SENG2250/6250 System and Network Security

School of Electrical Engineering and Computing

Semester 2, 2020

Lab 6: User Authentication and Access Control

Objectives

1) Review the knowledge of user authentication and access control.
2) Analyse and resolve security issues of the two-factor authentication protocol.
3) Apply access control models.
4) Programming exercises.

Part 1 Review Questions

1. What is multi-factor authentication?
2. Describe the (X.509) 3-way authentication. Does it require time synchronization? Why?
3. What is the difference between the verification mode and identification mode in biometric authentication? Give an application scenario for each.
4. What is the goal of access control?
5. What is the mandatory access control (MAC)?

Part 2 Exercises

6. **Two-factor Authentication**. Consider the following two-factor (password + biometric) authentication. System time is synchronised between the user and the server.
   Is it a secure two-factor authentication? Justify your answer.

$$User \rightarrow Server: N_u, E_k(ID, h(TS||pwd), E_k(Bio||N_u))$$

N_u	A nonce picked by user.
ID	User's identity.
E	A secure symmetric-key encryption scheme.
k	A session key.
h	A secure hash function.
TS	Timestamp.
Bio	User's biometric information. It is known to server.
pwd	A 12-character password including letters, digits and special characters.
$\|\|$	Concatenation of two bit strings.

7. Implement the BLP model which takes as input 1) access control matrix (ACM); 2) security label of subjects; 3) security label of objects. Output the accessible objects (with the permissions) of each subject. Test your program using the following input.
   "-" means no permission is granted; "r" – read; "w" – write.

	Key File	**Sys Log**	**Banner Info**
Alice	rw	rw	rw
Bob	rw	r	w
Carrie	-	w	w

ACM

	Security Label
Alice	Top-Secret
Bob	Secret
Carrie	Secret

Subject Labels

	Security Label
Key File	Top-Secret
Sys Log	Secret
Banner Info	Unclassified

Object Labels

The output content should be:

	Key File	Sys Log	Banner Info
Alice	rw	r	r
Bob	w	r	-
Carrie	-	w	-

8.

a. What is HMAC? Is it good for user authentication?

b. Implement the HMAC algorithm. Please refer to L2-S61 (Cryptographic Techniques, Slide 61). For the underlying hash functions, use a standard hash function such as sha-1 and sha-256. There are libraries for hash functions. For example,

- **Java**: java.security.MessageDigest
  https://docs.oracle.com/javase/8/docs/api/java/security/MessageDigest.html
- **Python**: hashlib
  https://docs.python.org/3/library/hashlib.html
- **C++**: Crypto++
  https://cryptopp.com/

Part 3 Discovery

9. Self-study: Role-based Access Control (RBAC) model

Refer to the file: "rbac.pdf" under lab 06

a. What is the relationship between RBAC and MAC (e.g., ACM) model?

b. What advantages and/or disadvantages can you think of about RBAC?