Christopher Foley
Z15092976
CIS6370

Assignment 2

Q1. We have a program to make bids to buy properties (real estate, art,…). A bid requires the following actions:

A1. Create the bid document. A2. Add buyer information. A3. Verify buyer credit information. A4. Make a deposit in an escrow account in a law office. A5. Register document in a law office.

Enumerate the possible threats for these activities (A11, A12,…Aij). Indicate for each identified threat its possible misuse (attacker goal). For example, reading the buyer information is a confidentiality misuse.

The Bid to buy properties use case is similar to the Open Account Use Case as explained in Chapter 2 of the book "Security Patterns in Practice: Building Secure Archetectures Using Security Patterns"[1] (excerpts provided in class):

A1 - Create the Bid Document

T1.1 – The Buyer is an imposter and opens the account in the name of another person - Goal: misuse of identity/create false bid

T1.2 – The seller is an imposter - Goal: misuse of buyer identity, theft of money

T1.2 – The goods are false/not properly described - Goal: Theft of negotiable currency

A2 - Add Buyer Information

T2.1 - Buyer enters false information – misuse of seller identity

T2.2 - buyer information intercepted – misuse of buyer identity

T2.3 - buyer information substituted – harm to buyer identity/reputation

A3 - Verify Buyer Credit Information

T3.1 - credit information intercepted – misuse of buyer credit

A4 - Deposit to an Escrow account in law office

T4.1 – Transfer of funds by external source – Goal theft

T4.2 - Transfer of funds to incorrect source – Goal theft

A5 - Register document in law office

[1] E. B. Fernandez, "*Security Patterns in Practice: Building Secure Architectures Using Software Patterns*" Wiley Series in Software Design Patterns, May 2013, Excerpt provided in class by author.

T5.1 Incorrect/false document registered – misuse of buyer/seller information

T5.2 document removed from registration – repudiate sale

Q2. Somebody had the idea of using PKI to send a page number and character number within the page of a prearranged set of 10 books. This information is described as (book_id, page#, char#) and it is the key to send messages using a code-book approach. Analyze critically this cryptographic approach, including advantages, disadvantages, degree of security, and possible use.

The specified approach has the following advantages:

- The cypher and key are easy to exchange
- If the message contains a recognition key sequence or decrypts to a coherent message:
    - authenticates the message easily
    - non-repudiation difficult
- does not require specialized algorithms
- Satisfies many of Shannon's principles:
    - effort to encrypt and decrypt similar
    - key is simple
    - a single encryption error will not necessarily invalidate the message. An encryption error in a recognition sequence will mark the message as invalid, but not halt or stop the encryption.
- Supports the principle – algorithm is known but the key is complex and hidden.
- Similar in length to plaintext message.
- Properly encrypted and decrypted message authenticates identity and makes repudiation difficult.

The following disadvantages:

- it requires that identical printings/editions/translations be used
- printings and translations must be reasonably common to sender and receiver
- written substitution key increases risk of interception.
- Cryptanalyst can easily recognize as a substitution cypher unless spaces, numbers and punctuation are allowed – which makes decryption more difficult.

