SOFTWARE ENGINEERING CS 487
Participation – P4

Name : Satyam Rajput
(A20537375)
srajput3@hawk.iit.edu

Participation – P4

1). Describe the authentication protocol for an ATM

An ATM's authentication system typically involves **several steps** to confirm the user's identification and provide **safe account access**.

Considering the **concepts and facts** of a **Safety-critical Systems**
I.e. Safety-critical is a **non-functional requirement** meaning that system operation must always be in a **safe state**

• **Primary safety-critical software**
– Embedded controllers where a failure can result in a hardware malfunction resulting in human injury or environmental damage

• **Secondary safety-critical software**
– Software which, in the event of failure, can result in injury
– For example, a defective computer-aided design tool which produces a flawed design

ATM authentication protocol:

Inserting a Card: The user places their ATM card into the card reader.

PIN Entry: Using the ATM keypad, the user inputs their Personal Identification Number (PIN).

Verification: The ATM compares the PIN entered with the encrypted PIN kept on the magnetic stripe or chip of the card.

Authorization: The ATM enables the user to carry out various operations, including cash withdrawal, balance inquiries, fund transfers, and more, provided that the PIN is successfully validated.

- **Explain why it is less than perfectly secure.**

The authentication protocol for an ATM, while effective, is less than perfectly secure due to several reasons:

1. **PIN-based Vulnerability:** Although PINs add an extra degree of protection, they can be broken into by techniques including social engineering, PIN theft devices, and shoulder surfing.
2. **Card Cloning:** Unauthorised access to accounts can be obtained by copying the data on ATM cards' magnetic stripes.
3. **Absence of Two-Factor Authentication:** In the absence of two-factor authentication techniques, the authentication procedure usually depends only on the card and PIN combination.
4. **Network Vulnerabilities:** The security of the authentication procedure may be compromised if communication between the ATM and the bank's network is subject to interception or unauthorised access.
5. **Susceptibility to Skimming:** Criminals may install skimming devices on ATMs in an attempt to get cardholder information and PINs, threatening the security of the authentication procedure.

- **And why it is less than perfectly easy to use.**

- And why it is OK for both of these to be true.

Despite being created for security, the ATM authentication procedure can be **difficult for people to utilise.** We know that **Requirements Drive the Design.** For the following reasons, using it is not entirely simple:

- Remembering the PIN
- Language and Interface challenges
- Security concerns about effective user behaviour
- Potential for error
- Transaction completion time

While there are security and usability issues with the ATM authentication procedure, **these issues are acceptable for the following reasons:**

- **Balancing Security and Convenience:** Getting the ideal security frequently requires making compromises with usability. Improving security protocols can strengthen the authentication process, but they can also add complexity that takes away from ease of use. To keep the process safe and usable for a variety of users, it is essential to strike a balance between security and usability.

- **Diverse User Needs:** The requirements and preferences of different users differ. For certain users, something that is secure could be inconvenient. For instance, while some consumers value the maximum level of security, others value usability and convenience.

- **Constant Improvement** is made possible by acknowledging that the ATM authentication procedure is neither flawlessly safe or user-friendly. It promotes the creation of fresh methods and technologies that can improve user experience and security. Addressing the changing nature of security threats and the variety of user demands requires this continual innovation.

- **User Understanding**: In order to protect their financial assets, users can be made aware of the significance of security precautions and given the ability to adjust to some inconveniences. This knowledge may assist consumers in appreciating the need for certain security precautions, which may render the procedure less than ideal for ease of use.

- Describe a mechanism for the ATM to assess the awareness of the human user during authentication.

Considering the concepts and points of **Human Awareness i.e.**

- **Human detection of exceptional states**
    - Similar to computer system exception detection in that the human is assuming normal and must be made to recognize the change to

exceptional – Therefore a similar protocol must exist which distinguishes the current state as exceptional

- **Human handling of exceptions**
  - The protocol should specify a clear set of actions for the human to take to return to at least “safe” if not normal
  - The protocol must contain acknowledgement-based verification to insure that the human has responded and has taken control of the situation

On the basis of the above points we can describe the mechanism :

Biometric Authentication: During the authentication procedure, scan the user's face using facial recognition technology.
Take a picture of the user's face and examine it to confirm their identity.
Provide a more user-friendly method by removing the requirement for the user to memorise and input a PIN.

