A Privacy-Preserving and Overhead-Free Protocol for Direct Donations to People Impacted by COVID-19 Lockdowns

Chang Liu
School of EECS, Ohio University
Athens, Ohio 45701, U.S.A.
liuc@ohio.edu

Lisa Liu
Athens High School
Athens, Ohio 45701, U.S.A.
lisaliu041@gmail.com

2020 IEEE Global Humanitarian Technology Conference (GHTC) | 978-1-7281-7388-7/20/$31.00 ©2020 IEEE | DOI: 10.1109/GHTC46280.2020.9342887

***Abstract*—COVID-19 caused large-scale, long-lasting lockdowns in many parts of the world, which resulted in many people in need for financial or other aids. Governments, charities, and communities rushed to provide help. To complement these efforts and to provide direct assistance to individuals who may not get sufficient and/or timely assistance otherwise, we designed a privacy-preserving and overhead-free protocol named "Fireside Help" for matching donors and people-in-need. This protocol aims to provide maximum privacy protection. Only the assigned volunteer verifiers can know about details of the applications from people-in-need and the donations from the donors that they verified. No one else, including the Fireside Help system itself, can gain any knowledge beyond digital checksums and information intentionally made public. This protocol uses proven, free, and widely available hash functions such as SHA-256, SHA-1, or MD-5 to ensure the integrity of the system without revealing private information. The protocol was designed initially to help students in Wuhan, China, the very first city to lock down. Later, it was revised to help anyone around the world who has been impacted by COVID-19. Several real-world transactions were completed in the system that demonstrated its utility and robustness.**

***Index Terms*—Privacy, hash functions, donations, COVID-19**

I. Introduction

Many organizations, both large and small, are providing assistance to workers who have been unemployed due to COVID-19, but both face problems when it comes to timely, efficient, secure, privacy-preserving, and need-matching donations. To address these issues, we designed Fireside Help, a privacy-preserving and overhead-free way of donating money or services directly to people-in-need that is trustworthy, efficient, and overhead free. There are safeguards designed to check information and protect the privacy of donors and recipients. This approach was tested in the real world during the COVID-19 pandemic and successfully supported several donation transactions that protected the privacy of both the recipients and the donors.

II. The Fireside Help Protocol Design Goals

The Fireside Help donation protocol is designed to offer maximum protection to the privacy of recipients and donors, require minimum overheads for donation transactions, and allow future scalability. In addition, this protocol allows people-in-need and donors to learn about each other's situations directly and facilitate accurate, need-matching, and targeted donations.

1) Privacy Protection: With Fireside Help, people-in-need only need to reveal their locations, so the system can assign local volunteer verifiers who are better positioned to perform the verification. Location information can be general, such as a city (e.g. Wuhan, China) or even a state (e.g. Ohio). With potentially over 10 million people in one location such as Wuhan, making this information public reveals minimum privacy.

The next piece of information that people-in-need often reveal is a free-form description of the situation. This is optional in the Fireside Help protocol, meant only for addition reference when donors make a donation decision. Help seekers have full control of what is put in the description, only revealing what is comfortable to them and letting them preserve their privacy.

Key private information about the help seekers remains in their own hands, including their names, contact information, and payment acceptance method. Only checksums of this information will be made public in Fireside Help, so others can check them later for frauds.

Donors can choose how their names are recorded in the system. Donors will need to reveal their contact information to contact the assigned verifiers and potentially reveal their financial payment methods to the recipients when making a direct donation. Nothing else is revealed or recorded in the system.

In summary, Fireside Help provide maximum privacy protection to both help seekers and donors. However, the privacy of volunteer verifiers are not protected. Their contact info will be publicly recorded in the system so that help seekers and donors can contact them privately. This is acceptable because the verifiers knew about this before they volunteered and this is a way to ensure that the system remains fair and just, and each transaction in the system is associated with an accountable person.

2) Zero Overhead: In Fireside Help, the donation transactions take place directly between donors and people-in-need. No third parties, including the Fireside Help system itself, are

involved. Therefore, there is zero overhead and zero risk of funds being cut in the middle of a transaction. This is not to say that the Fireside Help system itself is free. It does take time and resource to maintain the system and make the records permanently and publicly available. It will be costly if we in the future automate the system in software. For each transaction, though, Fireside Help is overhead free.