Security is reasonably good

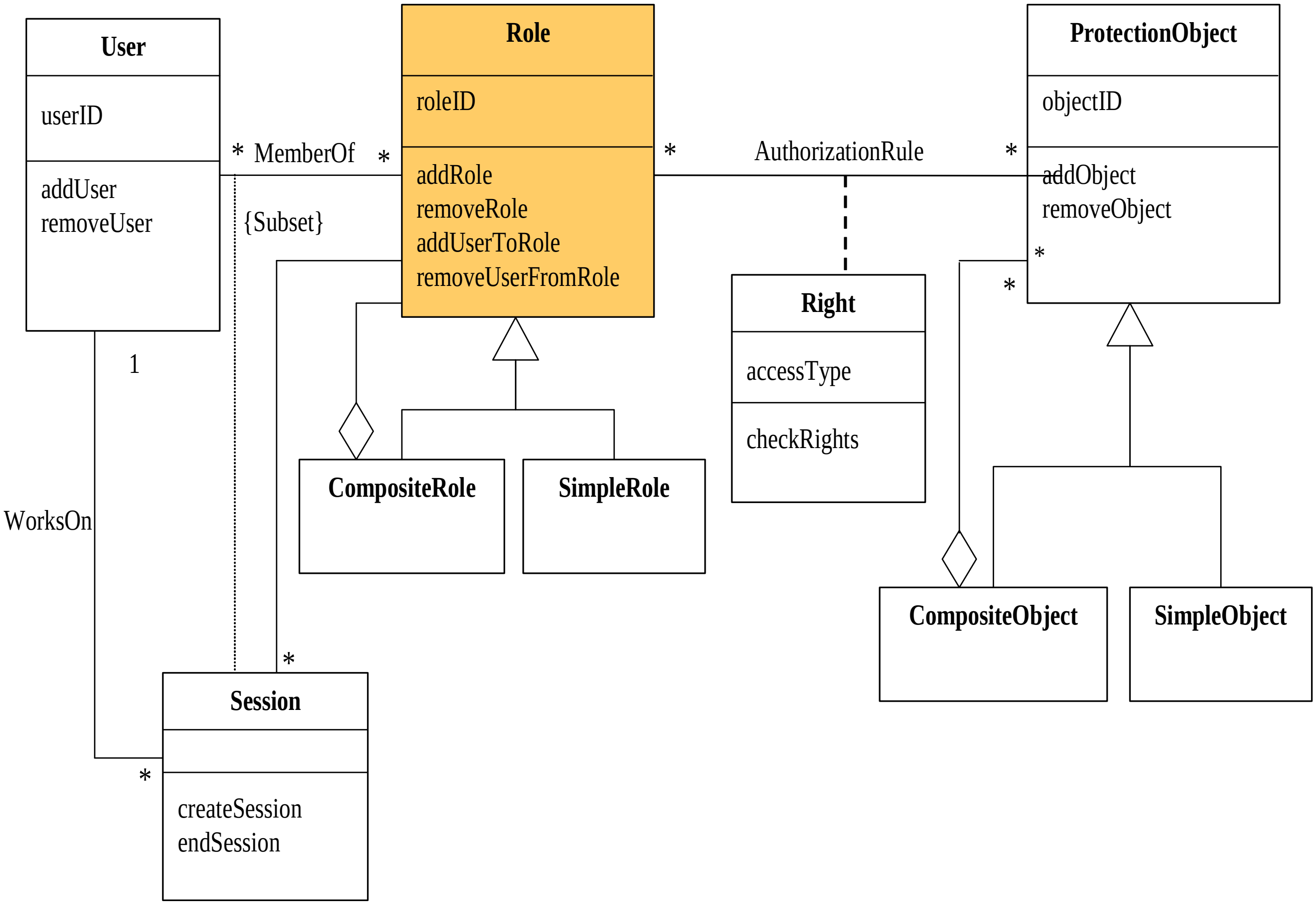
- since it is difficult to substitute a false message without a physical copy of the key.

- Difficult to decrypt without copy of all keys.
- keys can be easily exchanged

Q3. Study the authorization system of the Windows 10 OS. Relate its concepts to the models of Chapter 2; in particular, the (s,o,t,p,f) model. Are there concepts in their authorization model beyond this formal model. Indicate your sources of information.

The Windows Security Model is a RBAC model which provides access based on a security token created at authorization. The token is used to validate all access and is passed to processes created by the user.[2] This token contains the access rights of the user and the users groups and is used to validate access to any securable objects in the Windows secured system. This permits Windows to provide C2-Class security as defined in the DOD "Orange Book".[3] In the RBAC system the creator of a securable object is given roles as Owner of the object, until ownership role is transferred.

This may be diagrammed as follows[4]:



[2] "Parts of the Access Control Model", https://msdn.microsoft.com/en-us/library/windows/desktop/aa374876(v=vs.85).aspx , accessed 18-Oct-2017

[3] "C2 Level Security (Windows)", https://msdn.microsoft.com/en-us/library/windows/desktop/aa376387(v=vs.85).aspx , accessed 19-Oct-2017

[4] Diagram extracted from lecture notes. CIS6370 – Computer and Daat Security, Dr. Eduardo B Fernandez, Delivereed 9/20/2017

The protection model identifies the *subject* via a unique security token created at authentication which identifies the user and their role(s). Each securable object (*object)* is identified by a series of rights such as roles (owner/group/administriator/user) and the rights (read/write/execute/admin/copy) granted to each subject.

When a user attempts to access a securable *object,* the rights assigned to the subject as enumerated by the token are checked. If the subject has rights the access is granted. Depending on the subject rights, rights may be *transferred* or *copied*. Generally Windows operates on a principle of least permission with owners and administrators getting full rights, although either may change rights, requiring explicit permission to be granted to different security subjects. This matrix was first used by windows NT and has been continued into the .net framework.[5]

[5] E. B. Fernandez, “*Security Patterns in Practice: Building Secure Architectures Using Software Patterns*” Wiley Series in Software Design Patterns, May 2013, Excerpt provided in class by author.