Multi-Factor Authentication:
Combine biometric authentication with traditional methods such as the use of ATM cards and PINs.Implement a multi-factor authentication approach, requiring something the user knows (PIN), something the user has (ATM card), and something the user is (biometric data).
Enhance security while maintaining user-friendly authentication by reducing reliance on memory-based authentication alone.

CAPTCHA Implementation for User Awareness: One potential mechanism for an ATM to assess the awareness of the human user during authentication is through the implementation of a "CAPTCHA" (Completely Automated Public Turing test to tell Computers and Humans Apart) or a similar challenge-response test.

User Friendly Experience: Prioritize ease of use by integrating seamless biometric authentication methods into the ATM interface.
Minimize the cognitive load on users by reducing the need to remember and enter complex passwords or PINs.
Enhance accessibility for users who may have difficulty with traditional authentication methods.

2). Describe the role of automated awareness in engineering acceptable safety for a fully self-driving car.

– Explain the role of this awareness in managing exceptions.
– Explain why it is less than perfectly safe.

For describing the role of automated awareness for a fully automated self-driving car that involves the car's ability to perceive and understand its environment, anticipate potential hazards, and make real-time decisions to ensure the safety of the vehicle occupants and others on the road. We need to have a **good understanding of the following concepts and factors :**

- **Requirements Drive the Design**
  Evaluations concerning safety-criticality
  – Hazard avoidance
  – the system is designed to avoid hazards
  – Hazard detection and removal – the system is designed to detect problems and correct them before an accident occurs
  – Damage limitation – the system is designed to minimize the impact of a problem when it occurs
- **Safety Engineering Processes**
  - Safety Assurance
  - Formal Verification
  - Model Checking
  - Static Program Analysis

- **Dealing with Exceptions**
  - Exception detection
  - Exception handling

- **Human Awareness**
  - Human detection of exceptional states
  - Human handling of exceptions

Role of Automated Awareness in Managing Exceptions:

- Environmental Perception: To ensure awareness of their surroundings, self-driving cars employ sensors such as cameras, radar, and LiDAR to monitor traffic, road conditions, pedestrians, and other vehicles.

- Risk Assessment and Decision-Making: Automated awareness enables the vehicle to identify and react to unanticipated events, such as unexpected lane changes or the presence of pedestrians, by assessing possible dangers.

- Real-Time Adaptation: Using automatic awareness, the self-driving car may modify its course in real-time by changing lanes, braking completely, or reducing its speed in response to anomalies or unanticipated events.

- Automated awareness-equipped self-driving cars may coordinate and interact with infrastructure systems and one another to manage situations like traffic jams and road closures as a group.

– Use risk assessment to justify the imperfect design.
– Describe a strategy for safely testing the car design's effectiveness.

We know that **Requirements Drive the Design**
Much of **design is choosing the best solution by evaluating the degree** to which each **possible design satisfies the prioritized non-functional requirements.**
Also According to **Designing for Security :**
• Base decisions on an explicit security policy
• Use defence in depth by employing multiple layers of security
• Use redundancy and diversity to reduce risk (e.g., maintain backups, avoid reliance on single possibly vulnerable platforms)

Risk Assessment to Justify Imperfect Design:

- The complexity of **Real-World circumstances:** Complex and varied issues arise in real-world circumstances. Since it recognises how difficult it is to account for every event that may arise, particularly ones that are uncommon or unanticipated, the flawed design is acceptable.

- **Sensor limits:** The poor design can be justified by the sensor technologies' limits, which acknowledge that certain environmental circumstances or unanticipated challenges may present difficulties for the autonomous awareness system of the automobile.

- **Human Encounter and Interpretation:** The imperfect design takes into consideration the inherent problems of properly anticipating and responding to every human encounter on the road, given the unpredictable nature of human behaviour.

Strategy for Safely Testing the Car Design's Effectiveness:

- **Simulation Testing:** To test the self-driving automobile under controlled settings, construct a variety of real-life scenarios using advanced simulations.
- **Closed-Course Trials:** Conduct thorough tests in controlled settings to assess how well the vehicle handles difficulties like unexpected obstacles or severe weather.
- **Real-World Exposure:** Ensure that safety precautions are in place so that the self-driving automobile may be gently brought into real-world situations.
- **Data-Based Validation:** Analyse a large amount of test data to confirm the vehicle's functionality and improve its automatic awareness systems.
- **Regulation Compliance:** Make sure that safety regulations are followed, and work with authorities to create testing protocols that put safety first.
- **Iterative Testing:** Test every iteration of the design thoroughly to ensure that the automated awareness mechanisms work as planned.