Midterm Report

Max Dawson

Evan Hassan

Marcel Jonas

CSI-4480

**Due date: March, 7, 2019**

**Introduction/Background Information:**

When a user encrypts confidential data, it is crucial he/she be able to choose a specific access control to determine who will be able to decrypt this data. Enter Ciphertext Policy Attribute Based Encryption. CP-ABE is a system for realizing complex access control on encrypted data. Specifically, a user’s private key with a set of attributes and encrypted ciphertext will specify an access policy over attributes. A user will be able to decrypt if and only if his/her attributes satisfy the ciphertext’s policy. The encryption method was developed in 2006 by John Bethencourt, Amit Sahai, and Brett Waters in a response to a need for a more expressive type of access control. As sensitive data is increasingly stored across many servers, particularly cloud storage, it becomes increasingly difficult to guarantee confidentiality. CP-ABE encryption method along with other variations to date, is a useful tool for achieving access control policy.

**Project goal:** Investigate the Ciphertext Policy Attribute-Based Encryption (CP-ABE) cryptosystem, attempt to encrypt ciphertext, and evaluate the performance impact on a Kali Linux system.

**Project Schedule:**

|  |  |
| --- | --- |
| **Task** | **Deadline** |
| Research & Analysis | 2-13-19 (2 weeks) |
| Cryptographic tools & testing | 2-27-19 (2 weeks) |
| Midterm Report & midterm presentation preparation | 3-6-19 (1 week) |
| Implementation | 3-20-19 (2 weeks) |
| Final presentation preparation | 4-3-19 (2 weeks) |
| Final report & Peer reviews | 4-16-19 (approximately 2 weeks) |

**Implementation:**

After, selecting and investigating the cpabe toolkit, we are working toward implementation. Find a way we can use these encryption algorithms with efficiency and common use in a secure manner. Allow the transfer of files between users and not allow unauthorized users be able to view the documents.

**Challenges: GMP line 67 code missing ;**

In the implementation stage it took some fine tuning to get the cpabe-0.11 and libbswabe-0.9 working properly and together. One of the things that had to be done is to install a PBC library which is ciphertext-policy attribute-based encryption scheme which was built on the GMP library which had a line code error which was missing a (;) , so that was needed to be installed first then the PBC library then install the libbswade library first because that is the first part of the library which had to be allowed certain permissions ($ cd gmp-6.1.2/mpn and chmod +x m4-ccas) and then finally installing the cpabe library. As you can see it took quite a lot of configuring and searching forums to find the solutions to the errors the libraries had.

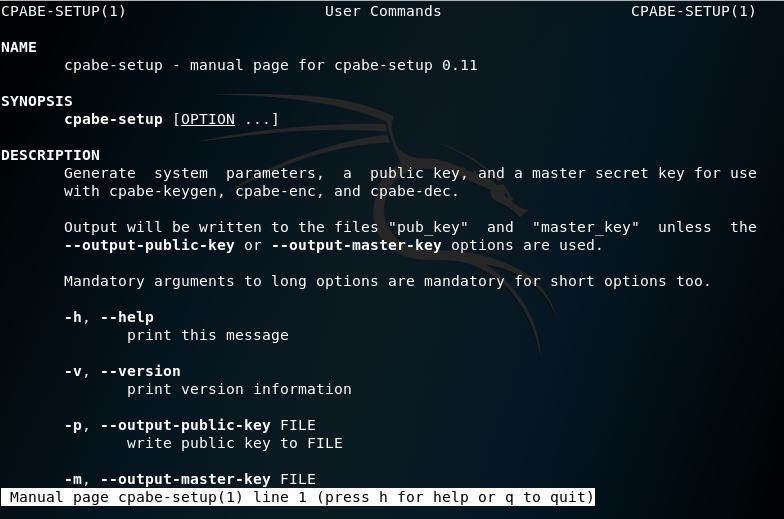
\*Note: We have tried doing other libraries and they require ATLAS library install and that is currently very difficult due to it requiring CPU throttling off.

