# Dispatch: Secure, Resilient Mobile Reporting

Kanak Biscuitwala[*]
kanak@cs.stanford.edu

Willem Bult[*]
wbult@stanford.edu

Mathias Lécuyer[†]
ml3302@columbia.edu

T.J. Purtell[*]
tpurtell@cs.stanford.edu

Madeline K.B. Ross[‡]
mkr2132@columbia.edu

Augustin Chaintreau[†]
augustin@cs.columbia.edu

Chris Haseman[§]
haseman@tumblr.com

Monica S. Lam[*]
lam@cs.stanford.edu

Susan E. McGregor[‡]
sem2196@columbia.edu

[*]Computer Science Department, Stanford University
[†]Computer Science Department, Columbia University
[‡]Graduate School of Journalism, Columbia University
[§]Tumblr, Inc.

## Categories and Subject Descriptors

C.2.4 [**Computer-Communication Networks**]: Distributed Systems—*distributed applications*

## Keywords

Mobile publishing; Disconnection resilience

## 1. INTRODUCTION

The rise of social media and data-capable mobile devices has transformed global journalism. Brief, text-based and easy to translate, social messages allow the public to skip the middleman and get news "straight from the source."

Whether used by "citizen" or professional reporters, however, social media technologies pose risks that endanger users. First, social media platforms are often proprietary, exposing users' data and activities to scrutiny from collaborating companies and governments. Second, the online networks that citizen reporters use are inherently fragile, consisting of easily targeted devices and relatively centralized message-routing systems that authorities may block or shut down. Finally, this same privileged access can be used to flood the network with inaccurate or discrediting messages, drowning the signal of real events in misleading noise.

A citizen journalist is someone who is simply **in the right place at the right time**. Untrained and unevenly tech-savvy, citizen reporters may not consider social media activities high-risk. **The dangers citizen journalists face are personal and physical**. Addressing their needs for protection, resilience, and recognition requires a move away from assumptions of *in vitro* communication security.

Our response to this pressing need is *Dispatch* project[1]. Dispatch allows citizen reporters to publish text and images using authenticated pseudonyms. Dispatch is built on the Egocentric Social Platform (ESP) [5], as well as the Musubi platform [2], allowing for encryption based on virtual identities while presenting a *feed-based interface*. ESP utilizes Identity-Based Encryption (IBE) [1] to avoid key exchange difficulties. Dispatch also provides censorship-tolerant functionality in the form of Bluetooth message passing when there is no Internet connection. With stable iOS and Android versions, Dispatch provides secure, networked publishing and communication tools to the journalism community.

[1]see `http://dispatchapp.wpengine.com`


*SIGCOMM'13,* August 12–16, 2013, Hong Kong, China.
ACM 978-1-4503-2056-6/13/08.

## 2. DISPATCH IMPLEMENTATION

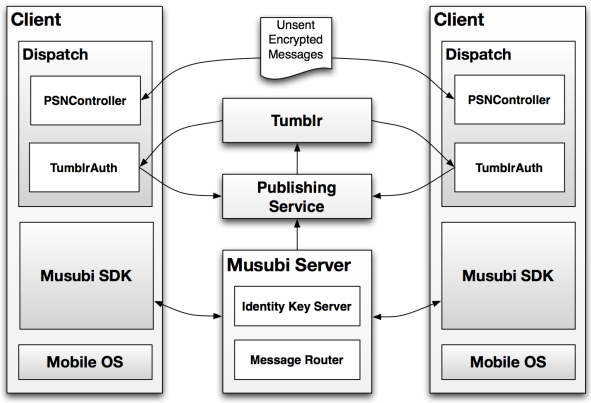


**Figure 1: Dispatch Architecture**

### 2.1 Secure Communication

On ESP, messages are encrypted end-to-end with IBE, allowing users to encrypt messages without exchanging public keys beforehand. Boneh and Franklin discovered a method to perform identity-based cryptography using Weil pairings [1]. Hess showed in [3] how a signature scheme can be enabled without accessing the trusted party for each message.

A *message router* routes encrypted messages based on hashed identities and cannot identify users using anonymous pseudonyms or view or modify messages. Thus, Dispatch messages are organized into disintermediated feeds which ensure that only mobile devices have access to the raw content. A key property of IBE is that because keys can be derived from identities, messages can be sent to a recipient even before the recipient has started using the application.

### 2.1.1 Virtual Identities

We call the identifier that a user chooses her *virtual identity*. In Dispatch, the virtual identity is a handle selected by the user the first time she logs in to Dispatch. Because it is anonymous, a separation between the virtual identity and the reporter's real identity is achieved.

