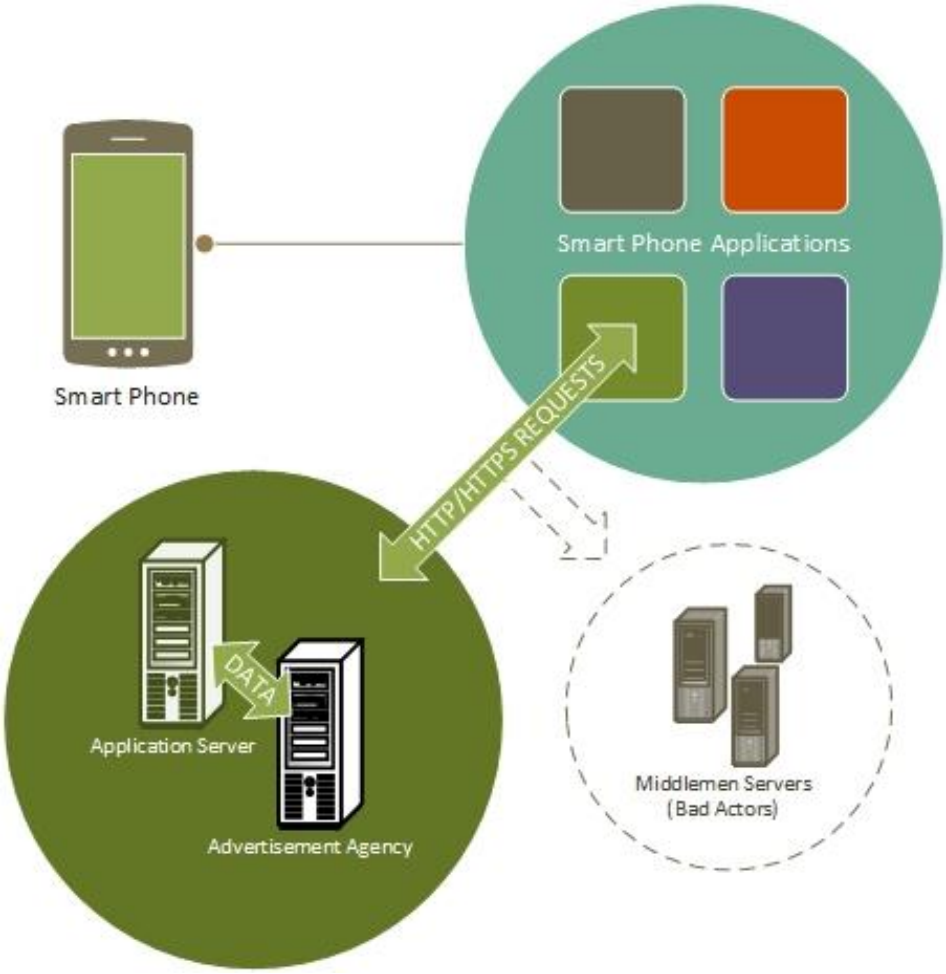
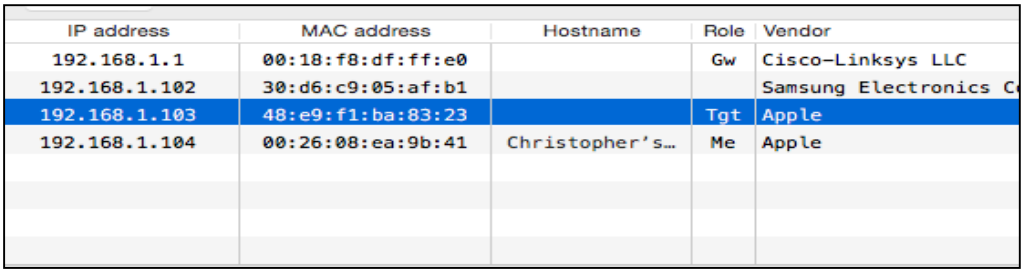



Figure A1 | *Slide from "Mobile Apps Doubleheader: BADASS Angry Birds" GCHQ presentation* (Lee, 2015)

