VALMIDO

White Paper

How to enhance employees' digital credentials?

Gilles Balsan Valmido VP Customer Projects

VALMIDO - 149 avenue du Maine 75014 PARIS France

https://www.valmido.com

contact@valmido.com

VALMIDO

Employees with weak Digital Credentials put businesses at risk

At the core, main IT/OT Security Issues are due to employee credentials theft

Considering the recent years of dramatic increase in company hacks, and their financial and branding impact, there is a clear emergency to address the minimal security enhancements required for all kinds of companies regarding their IT/OT Infrastructure, starting immediately. **(Cf 1)**

The issues that these companies encounter are of various kinds, depending on their business's characteristics and their key choices related to IT Architecture whether on premise, hybrid or cloud based.

For some companies, the roadmap for their planned IT security upgrades are delayed due to operational priorities, while for others it is not yet clear what to implement next. Choosing between different vendors' specific solutions and options also requires a lot of energy. To evaluate these competing offers, they have to start allocating resources, consultants and budget.

In other cases, the budget is shortened due to economic difficulties, and lastly there is also a general lack of skilled IT security people available to evaluate and implement IT security projects.

We saw a majority of hacks that were analysed to be at their origin AI proofed Identity thefts, resulting in data leakage, denial of service, ransomwares, etc. **(Cf 2)**

An immediate point of concern to address ASAP by companies is to enhance the level of assurance in their employees' login infrastructure in order to prevent information stealing which is a root cause for most of companies' hacks. **(Cf 3)**

Even worse, some study shows that current/ex disgruntled employees willingly leak vulnerability information in the majority of internal triggered attacks **(Cf 4)**

Only later, in the long run, can these companies envisage to address the submerged part of the iceberg (the IT systems security overall design).

References:

(1) https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025/
(2) https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/
(3) https://www.microsoft.com/security/blog/2020/03/05/it-executives-prioritize-multi-factor-authentication-2020/
(4) https://www.informationweek.com/security-and-risk-strategy/75-of-insider-cyber-attacks-are-the-work-of-disgruntled-ex-employees-report

The Digital Identity Technologies landscape

There are many ways to address this issue. Some organizations continue to bet on passwords, often at the expense of user experience with more length, more complexity, more frequent changes and some level of automation (e.g. password handlers). Other IAM solutions use behavioural algorithms.

One obvious solution is to use the mobile phone. This is a versatile consumer electronic hardware devices, capable of basic authentication (OTP or push notification), and can even be used as a biometric endpoint device (face recognition or fingerprint).

But smartphones also bring additional problems to the equation:

- "External dependency": organizations depend on the willingness and the security policy of the device manufacturer and/or the OS provider. Android or Apple offer multiple levels of security but typically reserve the best that they have for their own features & applications (For example, NFC was not open to third party usage in iPhones before iOS 14, even just to load a train ticket and the same Android version implementation varies significantly from one device to another).
- "Lack of homogeneity": how can organizations then provide the same consistent level of security to a large number of users who have different models & brands of smartphones? Or even just have their personal smartphones?
- "Permanent connectivity": smartphones are designed to be permanently connected and interact with many different systems. It is great for functionality, but in terms of security it means an increased attack surface at 360 degrees and open 24/7. Every week a list of new vulnerabilities is disclosed (some critical, others more benign)
- "Data is revenue": many Tech companies consider personal data & online history to be a goldmine that they want to resell (Google, Facebook, etc.) or use for themselves (Microsoft, Apple, Amazon, etc.). We are always told that our digital credentials are firewalled & protected, then we hear about remote smartphone hacks where all personal & corporate data is exposed.

So as much as smartphones are a fantastic "all purpose" device, they are made mainly with functionality in mind, not security or privacy.

It is also possible to use third party dedicated endpoints like biometric readers, cameras, or various sensors, wearables or remotely scanning individuals' characteristics. But what about the cost of this extra infrastructure? Is it a good idea for users to share these devices in a work environment in a post Covid world?

There are also third-party personal devices like Smart cards, dongles, or Bluetooth tokens. These are sometimes complex to use (smartcards with PKI) and some will provide limited security (just press the dongle button to authenticate) or will replace long/complex passwords with very short PINs (easy to spot when typing).

