# Meddle: Practical Mobile Diagnosis Through Traffic Monitoring

First
*First Institution*

Second
*Second Institution*

Third
*Third Institution*

Fourth
*Fourth Institution*

Fifth
*Fifth Institution*

Sixth
*Sixth Institution*

## Abstract

i

## 1 Introduction

## 2 Motivation

What is the problem we are targetting? Lack of transparency and control in what?

Why is this problem important?

### 2.1 Lack of Transparency and Control

What do we mean by transparency and control? Why is it important? What is the scope of transparency? What is the scope of control? Transparency includes awareness on *what* our mobile devices do with our information, with *whom* our mobile devices communicate, and *how* our mobile devices interact with other devices on the Internet and the impact of such interaction. Transparency enables the auditing. Control empowers us with the authority to exert our influence on how our devices participate in the mobile ecosystem

Why is there a lack of transparency and control? OSes require control to isolate applications and determine set of OS level services to maximize resource availability – battery life, data quotas etc. Vested interests backed by commercial agreements – preinstalled applications that cannot be removed point to commercial services of ISPs, creators of OS etc. For example, Deezer installed on Orange phones, Google Play on Android device. Advertisement based revenue model encourages opaqueness on how user profiles are built based on privacy leaks.

To whom is this problem interesting?

Why should the reader be interested?

### 2.2 Discussion on Existing solutions

#### 2.2.1 Instrumenting OSes

Taintdroid [2]. AppFence [4]. Eprof [5]. ProfileDroid [8]. mobile Application Resource Optimizer(ARO) [6]. Behavior of applications dependent on APIs provided by OSes. Applications can therefore behave differently Does not cover new OSes. Violates terms and conditions making it impractical for end-users.

#### 2.2.2 Instrumenting Applications

PIOS [1]. AppInsight [7] Limited applications. Does not consider application updates. Requires connections to specific stores with limited number of applications.

#### 2.2.3 Logging Application Behavior

[3]

#### 2.2.4 Traffic Logs From ISPs and Wi-Fi Gateways

Limited network coverage. Restricted to specific ISPs and access technologies. Region specific applications are not covered.

## 3 Goals

[**TBD: For each goal, What does it mean followed by why is it important?**]

1. *Deployable.* Easy to install/use/configure. It must not require warrant voiding of the device. This is important to support a large user-base.
2. *On-demand.* The user must be able to enable and disable service easily. It must be easy to fallback to the original state. This is important to ensure that users can easily opt-out and are not blocked if there are some problems with the system.

Figure 1: Figure showing traffic redirection and flow of traffic through VPN and HTTP proxy

3. *Agnostic to OS, ISP, access technology, and applications.*. The research work that comes out must not be limited to specific OS, ISP, or device manufacturer, or set of applications.
4. *Scalable.* Can support many users. To ensure that research results have statistical significance.
5. *Always On.* Capable of monitoring and controlling all the Internet traffic once the user enables the system. This is important to ensure passive and pervasive operations that do not demand periodic inputs from end-users.
6. Flexible - supports many services
7. Reliable - always works
8. Safe - does not adversely affect traffic (interaction between modules)
9. Secure - handles user data with care

# 4 Platform Description

We take an approach of traffic redirection. Proxying internet traffic meets above goals. Issues with network perspective of traffic

## 4.1 Architecture

Architecture as shown in Figure 1.

Explain two Proxies, one VPN and other HTTP.

Explain how each goal is met and why we need two proxies.

The role of the VPNs Proxy. VPNs allow tunnel everything (all IPv4 traffic). All IPv4 traffic can be monitored and controlled on the middlebox.

The role of HTTP Proxy. Check ISP interference. What How tripwires are implemented.

Configuration requirements. All iOS devices (version 3.0 and above) support *VPN On-Demand*, which forces traffic for a specified set of domains to use VPN tunnels. To ensure all possible destinations match this list, we exploit the fact that iOS uses suffix matching to determine which connections should be tunneled; accordingly, we specified the domain list as the set of alphanumeric characters (a-z, 0-9, one character per domain). Android version 4.2 and above supports an *Always On VPN* connection that provides the same functionality; for Android version 4.0 and above there is an app API that allows apps to manage VPN tunnels. We support both options.

