Encryption in today’s world

Encryption is a vital means of protecting information and people’s privacy in a world where evermore of our data, messages and personal information is used to deliver highly targeted and valuable digital products. Encryption is also vital for protecting corporate IP and national secrets, yet today it is challenging for different actors to co-operate with one another in a trustless environment.

Facebook’s end-to-end encryption dilemma

Facebook has made it clear the company plans to expand end-to-end encryption across its messaging services so people can ‘be who they want to be online’. This is a worthy objective and online privacy is a precious commodity that is disappearing. However, this move has surfaced a major challenge – how can Facebook offer encrypted messaging services whilst also complying with increasing pressure from governments to allow them access in order to prevent harm (for example by identifying terrorism or abuse).

The US, UK and Australian governments have asked Facebook to include a ‘backdoor’ so government agencies can monitor certain messages. In the UK there have been proposals for security agencies to be blind copied on messages to and from persons of interest. Should governments have an open backdoor into messaging services? That’s a point of philosophy as much as it is technology or cyber security. But practically speaking if a backdoor is implemented then anyone can find it and abuse it, whether it is the government in question, a rouge nation state or a criminal. A backdoor for one, is a backdoor for all. Here at Post Quantum we should know, as we’ve been here already.

PQ Chat and ISIS

In 2014 our firm developed the world’s only ‘quantum-safe’ instant messaging system, we were overjoyed with the achievement. So well encrypted were the users’ messages that not even a mature quantum-computer with its vastly more powerful code-breaking capabilities would be able to decipher the text. We decided to make the system available to all through the Apple app store as an easy to download application – it was a much needed victory for privacy in an age where the exploitation of user data was widely agreed to be out of control. The reality however proved vastly more complex when our application subsequently appeared on an Islamic State recommended technical tools list.

We were aghast. A tool we had developed to help people assert their fundamental human right for online privacy, to help people conduct their lives without the prying eyes of intrusive 'big tech' and to help uphold the enlightenment values of individual liberty had been co-opted by an organisation committed to destroying those very same values. To say this led to intense debate and soul searching amongst our team is a dramatic understatement. Little did we realise at the time but our own experience was a microcosm of the debate that rages to this day, what should be the trade-off between privacy and the protection of citizens from harm?

Quorum: a third way

The PQ Chat experience is why we decided to build a commercial multiparty computing system for protecting data. This uses the development of a technique known as threshold cryptography to split the master key to encrypted data into fragments. There are a pre-defined number of these key fragments that can be shared between stakeholders. The stakeholders can be servers located in different places, protecting a cloud-based system from data breaches.

When setting up the secure system, a number is set at which a quorum is established (say, 3). If 3 out of 7 fragment holders bring their fragments together in consensus then the archive can be decrypted. 3 is the minimum number of fragment holders in this example and it can include any combination from the pool of 7 fragment holders, so long as this minimum number is reached. The system is almost infinitely flexible, a quorum of 3 of 4 fragment holders can be set as easily as a quorum level of 17 of 853 fragment holders.

Beyond the standard security applications of this technique, it can also be used where there are stakeholders outside of the organisation who can be entrusted with key fragments. For example, for legal access requests to Facebook Messenger a fragment of the key might be held by Facebook, the government agency and perhaps a court – this provides a cryptographically secure, verifiable and mutually agreed arrangement to ease the complexity of access requests, whilst significantly limiting the ability of rogue actors to stroll through a backdoor uninvited. This technology already exists today and would allow each access request to be handled 'transparently', with immutability.

Other use-cases for Quorum include:

- A cryptocurrency private key which needs to be recovered should it be lost or corrupted.
    - Key holders: trusted friends and family who are pre-allocated key fragments.
- Regulated industries where archives of trading messages may need to be opened
    - Key holders: regulator, third party escrow agent, company.

- Internet companies where browsing logs may need to be opened for the national security or crime detection purposes.
    - Key holders: FBI, privacy group, law firm instructed to only release a fragment when a warrant is received, company compliance manager.

- Virtual data rooms for merger and acquisition transactions
    - Key holders: Transacting parties including M&A bankers, lawyers and financial PR personnel.