Safe aid: Protecting privacy in humanitarian operations

May 26 2023, by Tanya Petersen

ICRC humanitarian aid distribution. Credit: ICRC / EPFL 2023

EPFL researchers have worked with the International Committee of the Red Cross (ICRC) to develop a first of its kind, digital system to support humanitarian aid distribution. The design uses tokens to decentralize the storage and processing of recipients information, reducing the risk of harm, and uses advanced cryptography to enable accountability.

Humanitarian organizations exist to protect and assist the victims of violence, famine and disaster. One key area of their work is the distribution of goods such as food and blankets in emergencies. Traditionally, paper-based lists have been used to support aid-distribution and, while practical, do not scale well and at times are easy to circumvent.

Humanitarian organizations see digital solutions a promising way to address these issues; however, to date, these have relied on collecting significant amounts of recipient data. This may jeopardize recipient safety and can complicate the relationship of humanitarian organizations with local authorities. For example, in Yemen, the World Food Program clashed with Houthi authorities because of the disagreement over the use and control of biometric data. Ethically, it's also questionable whether gathering the personal information of vulnerable people is acceptable, given the risks that it entails for them.

For more than 12-months, researchers from the Security and Privacy Engineering Laboratory (SPRING) in the School of Computer and Communication Sciences (IC) partnered with staff in the ICRC Data Protection Office to gain a deep understanding of the humanitarian context.

"The ICRC field experts brought a lot of new perspectives, giving us a realistic and detailed view of the whole aid distribution program, which was critical for us to design the system. For example, we learned about their strong accountability requirements because of the need to maintain transparency as a humanitarian organization. The information required to fulfill this requirement is in conflict with the need for privacy to preserve the safety of recipients," said Boya Wang, Doctoral Assistant in the SPRING Lab and first author on the paper outlining the work.

"I've learned a lot from the collaboration with the ICRC in this project.

As a junior researcher, when I read papers about privacy-preserving system design, the process seems to be linear: abstracting the problem, summarizing the requirement, then proposing a design. But the real process was different. We designed, got feedback, amended, got feedback. We really needed a lot of iterations to find a solution that took account of all the trade-offs between the different requirements," she continued.

The new privacy-preserving humanitarian aid distribution system needed to address several other challenges identified with the ICRC. Most aid-distribution programs take place in crisis affected settings where there is often no last-generation hardware or internet connectivity so it had to avoid relying on these. As well, aid distribution systems are not targeted at individuals, they must permit aid allocation to households with several members, yet they must ensure that households can only request aid once per distribution round.

"We created two system design alternatives, the first on a smartphone, for situations in which recipients have access to one, and the second on a [smart card](), for when the ICRC needs to distribute cheap tokens in the field," explained Assistant Professor Carmela Troncoso, Head of the SPRING Lab and also an author on the paper., "We also demonstrate that these two alternatives are secure, and can easily scale to cover the needs of the ICRC in the field."

"In the Data Protection Office we monitor the implementation and application of the responsible use of personal data and provide recommendations on its use in ICRC operations. With this novel project, we have seen how impactful it is when solutions are designed for protecting individual privacy from the very start," said Justinas Sukaitis, Data Protection by Design Technology Adviser at the ICRC. "Nonetheless, there are some significant steps ahead for this system as, even though the theory and lab experiments hold, we need to do the

feasibility study on our end as we never test on people whose lives may be affected by a last minute bug," he continued.

Despite the challenges of the work, Troncoso believes the partnership shows that for computer scientists, collaboration with organizations can bring a lot of space and creativity in generating novel methods for research. "Working hand in hand with stakeholders, in this case the ICRC, is always very rewarding. Not only do we get to work on designs that can impact the life of people in need, but we also discover new scenarios that allow us to produce high-quality research."

Wang has also found the experience very positive and says it has helped her to realize that science is not really at arms' length from the everyday world. "As computer scientists we may think that we are distanced from a lot of problems, but I believe we are closer than we usually think. For me, it is important to understand the real need in the context and to reflect the societal aspects of our research. I would like to keep this kind of spirit in my future work."

Sukaitis was impressed with how the SPRING Lab could distill the ICRC's requirements to their core essence, a crucial but often times not evident task. "We want to adapt this type of approach for our own assessments. As an EPFL computer science alumni myself, I can say that the humanitarian field is an extremely rewarding and interesting field for engineers, and I wish more people from Computer and Data Science would join the ranks of humanitarian engineers."

The paper, "Not Yet Another Digital ID: Privacy-preserving Humanitarian Aid Distribution" received a Distinguished Paper Award at the 2023 IEEE Symposium on Security and Privacy in San Francisco, a forum for developments in computer security and electronic privacy. It is available on the pre-print *arXiv* server.