Biometric technology is now considered mature, so we need to leverage its usage and shift expectations to match the level of confidence that employees and consumers expect. No visible complexity, but a high level of confidence that a legitimate user is behind the transaction.

So, imagine for a moment a third-party multi-purpose device, acting as "the secure digital extension" of smartphones. Smartphones would provide the rich user interface and this device the security. The security and usage friendliness would be above anything we know with passwords!

Login/password is not the future

The login / password is too fragile to assure security and also cumbersome to manage for the users and organizations. Beyond that, there is no assurance that the legitimate user initiates the transaction. On the Dark Web, there are millions of leaked credentials, sometimes along with detailed step-by-step on how to exploit vulnerabilities for a given target company.

If the digital market initially created a disruption by dramatically changing the rules that were in the previous business environment and former industry economy, there are now new laws that are protecting the usage and sharing of people personal information and especially their biometric data. The remote capture, management and storage of biometric or behavioural data is problematic as it requires a constant guarantee that the system is entirely secure over its whole life cycle; what a challenge!

On the one hand, there are biometric data that are captured locally and are based on templates that are built as unique reference points. They use algorithms that are transparently reviewed by peers and security recognized organizations using state-of-the-art practices for security assessments.

In behavioural authentication solutions, there are data and algorithms that are more fluidly generated and require frequent updates over time. These can also be AI powered changing algorithms. The decision of these systems of “who is a legitimate user” is quite opaque for external evaluation or peer reviews.

This is the reason why there are more and more legislations that are applicable, not continent-wide but rather county-wide or city-wide, that set limits on the usage of AI based “individuals’ authentication systems”. Europe started with DGRP in 2018, but is now establishing its DSA (Digital Service Act) to ensure that citizens and professionals’ data are well protected online.

Additional security requirement is the confidentiality of the data, especially about the personal and uppermost the biometric data, and we have no clue of the enforceability of this information within the smartphone landscape, where the handsets/ OSs vendors do not guarantee anything regarding the confidentiality of the managed data on the device.

What is a “best in industry” digital credential solution today?

Security requires an open evaluation referential, a dedicated certified Hardware for security, (i.e. Secure Element) and a stable software which is also partially certified and with limited attack surface. The software must be upgraded on a regular basis to fix some major security issues (CVEs).

So, we need a system with the following characteristics:

- A certified hardware Secure Element as the security anchor of the solution
- An authentication device with its on-board biometric sensor
- The biometric match decision is directly made on the certified device itself
- The biometric data exclusively resides within the security device
- An on-board screen for a trustful user interface
- Cyphered communication links between the certified device and its external managing system
- Security upgrades available for the software security fixes

VALMIDO

A smooth way to increase the IT Security of your Company without impacting the whole company IT/OT Architecture

From what we have seen above, there is an emergency to both enhance the security and to simplify the usage of the digital credentials of employees in companies' IT Infrastructure. Today it is possible to have both a very high level of security AND a high level of user-friendliness. This is without changing the infrastructure itself.

We propose a simple scheme which is quick to deploy and using an Industry interoperable standard.

Your IAM solution has to change its authentication methods for employees and transition to FIDO v2 (supported by iOS, Android, MacOS, Windows and Linux), see https://fidoalliance.org/

Then you need to equip all your employees with a FIDO v2 hardware with biometric authenticator capability and a Bluetooth device (works in the same fashion on laptop or mobile) at minimum. This is regardless of the laptop or mobile models/brands.

With AI designed cyberattacks now a reality, it is mandatory for any company which is serious about their IT to adopt the highest levels of security available in an effort of futureproof-ness. Those who ignore the subject will unfortunately pay a dear price.

With this simple move, you can considerably limit the risk of having an employee's Digital Identity being stolen and used to penetrate your Infrastructure. Phishing, social media engineering and other similar attacks become obsolete threats overnight. The time and financial cost of managing password changes disappear.

The next step is then to think in depth, with less pressure, about more structural changes in your IT Infrastructure security.

This solution is Zero Trust by design, AI proofed, applicable for IT and OT, it offers traceability and non-repudiation and is compliant to all countries legislations schemes.