Improving strong mobile authentication with structural diversity and user-friendliness

Samy Kambou & Ahmed Bouabdallah
IMT Atlantique
IRISA, UMR CNRS 6074
F-35576 Cesson Sévigné, France
{samy.kambou, ahmed.bouabdallah}@imt-atlantique.fr

***Abstract*—This paper introduces an original and strong authentication method using a two-factor scheme enhanced by network channels and devices diversity. The proposed solution combines an OTP-based approach using an IoT object as secondary device in addition to the mobile phone. Authentication factors are transmitted over different channels (LTE, LPWAN, ...) via different devices thus greatly reducing the attack surface. To avoid depending on the protocol security specificities used to instantiate a channel, we use a security layer ensuring end-to-end encryption of the transferred sensitive contents. In addition, diversity can be leveraged by exploiting its inherent modularity to infer other approaches. We give an example of another authentication method equivalent for the robustness to the first one but which is more ergonomic and user friendly.**

***Index Terms*—strong authentication, multi-factor authentication, internet of things, one-time password, diversity, ergonomic authentication**

I. Introduction

The improvement of smartphones with their advanced features has gradually made them the preferred portable computing devices (replacing laptops) and personal trust devices. They are also increasingly used to access online services, including those particularly sensitive and/or critical ones requiring high security. Generally, the technique used consists in authenticating the subscribers by verifying the validity of the proof of their identity. Even if user authentication is a common requirement for those Web/Mobile online services, many still use weak authentication solutions (username/password) vulnerable to attacks. The design of modern systems combining mobility and criticality requires a higher level of security, which can only be achieved by incorporating robust identity protections based on strong authentication approaches.

Multi-factor authentication (MFA) [1] has emerged as an effective way to fill gaps and strengthen initial authentication techniques based on a single factor. By deftly combining several simple one-factor authentication methods, they reduce the overall attack surface of the entire method and thus increase its robustness. When the authentication process requires as in our case, to remotely attest the authenticity of a claimed identity, we argue that the multi-factor principle must also be applied to the communication channels as well as to end point devices.

This work has received funding from the France Brittany region research and innovation program AAP PME 2016, under grant agreement number 16004254, V2OLTERES project.

We investigate this view by designing a two-factor (2FA) method [2] resting on two distinct end points defined by a smartphone and a smart-Thing [3] and involving also distinct communication stacks when interacting with the authentication server. The mobile phone submits through LTE[1] (Wi-Fi is also possible) the first factor to the authentication server. After its validation, this one bootstraps the second OTP[2]-based authentication by transferring a nonce to the smart-Thing through the mobile phone. The smart-Thing finally computes the challenge and directly sends it to the authentication server using a communication protocol from the LPWAN[3] [4] family. To remain independent of the security features of the various communication stacks used, we introduce a security communication layer which ensures end-to-end encryption for the sensitive data. To the best of our knowledge, there have been no other authentication scheme proposed that use an LPWAN network as an alternative channel to provide 2FA from a mobile to web services.

The paper starts by recalling some iconic examples of multi-factor authentication schemes and a brief introduction to IoT[4] environment. It continues with a presentation of the proposed strong authentication method with a detailed description and analysis of the authentication protocol. The paper is concluded with an illustration of the inherent modularity involved by the diversity. We give an example of derivation of another authentication method as robust as the first one but which is more ergonomic and user-friendly.

II. Related works

A. Multi-factor Authentication

Several MFA systems have been proposed for a wide variety of purposes. Some of the most recently proposed mobile-based authentication are as follows.

TDAS [5] is a touch dynamics based MFA system for mobile devices. The proposed approach aims to study the feasibility and benefits of adopting an authentication method based on touch dynamics mechanism by integrating it with the PIN-based authentication method. The authors presented

[1]LTE : Long Term Evolution
[2]OTP : One-Time Password
[3]LPWAN : Long Range Radio Wide Area Network
[4]IoT : Internet of Things

how the data set may be used to strengthen the protection of resources that are accessible on mobile devices.

