ENHANCED MULTI-DEVICE TWO-FACTOR AUTHENTICATION USING PUBLIC-KEY CRYPTOGRAPHY

Jahangir Abbas Mohammed
Department of Computer Science
SRM University AP
Guntur, AP 522502
mohammed_jahangir@srmap.edu.in

November 10, 2021

ABSTRACT

This paper proposes a secure two-factor authentication (TFA) system that relies on a password and a crypto-capable device. In cases like a compromise of communication lines, server or device vulnerabilities, and offline and online attacks on user passwords, the approach provides the highest feasible security bounds given the collection of compromised components. Using either SAS Message Authentication or any PIN-based Authentication, the suggested approach constructs a TFA scheme. The paper also proposes a secure software architecture for implementing an enhanced public key cryptography system for mobile applications and an efficient implementation of this modular structure that can use any password-based client-server authentication method without relying on risky single-layer password authentication architecture.

Keywords Public Key Cryptography · RSA Cryptosystem · Two-Factor Authentication

1 Introduction

Passwords are the most used form of electronic authentication, and they protect a wide range of sensitive information. However, Both online and physical attacks can compromise passwords. Through internet connections with the server, a hacker can test password guesses. An attacker having access to the server's authentication data (i.e., a database of password hashes) can undertake an offline dictionary assault by comparing each user's authentication information to a dictionary of probable passwords. Offline dictionary attacks against commercial providers are common, resulting in billions of user accounts.[1][2][3][4]

Moreover, because most users reuse their passwords across platforms, compromising one site generally results in user accounts being compromised on other sites. User authenticates to the server by "proving possession" of an additional personal device (e.g., a smartphone or a USB token) in addition to knowing her password, which is a common safeguard against online password attacks and a backup line of defense in the event of password breaches.

TFA systems are typically implemented using a Time-Based One-Time Password (TOTP) mechanism [5], in which the server produces a one-time password in the form of a PIN or a Short String, which is then delivered to the user's device over a variety of communication channels, such as SMS or Email. The password is only valid for a short period of time and can only be used once. This password grants the user access to the protected information after it has been entered. Attacks on the database and communication routes between the server and the user's device are a significant threat to this system, which makes it extremely vulnerable to compromise. Such attacks have the potential to compromise the TOTP, allowing the attacker to obtain access to protected information. The approach provided in this research proposes a mechanism that can be used to avoid such assaults and keep TFA systems safe from intrusion and compromise.

2 Definitions

2.1 Public Key Cryptography

Asymmetric cryptography, also known as Public-Key Cryptography[6], is an encryption method that employs two keys that are mathematically related but not identical: a public key and a private key. Unlike symmetric key techniques, which use the same key to encrypt and decrypt information, each key has a distinct purpose. Encryption is done with the public key (shown in Fig. 1 (a)), while decryption is done with the private key (shown in Fig. 1 (b)). Computing the private key from the public key is computationally impossible. As a result, public keys may be widely shared, allowing users to encrypt material and straightforwardly verify digital signatures. In contrast, private keys can be kept private, guaranteeing that only the owners of the private keys can decode the content and establish digital signatures.

With public-key cryptography, it is also possible to do robust authentication. A sender can create a short digital signature on a message by combining it with a private key and sending it to the recipient. Anyone who has access to the sender's public key can combine a message with a claimed digital signature, and if the signature matches the message, the message's origin can be verified as having been sent by the sender.

Figure 1: Encryption and Decryption using Public Key Cryptography

2.2 RSA Cryptosystem

The Rivest-Shamir-Adleman (RSA) encryption algorithm [7] is an asymmetric encryption algorithm widely used in many products and services. The "factoring issue," which is the practical difficulty of factoring the product of two huge prime numbers, is at the heart of RSA's security. The RSA issue refers to the difficulty of breaking RSA encryption. If a large enough key is utilized, there are no published techniques to circumvent the system.

The RSA scheme is a block cipher using plaintext and ciphertext as integers ranging from 0 to $n-1$ for any n . An exponential expression is used in the system. The plaintext is encrypted in blocks with a binary value of less than n . For some plaintext block M and ciphertext block C , we have:

$$C = M^e \pmod{n}$$

$$M = C^d \pmod{n} = (M^e)^d \pmod{n}$$

$$M = M^{ed} \pmod{n}$$

Both the sender and the recipient are aware of n . Only the recipient knows the value of d , whereas the sender knows the value of e .

3 Problem Statement

The fact that tens of millions of user accounts have been compromised on several instances through internet hacking attacks is no longer surprising news these days. Adobe (150 million), Evernote (50 million), Anthem (40 million), Rockyou (32 million), Tianya (30 million), Dodonew (16 million), and 000webhost (15 million) are just a few of the latest password data breaches. Some services have even been repeatedly hacked in the last five years, according to the sources. It is known as the "domino effect" because it illustrates how a breach of one server would result in the failure of all other servers in a network.

Further research into these attacks resulted in the widespread usage of smart-card-based password authentication (as seen in Fig. 2), sometimes known as "two-factor authentication." Since its introduction more than thirty years ago, this type of authentication has become extensively used in many security-critical applications, including online banking and social networking sites, among others.

Figure 2: Traditional smart-card based authentication system

A client user and an authentication server are the key-partners in this type of authentication (TFA). The user initially registers with the Server by providing their data (e.g., their identity and password), after which Server safely issues the user a smart card with security parameters. The user registration process is what it is called. Later, during the login step, the User and Server authenticate themselves to one other.

