Cyber Security for Europe

Policy Recommendation

Support research in the password-less authentication

Context and Findings

A strong password is not enough to guarantee security and, even though it can be safely stored (e.g., as a hash value), it can be subject to various attacks that target the user (e.g., through social engineering) or the system (e.g., password leakage). On average, EU citizens handle **hundreds of passwords** which may lead them either to select easily guessed passwords or password reuse that seriously affects security.

Weak and obsolete authentication methods may compromise individual accounts and put at risk via privilege escalation whole European organisations and critical infrastructures. Most of the existing **password-less authentication** solutions are password managers trying to address password overload and password typing problems. Nevertheless, they **still employ passwords**.

Therefore, the EU should request from Member States and other stakeholders to develop and implement **secure, true password-less authentication solutions such as FIDO**, which have been designed and implemented to counteract password attacks, while they ensure user-friendliness and high interoperability following the latest standards.

Nevertheless, the existing solutions cannot cope with the newly emerging **autonomous and distributed networking ecosystem**, which encompasses users, machines and IoT devices. Thus, **innovative** and **flexible authentication methods** and **protocols** are required that also satisfy the concept of **zero-knowledge proof** and **zero trust**.

The Problem

Although authentication (i.e., the procedure of verifying the identity of a person or a device) is one of the pillars of cybersecurity, most authentication systems today are still based on outdated approaches including the use of passwords. Indeed, password-based authentication solutions are subjected to various attacks, such as phishing, guessing and password file leaks, all of which enable attackers to impersonate their victims. According to Verizon's Data Breach Investigations Report, more than 67% of the data breaches in 2020 were caused by password vulnerabilities[1].

As people use an increasing number of passwords – several hundred passwords per user in some cases – they find it difficult to remember them all, and thus tend to reuse the same weak passwords[2].

Multi-factor authentication (MFA) solutions (such as USB tokens, one-time codes, SMS etc) overcome some of the weaknesses caused by passwords. However, it has been proven that MFA can also be vulnerable to several attacks including theft, bypassing, phishing, etc. Password-less authentication solutions, such as biometrics and USB tokens, have been proposed over the years to replace traditional password-based authentication, which indeed address some of its drawbacks (e.g., password stealing and cracking). Nevertheless, these solutions have not managed to prevail due to several issues, such as applicability, security concerns and lack of knowledge[3].

Currently, the majority of password-less authentication deployments mainly act as password managers, which retain many of the weaknesses of passwords.

The Scene

Over recent years, a new approach to authentication has emerged: password-less authentication. In this approach, users prove their identity by convincing the server that they know a secret without ever revealing it. One such approach is FIDO 2 – a password-less authentication and web standard[4]. Nevertheless, the research that has been conducted in the password-less authentication domain is in its infancy because previous and current work has mostly focused on user-to-device authentication with one-time passcodes. Indeed, there are several issues that are yet to be studied including the complexity and applicability of password-less as well as device-to-device authentication. Finally, further research is needed to establish a common framework that will facilitate the evaluation and validation process of new password-less authentication methods.

Despite its importance, EU research funding has not managed to offer the appropriate technologies and solutions for authentication, which will satisfy all the different networking environments, since only a limited number of research projects focus on advancing authentication. Nowadays, with an autonomous and distributed networking ecosystem, the authentication process involves different entities, (i.e., users, machines, IoT devices, etc), in which each one has different requirements and capabilities.

The Implications

The authentication process is an essential part of ICT and has an immediate application to every sector that appears in the Joint Research Council's taxonomy "A Proposal for a European Cybersecurity Taxonomy"[5]. Thus, the implementation of obsolete or weak authentication solutions in critical sectors, such as energy, health, government, transportation, supply chain, etc., might lead to catastrophic consequences for Europe.

New robust authentication solutions should be studied and introduced to cope with the attack surfaces, due to the evolution of the networking ecosystem and the increase in computing power. Otherwise, Europe will be compelled to import secure password-less authentication solutions from overseas, risking its digital sovereignty.

How does password-less authentication work?

During the authentication process, a client (say, Alice) tries to convince a server (such as her bank) about her identity. Once Alice manages to prove her identity, the bank logs Alice in and gives her access to her bank account(s). In password-based systems, authentication proceeds as follows:

(i) There is a registration phase where Alice gives a secret (e.g., the password) to the bank which stores it in a password database; the secret should not be revealed to anyone else.
(ii) When Alice wants to log in, she provides the bank with her password; if it matches the password stored in the database, Alice is granted access.

