**COMP3028 Coursework 3 Group 12 (Task 2)**

**How MFA Improves Security Compared to Single Password Authentication**

Multi-Factor Authentication significantly enhances security by requiring users to verify their identity through multiple independent factors, typically:

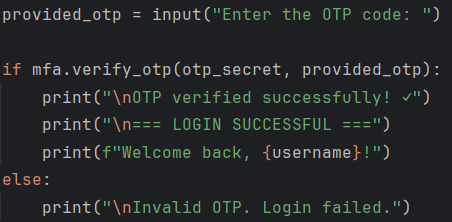
* **Something you know** (password)
* **Something you have** (physical device that generates OTP codes)
* **Something you are** (biometric data)

The code implements a two-factor authentication system using password (first factor) and time-based one-time passwords (TOTP as the second factor).

**Key Security Benefits:**

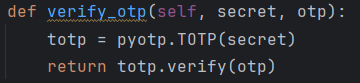
* **Defense Against Credential Theft**:

Even if an attacker obtains your password through phishing, keylogging, or data breaches, they still can't access your account without the second factor.

****

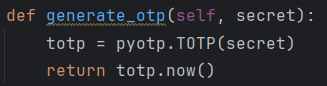
* **Protection Against Brute Force Attacks**:

Attackers can't simply guess passwords repeatedly since access requires the time-sensitive OTP code.



* **Mitigation of Password Reuse Risks**:

Many users reuse passwords across services. MFA provides protection even when credentials are compromised on other platforms.



* **Reduced Impact of Weak Passwords**:

The second authentication factor provides security even when users choose weaker passwords.

* **Protection Against Replay Attacks**:

The TOTP implementation generates codes that are only valid for 30 seconds, making captured codes quickly useless to attackers.

**Threats Mitigated by MFA:**

* **Phishing Attacks**:

Even if users are tricked into revealing their passwords, attackers would still need physical access to the authentication device.

* **Credential Stuffing**:

When attackers try breached username/password combinations on multiple services.

* **Social Engineering**:

When attackers manipulate users into revealing login credentials.

* **Keyloggers and Malware**:

Software that captures keystrokes would only record the password, not the constantly changing OTP.

* **Database Breaches**:

Even if password hashes are stolen, they're useless without the second factor.