ENPM809W – Introduction to Secure Coding

Homework – 4

Author – Syed Mohammad Ibrahim

UMD ID: iamibi

Email: iamibi@umd.edu

1. The paper talks about challenges in using authentication mechanisms in the medical care cycle. What are the four use cases identified by the paper where authentication mechanisms need to be considered?

A. The four use cases which require authentication mechanisms are:

- Emergency care and vehicle services (management.
- Medical care in hospitals (diagnosis and treatment).
- (Mass) Testing and Contact (prevention and diagnosis).
- Patients' physical and mental handicaps (rehabilitation).

2. What are the four categories of authentication methods identified by the authors of the paper?

A. The four authentication methods identified by the authors of the paper are:

- Something you know: Knowledge.
- Something you have: Possession.
- Something you are: Inherent or biometric characteristics.
- Something you do or how you do something: Actions.

3. What are the six superordinate groups the authors of the paper mapped the requirements collected for authentication to?

A. The six superordinate groups are:

- Reliability
- Security
- Usability
- Environmental Requirements
- Data Protection & Privacy
- Interoperability

4. What do the authors mean when they assign a requirement to a super ordinate group called Reliability? As per the authors, which requirements map to this group?

A. By assigning the requirements to superordinate group Reliability, the authors want to map the scenarios based on how certain factors affect reliability like online or offline status, false negatives, etc. The requirements REQ1 - Timesaving, reliable methods, REQ10 - (Mass) availability of authentication tools and REQ13 - User-substitutable authentication methods are mapped to Reliability.

5. As per the authors, if an authentication mechanism has to work offline, be easily available (as highlighted by the requirement for mass availability of authentication tools), be easily replaceable (as highlighted by the substitutable authentication mechanism), why have an authentication mechanism at all? Do you agree with the authors that an authentication mechanism is still required? Please explain why or why not.

A. Yes, I agree that we still need the use of authentication as any software or hardware that can work offline should still be mapped to a user who is going to use it. And that user needs to be identifiable in some way by the device/software to process the requirement.

6. The authors of the paper refer to the “NIDAPad”, a device presumably used by the ambulance personnel that collects personal patient information which only uses a four-digit code when personnel transfers/shift changes occur. What threats can you identify that might be present with such a mechanism?

A. Identified threats as per STRIDE are:

- Spoofing Identity
- Tampering with Data
- Information Disclosure

7. In section 5.2 of the paper, the authors discuss the security super ordinate group. Which two attack vectors do the authors describe?

A. The two attack vectors are compromised server and social engineering.

8. In Figure 2, which shows the Matrix weights for environment requirements. Which of the environment requirements has really poor coverage for authentication mechanisms? Why?

A. The input restrictions and operational restrictions have a poor coverage for authentication mechanism. This is because the knowledge about the system/operation in both the cases can be helpful for an attacker.

9. What is the difference between what is shown in Figure 3 vs Figure 4 in the paper? How do you use the matrix?

A. Figure 3 shows decision matrix for proper and scenario-based authentication mechanisms selection whereas Figure 4 shows Application of the decision matrix on scenario 1 (Something you know: knowledge).

Figure 3 uses assigned weights from W1 to W6 to individual groups to adapt to the current use case. Then, for each row representing a different authentication scheme, the evaluated value must be multiplied to the corresponding weights.

Figure 4 uses the concepts from figure 3 matrix to assign respective weights to the scenarios mentioned by the authors and assign points to each of them.

10. The following paper proposes using brainwaves to perform authentication of identities: https://www.usenix.org/system/files/sec21fall-arias-cabarcos.pdf. As per the paper you read above, the authors identified four types of existing authentication mechanisms. Which authentication mechanism would this brainwave based authentication fall under? Why?

A. The brainwave-based authentication will fall under possession based authentication and mechanism as it requires the presence of human brain to perform the authentication, and behavioral based authentication as it defines the identity of human being.