Vision for a backup system with focus on media

October 2, 2015

1 The setup

The setup consists of n people $P_1, \ldots, P_n$ partitioned into m homes, $H_1, \ldots, H_m$. We will work with an example of $n = 6$ people grouped into homes $H_1 = \{P_1, P_2\}$, $H_2 = \{P_3, P_4\}$ and $H_3 = \{P_5, P_6\}$.

Each person P_i owns a range of devices δ_i^j which has the capability of storing files of particular formats such as music files, pictures and documents. Each device is assumed also to have the capability of creating new files locally, e.g. people will take photos with their smartphone or create new documents on their laptop. The devices are to some extent "general purpose", and can be assumed to run a high-level operating system such as Windows, Linux or OS X. In particular, the devices will be laptops, smartphones and tablets, including laptops running OS X, Linux and Windows, Android phones, iPhones and iPads.

2 The desired solution

We are seeking a solution, in which a piece of hardware B (the backup device) is located *somewhere*, e.g. in either of the homes H_i. Device B should be connected to the Internet, such that it is accessible by each person P_i from anywhere in the world.

2.1 Primary functionality

The primary functionality of the system is the *backup capability* which we describe in the following. For each person P_i, it should be possible for each device δ_i^j to define which files on the device (whether they are existing or files that will exist in the future) are to be backed up to the backup device B. We say that such files, that are to be backed up, *satisfy the backup criteria*.

Person P_i should be in control, for each of his devices, whether backup of files that satisfy the backup criteria should happen *automatically* (when new files come into existence) or *manually* (that is, an active choice is made, for example when connected to a high-speed network).

The backup should happen in a *secure* manner. In other words, the transfer of data to/from a device δ_i^j to the backup device B should be encrypted and authenticated, using e.g. TLS. Furthermore, access control should be implemented for the backup device B, such that person P_i can not access the backed up data of person P_j, where $i \neq j$. Encrypted storage of files on device B should be possible, but not necessarily default.

It should be possible for person P_i to give access to a subset of his backed up files, residing on device B, to a range of other people. This becomes important in the next part.

2.2 Nice functionality (in lack of better word)

In this part, we describe a nice feature which is geared towards photos and video which is backed up to the backup device B. We feel that nice photos, for example from a vacation, are not being used in a good way because we do not have a good way to put them to use.

What we would like is the capability for each person P_i to be able to create *albums* that are located on the device B. At an abstract level, such albums should simply consist of pointers to files (photos or video files) that either person P_i has himself backed up to the device B, or is shared by another person P_j (see the sharing capability above).

The software supporting the creation of such albums should reside solely on the backup device B. In other words, a person should require no additional software on his devices δ_i^j to maintain these albums. An ideal way to manipulate such albums residing on the backup device B would be through a web interface. This would also facilitate an easy way of sharing photos with third party people (not involved in the backup system) via the Internet.