Another approach is by Crossman and Liu [6], who propose a 2FA based on NFC[5] smartphone devices. Firstly, users are asked to enter a password which unlocks the protection of the key on their mobile phones. Then, the key is transferred through NFC to complete the authentication process. In this system, the two factors are managed by the same mobile phone. This assumes a central point of vulnerability that can potentially be used by an attacker. Indeed, if the attacker compromises the mobile phone, the two authentication factors will be easily available.

Barkadehi et al. [7] proposed another 2FA solution by using the mobile phone as a mirror. In their proposal, a web application uses a username/password as an authentication factor in the first step and then a white box will be shown to the users. The users cannot see the mouse cursor in the box but must move their mouse in the box in order to click the right second password. At the same time, they receive a notification on their mobile phone to open the mirror application. Then, they must accept the received request to continue the authentication process and they will see their web-based cursor on a shuffled keyboard in their mobile application. To conclude the authentication process, the users need to select their second password. After a valid authentication process, the users will have access to a web service through their laptop.

B. IoT environment

With the evolution of wireless networks and Internet services, intelligent objects are well integrated into our daily life to provide customized IoT to individuals. Currently, smart-Things are able to interconnect, store data, send and receive commands to perform tasks requested by users. Heterogeneous system architectures are formed, in which different types of smart devices and relevant communication techniques are deployed. Therefore, conventional security mechanisms [8] must be refined to fit the requirements from IoT environment.

We used an IoT device in the proposed OTP-based 2FA scheme. This smart-Thing must provide a network of the LPWAN family such as LoRa/SigFox networks or more recently the 3GPP technologies dedicated to the IoT which are LTE Cat-M and NB-IoT. The device must be an active object capable to perform cryptographic operations.

III. Strong Authentication for Web Services

Strong authentication is a technique relying on more than one authentication factor. By combining *"something you have"* defined as a *Possession factor (Pf)* and *"something you know"* representing a *Knowledge factor (Kf)*, an attacker needs to physically steal your hardware token and also learn your password. This 2FA scheme provides improved protection. In addition, communication channels' and devices' diversity is another way to further improve the security of an authentication scheme. By this ways, attacks such as man in the middle or eavesdropping are much more difficult to carry out since the attacker must simultaneously control both channels and devices. We introduce below a strong authentication method on mobile using an IoT device and exploiting these two improvements.

To authenticate a user on his smartphone and using an IoT device as a security token, some components must be in place. Fig. 1 shows the basic architecture and the main components used to design the proposed strong authentication scheme.

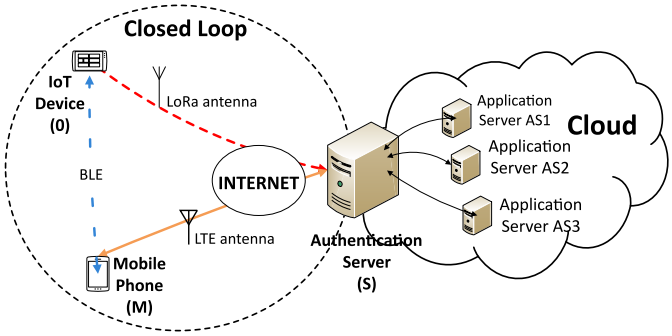

Fig. 1. Architecture of mobile authentication using an IoT device

The user must have a smartphone (M) connected to Internet through LTE or Wi-Fi and also be in possession of an IoT device (O). These two devices must be equipped with BLE[6] or NFC technology that is increasingly be leveraged to create more mobile-friendly experiences. By using his mobile, the user can access to web services subject to prior authentication. The web services hosted by servers disseminated in the Cloud are connected to S which is the front-end that will manage the authentication process. S is also connected to a LPWAN network (LoRa/SigFox) via Internet allowing in this way its communication with O.

We propose a strong authentication scheme involving two distinct user's devices which communicate over different networks. One important point concerns the fact that both devices are controlled by the same user. This is ensured by a *closed loop* going through all the components involved in our architecture illustrated in Fig. 1. The loop starts in the mobile requesting the service, goes through the network with S and then via the IoT device and back to the mobile. This closed loop can be realized in several ways. Below, we describe how to use it in our strong authentication scheme.

IV. Authentication Protocol in Detail

We first summarize in the following table, all the notations used in the descriptions below.