3) Future Scalability: The current Fireside Help system is manually operated and deployed on GitHub as a git repository[1]. It apparently will not scale well with the manual operation. If in the future it is automated with a software platform with mobile apps and Web apps, the protocol can be highly scalability because there is no inter-dependency between different transactions. All transactions can be processed independently and therefore allow for linear scalability.

III. The Fireside Help Protocol

The Fireside Help Protocol went through two revisions, first to help students-in-need in Wuhan, China, and later expanded to help all people-in-need from around the world. There are currently two procedures for donation, one initiated by the recipient and the other by the donor. Both procedures require public information to be recorded in the GitHub repository, which is also referred to as the system, while private information will be kept by the owner and only shown to assigned verifiers for verification purposes.

Both procedures involve three parties: the donor, the recipient, and the verifier. The donor donates the money, the recipient receives the money, and the verifier acts as the intermediary between the donor and the recipient, as well as confirming the validity of the information. The money is directly transferred from the donor to the recipient without an intermediary, leaving no room for overheads when it comes to the money itself.

To preserve the parties' privacy as much as possible, proofs of information verified directly outside the Fireside Help system and encoded in SHA-256, SHA-1, or MD-5 codes are permanently recorded in the Fireside Help system.

A. People-in-need initiatives

Initially, we only targeted middle school students in Wuhan, China, so the following procedure may contain specific references to a student's information. The recipient requirements have since been updated to encompass more people. First, the recipient must submit an application, with two parts: private (name, contact information, optional information) and public (location, description, verification codes (SHA-1 or MD-5) for required information and QR code for payment).

Next, a volunteer is randomly selected according to location to be the verifier. The verifier will complete the following: provide location to facilitate selection and matching process, post contact information publicly so donors and recipients can contact him/her, generate an anti-double-dipping code (using school class and recipient's name) to prevent a recipient from applying repeatedly (code is recorded, but actual information is not), send recipient's payment QR code to donor, update chosen name of donor in system, agree to keep both parties' information confidential, and delete relevant information after the donation is completed.

Donors can choose the amount they donate, allowing for multiple donors' donations to be pooled for one recipient. The donor will do the following: choose a verified recipient, contact the recipient's verifier, get the receipt QR code, check the receipt QR code against the public receipt QR code (to prevent the verifier from secretly sending a different QR code to receive the donation), directly transfer the money to recipient, preserve proof of payment (through screenshots or otherwise), and pick a name to be displayed publicly. After the above processes complete, the recipient's entry on GitHub will be marked as complete by the verifier.

Two donation transactions initiated by people-in-need had been completed in Fireside Help. Two anonymous student families from Wuhan negatively impacted by COVID-19 received 1000 RMB (about 140 USD) each from three donors.

After the system was expanded to serve people outside the initial COVID-19 hotspot, another people-in-need initiated transaction was posted. The request was to seek shipping fee to ship over 10,000 donated masks from China to the United States. The request was verified and donors contacted the verifier to pledge support beyond that amount. Ultimately, donations did not happen for this transaction, because the applicant found an alternative source to cover the shipping cost before the transaction is completed. This shows that the protocol was robust and flexible enough to support complex transactions in the real world. The verifier can ensure that donations from multiple donors would not exceed the requested amount and that money would not change hands if the situation changed and the donation was no longer needed.

B. Donor initiatives

The system was later expanded to support donor initiated transactions. An example of the donor-initiated donation was the 140 USD commitment from a donor in the Fireside Help system that was already independently verified. It is currently waiting for a recipient.

C. How to interact with the Fireside Help system

Instructions for how to apply as a donor, an applicant, or a verifier are listed in a document in the Fireside git repository[2]. A key technical step involves checksum generation. SHA-256, SHA-1, or MD-5 checksums can be generated in many ways. For example, on Mac, free utility programs (*md5* and *openssl*) can be used to generate these checksums for any files.

To post the public application or pledge info to the Fireside Help system, tech-savvy people can directly work on the public GitHub repository[3]. One popular way to contribute to a public Git repo is through Git pull-requests.

[1] https://lisasiliu.github.io/FiresideScienceChat/Donations

[2] https://lisasiliu.github.io/FiresideScienceChat/Donations/Donations.docx

[3] https://github.com/lisasiliu/FiresideScienceChat