SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com

Gatekeeper of Keys

SecurEnvoy Whitepaper

Version 2.0 – 11/2018

Two Part seed Records

Contents

1.1 Introduction

As a house is to a family, so a network is to a company - a place where its own property and belongings are located.
In both cases, the top priority is to ensure 100% security at all times. Many people lock up their possessions in storage with padlocks, because these are considered very secure - after all, only the house owner has the key to open it.
When buying this kind of lock, hardly anyone considers that the locksmith who sold it, or a caretaker in the case of rental buildings, might have a spare key as a security copy. But locksmiths may be robbed by thieves, who would then have direct access to hundreds and hundreds of spare keys. There would be nothing to stand in the way of houses and villas being robbed. This means that constant danger lurks in the background for the residents of houses and apartments - and most people are not even aware of it.

A virtually parallel situation can be found in the digital world - especially where networks are accessed using two-factor authentication (2FA). The method is intended to protect sensitive company documents, but some 2FA providers expose their clients to new, external IT threats. This White Paper explains what damage this could cause, and what aspects companies should pay particular attention to.

1.2 Password Protection no longer enough

House and apartment owners are not the only ones who lock up their possessions; companies also protect their internal data and information from hackers and other cyber-criminals. Passwords are still the most widespread form of protection. Therefore, employees must first prove their identity in order to access the company network. This is done by entering their usernames and personal passwords. But simple password protection alone does not offer enough security, as is made clear by current headlines about massive company hacking: large companies like eBay and Dropbox have recently been affected by thefts of millions of passwords. Damage to a company's finances and reputation is the logical consequence here. So, for network access, companies should introduce a second security check beyond user name and password - as is typical for two-factor authentication solutions.

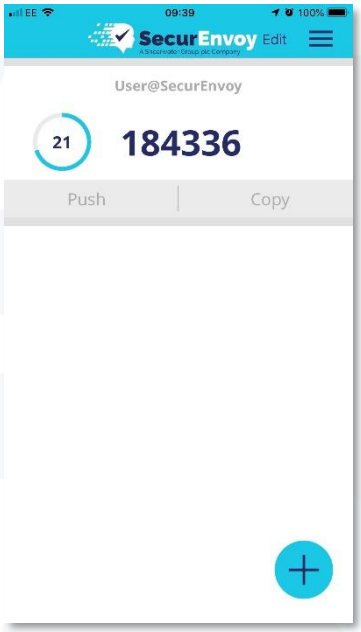
1.3 Losing the Spare Key

Employees install the Authenticator Apps for iOS, Android etc. on their private/corporate smartphones. The app generates the OTP required for the second step of authentication. By entering a PIN and the OTP, employees can gain access via the application to the protected resources in the network. But companies should be aware of one thing in particular: Most 2FA providers create cryptographic keys called seed records when they distribute OTPs, and these keys contain fundamental security loopholes.
Clients must be able to trust that the copy of the key saved by the manufacturer is kept securely and is not accessible to hackers or government authorities. This means the manufacturers have a similar responsibility to that of locksmiths or building caretakers, who must securely store their spare keys just in case something happens.

However, it is known that some 2FA vendors have suffered attacks, in which sensitive seeds were stolen from the company servers.
From the seeds, it was possible to derive millions of OTPs.
Tokens and soft token apps lost an enormous amount of credibility and therefore, many 2FA users are asking themselves whether such providers can even be trusted any more in holding this sensitive information. Are OTPs even safe anymore - their transport methods, and the ways in which they are generated? Is it possible for governments to enforce manufactures to hand over seeds and create easy access to company servers, and thus to commit industrial espionage? In view of the known attacks, these concerns are absolutely justified.
So how can 2FA providers secure the seeds and protect them from third parties?

1.4 Dual protection from password thieves

In contrast to the known attacks and loss of seed records, SecurEnvoy has added an extra level of security.
Unlike the usual process, SecurEnvoy as the 2FA manufacture does not itself generate or save the seed records at any time.
SecurEnvoy ensures this by the automatic separation of the records: one part is created locally on the customers server, while the second is generated using specific characteristics of the mobile device that make it unique, e.g. information about the SIM card, the CPU or equivalent.
When the app generates a passcode, the end device decrypts the first half of the seed record and derives the second half accordingly.
Since one part of the two seed record parts are never located on the employee's mobile device, SecurEnvoy excludes the possibility that attacking malware can steal a seed record. Since the seed record is derived in part from the phone's own hardware fingerprint at time of enrolling, SecurEnvoy clearly can't have a copy of the seed.