[**AR:TBD:** ] x axis contains Android iOS — Android iOS — Android iOS — Android iOS
Location 1 — Location 2 — Location 1 — Location 2
Wi-fi — Cellular With error bars for min and max.

Figure 2: Latency Overheads. Tests performed by Adrian and Sam

## 4.2 Existing Deployment

Where is this currently deployed?

What is the objective of this deployment?

Who are the ones signed up?

What was the incentive given?

## 4.3 Overheads

1. **Increase in Network Latency.**

   Figure 2. Cite results from latency to home gateways based on DSL results in PAM and IMC.

2. **Increase in Power Consumption.** Results from battery tests performed by Dave for Android battery monitoring tests performed by Ashwin for Android and iPhone.

3. **Increase in Traffic Volume.**

## 4.4 Limitations

1. **At most one tunnel.** [**TBD: Not true for http proxy**] Currently iOS and Android support exactly one VPN connection at a time. This allows *Meddle* to measure traffic over either WiFi or cellular interfaces, but not both at once. The vast majority of traffic uses only one of these interfaces, and that interface uses the VPN

2. **Proxy location.** When traffic traverses the *Meddle* box, destinations will see the *Meddle* box address, not the device IP, as the source. This might impact services that customize (or block access to) content according to IP address (e.g., in case of localization). A solution to this problem is to use a *Meddle* instance with an appropriate IP address

3. **ISP support.** Some ISPs block VPN traffic, which prevents access to our current *Meddle* implementation. We note that few ISPs block VPN traffic, and there is an incentive not to block VPN traffic to support enterprise clients.

4. **IPv6.** *Meddle* cannot be currently used on networks using IPv6 because IPv6 is not fully supported by mobile devices. Indeed, we observe that though iOS

and Android support IPv6 they currently do not support IPv6 traffic through VPN tunnels

## 4.5 Costs

1. **Deployment and Running Costs**

2. **Trust Provider**

## 4.6 Incentive for End-user Deployment

1. **Deploy on Home Gateway.** This is why we need the single machine constraint.

2. **Packet Filtering.** Custom ad blocks. Protect against data leaks.

3. **Security from untrusted Wi-Fi APs.**

4. **Modular Architecture for Offloading Activities.**

# 5 Evaluation

# 6 Conclusion

# References

[1] EGELE, M., KRUEGEL, C., KIRDA, E., AND VIGNA, G. PiOS: Detecting Privacy Leaks in iOS Applications. In *Proceedings of the Network and Distributed System Security Symposium* (2011).

[2] ENCK, W., GILBERT, P., CHUN, B.-G., COX, L. P., JUNG, J., MCDANIEL, P., AND SHETH, A. N. TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones. In *Proc. of the USENIX Operating Systems Design and Implementation (OSDI)* (2010), pp. 1–6.

[3] FALAKI, H., MAHAJAN, R., KANDULA, S., LYMBEROPOULOS, D., GOVINDAN, R., AND ESTRIN, D. Diversity in Smartphone Usage. In *Proceedings of the International conference on Mobile systems, applications, and services (Mobisys)* (2010), pp. 179–194.

[4] HORNYACK, P., HAN, S., JUNG, J., SCHECHTER, S., AND WETHERALL, D. "These Arent the Droids Youre Looking For": Retrofitting Android to Protect Data from Imperious Applications. In *Proc. of CCS* (2011), pp. 639–652.

[5] PATHAK, A., HU, Y. C., AND ZHANG, M. Where is the energy spent inside my app? Fine Grained Energy Accounting on Smartphones with Eprof. In *Proc. of Eurosys* (2012).

[6] QIAN, F., WANG, Z., GERBER, A., MAO, Z., SEN, S., AND SPATSCHECK, O. Profiling Resource Usage for Mobile Applications: A Cross-layer Approach. In *Proc. of MobiSys* (2011).

[7] RAVINDRANATH, L., PADHYE, J., AGARWAL, S., MAHAJAN, R., OBERMILLER, I., AND SHAYANDEH, S. AppInsight: Mobile App Performance Monitoring in the Wild. *Proc. of the USENIX Operating Systems Design and Implementation (OSDI)* (2012).

[8] WEI, X., GOMEZ, L., NEAMTIU, I., AND FALOUTSOS, M. ProfileDroid: Multi-layer Profiling of Android Applications. In *Proc. of MobiCom* (2012).