Operating Systems Security and DevelopmentCoursework- Part 2: Understanding and modifying an OS- File Encryption

1. A description of your File Encryption (5% of the assessment component mark).

This report outlines the implementation of encryption solutions in a Windows networking environment. Specifically, covers the step-by-step installation of Encrypted File System , IPSec-encrypted transport communications between Windows devices, 802.1x wireless encryption, and certified-based encryption in a Microsoft Exchange environment. The design is suitable for one or two systems (or virtual session) in a test environment. The report focuses on encryption in a Windows environment as a method of securing information. The traditional method of securing information is to provide access lists of users who have access to the information. However, the problem with access list security is that once security access is provided to a user, the only way to protect the content is to remove the user from the access list. This mechanism is common in most File Encryption Systems.

2. A list of functional and non-functional requirements and security features of a File Encryption (10%).

- Functional requirements

* Actual encryption and decryption are done to the data.
* Support for different algorithms such as RSA, AES (symmetric and asymmetric encryption algorithms)
* Ability to encrypt files of different types such as plain text, images, video.
* Availability of integration with different operation systems and file management tools.
* User authentication for accessing the encrypted files.

- Non-functional requirements

* Scalability to support large volumes of files.
* Reliable and fault-tolerant
* Easy to use.
* Low level performance overhead.

- Security features

* Strong encryption algorithms that are known for low faults and ensure confidentiality of data.
* Secure key management to protect the keys which are used for encryption and decryption.
* Secured transmission of encrypted files
* Compliance with relevant data protection and privacy regulations.
* Audit trail and monitoring to prevent from fraud and malicious attacks on files/data.

3. Design of your software/patch that includes communications with the OS (10%).

The method that I decided to use to add extra security is certificate-based encryption. Certificate-based means that credentials are issued by a security administrator to a user or to a computer for access to data. The certificate can be revoked and a new certificate can be issued to the same user or computer, thus allowing a user's access rights to be renewed with a new certificate in the event that the user's access information was compromised. Using encryption scrambles the information so that someone without a valid certificate cannot read or access the information, thus providing the privacy that security and compliance auditors want for information access in today's regulated environment. The encryption is set by the certificate so that the certificate, as well as encrypted content, can be shared with others. Additionally, the certificate can be revoked and reissued for the same encrypted content to provide private and secured access to information on an ongoing basis.

For the sake of the assignment, we can assume that the part taken by the user is changed to being a file and the administrator that issues certificates is the user/admin of the computer/device. Furthermore, assumption is that the Active Directory needs to be at a Windows level in order for autoenrollment of certificates to work, which is a core component for certificate-based security.

4. Implementation of your File Encryption including annotated C code (20%).

5. Testing plan for validating your software (10%).

6. Description of integrating/adding the implemented component/patch to OS (10%).

7. Integration testing plan for integrating your component/patch into the system. This includes designing and running an experiment that evaluates the performance of the implemented functionalities (10%).

8. Reporting the possible limitations, failures, and/or difficulties you experience in your work (5%).

The only problem with certificate-based encryption was that certificates previously had to be issued manually, which meant that every time someone needed a certificate, a security administrator had to issue the certificate and then email it to the user. When the user felt his certificate was compromised, a new certificate had to be issued, and the user had to manually reinstall the new certificate. Depending on the sophistication of the user, issuing certificates could be a help desk nightmare.

9. A conclusion section that includes recommendations for extending the conducted work and personal reflection (5%).

10. References (using Harvard or Numerical style of referencing) and proper citation (5%).

11. Demonstrate a thorough understanding of multi-threaded/process systems through the design and implementation of your system. This is not a

separate section in your report. Instead, it has to be addressed and present in the other sections, e.g., 2, 3, 4, and 6 (10%).