

An OTP scheme robust against man in the middle or realtime phishing.

By Morten Storm Petersen,
Signaturgruppen A/S.

Realtime phishing in OTP authentication infrastructures

As phishing attacks has ruled out username/password solutions, and as attacks against end user computers has driven banks and others away from authentication with keys stored on the user harddrive, OTP solutions has regained momentum.

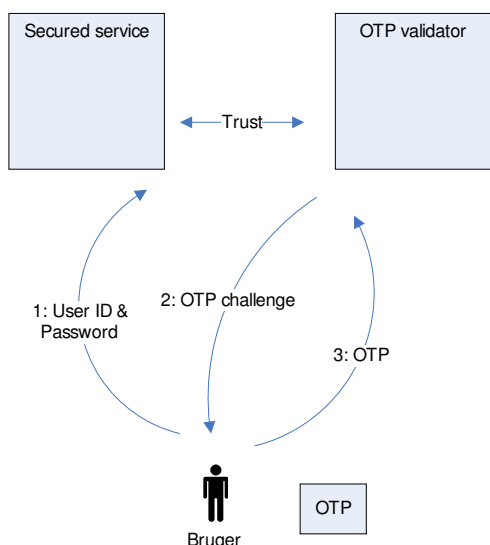


Fig: Simplified flow in an OTP solution with external validator.

Having gone through huge investments in two factor OTP solutions for large customer bases, many companies must realise, that real-time phishing is an easy next step for the hackers to get by the

OTP and back into the customer accounts.

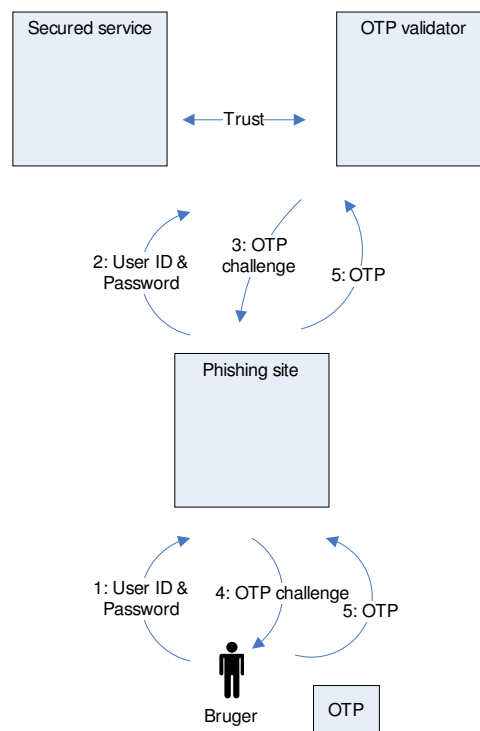


Fig: OTP with realtime phishing

If many different sites uses the same OTP solution (is part of an OTP infrastructure), the job is made a lot easier for the hacker, since the phishing site just has to look like a genuine participant in the OTP infrastructure and not a specific site.

Signaturgruppen has implemented a demonstration attack against a live bank implementation. The demonstration was concluded within one days of coding. After this initial effort, a general attack implementation could be offered on the "market", for others to adjust to a specific target.

So one might think, that a lot of effort and investment in two factor

authentication solutions has gone wasted?

The weakness of the OTP solution is that the shared secret (OTP) is transferred in full to the attacker by the user, and further there is no binding of the secret to the intended transaction.

Real-time phishing or man in the middle attacks against OTP are well known and well described, and several countermeasures has been proposed and implemented. Some of these involves the use of an independent channel, or an advanced OTP device, that allows the user to “sign” a transaction e.g. account number and amount. These countermeasures are costly and not very user friendly.

Solution: binding the OTP to the users computer

Signaturgruppen suggests a new OTP scheme, that rules out the real-time phishing threat.

The scheme takes its offspring in the observation, that in a real-time phishing attack, the OTP will be transmitted to the secured service from a computer, that the user has not used before. The scheme does NOT protect against attacks launched directly from the users computer. This type of attack, often named “man in the browser” as opposed to “man in the middle”, are generally very hard, if not impossible, to safeguard against.

The scheme is based on the fact that the OTP service can perform some fingerprinting of the users

computer either by writing a local file or by registering hardware specifics.

The scheme introduces a special registration process for each new computer, from which the user transmits the OTP. The user must understand, that when this special registration process is requested, it must be done as originally instructed.

Each time that the OTP supplier detects, that a user starts the OTP identification process from an unknown computer, a special “new computer registration” is carried through directly towards the trusted OTP supplier. The registration process can be implemented in a number of ways, as long as it ensures, that it is indeed the computer of the real user, that is registered.

This registration can e.g. be carried out, by having the user open a new browser window on his computer and type in a known web address of the OTP supplier. After a successful identification of the OTP holder, e.g. by using a shared secret, the users computer is registered with the OTP supplier, and the computer is from now on allowed to send in OTPs to the OTP supplier.

The solution preserves the basic mobility of the OTP solution, burdening the user only the first time the user uses a new computer.

The actual registration of the computer can take form of a



“watermark” of the computer hardware, or by simply writing a private RSA key to the user filesystem and registering the corresponding public key to the user account at the OTP supplier.

This process ensures, that a man in the middle can not “pass on” any OTP’s that the attacker might have tricked from the user to the OTP validator, since the attacker is not able to send the OTP to the OTP validator from a computer, that is already registered to the user.

Simple rules for the user to follow

The solution demands only one rule to be understood by the user:

When asked to carry through the special “new computer registration”, only do it directly towards the OTP supplier (in a new browser window, by SMS or how you were instructed), no matter what the given website you want to identify towards says!

Given that the integrity of the user computer is intact and given that the security protocol and implementation of the OTP validator is sound, these countermeasures would provide a real barrier towards real-time phishing and man in the middle attacks , sending the hackers back to the drawing board.

Intellectual property reserved

Signaturgruppen reserves the intellectual property of the ideas presented in this paper, especially concerning the acceptance of OTP at

the OTP validator only after verifying, that the computer transmitting the OTP to the OTP validator has formerly been safely registered with the OTP validator.

