Securing Communication 2FA Using Post-Quantic Cryptosystem: Case of QC-MDPC- McEliece Cryptosystem

Kouraogo Yacouba, LabMiA-SI, Faculty of Sciences, Mohammed V University in Rabat, Rabat, Morocco
Orhanou Ghizlane, LabMiA-SI, Faculty of Sciences, Mohammed V University in Rabat, Rabat, Morocco
Elhajji Said, LabMiA-SI, Faculty of Sciences, Mohammed V University in Rabat, Rabat, Morocco

ABSTRACT

Many financial institutions interact with their customers via short message services (SMS), which is today one of the fastest and most powerful means of communicating information around the world. This information can sometimes be an access code such as the unique password (OTP) for two-factor authentication (2FA) or banking information and personal identities. All this data is confidential, and it is a major disadvantage to send them since an SMS service does not provide data encryption during network transmission and on mobile. Recently, OTPs via SMS have suffered from strong attacks that intercept messages. In order to avoid attacks and offer effective content security to 2FA credentials sent via SMS, the authors propose an SMS encryption mechanism using a post quantic cryptosystem quasi-cyclic MDPC and an electronic signature of the OTPs. Finally, this article performs an implementation and a security analysis of the proposal.

KEYWORDS

2FA, ECDSA, Mobile Security, mTAN, QC-MDPC McEliece

INTRODUCTION

Nowadays, many organizations and companies operate online. Commercial institutions, banks and many other parts of the society are taking advantage of the benefits of e-business by opening the access to networks and services to their employees, partners and customers. Thus, mobile devices are used today as an alternative to online transaction systems for authentication.

In this context, the traditional login / password authentication mechanism is not considered secure enough to be used in many security-critical applications, such as online banking. Two-factor authentication systems (2FA) promise a higher level of protection by extending the authentication factor to what the user owns (a hardware token or a smartphone) or who the user is (biometrics) (Dmitrienko, Liebchen, Rossow, & Sadeghi, 2014) However, today, it is very easy to carry out increasingly sophisticated attacks on two-factor authentication systems (2FA), which not only compromise a device (PC) but also take control of other devices (Mulliner, Borgaonkar, Stewin, & Seifert, 2013) On the other hand, biometric authentication is relatively expensive. Hardware tokens

DOI: 10.4018/IJISP.2020040106

Copyright © 2020, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
such as OTP generators (Schartner & Burger, 2011) are cheaper, but still generate additional costs for users. In this context, single passwords (OTPs) offer a promising alternative for 2FA systems. Thus, 2FA systems that use mobile devices (such as smartphones) to manage OTPs have become popular recently and have been adopted by many banks and major service providers. These 2FA mobile systems are considered to offer an appropriate compromise between security, ease of use and cost. An important example of 2FA mobile are SMS-based TAN (Transaction Authentication Number) systems, such as mTANs, smsTAN, mobileTANs.

Unfortunately, today, OTP SMS can not be considered secure for two different reasons:

1. First, the security of OTP SMS relies on the confidentiality of SMS messages that depends heavily on network security. Several attacks against GSM and even 3G networks have shown that the confidentiality of SMS messages is not offered by default;
2. Second, attackers have adjusted and created specialized trojans for mobile phones (Maslennikov, 2018; Klein, 2017) in order to recover the OTPs, since many service providers have adapted SMS OTP to secure transactions (Mulliner, Borgaonkar, Stewin, & Seifert, 2013).

Today, there are several mechanisms for encrypting SMS content using cryptography based on difficult mathematical problems like factorization and discrete logarithm. However, the advent of the quantum computer, which could have a much higher computational power than our conventional computers, would be able to break most conventional encrypted systems based on the discrete logarithm and the factorization problem. To solve and anticipate this security problem, the authors propose to use post-quantum cryptography that would be a priori resistant to the quantum computer. Thus, in this paper, they will use post-quantum cryptography to ensure confidentiality of the transmitted information such as SMS OTP on the unsecured public channel. They propose an SMS encryption mechanism using the Quasi-Cyclic MDPC version of the McEliece cryptosystem and an electronic signature of OTPs based on elliptic crossovers ECDSA (Elliptic Curve Digital Signature Algorithm).

After presenting in section 2 the various existing research works, the authors will then describe briefly the cryptosystems which will be used in their proposal. In section 4, they will present their proposed SMS-based 2FA system using post quantum cryptosystems. Finally, the authors will present an implementation of their proposed system and a security issues discussion.

RELATED WORK

Many articles have been written about attacks and securing two-factor authentication methods. In this section, the authors will present the mobile application security related work, the existing two-factor authentication systems, then the SMS-based attacks on 2FA. Finally, some existing security proposals on 2FA based on SMS will be presented as well.

Mobile Application Security Related Work

- Kumawat et al. (2017) propose in an Android application allowing the user and the developer to easily test the application, whether it is benign or vulnerable. Thus, the authors have implemented the static and dynamic analysis of Android application for the detection of vulnerable and malicious applications;
- Kouraого et al. (2017) discuss the security issues of android applications. Then, they perform the reverse engineering of banking applications and a DDOS attack on the bank server. Finally, they propose countermeasures to better secure these vulnerable applications;
- Vidyarthi et al. (2017) propose a complete approach combining static verification and dynamic analysis for the detection of malicious programs. Static analysis is used to check the specific characteristics of the code while dynamic analysis is used to analyze the runtime behavior of malware.
Inducing Six-Word Stories From Curated Text Sets to Anticipate Cyberwar in 4IR
www.igi-global.com/chapter/inducing-six-word-stories-from-curated-text-sets-to-anticipate-cyberwar-in-4ir/206792?camid=4v1a