Password-less systems work in a similar way: they have a secret, they have a registration phase and they require Alice to prove that she knows the secret.

There is, however, one major difference: the bank will never receive a copy of the secret, not even at registration. Since the secret is not stored in the bank and is not transmitted over the network, it is not subject to traditional attacks such as phishing and password database leaks. However, the obvious challenge now is: *"How is Alice going to prove to the bank that she knows the secret when the bank does not even have a copy of this secret?"*.

Although this sounds very difficult (if not impossible), it can be easily solved with public key cryptography: Alice generates two keys:

(i) her private key (the secret) which is stored in a secure space and never revealed (not even to the bank); and
(ii) her public key which is given to the bank.

The two keys are complementary: what is encrypted with the one can be decrypted with the other.

To verify Alice's identity, the bank proceeds as follows:

(i) it chooses a long random number – say, X (a different one each time) and sends it to Alice
(ii) Alice encrypts X with her private key and sends the result (say, Y) back to her bank;
(iii) the bank decrypts Y with Alice's public key; if the result is X, Alice is granted access.

Policy Recommendations

In the era of ubiquitous access to myriad applications and services that can be granted via different devices and networks, a password, no matter how strong, is not enough to preserve security as it can be subject to theft and phishing. Although EU generously funds the area of cybersecurity, the relevant calls for proposals do not explicitly ask for innovative, user-friendly and secure authentication solutions. This results in the recycling of obsolete password-based authentication techniques.

In this setting, the cybersecurity strategy of EU should focus on stimulating research into password-less authentication to address questions such as exploring ways to enhance the security of device-to-device authentication, to increase the applicability of password-less authentication methods and to evaluate and validate password-less authentication solutions.

In addition, it would be worth investigating whether there are any password-less authentication methods that have not been studied.

1) **Support the design and development of new password-less authentication methods**
Over the next few years, the progress in computing power is anticipated to bring evolutionary changes in the fields of computer science and ICT. This will have an immediate negative effect on the current, mostly password-based authentication methods, since the problems they already have, such as brute-force attacks and lack of user-friendliness, will have increased. Thus, the EU should support research into password-less authentication in order to design and develop methods that are able to cope with the expected advances in computer science. This goal could not be accomplished without supporting research for alternative password-less authentication solutions: for example, attribute-based and device-based authentication.

2) **Provide funding for research on user-machine-IoT authentication**
IoT is a relatively new paradigm that has changed our everyday lives. However, authentication among different entities has not been adequately covered by existing funding schemes leaving a gap in the emerging autonomous and distributed networking ecosystem that is comprised of users, machines and IoT devices. The EU should offer new funding schemes to researchers to design and develop innovative and flexible authentication schemes and protocols, that will satisfy novel concepts such as zero-knowledge proof and zero trust.

References

1 Verizon, 2020 Data Breach Investigations Report, https://www.verizon.com/about/news/verizon-2020-data-breach-investigations-report

2 Papadamou, K., Zannettou, S., Chifor, B., Teican, S., Gugulea, G., Caponi, A., ... & Sirivianos, M. (2019). Killing the password and preserving privacy with device-centric and attribute-based authentication. IEEE Transactions on Information Forensics and Security, 15, 2183-2193.

3 Angelogianni, A., Politis, I., & Xenakis, C. (2021). How many FIDO protocols are needed? Surveying the design, security and market perspectives. arXiv preprint arXiv:2107.00577.

4 W3C, 2019, W3C and FIDO Alliance Finalize Web Standard for Secure, Passwordless Logins, https://www.w3.org/2019/03/pressrelease-webauthn-rec.html

5 Nai, F., Neisse, R., Hernandez Ramos, J. L., Polemi, N., Ruzzante, G. L., Figwer, M. and Lazari, A., A Proposal for a European Taxonomy, JRC118089, Publications Office of the European Union, Luxembourg, 2019.

Contact

This brief was produced by members of the CyberSec4Europe consortium.
Contact person: Professor Christos Xenakis xenakis@unipi.gr

CyberSec4Europe is funded by the European Union under the H2020 Programme Grant Agreement No. 830929. These results reflect only the authors' view and the Commission is not responsible for any use that may be made of the information it contains.