Armaan Shamsaasef

Race Conditions

Race Conditions - SY0-701 - 2.3

Definition: A vulnerability that occurs when a system's security or output is dependent on the sequence or timing of uncontrollable events, and this sequence is exploited to achieve an unintended state.

Core Concept: The system performs a check on a condition and then later takes an action based on that check. An attacker exploits the tiny window of time *between* the check and the action to change the condition, causing the system to act on outdated or invalid information.

Time-of-Check to Time-of-Use (TOCTTOU or TOC/TOU)

- This is the specific type of race condition discussed.
- Time-of-Check (TOC): The system verifies a condition (e.g., "Does the user have permission to open this file?").
- Time-of-Use (TOU): The system performs the action based on that check (e.g., it opens the file).
- The Exploit: The attacker changes the situation *after* the check but *before* the use.

Video Example: The Privilege Escalation Attack

This example demonstrates how a race condition can be used to gain unauthorized elevated privileges.

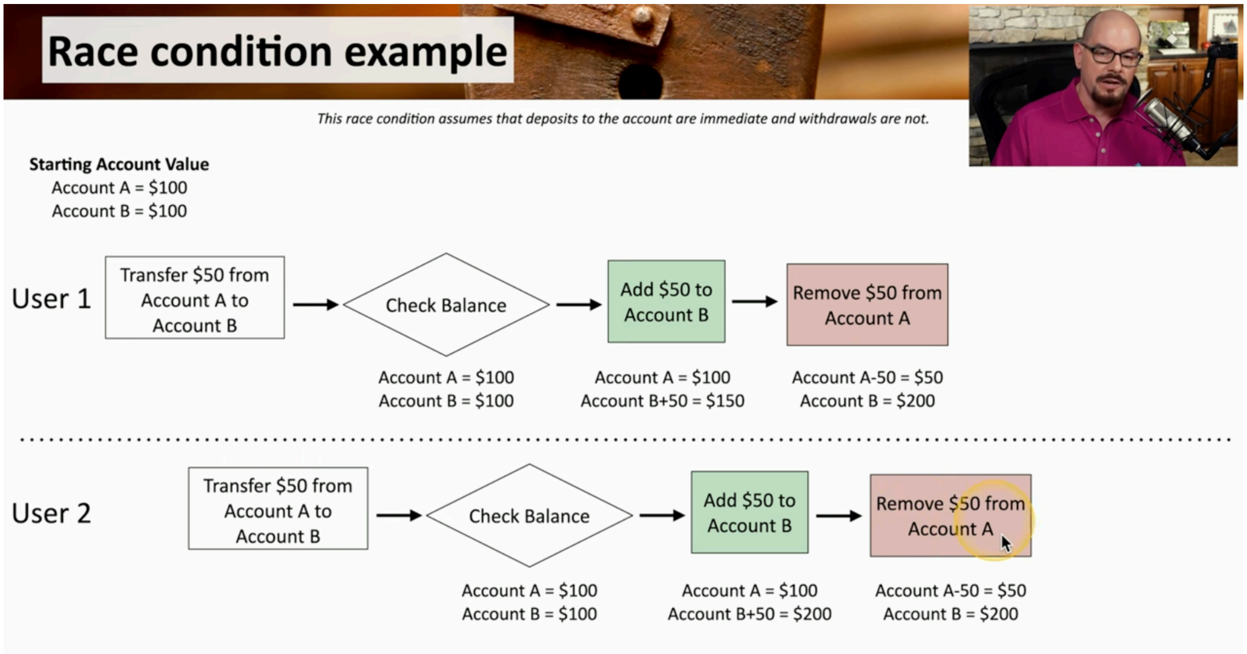
1. The Normal Process:
    - A user needs to change their password. They run the `passwd` command.
    - The `passwd` program runs with elevated privileges (as root) because it needs to write to the protected `/etc/shadow` file.
    - Normally, `passwd` checks if the user has permission and then allows them to change their *own* password.

2. The Race Condition Exploit:
    - Step 1 (The Check): The `passwd` command, running with high privileges, checks the user's permissions and prepares to write to the `/etc/shadow` file. At this moment, the file it intends to modify is the legitimate shadow file.
    - Step 2 (The Switch): In the tiny window *after* the check but *before* the write operation, the attacker quickly replaces the `/etc/shadow` file with a symbolic link pointing to another sensitive file, like `/etc/passwd`.
    - Step 3 (The Use): The `passwd` command, still operating with high privileges, now writes the new password data. However, it is no longer writing to the shadow file—it's writing to the `/etc/passwd` file because of the swapped symbolic link.

Result: The attacker has successfully corrupted or modified the `/etc/passwd` file, which can be used to create a new root-level user account or otherwise compromise the system.

Summary

- A Race Condition is a flaw where the output is dependent on an unpredictable sequence of events.
- TOCTTOU is a common race condition where the state changes between the time a condition is checked and when it is used.
- The exploit relies on the attacker interceding during the tiny gap between the check and the action.
- The consequence is often privilege escalation or unauthorized access, as the system performs a powerful action based on outdated information.



Race condition example

This race condition assumes that deposits to the account are immediate and withdrawals are not.

Starting Account Value

Account A = $100

Account B = $100

User 1

Transfer $50 from Account A to Account B → Check Balance → Add $50 to Account B → Remove $50 from Account A

Account A = $100
Account B = $100

Account A = $100
Account B+50 = $150

Account A-50 = $50
Account B = $200

User 2

Transfer $50 from Account A to Account B → Check Balance → Add $50 to Account B → Remove $50 from Account A

Account A = $100
Account B = $100

Account A = $100
Account B+50 = $200

Account A-50 = $50
Account B = $200