WHITE PAPER
AUTHENTICATION

INTRODUCTION

Spurred by the convenience and availability of cloud services, businesses and other organizations are increasingly moving their operations online.

Furthermore, with many employees working outside a typical office environment and a growing number of external consultants or partners involved, remote access is no longer an optional enhancement but a necessity of modern business. Meanwhile, rising outbreaks of cybercrime and internet fraud have put the question of security in the spotlight.

Under the circumstances, identity management and access control are becoming a necessity as well as a major competitive factor. In addition, it is of no small importance that a security model should allow the possibility of scaling the number of users and applications it protects, preferably without incurring additional expenses.

An unreliable security framework can cause great damage on any system; one which is too rigid can curb the very opportunities it is meant to enable. In matters of IT security, flexibility and adaptability also merits careful consideration.

WHAT ABOUT PASSWORDS?

Though fixed passwords remain the most widely used means of keeping data safe, there is mounting evidence that shows they are neither secure nor easy to use. Furthermore, they require expensive administration at the best of times, taking their toll on employee productivity.

Encumbered by multiple digital identities, users often choose memorable but easily crackable passwords, while password reuse greatly increases the cost of any potential breach. At the same time, freely available password-cracking tools are being developed at an alarming rate. Nowadays even so called strong passwords – those that aren't recognizable dictionary words with common number substitutions – do not pose much of a challenge for cyber criminals equipped with these tools.

Fixed passwords are also extremely vulnerable to attacks by other means, than brute force. Phishing and social engineering exploit the weakest link of a password-based arrangement – the human factor.

In short, while on the face of it, a fixed password may appear to be the simplest and cheepest alternative, in the long run it is a solution that can cause extensive damage, with much time and resources needed to make up for its deficiencies.

STRONG AUTHENTICATION

Instead of banking on a single factor – especially such a frail one such as a fixed password – security-conscious organizations are increasingly turning to strong, two-factor authentication. This means that the authentication takes two of the following credentials into account:

- Something the user knows – a static password or a PIN code
- Something the user has – an object, e.g. a credit card, a token for generating one-time passwords (OTPs) or a smartphone with an application of a similar function
- Something the user is – biometrics, such as a fingerprint or voice recognition

Solutions which combine a fixed password or PIN with an OTP device have gained wide acclaim. After all, a password is a piece of information potentially exposed every time you submit your credentials, and typically unchanged over a period of time, while a one-time password is only valid for one user session.

Since a token is a physical object rather than an easily copied string of characters, getting hold of both the device and the static password poses a greater difficulty and risk for the criminally intent. At the same time, the probability of guessing a one-time code compared to a fixed password is dramatically reduced.

Phishing and social engineering exploit the weakest link of a password-based arrangement – the human factor.

Strong authentication can benefit environments such as educational or health care systems as well as businesses and their clients, making it possible to access sensitive data more conveniently, yet safely. An array of 2FA products and services exist on the market, each with different advantages and disadvantages.

IDENTITIES AND PRIVILEGES

Despite its tremendous importance, authentication is merely one half of the picture. The other aspect of identity management is authorization; establishing not only that the user is who they claim to be, but also whether they have the right to access the resource they requested. The distinction is subtle, but significant.

Managing both authentication and authorization becomes more difficult if it entails different types of users. Consider a system with a large number of users, some of whom have more restricted access than others to sensitive information. For instance, one set of privileges is granted to the majority of employees of a company, another to the management, and a third to external consultants.

With the users' data stored in different systems, it takes additional time and expenses to unify these disparate records and map user credentials to the appropriate permissions. Consequently, introducing a comprehensive security framework can be a complex, time-consuming process, and migration from one such system to another even more problematic.

CAN SECURITY BE SIMPLE?

The most obvious – and probably the only – advantage of traditional passwords over more advanced alternatives is the fact that they take little time and effort for initial deployment and can be applied in a system of any size and structure. However, the cost of password reset is often underestimated and studies show that nearly 20% of helpdesk calls concerns questions about how to solve issues with lost or forgotten passwords.

2FA can sometimes impose certain limitations, whether regarding the number of users included or the devices permitted to access sensitive information. When it comes to the protected resources themselves, one solution may be suitable for a VPN, for example, but not for a cloud service or web application. Introducing or changing the security framework can be taxing in terms of making adjustments to the existing infrastructure.

The login devices mentioned above may not be equally suited for all users. Hardware tokens need to be purchased and distributed safely. Another option is to use text messaging or e-mail to distribute OTPs through something the users already have, like a smartphone with an software token app installed. In terms of security, a hardware token is unsurpassed, but for the kind of information larger user groups needs to access, a software token is often enough to meet the security standards.

An adequate security model should expand the opportunities available to the system in which it is deployed, without intruding upon its operations. Better control over the access to sensitive information should empower the workflow and productivity of users – staff, partners and clients alike.

THE VERISEC SOLUTION

Verisec provides end-to-end security solutions, covering every aspect of the process. The centrepiece is our Freja appliance, an innovative product for securing and managing digital identities with strong two-factor authentication.

However, in addition to the authentication appliance, not only do Verisec provide a variety of login devices, including both hardware tokens and software based ones such as Google Authenticator, but we also handle logistics and programming associated with tokens through Verisec Services. Freja is based on open standards (OATH), enabling you to choose from a broad range of login devices, both hardware and software tokens. User enrolment can be facilitated with our Self-Service Portal, which further reduces administration expenses.

Freja's design is guided by the idea that a good identity management solution ought to include every user – it wouldn't do to provide secure access only for key persons in an organization, while the rest make do with fixed passwords. Therefore Freja comes with a unique pricing model, which remains the same regardless of the number of users. Future proof for growing needs, Freja allows an unlimited number to be added without increasing the licensing cost.

Furthermore, Freja can include different kinds of users, drawing on the resources of existing records and databases without interfering with them. The appliance itself does not store user data; it simply refers to existing directories, as many of them as needed and connects through widely used protocols such as SOAP, Radius and SAML2. This way all types of users can be managed in one centralized system with total control and full flexibility.

Similarly, we provide secure access to an unlimited number of applications without additional cost. Along with remote access to internal networks, web mail, cloud services and web applications, Freja also supports identity federation and single sign-on.

The possibility of a smooth, seamless transition from a legacy authentication scheme to Freja is built in. Users can gradually switch to Freja's authentication, at the pace which best suits your organization, with no impact whatsoever to either business or security.

A flexible solution which allows great freedom of choice, Freja takes remarkably little time to install and is easy to upgrade. It's not only the business model that is based on simplicity – the technology itself is founded on the same philosophy.

ABOUT VERISEC

Verisec is an international IT security company that provides innovative solutions for banking, government and medium to large corporations worldwide. Through a unique combination of products and services, Verisec offers end-to-end solutions in order to secure digital identities and reinforce IT security in our clients' businesses. Verisec has delivered products to more than 7 million users worldwide.

Verisec AB, Box 2034, 131 02 Nacka, Sweden. sales@verisec.com. +46 (0)8 723 09 00. UK phone (toll-free) 0800 917 8815
For more information about Verisec and contact information to our offices in UK and Serbia, please visit www.verisec.com