**Threat attacks**

1. Shoulder Surfing x

This involves an attacker observing a user entering their password or PIN. Despite the number pad being jumbled, a keen observer might deduce the pattern based on finger movements, especially if they can make multiple observations over time.

2. Smudge Attacks x

Attackers can analyze smudge marks on the device's screen left by oily residues from fingers to infer commonly used keys or patterns. Even with a jumbled keypad, repeated entries might leave discernible traces that could be exploited.

3. Brute Force Attacks x

An attacker could systematically attempt every possible combination to gain access. While the jumbled keypad introduces a layer of complexity, a machine learning model that’s not properly calibrated might still be vulnerable to such exhaustive methods, especially if there's no lockout mechanism after several failed attempts.

4. Machine Learning Model Poisoning x

If the system adapts and learns from ongoing user behavior, an attacker with access to the learning data might inject malicious data, skewing the model's learning process and potentially allowing unauthorized access.

5. Reverse Engineering the ML Model

An attacker might try to reverse engineer the machine learning model to understand its decision-making process. This could involve probing the system with various inputs to infer patterns or vulnerabilities in how it validates authentication attempts.

6. Spoofing Attacks x

This involves mimicking a legitimate user's behavior. If the attacker can accurately replicate the timing, pressure, and pattern of the legitimate user's interactions with the jumbled keypad, they might fool the system.

7. Replay Attacks x (depends)

An attacker could capture legitimate authentication data (like a sequence of key presses, timings, and pressures) and replay them to gain unauthorized access. This threat is particularly relevant if data transmission between the user interface and the authentication system isn't securely encrypted.

8. Social Engineering

Attackers might use social engineering techniques to trick users into revealing their passwords or other authentication-related information. While not a direct attack on the system, its effectiveness could compromise overall security.

**Attack Models**

1. Observation Attack Model

Shoulder Surfing: Attacker observes the user entering their credentials to learn the password or deduce the pattern of key entries on the jumbled keypad.

Visual Recording: Use of hidden cameras or other recording devices to capture the user's authentication process.

2. Analytical Attack Model

Smudge Analysis: Examining the touchscreen for oily residues left by fingers to infer frequently used keys or swipe paths.

Pattern Analysis: Analyzing the timing and sequence of key entries to identify likely passwords or PINs, even without knowing the exact keypad layout.

3. Algorithmic Attack Model

Brute Force Attack: Systematically trying all possible combinations to guess the correct password. The complexity might be reduced if the attacker gains insights into the machine learning model's behavior or user habits.

Dictionary Attack: Using a precompiled list of common passwords, PINs, or observed patterns specific to the target user or user group.

4. Machine Learning-Based Attack Model

Model Inversion Attacks: Attacker aims to reverse-engineer the machine learning model to understand its decision-making process, exploiting weaknesses in the model's architecture or training data.

Adversarial Machine Learning: Crafting input data that is designed to fool the machine learning model into making incorrect predictions or classifications, potentially allowing unauthorized access.

5. Physical Attack Model

Direct Device Manipulation: Gaining physical access to the device to bypass authentication mechanisms, possibly through hardware modifications or exploiting physical vulnerabilities.

Side-Channel Attacks: Exploiting indirect information leakage from the physical device, such as power consumption, electromagnetic emissions, or acoustic signals, to deduce sensitive information.

6. Network-Based Attack Model

Man-in-the-Middle Attack (MitM): Intercepting communication between the authentication system and the server to capture or manipulate authentication data.

Replay Attacks: Capturing legitimate authentication data and retransmitting it to gain unauthorized access.

7. Social Engineering Attack Model

Phishing: Tricking users into revealing their passwords or security-related information through deceptive emails or websites.

Pretexting: Creating a fabricated scenario or pretext to engage with the user and extract sensitive authentication information.

8. Insider Threat Model

Malicious Insider: An authorized user with malicious intent exploits their access to manipulate or bypass the authentication system.

Accidental Insider: Unintentional actions by legitimate users, such as sharing passwords or leaving devices unlocked, that compromise system security.