A. Protocol description

The proposed method rests on three distinct channels:

- a *primary* channel between the mobile phone M and the authentication server S
- a *secondary* channel between S and the IoT device O

[5]NFC : Near Field Communication

[6]BLE : Bluetooth Low Energy

TABLE I
NOTATIONS

u_{id} / pwd	user identity / password
M	mobile phone
O	IoT device
S	authentication server
id_m / id_s	mobile identity / server identity
t_1 / t_2	authentication token / access token
sec_{OTP} / cod_{OTP}	OTP secret / OTP Code
K_*^{priv}, K_*^{pub}	private/public key
h_1/h_2	hash functions
$E_{sec}(*)$	encrypt function with the secret sec
$Sg_{see}(*)/XSg_{see}(*)$	signature/verification with the seed see

- an *inter device* channel between O and M

In the developed prototype, we instantiate these three categories respectively with LTE, LoRa and BLE. There are thus plenty of other choices which must however take into account the technical constraints imposed by the devices. These three channels require at least confidentiality and integrity for the exchanged messages. To avoid depending on the security features of the protocol used to instantiate a channel, we use a security layer detailed in section IV-B to independently guarantee the requirements for each communication channel.

We focus on the data flow required for an authentication as outlined in Fig. 2, the steps of which are detailed below:

1) By using his mobile phone M, the user submits a username (u_{id}) and password (pwd) to the authentication server S. These credentials (F1) are transmitted over an LTE link. This is the initial step of the authentication protocol during which the first *Kf* factor is used.
$$M \rightarrow S : [u_{id}, pwd]^{LTE}$$

2) S verifies the received data. If the data match with those stored in the database (DB), S replies with an authentication token (t_1) and an OTP secret (sec_{OTP}). t_1 is represented as a JWT (JSON Web Token) containing at least the u_{id} and works as a session identifier. sec_{OTP} is a random number generated at each authentication request. It is used as a seed in step 4 below.
$$S : u_{id}; pwd =? \ DB\{u_{id}; pwd\}$$
$$S \rightarrow M : [t_1, sec_{OTP}]^{LTE}$$

3) M verifies that S generated the OTP secret sec_{OTP}. Both received data are sent to O through a BLE link.
$$M : Generator(sec_{OTP}) =? \ S$$
$$M \rightarrow O : [t_1, sec_{OTP}]^{BLE}$$

4) O generates an OTP code (cod_{OTP}) by applying a function ($func$) involving sec_{OTP}. cod_{OTP} has a predefined validity period and is associated with t_1 to build a new credential (F2) needed to the second step of the authentication protocol. This second *Pf* factor is sent to S via a LoRa network.
$$O : cod_{OTP} = func_{OTP}(sec_{OTP})$$
$$O \rightarrow S : [t_1, cod_{OTP}]^{LoRa}$$

5) S computes its own version of OTP code ($Xcod_{OTP}$) and compares it to the one contained in the credential (F2). If the data match, S validates the authentication and replies to O with an access token (t_2).
$$S : cod_{OTP} =? \ Xcod_{OTP}$$
$$S \rightarrow O : [t_2]^{LoRa}$$

6) O forwards the access token to M via the BLE link.
$$O \rightarrow M : [t_2]^{BLE}$$

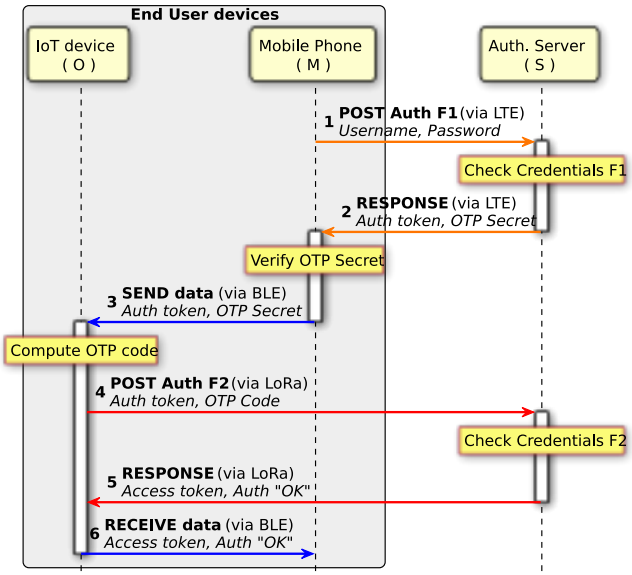

Fig. 2. Data flow of Authentication Procedure

B. Security enforcement of the protocol

Security brings a panoply of challenges in the authentication protocol design. It is therefore very difficult to build a secure authentication protocol [9]. Formal proofs could provide guarantees on the correctness of the protocol. However failing to provide a formal proof which at the time of writing this paper is still in progress, we introduce below the sound principles followed in the design of this protocol.