**Technical reference dictionary for cpabe:**

# Generates a public key and a master secret key.

$ cpabe-setup

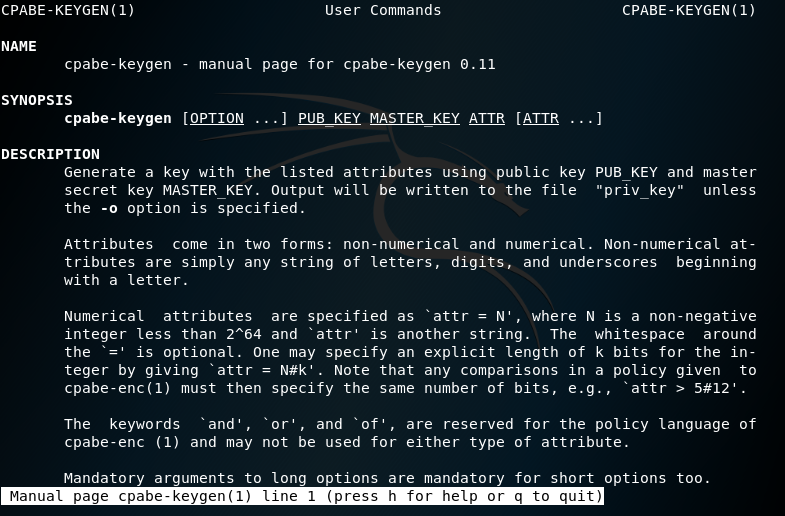
Screenshot of cpabe-setup manual page:



# Generates a private key with a given set of attributes.

$ cpabe-keygen

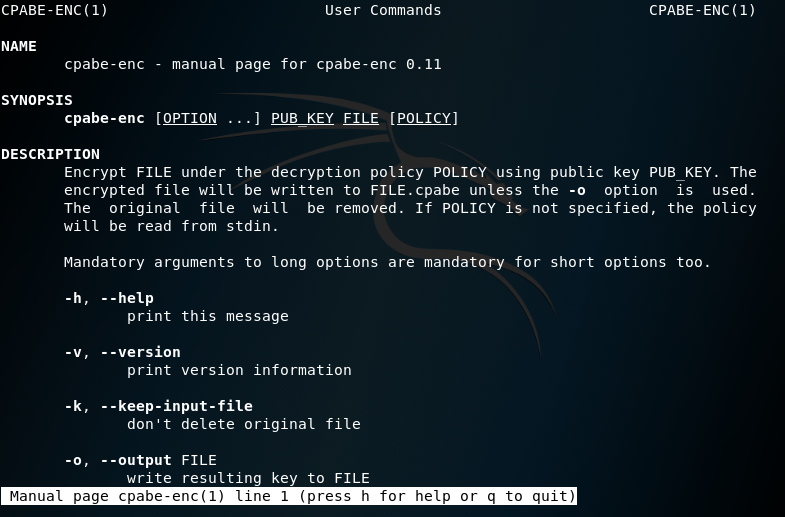
Screenshot of cpabe-keygen manual page:



# Encrypts a file according to a policy, which is an expression in terms of attributes.

$ cpabe-enc

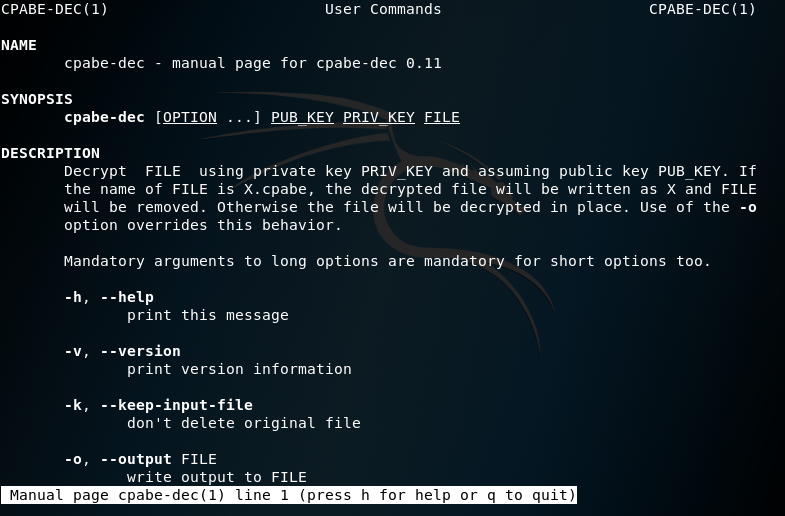
Screenshot of cpabe-enc manual page:



# Decrypts a file using a private key.

$ cpabe-dec

Screenshot of cpabe-dec manual page:



References:

1. Lai, Junzuo & Deng, Robert & Yang, Yanjiang & Weng, Jian. (2014). Adaptable Ciphertext-Policy Attribute-Based Encryption. 10.1007/978-3-319-04873-4\_12.
2. Bethencourt, John & Sahai, Amit & Waters, Brent. (2007). Ciphertext-Policy Attribute-Based Encryption. Proceedings - IEEE Symposium on Security and Privacy. 321-334. 10.1109/SP.2007.11.
3. “Ciphertext-Policy Attribute-Based Encryption.” *Advanced Crypto Software Collection*, 1 Dec. 2006, <http://hms.isi.jhu.edu/acsc/cpabe/>
4. Buchanan, Bill. “Ciphertext-Policy Attribute-Based Encryption.” *YouTube*, uploaded by Bill Buchanan OBE, 3 January 2019, <https://www.youtube.com/watch?v=pd42NCGiryQ>.