Why Logistical Networking is not a Content Sharing Service

Micah Beck
Associate Professor, Computer Science
Director, Logistical Computing and Internetworking Laboratory
University of Tennessee

Technical Report UT-CS-04-516
Department of Computer Science
University of Tennessee

Dec 9, 2003

Logistical Networking is sometimes compared to Peer-to-Peer content sharing services as a means of transferring data between network users. The key point of commonality is that both Logistical Networking and Peer-to-Peer services make use of storage that is not owned or operated by the publisher of the content. In the case of Logistical Networking the intermediate storage takes the form of systems that we call "depots" which support the Internet Backplane Protocol (IBP); in the case of Peer-to-Peer services, the intermediate storage is located in desktop systems of other users.

While there are many differences between Logistical Networking and Peer-to-Peer systems, one key difference is in the steps taken to make sure that the user of Logistical Networking services retains control over the content stored on depots. Storage space allocated on an IBP depot is not given a semantically meaningful name; its only identifier is a long random string that is assigned by the depot itself. Because it is randomly chosen, the identifier cannot be guessed by other users; an allocation made by one user cannot in fact be detected by other users except for an increase in total storage allocation reported by the depot. Even monitoring the network to snoop these random identifiers can be ruled out by using a secure variant of IBP based on SSL.

In contrast, many Peer-to-Peer content sharing systems are designed with the explicit intent of making information public by giving it a meaningful name that can be directly searched by other users. Without passing judgment on the propriety of such systems, it is clear that participation in them assists all users in not simply moving and storing data, but also in making it accessible to all other users.

Given that IBP takes such steps to keep storage allocations private, can data stored there be considered secure? The answer is no, because users have no control over the operators of IBP depots or the network that connects them. True security can only be accomplished by encrypting data before it is written to the depot and decrypting it only after it has been retrieved. The suite of end-user tools called the Logistical Runtime System (LoRS) implement end-to-end security using the standard AES encryption algorithm.

Given that the names assigned by IBP can enable any user who knows them to access data stored on the depot, can data stored in IBP be considered to be public? The answer is no, because as described above, the identifiers cannot be listed, searched or even guessed by any other user. The only way for users to share data is by sharing those identifiers. Data can only be shared when there is a name or searchable attribute associated that is known to more than one user.

Thus, IBP neither protects data securely nor does it publish it publicly; it provides sufficient privacy and control to avoid being a publication service, but sufficient access to support one. It provides the fundamental resources required to implement private, secure sharing of data, but

ultimately leaves security to the end user's system, as is necessary in any scalable, distributed public infrastructure. Like communication on the Internet itself, data storage using Logistical Networking is ultimately a way of sharing resources that is neutral to the intent of the end-user, and seeks only to support the implementation of all applications in the wide area.