Firstly, OTP is used as the second authentication factor. The OTP codes are generated by the IoT device (*Pf*) and can therefore appear totally random. Each OTP code is only used once. By changing each time a code is needed, OTP solution introduces liveness. This is an important security issue. Secondly, we took advantage of JWT (JSON Web Token) which are tokens using a container to transport data between interested parties in JSON. We use them to authenticate all exchanged requests in a RESTFUL approach. They are defined with an expiration time that avoids forever valid tokens. The tokens are also protected against replay attacks by applying timestamps. Finally, The three communication links are secured with encryption algorithms.

1) Channel Mobile Phone ↔ Authentication Server:

a) Key Agreement: Before any data transmission, ECDH(E) (Elliptic Curve DiffieHellman, where final "E" stands for "ephemeral") and ECDSA (Elliptic Curve Digital Signature Algorithm) algorithms are used to create a secure channel between each mobile phone and the authentication server. These algorithms allow to define a trusted session key (ms). ECDH [10] is a well-known key agreement protocol used to define a shared secret over an insecure channel. Each involved party must have an elliptic curve public-private key pair. ECDH(E) is a variant of ECDH which provides temporary key pair instead of trusted static key pairs (via a certificate). ECDSA [11] is a variant of Digital Signature Algorithm (DSA) which uses the elliptic curve cryptography. This algorithm is used by a signatory to affix a *digital signature* on data and by a checker to prove the validity of the signature. Each party involved has a public-private key pair. The private key operates in the signature generation process and the public key is used for the signature verification. ECDSA provides message authentication, integrity and non-repudiation.

- M generates its keys pair (K_m^{priv}, K_m^{pub}) and sends its public key and its signature to S.
$$M : K_m^{priv}, K_m^{pub}$$
$$M : Sg_{K_m^{pub}}(h_1(id_m))$$
$$M \rightarrow S : [K_m^{pub}, Sg_{K_m^{pub}}(h_1(id_m))]^{LTE}$$

- S verifies the received signature to ensure that the data come from M (we make the assumption that S has previously registered the respective identities of all the legitimate devices which can be used for a user authentication). If the data come from a known device, S generates its pair of keys (K_s^{priv}, K_s^{pub}). Then, it computes the session key (ms) using its private key and the public key of M. Finally, S replies to M with its public key and its signature.
$$S : XSg_{K_m^{pub}}(h_1(id_m)) =? Sg_{K_m^{pub}}(h_1(id_m))$$
$$S : K_s^{priv}, K_s^{pub}$$
$$S : ms = Compute\ [K_s^{priv}, K_m^{pub}]$$
$$S \rightarrow M : [K_s^{pub}, Sg_{K_s^{pub}}(h_1(id_s))]^{LTE}$$

- M verifies the received signature to ensure that the data come from S (we make the assumption that M has previously registered the identity of the authentication server S). Then M computes the session key (ms) using its private key and the public key of S.
$$M : XSg_{K_s^{pub}}(h_1(id_s)) =? Sg_{K_s^{pub}}(h_1(id_s))$$
$$M : ms = Compute\ [K_m^{priv}, K_s^{pub}]$$

b) Symmetric Encryption: After this negotiation, the channel is secured with the AES cipher [12] (standard recommended by NIST) using the session key (ms) to provide end-to-end data encryption and integrity ($E_{ms}(*)$). Furthermore, OTP secret is signed ($Sg_{id_m}(*)$) by the authentication server using the mobile identifier as a seed. Thus, the secure data are completely binded to a specific mobile phone which is by the way ensured that sensitive information received on this channel come from the authentication server. The complete respective expressions of step 1 and 2 introduced in section IV-A are:

$$M \rightarrow S : [E_{ms}(u_{id}), E_{ms}(h_2(pwd))]^{LTE}$$
$$S \rightarrow M : [E_{ms}(t_1), Sg_{id_M}(E_{ms}(sec_{OTP}))]^{LTE}$$

