Meddle: Controlling and Characterizing Mobile Network Traffic

David Choffnes, Justine Sherry, Ashwin Rao, Arnaud Legout,
Arvind Krishnamurthy, and Walid Dabbous.

We present Meddle, a platform that provides control and transparency for mobile network traffic without requiring any operating system modification. This platform can improve visibility into mobile networks and enables a wide range of new experiments in this space. We would like to get feedback on Meddle from researchers attending IMC and recruit them to participate in an IRB approved measurement study.

Meddle is motivated by the following characteristics of today's mobile systems. Currently users have little control of how their devices use the mobile networks they pay for. In the mobile environment, users are forced to interact with a single operating system tied to their device, generally use closed-source apps provided for the OS that routinely violate user privacy [2], and subscribe to network providers that can (and do) transparently modify, block or otherwise interfere with network traffic [3].

Researchers face a similar set of challenges for characterizing an experiment for mobile systems. To characterize mobile traffic and design new protocols and services that are better tailored to the mobile environment, we would like a framework that allows us to intercept and potentially modify traffic generated by mobile devices as they move with users, regardless of the device, OS or carrier. However, implementing this functionality is difficult on mobile devices because it requires warranty-voiding techniques such as jail breaking to access and manipulate traffic at the network layer [1]. Even when using such an approach, carriers may manipulate traffic once it leaves the mobile device [3], thus rendering some research impractical. Last, some protocols and services should be implemented in the network instead of the device (e.g., prefetching and security filters) but researchers generally have no ability to deploy such solutions.

In this presentation, we will show that we can provide the necessary framework to simultaneously address these issues for users and researchers by using middleboxes accessible through VPN tunnels, an approach we call Meddle. Once packets arrive at VPN servers, we can use a variety of middlebox approaches to transform traffic to and from mobile devices. This enables new research in both measuring and characterizing mobile traffic, and designing new in-network features to improve the mobile experience. In addition to avoiding transparent interference from any middleboxes inside mobile carrier networks, Meddle enables researchers to investigate what-if scenarios for the impact of new middleboxes as if they were deployed in carrier networks.

To obtain a large number of participating users for characterization and experimental evaluation, we need to explicitly align the goals of researchers and users. Meddle offers sufficient incentives for users to adopt the service by offering device-wide ad-blocking, privacy/security filters and parental controls at the network layer – functionality that mobile network providers do not currently make available.

We are currently using our prototype Meddle architecture to build out a system for public deployment. We are also recruiting users for an IRB-approved study.

References

[1] 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 USENIX OSDI* (2010).

[2] Hornyack, P., Han, S., Jung, J., Schechter, S., and Wetherall, D. These aren't the droids you're looking for: retrofitting android to protect data from imperious applications. In *Proc. of CCS* (2011).

[3] Wang, Z., Qian, Z., Xu, Q., Mao, Z., and Zhang, M. An untold story of middleboxes in cellular networks. In *Proc. of ACM SIGCOMM* (2011).