Security and resilience of collaborative applications

Statement of proposed research — Martin Kleppmann

Background

In recent years, the Internet has enabled the creation of many services for communication and collaboration: for example, we use Google Docs to collaborate on documents, spreadsheets and presentations; we maintain social contacts via Facebook; we copy files between devices using Dropbox; and we communicate with colleagues using Slack. Individuals and businesses depend on these and many other online services, e.g. for task tracking, note taking, project planning, and knowledge management. As we move towards a digital economy, these services are becoming crucial machinery for the functioning of society.

While these services are very valuable and convenient, their use also carries risks, because they are provided through a centralised server infrastructure. If the company providing the service goes out of business, or decides to discontinue a product, the software stops working, and users are locked out of the documents and data created with that software. Servers are also vulnerable to disruption by denial-of-service attacks.

Moreover, since those servers typically process user data in unencrypted form, a rogue employee, or a hacker who gains access to the servers, can read and tamper with vast amounts of sensitive data. The provider may also allow the data to be used in problematic ways, as exemplified by the Cambridge Analytica scandal about the misuse of personal data collected by Facebook.

When these risks are unacceptable, we can fall back to what we might call "old-fashioned" collaboration methods: for example, one person creates a spreadsheet with Excel and emails it to their collaborator, who makes changes and then sends the modified file back again by email. This approach has merits: it does not rely on any external services that might go away (besides the email infrastructure), and the file can easily be encrypted. However, it quickly becomes messy if the file is modified by more than one person at a time.

Research goals and impact

This fellowship will develop the foundations for collaboration software that achieves the best of both worlds: allowing the user-friendly real-time collaboration of applications like Google Docs, in which several people can make changes simultaneously without suffering conflicts, but without relying on centralised servers.

While most of today's Internet services keep the primary copy of the shared data on a server, my approach stores primary copies of the data as files on the collaborators' devices, like in "old-fashioned" collaboration. Servers may still be used, but rather than being a linchpin, they become an optional enabling component. Because all the data is local, the software continues working, even when the device has no Internet access or the servers are unavailable. When a user modifes a document, the software in my approach automatically sends the changes to collaborators whenever a network connection is available, so there is no need to email files back and forth.

My proposed approach allows multiple users to make changes to the same document concurrently, even while users are offline, and ensures that all of the changes are automatically merged into a consistent result. In this regard it differs from version control systems such as SVN or git, which are used by software developers to manage changes to files: such systems require conflicts to be resolved manually, and only offer merging of plain text files. By contrast, my approach performs all merges automatically, and is able to support arbitrarily complex file formats such as spreadsheets, CAD drawings, or databases with various data models.

Collaborators' devices can either communicate directly, using fast local networks in a *peer-to-peer* manner, or indirectly via servers. To protect the confidentiality and integrity of the communication between collaborators I propose using *end-to-end encryption*. In this approach, if servers are used, they only ever handle encrypted data that they cannot decrypt. Thus, even if communication networks or servers are compromised by an attacker, user privacy and data confidentiality are protected. This approach is particularly suitable for sensitive data such as a university's student records, a hospital's patient records, legally privileged communication, journalistic investigations, law enforcement, diplomatic correspondence, and many other settings where regulations and confidentiality obligations prohibit the sharing of unencrypted data with third parties.

To maximise the impact of this research, I plan to publish the results in two forms: as traditional research papers in top-tier academic venues such as SIGMOD and VLDB, and in the form of software. The software created during this fellowship will be made freely available as open source, and I hope to develop the protocols into open industry standards. My goal is to create the foundational technologies upon which the next generation of secure, resilient collaborative applications will be built, thus revolutionising the implementation of Internet services. Through my high-profile public presence in industry I will draw attention to my research outputs, and grow a community of software developers who will build upon the foundations that I create. I believe that my combination of industrial open source experience, my research track record, and my proven communication and public speaking skills make me uniquely positioned to successfully realise this vision.

Timeliness and novelty of the proposed research

Today, end-to-end encryption is used by messaging applications such as WhatsApp and Apple's iMessage to protect the data of over 1 billion users, which demonstrates that these security technologies can be deployed at massive scale without requiring users to be technical experts. However, these protocols are designed only for messaging, and do not work for other forms of collaboration, such as working together on a document or sharing access to a database. In the proposed research I am, for the first time, bringing end-to-end encryption to collaborative applications.

The collaboration algorithm used by Google Docs (Operational Transformation) fundamentally relies on a centralised server, and cannot be used in a peer-to-peer setting. Moreover, it requires that Google's servers process unencrypted data, and is therefore incompatible with end-to-end encryption. The same is true of most other existing collaboration systems.

Collaboration algorithms for peer-to-peer settings have proved very challenging to devise: despite peer review, all five such algorithms published in the scientific literature between 1989 and 2004 subsequently turned out to be fatally flawed – they do not satisfy their purported consistency properties [4]! The problem has only been solved in the last few years through the invention of Conflict-Free Replicated Data Types (CRDTs) [5]. I was the first to produce a formal proof of correctness of a CRDT for document collaboration [1], and the first to develop a CRDT for compound data structures (JSON, XML) that are required for advanced applications [3].

Programme of work

As described under "Details of current and past research" above, I have been working on CRDTs since 2015. While the initial results have been very promising, there are still several open problems in CRDT research (both theoretical and practical aspects) that need to be solved before the technology is ready for widespread adoption. During the proposed fellowship I plan to build upon my existing work on Automerge [2] to address these open problems. Specifically, I plan to work on the following problems:

- To improve the performance and efficiency of CRDTs (in terms of memory, CPU, and network bandwidth), making them competitive with centralised approaches;
- To define *move* and *undo* operations for CRDT trees, which are required by many applications, but which are poorly understood and not implemented by most CRDTs;
- To strengthen the security properties of CRDTs by integrating them with secure messaging protocols providing end-to-end encryption and data integrity guarantees;
- To introduce a mechanism for applications to define custom datatypes whilst guaranteeing data consistency, and a schema language for describing the structure of the data;
- To develop storage, search, and indexing facilities for CRDTs, enabling the management of large datasets and large numbers of devices;
- To establish collaborations with researchers and software developers in fields that would benefit from secure and resilient collaboration technology, such as medical records management and journalistic collaboration tools, and to apply my research to those domains.

Through the fellowship I hope to establish myself as an independent researcher and build a track record that paves the way to a permanent research position (in Cambridge or another leading research institution). I hope to grow the team through further funding and collaborations, both within academia and through my strong connections to industry.

References

[1] V. B. F. Gomes, M. Kleppmann, D. P. Mulligan, and A. R. Beresford. Verifying strong eventual consistency in distributed systems. *Proceedings of the ACM on Programming Languages*, 1(OOPSLA), Oct. 2017. doi:10.1145/3133933.

[2] M. Kleppmann. Automerge, 2018. URL https://github.com/automerge/automerge.

[3] M. Kleppmann and A. R. Beresford. A conflict-free replicated JSON datatype. *IEEE Transactions on Parallel and Distributed Systems*, 28(10):2733–2746, Apr. 2017. doi:10.1109/TPDS.2017.2697382.

[4] G. Oster, P. Urso, P. Molli, and A. Imine. Proving correctness of transformation functions in collaborative editing systems. Technical Report RR-5795, INRIA, Dec. 2005. URL https://hal.inria.fr/inria-00071213/.

[5] M. Shapiro, N. Preguiça, C. Baquero, and M. Zawirski. Conflict-free replicated data types. In *13th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS)*, pages 386–400, Oct. 2011. doi:10.1007/978-3-642-24550-3_29.