2) Channel Mobile Phone ↔ IoT device: This channel is secured with the AES symmetric encryption scheme. More precisely, the AES cipher with 128-bit pre-shared key length (mo) is implemented to provide end-to-end data encryption. The data being transferred over this channel are tokens and OTP secrets which are already secure. Step 3 and step 6 of IV-A are refined below:

$$M \rightarrow O : [E_{mo}(E_{ms}(t_1)), E_{mo}(sec_{OTP})]^{BLE}$$
$$O \rightarrow M : [E_{mo}(E_{ms}(t_2))]^{BLE}$$

3) Channel IoT device ↔ Authentication Server: This link is secured with the AES cipher with 128-bit pre-shared key length (so) to provide end-to-end data encryption. Step 4 and step 5 of IV-A are refined below:

$$O \rightarrow S : [E_{ms}(t_1), E_{so}(cod_{OTP})]^{LoRa}$$
$$S \rightarrow O : [E_{so}(E_{ms}(t_2))]^{LoRa}$$

V. Leveraging diversity of the proposed method

A. Modularity of the authentication

The diversity of the proposed approach can be nicely leveraged to clarify the modular structure of the protocol. Fig. 3 gives an abstract representation of the main components of the protocol by emphasizing this diversity.

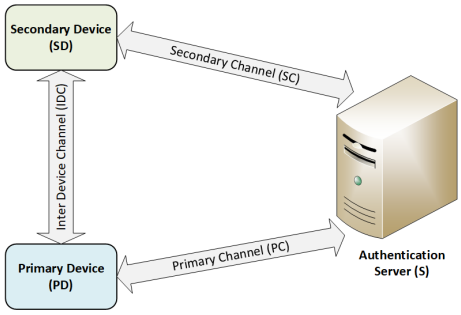

Fig. 3. Generic two-factor mobile authentication (2FA)

The proposed approach consists of two separate phases each one centered on a device and articulated to each other via the authentication server S. We define the first phase ϕ_1 of our method as the one involving the first authentication factor *password*. Similarly, the second phase ϕ_2 is the one resting on the second factor *OTP code*. Each phase ϕ includes an *ascending* part written ϕ^{up} defined by the transfer and the validation of the authentication factor and a *descending* one written ϕ^{down} consisting in the distribution of the result towards the primary device:

- ϕ_1^{up} : PD → PC → S
- ϕ_1^{down} : S → PC → PD
- Articulation between the two phases : S
- ϕ_2^{up} : S → PC → PD → IDC → SD → SC → S

- ϕ_2^{down} : S $\rightarrow$ SC $\rightarrow$ SD $\rightarrow$ IDC $\rightarrow$ PD

The robustness of the protocol is ensured by the second phase. We argue that the granularity of the previous decomposition can be leveraged to derive another protocol satisfying complementary requirements while keeping the same robustness. We are interested in what follows to improve the ergonomy of our approach. We will in this way focus on modifying the first phase which concerns the relation between the end user and his primary device. Such modification has to be transparent to the second phase.

B. Ergonomic alternative to password

As modern portable devices, smartphones have become widespread and are often used as the main gateways for many online services requiring authentication. However, traditional authentication method using username/password credentials may not be convenient or applicable in certain use cases. For example, people with difficulties in fine motor control or soldiers on a battlefield may not be able to enter their credentials in a timely manner. Furthermore, it has been demonstrated that username/password authentication causes serious security vulnerabilities for people and web services since they are easily guessed, difficult to manage across a variety of systems, susceptible to major hacks and stolen.

Biometric authentication is a system that uses a unique physiological characteristic of the user to replace the need for a username/password. Indeed, many persons already use fingerprint scanner on their smartphones to avoid manually typing a password every time they want to unlock their mobile. Using fingerprint approach to log into a web service can be a natural way to improve the robustness of the traditional username/password credentials and also make the authentication process fast and easy to use.

