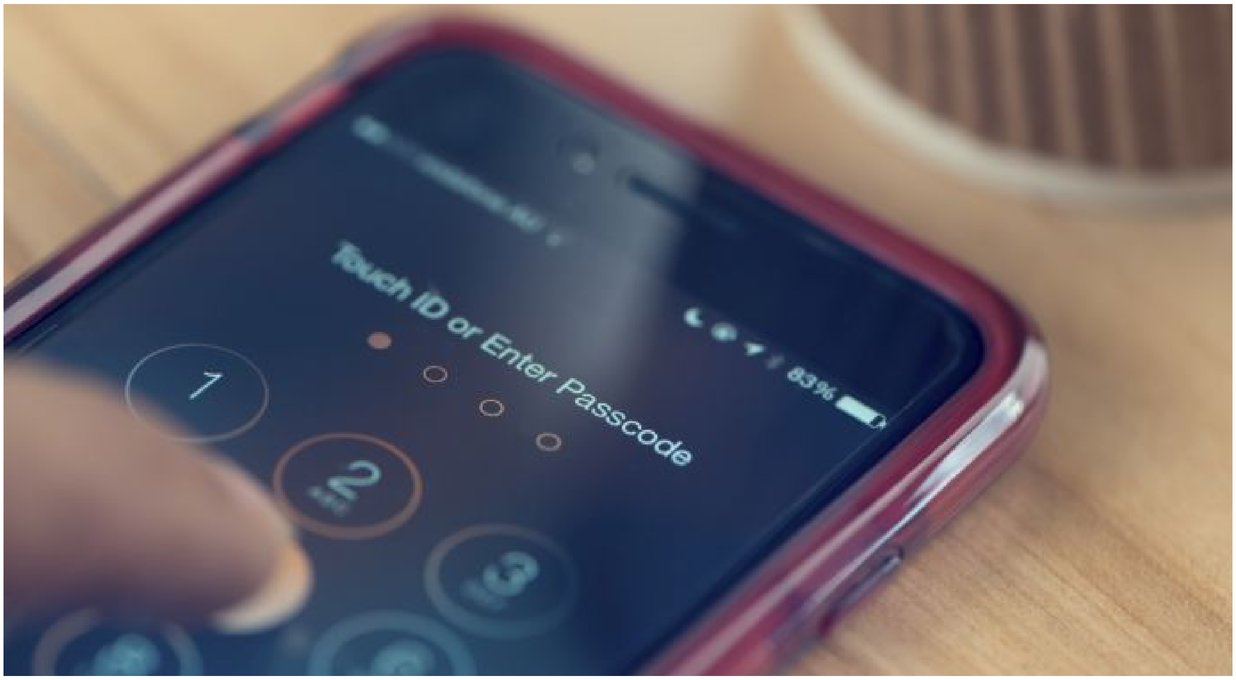
Researchers find vulnerability in two-factor authentication

February 3 2016



Two-factor authentication is a computer security measure used by major online service providers to protect the identify of users in the event of a password loss. The process is familiar: When a password is forgotten, the site sends an SMS text message to the user's mobile phone, providing a verification code that must be entered to reset the password. Two-factor authentication may also be triggered if a user signs on from an unrecognized computer IP address.

Security experts have long endorsed two-factor authentication as an effective safeguard against password attacks. Most methods of compromising this verification process are complex, requiring the malicious actor to be in control of both channels—the one generating the one-time passcode and the channel through which the user completes the verification.

But what if two-factor authentication could be cracked not by computer engineering but by social engineering?

Nasir Memon, Professor of Computer Science and Engineering at the New York University Tandon School of Engineering, along with doctoral students Hossein Siadati and Toan Nguyen, tested the premise that users may be tricked into sharing their verification code with a malicious party using a much simpler tactic: asking them.

Memon and his team constructed a scenario in which a hacker, armed only with the target's mobile phone number, attempts to log into a user's account and claims to forget the password, triggering a verification SMS text. The true user, unaware of hacker's attempt, is likely to ignore the SMS message. But what if the hacker follows up directly with a second SMS requesting that the user forward the verification code to confirm that the phone is linked to the online account? The researchers found that users are as likely to fall for the ruse as they are for a traditional phishing scam. In a pilot test of 20 mobile phone users, 25 percent forwarded the verification code to an attacker upon request. The researchers termed this a Verification Code Forwarding Attack, and published their results at the PasswordsCon 2015, an international conference on password security at the University of Cambridge in December 2015. (Read the full paper).

The researchers followed the test with personal interviews to better understand how they perceived the attack. Were they suspicious? If so, what raised their suspicion? The researchers probed to find out what motivated them to forward the verification code. In this small sampling, most targets were not aware that the two-factor authentication process could be compromised, nor did they notice that the two SMS messages came from different sources—in this case, one from Google and one from the researchers pretending to be hackers. Others explained that they often check their email from public computers in libraries or labs, so requests to verify their identity are common.

Memon and his team acknowledge that while their pilot test was small, the high rate of success lends credence to the Verification Code Forwarding Attack as a method worthy of further study. "Because this kind of attack doesn't require victims to click phishing links or enter sensitive information, like an account or Social Security number, it's easy to understand how it could be very effective," said Memon. "Users are only being asked to forward a random string of numbers that have no real meaning."

Further, he explained that SMS poses particular challenges with confirming the source of messages. "It's not like email, in which you can carefully examine an address to see if it is real. Even sophisticated users don't always know how to source an SMS message, and even if they do, this kind of attack takes advantage of the fact that the target has no context for the message—it appears out of nowhere."

The researchers took the study one step further, surveying 100 email account holders who use two-factor authentication. The survey, conducted on Amazon Mechanical Turk, queried users about their beliefs regarding the security of two-factor authentication, as well as whether they had ever received an unsolicited verification request. The researchers also asked what respondents would do if a major email provider, Google, requested that they forward a verification code.

The results showed that more than 30 percent of those surveyed were unaware that two-factor authentication could be compromised, and more than 60 percent said that they do not routinely verify the source of SMS verification requests. Finally, a full 20 percent reported that they would forward a verification code if Google requested it—about the same percentage as those who fell for the scam in the pilot test.

Memon and his colleagues believe online businesses and service providers may be able to ward off some attacks with simple changes to the two-factor authentication process. First, they suggest appending each SMS text to include a warning about forwarding verification codes. They also note that standardizing the phone numbers that each provider or business uses to send verification requests may help users readily source these SMS messages and feel assured of their authenticity.

Memon pointed out that human decisions prove a much harder process to change than any computer system. "There's trust by association, and as long as there's the sense that a message is coming from an email provider or another trusted site, the hackers will stay in business," he said.

Memon heads the Department of Computer Science and Engineering at NYU Tandon, where he founded one of the nation's first cybersecurity master's degree programs. His recent research has centered frequently on the human elements of security. NYU Tandon has joined with other NYU schools to form the new NYU Center for Cyber Security to research approaches to security and privacy by combining security technology, psychology, law, public policy, and business.

Provided by New York University

Citation: Researchers find vulnerability in two-factor authentication (2016, February 3) retrieved 24 April 2024 from https://phys.org/news/2016-02-vulnerability-two-factor-authentication.html