RESEARCH NOTES

Server Workings

Brief overview of server workings

---

25 October 2018

Server only ever handles encrypted data, so files are uploaded as a pre-encrypted cipher/binary with metadata only. Similarly files can be downloaded in said encrypted format only, thus the server is safely "dumb" and any attacks on the server would have limited damage since an attacker could not access any data from the binaries.

Obviously metadata **would** be vulnerable, but should not be confidential.

In this case of the server, users would most likely by responsible for the decryption and encryption of resources directly. This would probably be through the use of a CLI tool, with the assumption that users are comfortable with consoles/terminals and most simple(r) CLI tools. This is a fair/justified assumption since users will most likely be Department of Computing Science (DCS) staff and/or students.

A file should show to the user if (and only if) they have certain attributes paired with environment attributes that are compared to a resource's attributes. This show or hide service would rely on the metadata of resources to determine if a user should be able to see - and thus download - a particular resource.

This service need not be especially secure, as should a file be downloaded accidentally, the user's Key will not have attributes that match the resource to a level that the resource's Policy allows. Essentially the Policy Language (PL) provides the security of the system in partnership with the Attribute-Based Encryption (ABE) that incorporates it.

Attributes are config based from files; defined therein and imported into the application. May have to hard code attributes and state that configuration is future work to make the system flexible and portable to new environments.