Bank of America: A Perfect Target for the Man in the Middle Attack

By Ramtin Shams, Chief Technology Officer, GPayments Pty Ltd

Bank of America with 14.3 million Internet banking users and a two factor authentication solution, marginally better than static passwords, could become the first example of a large scale MIM attack when they finalize their two-factor authentication rollout based on PassMark SiteKey, in 2006.

MIM or “Man in the Middle” attack, a term borrowed from cryptography, is where an attacker gains access to a secret key used for encrypting data between a sender and a receiver. The attacker can then eavesdrop between the two parties while passing the information or changing it as needed. In the context of credential theft this is a counterfeit website that interacts with the user on behalf of the real site and passes the information behind the user’s back to the real website.

SiteKey uses computer profiling combined with two-way authentication, to identify the bank to its users, in order to protect them from falling for phishing counterfeits. When a user registers with the system, certain information from the user’s computer is registered with the remote server. The user is also required to load a personalized image or select an image from the bank’s repository as a shared secret. The shared secret is shown, before the user enters their password for login, as proof that they are visiting the genuine bank website.

Bank of America’s two-factor authentication is indeed an improvement over its existing static password authentication but the important question is: ‘How much of an improvement is it?’ Unfortunately the answer is: ‘not much’. The system neither repels attackers nor prevents phishing attacks and is prone to a simple man in the middle attack. Typically a solution repels attackers by increasing their cost and minimizing their gain and it prevents attacks by making it impossible to break in, SiteKey does neither.

SiteKey provides attackers with an unlimited window of opportunity. As far as the attacker is concerned, BofA’s SiteKey authentication is not dissimilar to authentication with static passwords. Once compromised, there is no element of the solution that can contain or limit the attacker’s access to the system. This alone

would justify the effort for attackers to focus their efforts on a large bank such as BofA, where the gain is likely to be substantial.

Using an image authentication as a secret key not only, does not improve the security of the system, but also is a liability. The secret image can be easily compromised by an attacker, while at the same time giving the victim the ultimate proof that the counterfeit site is genuine.

Here is a simple phishing attack that combined with a simple MIM technique can be used to register the attacker's computer with Bank of America and retrieve customers' secret image at the same time:

- A phishing scam hits the customer. The customer takes the bait and visits the counterfeit site.

- The fake site's cover story is that a change has been detected in the customer's configuration, which requires them to re-register their computer for access.

- Bank of America's re-registration requires the customer to provide an alternative authentication such as answering a pre-defined challenge question, which the attacker retrieves from the actual bank website. The attacker passes the question on to the unsuspecting user and the response is simply returned to the bank.

- With the correct response, the bank not only registers the attacker's computer as a legitimate terminal for the customer but also returns the customer's secret image to the attacker as gesture of good faith.

At this stage with the attacker's computer registered, the secret image at hand and a customer who has been trained to trust the secret, well let's just say its up to the attacker what to do with the user next.

About the author:

Ramtin Shams is a security analyst and CTO at GPayments Pty Ltd with more than six years experience in authentication and payment technologies for the financial sector. The author can be contacted at ramtin@gpayments.com