Figure A2 | *Communications between smart phone applications and servers*





| IP address | MAC address | Hostname | Role | Vendor |
|---|---|---|---|---|
| 192.168.1.1 | 00:18:f8:df:ff:e0 | | Gw | Cisco-Linksys LLC |
| 192.168.1.102 | 30:d6:c9:05:af:b1 | | | Samsung Electronics C |
| 192.168.1.103 | 48:e9:f1:ba:83:23 | | Tgt | Apple |
| 192.168.1.104 | 00:26:08:ea:9b:41 | Christopher's… | Me | Apple |

Figure A3 | *Debookee screenshot (note IP address 192.168.1.103)*

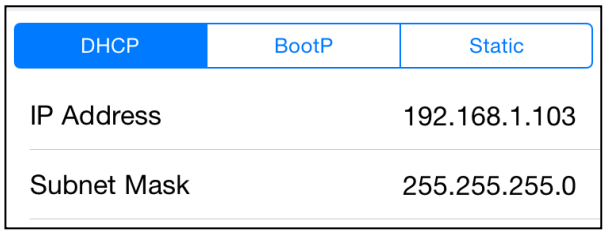



Figure A4 | *iPhone screenshot (note IP address 192.168.1.103)*

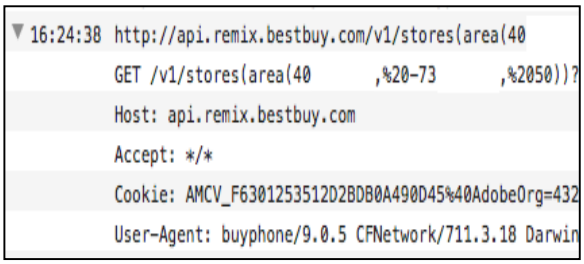



Figure A7 | *Excerpt of captured HTTP request from BestBuy*

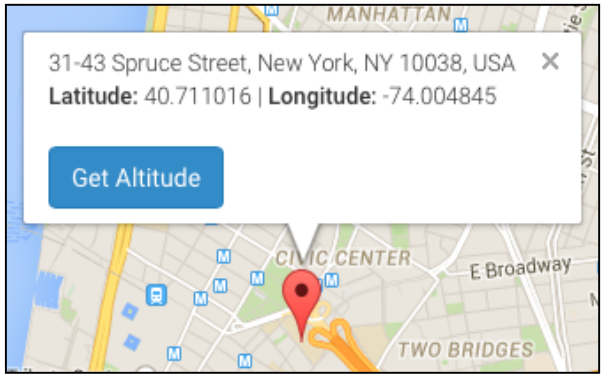



Figure A5 | *Destination coordinates, toPlace*


Figure A8 | *Full screen ad shown on Kick the Buddy game*

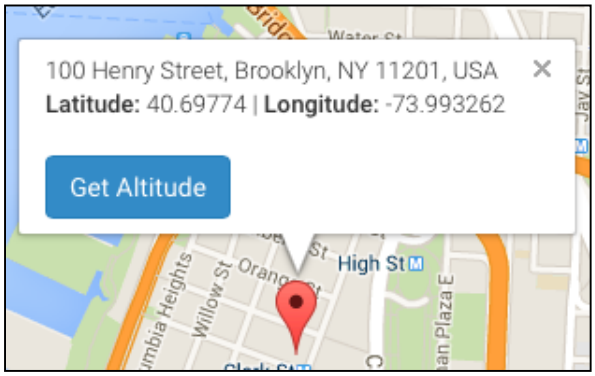



Figure A6 | *Beginning coordinates, fromPlace*


Figure A9 | *Bottom right corner ad shown on Kick the Buddy game*

```
22:59:32  H https://www.hopstop.com/...[encrypted]
22:59:40  H https://www.hopstop.com/...[encrypted]
22:59:42  H https://www.hopstop.com/...[encrypted]
22:59:43  H https://www.hopstop.com/...[encrypted]
```

Figure A10 | *Excerpt of captured HTTPS requests*