protectoria

www.protectoria.com

Synthetic PIN for Authentication and Authorisation

WHITEPAPER

VERSION 1.0

OSLO · SEPTEMBER 2013

INTRODUCTION

Large-scale, automated attacks have recently been carried out against private and corporate bank customers in many countries. The attackers install malware on customers' computers and in some cases on their phones, and then they carry out illegitimate transactions without customers' knowledge. Examples of high-profile attacks are Operation High Roller[1] and Eurograbber[2], which resulted in the combined loss of 90 million Euros. Also, social networking accounts are being hijacked using similar methods.

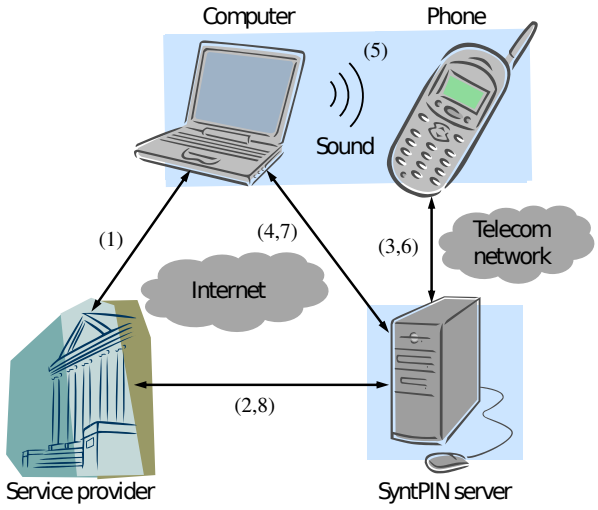
This whitepaper presents Protectoria AS's[3] novel approach to authentication and authorisation, called Synthetic PIN. It is intended for service providers that want to strengthen the security of their services. The Synthetic PIN solution is specifically designed to prevent large-scale, automated attacks against many users.

Problems with existing solutions

Existing commercial solutions for authentication and authorisation, including PIN over SMS, have inherent problems. Some rely on insecure mechanisms such as SMS that are susceptible to forgery or eavesdropping, or they require the user to type PIN codes in cleartext, thus potentially exposing codes to malware. Also, deploying token generators, smart card equipment, or other hardware to users is costly and inflexible as it may require the user to have a formal agreement with the solution provider.

THE SYNTHETIC PIN SOLUTION

The diagram below shows the overall architecture of the Synthetic PIN solution and its environment, consisting of four components: The user's computer and his phone, depicted at the top of the diagram, and a service provider (for example, a bank) and the SyntPIN server, shown at the bottom of the diagram. In addition, the components are connected via networks or sound, drawn as grey cloud shapes in the case of the Internet and the telecom network, and drawn as sound waves in the case of sound played over the computer's loudspeaker. A network communications channel is shown as a line, with arrowheads showing directions of communication. The numbers are explained below.



[1] https://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf
[2] https://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf
[3] Formerly Message Management AS.

Mode of operation

The Synthetic PIN solution supports authenticating users, that is, establishing that a user has the identity he claims to have, and authorising transactions, that is, making an authenticated user confirm or deny a suspicious transaction. For authentication the Synthetic PIN solution may be used as an additional security mechanism following the service provider's own identification or authentication solution.

To perform an authentication or authorisation task the Synthetic PIN solution proceeds as follows. The user is already logged into the service provider's web site, see the channel marked (1) in the diagram. The service provider requests the task by sending a message to the SyntPIN server (2), including the phone number of the relevant user. The SyntPIN server calls the user's phone and waits for the user to answer. Assuming the user answers the call, the server plays a voice message to the user (3). In the case of authentication, SyntPIN server instructs the user to hold the phone up to the loudspeaker of the computer. Then the server sends a unique sound fingerprint[4] to the user's computer (4), and the computer starts playing this sound through its loudspeaker (5). This sound is picked up by the phone and transmitted back to the SyntPIN server in the call (6). Once the sound has been received and verified by the SyntPIN server, authentication has succeeded. If the user does not answer the call or hangs up before the sound is transmitted, then the authentication has failed. The SyntPIN server informs the user about authentication success or failure on the user's computer screen (7). Authorisation of a transaction proceeds similarly, the only difference being that the SyntPIN server's call to the user also informs the user about the details of the transaction, using a synthetic voice. Then, the user is instructed to hold the phone up to the loudspeaker of the computer in case he wants to authorise the transaction, or to hang up the call not to authorise it. Last, the SyntPIN server informs the service provider about the result of the authentication or authorisation task, allowing the service provider to take appropriate action (8).

Trust model

The service provider and the SyntPIN server are trusted parts of the solution, but the user's computer is not assumed trusted and the phone is only partly trusted: The solution relies on trust only in the dedicated voice call part of the phone, not in smartphone capabilities or apps. Furthermore, the solution assumes that the user is aware of all calls placed to his phone and is able to answer and end such calls in the normal manner, that is, the user is in physical control of his phone. See also the section 'Other security mechanisms' below regarding positioning of the user's phone.

SECURITY

Compared with existing solutions the Synthetic PIN solution has the following properties that increase protection against large-scale, automated attacks:

No PIN code sent to the user

This means that there is no security vulnerability related to theft of PIN codes directly from the user's phone, from the Internet, or at the time when the user enters the PIN code—via the computers' keyboard—in the service provider login screen. The latter is vulnerable to keyboard logging malware.

[4]The role of this sound is that of a cryptographic nonce.

SyntPIN server places a call to the user's phone

This lets the user verify the authenticity of the call based on caller identity. Diverting this call to another number without the knowledge of the user or the SyntPIN server is hard since it requires compromising the telecom network or accessing low level functionality on the phone in order to configure call forwarding. Note that making the user's phone answer a call without the knowledge of the user is hard since to achieve this an attacker must compromise the voice call part of the phone and furthermore the attacker must divert sound from the computer loudspeaker into the answered call.

Additional security is ensured if the user's phone is a landline. Mobile phones may be stolen, while landline phones can be protected using traditional physical security measures.

Other security mechanisms

The Synthetic PIN solution offers further security mechanisms that service providers can enable. Tracking the position of a user's phone or computer can help to thwart attacks: these two units should be in close proximity, otherwise there could be a man-in-the-middle attack in progress. One may also require the user to authorise a transaction by tapping a pre-determined code on the phone's touch-screen or its keyboard. In addition, attacks based on setting up hostile call forwarding may be detected through call forwarding detection mechanisms, depending upon telecom network peering agreements.

SCALABILITY

As the Synthetic PIN solution is based on voice calls it is possible to communicate with the user also when he is not on a GSM network, or even not using a mobile phone. Examples of this would be when the user is ported or roaming abroad on a CDMA network (for example, in the United States), or using a landline office phone. For the user this gives extra assurance, as the user can authorise transactions as long as he may be reached with a voice call, which is generally more often than with an SMS.

In addition, variable cost of international calls are lower and more predictable than international SMS. Since there are no PIN codes sent to the user, there is no problem of late delivery or missing PIN codes, especially for ported or roaming mobile users on GSM or CDMA networks.

USABILITY

With the SyntPIN solution users do not have to read or type PIN codes, thus avoiding a cumbersome and error prone step. This can be especially important for users with certain kinds of disabilities, for example, visually impaired or dyslectic users.

This document was written by the Norwegian Computing Center. www.nr.no