LEE JIHU

34061648

ICT379 assignment part1

**Subject credential management.**

Subject credentials are managed through the Credential Management System (CMS). For an organization to ensure security against fatal information, an element called CMS must be implemented. To access the Microsoft Word document file, the credentials in the title must match the credentials in CMS. If an attacker attempts to access a word file, the document cannot be accessed because the attacker's credentials do not match the CMS for the above reasons. One of the specific types of CSM for Windows is Active Directory Rights Management Services (ADRMS). ADRMS works in the form of providing licenses to authenticated users if owners of certain files, such as word documents, want to protect their files. *(Roger A. Grimes.2021)*First, the document is encrypted by ADRMS using the Client Licensee Certificate (CLC), and then the Publishing License (PL) binds to the encrypted document. A final license is required for users to access encrypted documents. The ADRMS then refers to the PL to verify that the user requesting access has legitimate credentials to access the encrypted file. For users with legitimate credentials, the child can access the file, but if an attacker who does not try to access the file, ADRMS will refer to PL to check the absence of credentials. Of course, the attacker cannot access the file because he does not have a valid credential account. ADRMS can also restrict authenticated users from performing only certain tasks, such as reading or printing, which prevents the PL from violating policies set by the file owner.

**Access Control Mechanisms**

The access control mechanism is a control device installed to ensure the security of the system so that only authenticated users can access it. Access control has two main parts: authentication and authorization. Authentication determines the user's ID and whether the user is allowed to access and is a procedure for identifying who he or she claims to be. On the other hand, authorization is a process that determines what can be done by limiting verified users to specific authority, allowing them to go where they want to go or get the information they want. When an attacker tries to open a word document, access control verifies the ID to authenticate the attacker. The attacker does not have access to the word document, so the ID is determined by the access control mechanism and the file is not accessible. There are three types of entities in access control. In other words, a user ID (or subject) that exists as an individual in the real world and a user connection to a machine (username is part of a system and is a process (or subject) that runs according to a given topic. Access control may have a list of users and permissions called Access Control List (ACL). *(Messaoud Benantar.2006)*

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | OS | Accounting program | Accounting data | Insurance data | Payroll data |
| A | rx | rx | r | - | - |
| B | rx | rx | r | rw | rw |
| C | rwx | rwx | r | rw | rw |
| Accounting program | rx | rx | r | rw | rw |

The table displays objects in rows and columns with specific permissions for each object. For example, A (subject) can read and run in an accounting program (object), but only accounting data can be read and cannot be executed. If this ACL has another column for that word file, the attacker does not belong to this ACL and is not authorized to do so. A, B, C, and accounting programs (all read (r--), write (w-), run (--x) to access word documents.

**Low level of security mechanism**

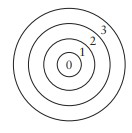
First, the need for a low-level security mechanism will be briefly discussed. This is significant in that it prevents attackers from manipulating low levels of data (e.g., kernels). It aims to secure the task of the lower level by authenticating and approving the item by controlling access. Now, let's take an example of hardware-based access control to the protective ring. *(Dieter Gollmann. 2011)*

0 - Operating system kernel.

1 – Operating system.

2 – Utility.

3 – User process.



The protective rings are numbered according to their importance. The higher the importance, the lower the number is assigned and placed in the center of the ring. The kernel is the most important object, so it is marked 0 and is in the center of the ring. Less important objects are relatively away from the center. In other words, the lower the assigned number, the more reliable and authoritative it is. (Alsmadi & Karabatis & Aleroud. 2017) I will explain this by substituting it into a word document. Attackers who do not have access to word documents become part of the user process, which is the lowest privilege of the protection ring mechanism. For an attacker to access a confidential word document, it must go further into the ring to obtain kernel rights. One of the many ways an operating system can protect a kernel is to refer to a memory management device (MMU). If an attacker attempts to open a word document and calls the system, the attacker cannot open the word document in the kernel because he does not have access to the MMU.

**RFERENCE**

Roger A. Grimes.2021. Hacking multifactor authentication. WILEY

Messaoud Benantar.2006. Access Control Systems: Security, Identity Management and Trust Models. SPRINGER

Dieter Gollmann. 2011. Computer Security (3rd ed)

Izzat M Alsmadi & George Karabatis & Ahmed Aleroud. 2017. Information Fusion for Cyber-Security Analytics. SPRINGER