1.5 Offline Authentication

The soft token app therefore serves the employees as a secure authentication aid in everyday work. For cases when the mobile signal fails suddenly and the app cannot receive the OTPs, SecurEnvoy has developed the One Swipe technology. It generates secure OTPs in real time, without the need for an internet or mobile phone connection. Similar to a physical token, a new number sequence is provided every 30 seconds for the passcodes. Employees can use the One Swipe app on smartphones, tablets and laptops with the operating systems iOS, Android, Mac OSX, Windows 8, 10

1.6 Token Device Lifecyle

Trying to manage the life cycle of phones being upgraded or repaired will inevitably lead to at least one of them being re-deployed or sold on by mistake.
SecurEnvoy's approach is to only allow the use of one token device per user but to make it very easy for the end user to switch his device should he feel the need to do so.
This approach simply means it is impossible to splatter user's identity across multiple devices as all old seed records are automatically deleted from the SecurEnvoy security server when enrolling a newer device, so that the old mobile device can be used or resold without any concerns.

1.7 No Mobile Device

If an employee has forgotten their mobile device or simply does not own one, they can still participate in virtual legitimisation.
SecurEnvoy facilitates this via a voice call function. The user enters their login details on the login screen as usual.
At the same time, they receive the passcode via a landline phone call from the SecurEnvoy system. The employee then enters the received OTP using the telephone keyboard. In this way they can be authenticated and gain access to the network.

1.8 Text Messages not extinct

But now we return to the present, where many companies continue to use the classic text message method for authentication.
SecurEnvoy enables not only smartphones but also conventional mobile phones, also called feature phones, to be used as tokens.
Thanks to the text message facility, they simply receive the passcodes via SMS.
But what happens if the user has no mobile signal or there is a delay in transmission?
To circumvent this problem in advance, SecurEnvoy has developed a patented process by way of pre-loaded SMS.
This means that once a code has been entered it is immediately replaced by a new numeric sequence for use during the next authentication process. A little SMS trick helps to update the existing message with a new passcode. No new message needs to be sent, and users do not need to delete their old messages.

1.9 Summary

Providers of two-factor authentication, bear considerable responsibility for ensuring that their clients receive the second passcode (OTP) required for a secure login, without third parties being able to see it or trace it back.
If 2FA manufacturers lose cryptographic keys (seed records), hackers can recreate all of a company's passcodes.
SecurEnvoy uniquely removes this glaring security loophole by separating the seed records.
One part is generated locally on the client's server, and the employee's mobile device characteristics derives the second part.
As there is never a time when both parts of the seed record are located on smartphones, tablets etc., malware attacks are 100% extricated.
Two-factor authentication by SecurEnvoy therefore protects the contents of your company network at all times and cannot ever have a copy of the seed.

Please Reach Out to Your Local SecurEnvoy Team...

UK & IRELAND

The Square, Basing View
Basingstoke, Hampshire
RG21 4EB, UK

Sales

E sales@SecurEnvoy.com
T 44 (0) 845 2600011

Technical Support

E support@SecurEnvoy.com
T 44 (0) 845 2600012

EUROPE

Freibadstraße 30,
81543 München,
Germany

General Information

E info@SecurEnvoy.com
T +49 89 70074522

ASIA-PAC

Level 40 100 Miller Street
North Sydney
NSW 2060

Sales

E info@SecurEnvoy.com
T +612 9911 7778

USA - West Coast

Mission Valley Business Center
8880 Rio San Diego Drive
8th Floor San Diego CA 92108

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA - Mid West

3333 Warrenville Rd
Suite #200
Lisle, IL 60532

General Information

E info@SecurEnvoy.com
T (866)777-6211

USA – East Coast

373 Park Ave South
New York,
NY 10016

General Information

E info@SecurEnvoy.com
T (866)777-6211

SecurEnvoy
A Shearwater Group plc Company

www.securenvoy.com