Fig. 4. Fingerprint authentication with smartphone

In this section, we propose to substitute the first traditional *password* factor (*Kf*) with a biometric factor defining an *Inheritance factor If* and referred as *something you are*. As illustrated in Fig. 4, fingerprint process is simple and intuitive. With his mobile M, a user just needs to rest his thumb on the mobile's fingerprint scanner. Once the user's thumbprint is *locally* confirmed, some data that codes the user's biometric identity is encrypted and transmitted to the authentication server S for verification. S decrypts that information and after its verification triggers the second phase.

VI. Acknowledgment

The authors thank the company Acklio which graciously provided them with access to their LoRa network.

VII. Conclusion

In this article, we have proposed an original and strong authentication method dedicated to mobile phones based on IoT devices. The user owning an LPWAN-enabled hand-held device may directly access any web-based service through his mobile phone. Using an IoT device as a secondary device provides a very flexible and secure solution appearing as a very interesting alternative. As far as we know, this is the first authentication scheme using an LPWAN network as an alternative link to provide two-factor authentication from a mobile to web services.

The proposed method involves a first traditional authentication factor enforced by a second factor based on OTP. The inherent modularity of the global approach allows the transparent substitution of the first factor by other user friendly and cheap authentication methods. We have shown how this works by moving from the first factor to a basic biometric technique. This last part concerns the development of an authentication method which is simultaneously highly robust, ergonomic and user friendly. It will deserve more attention and it will be systematically investigated in a future work. A test platform has been implemented to evaluate the feasibility of the proposed schemes.

References

[1] A. Ometov, S. Bezzateev, N. Mkitalo, S. Andreev, T. Mikkonen and Y. Koucheryavy, "Multi-factor Authentication : A Survey," Cryptography, Vol. 2, Issue: 1, 2018.

[2] M. H. Eldefrawy and K. Alghathbar and M. K. Khan, "OTP-Based Two-Factor Authentication Using Mobile Phones," 2011 Eighth International Conference on Information Technology: New Generations, pp. 327–331, Apr. 2011.

[3] M. Kuniavsky, "Smart things: ubiquitous computing user experience design," Elsevier, 2010.

[4] L. Krupka, L. Vojtech and M. Neruda, "The issue of LPWAN technology coexistence in IoT environment," 17th International Conference on Mechatronics - Mechatronika (ME), pp. 1-8, Dec. 2016.

[5] P. Shen Teh, N. Zhang, A. Beng Jin Teoh, K. Chen, "TDAS: a touch dynamics based multi-factor authentication solution for mobile devices," International Journal of Pervasive Computing and Communications, Vol. 12 Issue: 1, pp.127–153, Feb. 2016.

[6] M. A. Crossman and H. Liu, "Two-factor authentication through near field communication," IEEE Symposium on Technologies for Homeland Security (HST), pp. 1–5, Mar. 2016.

[7] M.H. Barkadehi, M. Nilashi, O. Ibrahim, "A novel two-factor authentication system robust against shoulder surfing," J. Soft Comput. Decis. Support Syst., Vol.4 Issue: 1, pp. 19–25, Feb. 2017.

[8] Z.K. Zhang, M.C.Y. Cho, C.W. Wang, C.W. Hsu, C.K. Chen, and S. Shieh, "IoT security: ongoing challenges and research opportunities.," IEEE 7th international conference on service-oriented computing and applications, pp. 230-234, Nov. 2014.

[9] M. Abadi and R. Needham, "Prudent engineering practice for cryptographic protocols," IEEE transactions on Software Engineering 22 (1), 6-15, 1996.

[10] A. Maryam, S. Baharan, A. Difo, R. Amirhossein and O. Habeeb, "Diffie-Hellman and its application in security protocols," International Journal of Engineering Science and Innovative Technology (IJESIT), Vol.1, pp. 69–73, Nov. 2012.

[11] J. Don, M. Alfred and V. Scott, "The elliptic curve digital signature algorithm (ECDSA)," International journal of information security, Vol.1 Issue: 1, pp. 36–63, Jul. 2001.

[12] V. Saicheur and K. Piromsopa, "An implementation of AES-128 and AES-512 on Apple mobile processor," 14th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), pp. 389-392, Nov. 2017.