Self Encrypting USB Password Manager

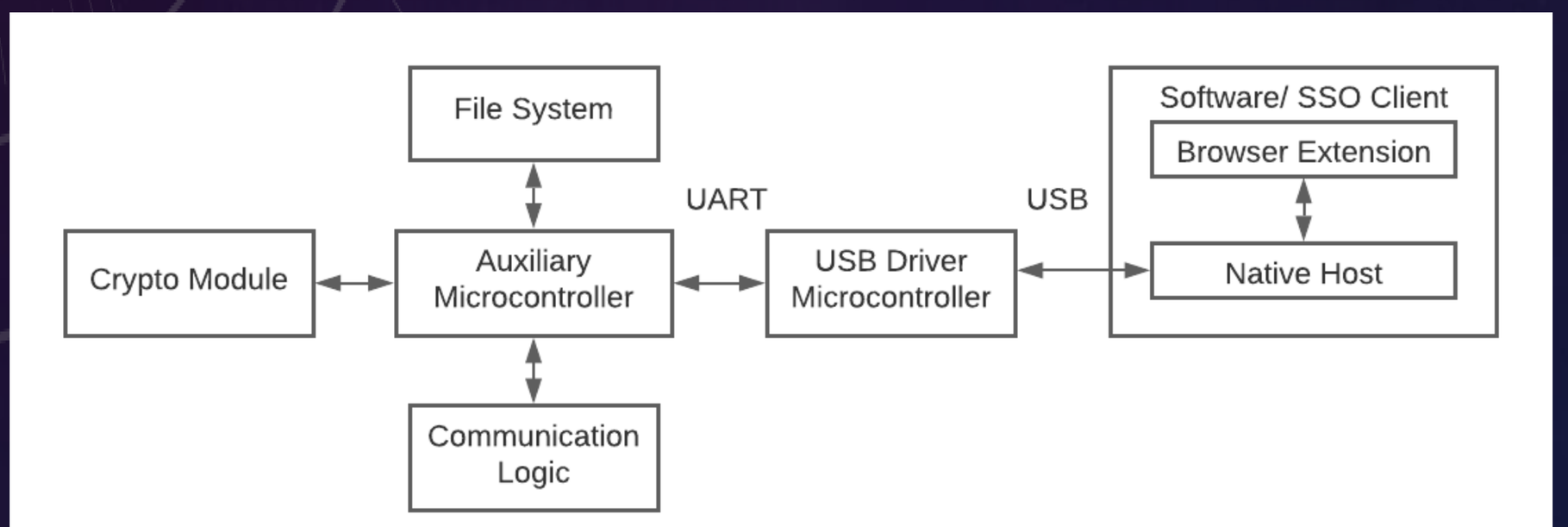
With Pseudo Single Sign-On Capability

Background

- The average internet user retains approximately 25-30 credentials.
- Storing these credentials online poses risks.
- Hardware based password managers are a solution to this problem.
- Single Sign-On technologies are helpful in managing account sign on.

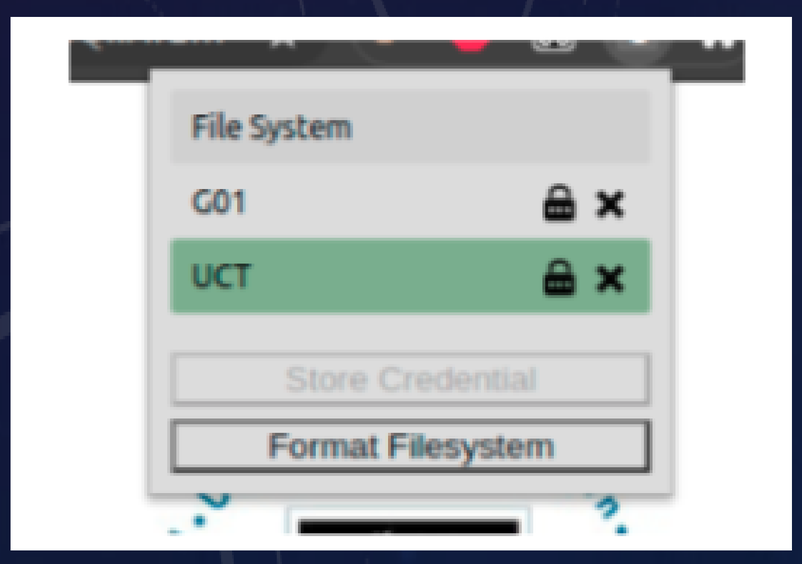
Solution

- Implement a USB based password manager solution, isolated from the internet.
- Secure credentials using RSA-1024 encryption.
- Design a custom EEPROM based file system.
- Software client to interface with device and implement SSO.



Results and Conclusions

- Authentication model consists of a unique RSA PEM formatted key file stored in a users home directory. Decryption is not possible without this key.
- Browser extension allows users to interact with the device.
- An attack analysis of the system revealed that the resulting system provides robust security.



Process	t1 /ms	t2/ ms	t3 /ms	t4 /ms	tavg /ms
Encryption	4.25	4.55	4.31	4.11	4.31
Decryption	1.12	1.14	1.12	1.13	1.13
SSO (Login)	1.62	1.78	1.88	1.75	1.76

Table 14: Performance metrics of end system.

Dylan Muller (MLLDYL002), University of Cape Town