OTP exploit

SMS OTP Security Challenges

https://www.unboundsecurity.com/blog/sms-based-otp-is-just-not-good-enough/

SMS OTPs are easy to implement but are very insecure. NIST recommends against using them because they are easily hacked.5 years after the first attack, most organizations still use SMS OTP as their 2FA mechanism. As a result, millions of dollars were stolen due to an exploit in SMS OTP. This vulnerability was caused by the lack of proper encryption when using SMS OTP. To prevent such attacks, virtual enclave should be used instead of SMS OTP based two-factor authentication.In order to achieve security, we need strong authentication methods. But SMS-based 2FA systems create new vulnerabilities that can be used by attackers.

SMS OTP verification systems rely on users' mobile numbers. So if you lose your phone or someone steals it, they could gain access to your accounts. This means that attackers can use SIM swaps to steal your passwords. In 2017, Twitter CEO Jack Dorsey became a victim of this type of attack.

SMS OTPs should never display any message when the phone is locked. This makes them more secure than passwords because an attacker does not need to be nearby to steal the phone or the password.

In order to avoid being hacked by hackers, organizations should implement two-factor authentication (2FA) for their customers. Users must be authenticated using something they know (e.g., password), and something they possess (e.g., smartphone).

SMS OTPs are insecure because they are vulnerable both at the endpoint and during transmission. Organizations should consider using software-based OTPs instead. These are more secure than SMS OTPs because they do not require a third party to verify the user. Software-based OTPs work by generating random numbers and verifying them when needed. However, there are still risks associated with this type of authentication. Users must trust the software vendor to not leak information about the keys, and attackers may use reverse engineering techniques to obtain the secrets.Software OTP authentication eliminates the need for a physical token, but it doesn't solve the problem of switching between apps. Users still have to switch between applications. Third party authenticators are still vulnerable to malware attack. Cloning keys is easy, and the user won't be aware of this.