Traditional TFA systems are riddled with vulnerabilities, making them extremely vulnerable to attacks like Man-in-the-Middle. Several vulnerabilities have gone unaddressed by existing techniques of combining standard password-over-TLS authentication with two-factor authentication based on PINs. It is the goal of this article to address many of these vulnerabilities. These vulnerabilities include

- PINs transmitted from the server to the device are subject to PIN redirection attacks, such as SMS hijacking and SIM card swap attacks. [8]
- The user's PIN input into the host computer is subject to eavesdropping through key-loggers, screen scrapers, PIN phishing[9], PIN recording, and other methods.[10]
- If the attacker has access to the keys exchanged between the TFA device and the server, the TFA protection is compromised.
- Login attempts at the server can be used to verify password guesses

A solution to the security issues stated above is presented in this work, which makes use of Public-Key Cryptography Systems and Secure Software Infrastructure.

4 Proposed Solution

In the proposed solution, an end-to-end encryption layer for two-factor authentication is provided by using a Public-Key Cryptography system that has undergone extensive testing and evaluation. The first factor of the model is a typical alphanumeric password, and the second factor is a Time-Based Unique Token, which can be either a short string or a numeric PIN. In a typical TFA arrangement, the pin is generated by the server and sent to the user's registered device; the user then gains access to the system by inputting the pin received from the server. This system might be compromised because of a server breach if the PIN is made available to an attacker by the assault. However, in the proposed system, PIN is signed by the device's private key and validated by its public key, which is available on the server. Even if the opponent knows the PIN (TFA Token), he will not break into the system since he will not have the Private Key used to sign the token.

Figure 3: Sequence Diagram of Proposed Model

Figure 4: System Architecture for Proposed Model

According to the configuration of this system, each device/client generates a public key pair using the RSA algorithm, which is then stored in the server database and mapped to the user's account. A one-to-many link between each user's public key and the public keys of all devices is established in the database structure, allowing each user to register any number of devices.

After entering their password into the proposed Two-Factor Authentication system, the client sends a request to the server that comprises both the password and the public key of their device accessing the system, which is then accepted by the server. The server then checks the password to ensure it is correct. After the user's password has been successfully confirmed, the server checks to see if the public key given in the request is connected with the user's account. Otherwise, the user is prompted to register his device by registering his other previously registered devices, unless this is not the case. A request is made to the server if the device has already been registered, and the server then produces a unique TFA Token (PIN or String) for the user (which is only valid for a short period) and transmits it to the user through SMS, Notifications, Email, or other channels. After that, the user will be prompted to enter the TFA Token into the client application. After properly inputting the token, the client signs the token with the device's private key, stored on the device. Finally, the TFA token is encrypted and given to the server, where it is verified that both the signed token and the token itself were provided correctly.

This system provides an end-to-end encryption to the existing TFA system with minimal software requirements.

5 Conclusion

This paper proposes an end-to-end encryption system based on the RSA algorithm, which may be used in conjunction with a Two-Factor Authentication system. The proposed model and criteria are intended to serve as a benchmark for the evaluation of current and future two-factor authentication systems and the development of a novel system that satisfies the requirements of practicability, simplicity, and strong security conceptions while remaining cost-effective. The algorithm (RSA) utilized in this solution has been thoroughly tested and is widely regarded as the industry standard globally. The feasibility of cracking this encryption has been debated several times, but without result. This paradigm is made possible by the RSA cryptosystem, which offers extremely high levels of security. An illustration of the attack sustenance metrics for the RSA cryptosystem can be seen below.

Number of Decimal Digits	Approximate Number of Bits	Date Achieved	MIPS-years	Algorithm
100	332	April 1991	7	quadratic sieve
110	365	April 1992	75	quadratic sieve
120	398	June 1993	830	quadratic sieve
129	428	April 1994	5000	quadratic sieve
130	431	April 1996	1000	generalized number field sieve
140	465	February 1999	2000	generalized number field sieve
155	512	August 1999	8000	generalized number field sieve
160	530	April 2003	—	Lattice sieve
174	576	December 2003	—	Lattice sieve
200	663	May 2005	—	Lattice sieve

Figure 5: RSA Factoring Benchmarks

References

- [1] LinkedIn confirms passwords were 'compromised'. *Article by Elinor Mills*, June 6, 2012.
- [2] *Russian Hackers Amass Over a Billion Internet Passwords*. *Article by Nicole Perlroth and David Gelles*, Aug. 5, 2014.
- [3] Hack Brief: Yahoo Breach Hits Half a Billion Users. *Article by Andy Greenberg*, Sep. 22, 2016.
- [4] *RSA breach leaks data for hacking SecurID tokens*. *Article by Dan Goodin*, Mar. 18, 2011.
- [5] Plata, Irma Calpito, Jomar. Application Of Time-Based One Time Password (TOTP) Algorithm For Human Resource E-Leave Tracking Web App. In *International Journal of Scientific Technology Research*. 9. 4070-4077.

- [6] *Liestyowati, Dwi. Public Key Cryptography. In Journal of Physics: Conference Series. 477. 052062. 10.1088/1742-6596/1477/5/052062.*
- [7] *Xin Zhou and Xiaofei Tang Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 2011 6th International Forum on Strategic Technology 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.*
- [8] *SIM swap attack. Article by Cryptopedia Staff , Oct. 6, 2021.*
- [9] *London calling: Two-factor authentication phishing. Article by Katie Kleemola and John Scott-Railton , 2015*
- [10] *Chia-Chi Lin, Hongyang Li, Xiao-yong Zhou, and XiaoFeng Wang Screenmilk: How to milk your android screen for secrets. In Network Distributed System Security Symposium 2014*