COMP3334 Computer System Security Assignment 2

Poon Yat Sing (13040015D) <star.poon@connect.polyu.hk>

***Abstract*—Lightweight embedded systems such as home routers and Raspberry Pi are easy to deploy as a measurement probes. It is important to understand the pros and cons of using these devices as probes. In this article, we will compare the operating system and hardware architecture of embedded devices and routers. The data bus problem of Raspberry Pi will also be addressed.**

Keywords*—Scrypt, key derivation function, Galois/Counter Mode(GCM), AES, RSA, Digital Signature, password storage, salt, Authenticated Encryption (AE)

I. Operating system

Most of the routers come with a default operating system and a web interface. These OSes usually have been optimized by the manufacturer to enable some hardware specific functions, such as hardware NAT. However, the lack of command prompt and root privilege limit the feasibility of executing measurement tools.

References

[1] libscrypt. https://github.com/technion/libscrypt

[2] Assurance Technologies. *Modular Crypt Format*[Online]. Available: https://pythonhosted.org/passlib/modular_crypt_format.html
http://stackoverflow.com/questions/1220751/how-to-choose-an-aes-encryption-mode-cbc-ecb-ctr-ocb-cfb
http://cseweb.ucsd.edu/ mihir/papers/oem.pdf
http://crypto.stackexchange.com/questions/6842/how-to-choose-between-aes-ccm-and-aes-gcm-for-storage-volume-encryption
http://hayageek.com/rsa-encryption-decryption-openssl-c/
http://web.cs.ucdavis.edu/ rogaway/papers/modes.pdf

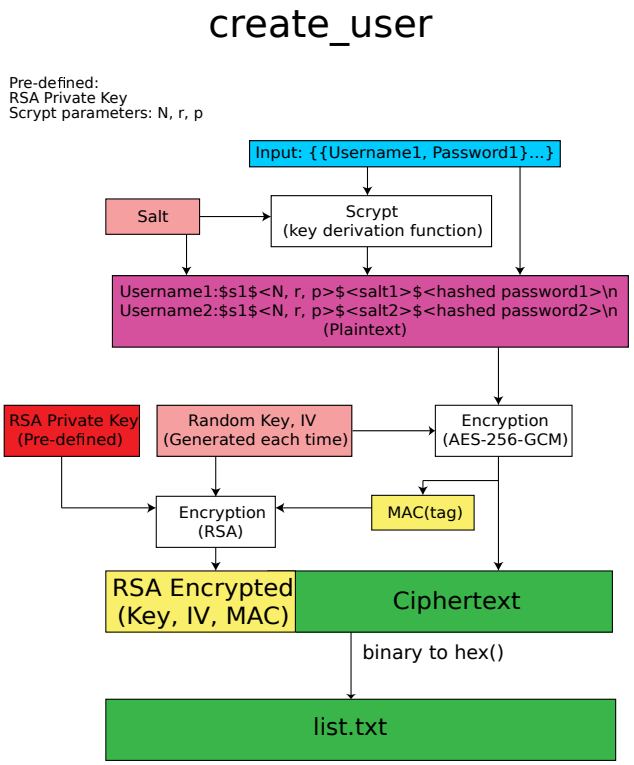

Fig. 1. Workflow of create_user module

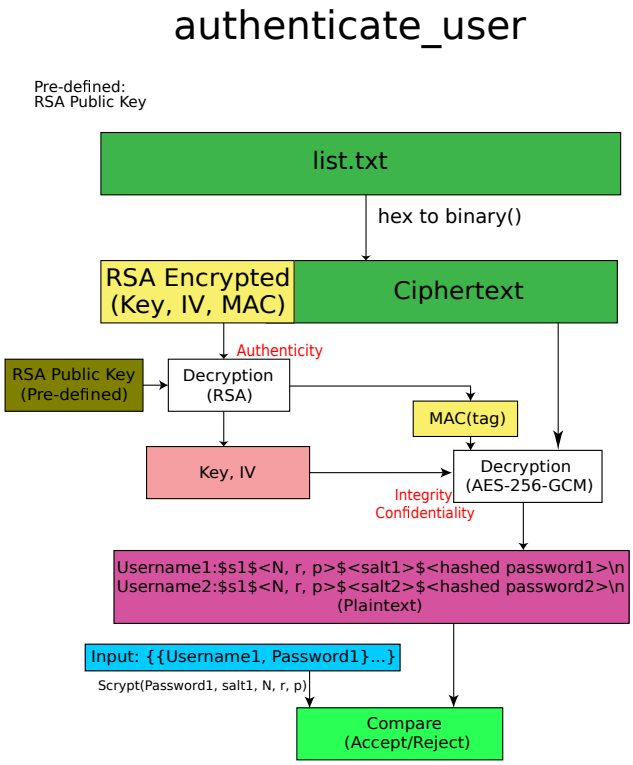

Fig. 2. Workflow of authenticate_user module