Messages can be addressed to anyone, although the common candidates are the virtual identities of other reporters and the virtual identities owned by *publishing servers*. A one-way SHA-256 hash function is applied over the virtual identity, to further protect the identity inside the system. Because of the negligible probability of hash collisions [4], the hashed identifier is available to use as a unique property of the reporter, allowing her to establish a reputation based on the content she anonymously delivers.

## 2.2 Publishing Server

The publishing server securely receives content intended for publishing. It can then either automatically post the content, or support human review before posting.

The key component of the publishing server is an Android device that runs the same software as the client. The software is able to leverage ESP to securely receive messages and report success and failure status, if the publisher desires, and has the same user-friendly interface should human review be required. A publisher can send high-level object types that map well to object types provided in publisher APIs to have them posted by the publishing server. A second benefit to using the Dispatch Android software is that it has few system requirements, ensuring that it can be installed and used virtually anywhere. Furthermore, by adding the server as a group user, the server becomes addressable and reachable even its IP address changes. Content can be securely disseminated to any number of publishing endpoints over ESP.

## 2.3 Bluetooth Message Forwarding

In the unstable regions that Dispatch targets, interrupted infrastructure is a significant risk. The unavailability of Internet access may be caused by a number of forces, including short range Internet jamming, nationwide Internet cut-offs, or IP address blockage at central hubs by governments.

### 2.3.1 Forwarding Protocol

Dispatch addresses this problem building on two important notions. Fundamental to our approach is the concept of Content Based Routing (CBR). Because the messages in ESP contain the hashed recipient identity in the payload, the messages can be routed through arbitrary means.

The second notion that underlies our solution is that in the absence of infrastructure, human mobility can be used to transport messages. In Dispatch, we have developed a "sneakernet" where Dispatch users physically carry messages to aid in forwarding. Messages are routed from device to device by explicit handoff, until eventually a "gateway" device reaches global connectivity and can deliver the message to the message router. When two users meet, they transfer unsent messages amongst themselves. These meeting points form the "hops" in our network.

It is important to note two properties of this protocol. First, because the messages are signed and encrypted, they can not be read nor tampered with by any user serving as a message carrier. Secondly, messages that a user transports for someone else, which are not addressed to that user, can not be viewed in raw form on that user's device. This saves him from being implicated by the message content.

### 2.3.2 Implementation on iOS

The "sneakernet" in the iOS version of Dispatch allows users to explicitly exchange unsent messages. This way, a user can select people he trusts to transport the messages, alleviating the risk of malicious flooding in the system by adversary parties. To initiate the transfer, both parties simply push a button inside the app and follow a guided pairing process. This establishes an ad-hoc peer-to-peer Bluetooth connection between the two phones and then transfers all unsent messages both ways.

After a transfer, the message contents remain signed and encrypted, and the hashed identifier of the recipient is still present in the message. Thus, to publish, only one of the devices must be able to reach connectivity to the message router. At that point, the device will automatically transmit the messages it currently carries. Each device and the message router will automatically remove duplicate messages.

# 3. CONCLUSION

Dispatch is an application that simultaneously seeks to provide protection and usability for both professional and citizen journalists. It is built specifically for conflict reporting scenarios, allowing for dissemination of content quickly and in such a way that is resilient to Internet disconnection. Dispatch is designed so that components including the key issuer, publishing server, and message router can be deployed privately, ensuring that reporting organizations or community groups can control the visibility of the content.

Development of Dispatch is a work in progress. However, as the journalism community begins to adopt Dispatch and incorporate it into reporting workflows, the resulting feedback will serve to continuously improve the platform. The ultimate goal of Dispatch is to create an intuitive reporting tool that can be used in any situation of any threat level.

# 4. ACKNOWLEDGEMENTS

Dispatch is an inaugural recipient of a "Magic Grant" from the Brown Institute of Media Innovation. Our research is also supported in part by NSF Programmable Open Mobile Internet (POMI) 2020 Expedition Grant 0832820 and the Stanford MobiSocial Computing Laboratory.

# 5. REFERENCES

[1] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. In *Advances in Cryptology - CRYPTO 2001*, pages 213–229. Springer, 2001.

[2] B. Dodson, I. Vo, T. Purtell, A. Cannon, and M. Lam. Musubi: Disintermediated Interactive Social Feeds for Mobile Devices. In *21st International WWW Conference (WWW2012)*, 2012.

[3] F. Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography*, pages 310–324. Springer, 2003.

[4] National Institute of Standards and Technology. *Secure Hash Standard (SHS)*, March 2012.

[5] T. Purtell, I. Vo, and M. Lam. A Mobile Social Network on ESP: an Egocentric Social Platform. `http://mobisocial.stanford.edu/papers/pets12.pdf`, 2012.