Research and Practice of Identity Authentication Systems in New Media (Postprint)

Authors: Hu Pengcheng

Date: 2023-10-08T00:00:00+00:00

Abstract

As a product of information technology in the Internet era, new media—with its characteristics of openness, interactivity, timeliness, and mobility—has brought people convenient and efficient enjoyment to a certain extent. However, the accompanying information security issues are also emerging endlessly. Especially in the new media environment, ordinary users can participate in the production and processing of news information through various means. Therefore, in-depth research on how to employ multi-factor authentication systems to ensure confidentiality, integrity, and availability during news information collection and transmission, including the authenticity of identities of news information publishers and recipients as well as the security of information transmission channels, is of great significance.

Full Text

Preamble

Abstract: As a product of information technology in the Internet era, new media's characteristics of openness, interactivity, timeliness, and mobility have brought people convenient and efficient experiences. However, the accompanying information security issues have also emerged endlessly. Particularly in the new media environment, ordinary users can participate in news information production and processing through various means. Therefore, in-depth research on how to employ multi-factor identity authentication systems to ensure the confidentiality, integrity, and availability of news information during collection and transmission, including the authenticity of news publishers and recipients' identities and the security of information transmission channels, holds significant importance.

Keywords: new media; information security; multi-factor identity authentication; authentication system

CLC Number: G202
Document Code: A
Article ID: 1671-0134(2017)04-108-02
DOI: 10.19483/j.cnki.11-4653/n.2017.04.033

Author: Hu Pengcheng

With the advancement of biometric recognition technology, user identity authentication based on biological characteristics has gained widespread favor, including fingerprint, iris, voice, and facial feature extraction. Identity authentication technology is evolving toward greater security and usability, combining multiple technical approaches to establish secure, efficient, and concise authentication systems.

2.1 Introduction to Traditional Identity Authentication Technology

Traditional identity authentication employs a "user account + static password" recognition mechanism [3-4]. Since criminals can easily steal usernames, traditional identity authentication is essentially single-factor authentication, with the static password serving as the sole basis for security. While this method offers simplicity and operability, it lacks adequate security protection.

2.2 Common Multi-Factor Authentication Technologies

2.2.1 Token Authentication Technology

With the advancement of network technology, dynamic password authentication technology—also known as token authentication technology [5-7]—has been introduced to better protect user account and password security. This system automatically generates a new random password every 60 seconds according to a special algorithm. This random password is called a dynamic password or one-time password. The technology includes three types: time-based synchronous password technology, event-based synchronous password technology, and challenge-response asynchronous password technology.

2.2.2 Biometric Recognition Technology

Biometric recognition technology is currently the most convenient and secure identification technology available. It is not easily impersonated, simulated, or stolen, and solves the problem of forgetting traditional keys or tokens. It is convenient to use and requires no regular maintenance, making it more convenient and secure than traditional identity authentication methods. Human physiological features already used for identification include facial images, fingerprints, iris patterns, and DNA [8-10], while behavioral features include gait and signature. The application of biometric recognition technology has grown significantly in the past two years. With this technology, we can effectively

ensure that various types of information about identified biological entities are secure and reliable, while also safeguarding the stability of interactions between applications and systems.

3. Practice of Identity Authentication Systems in the New Media Environment

In the new media environment, news information utilizes digital technology to conduct real-time interactive information exchange and dissemination through channels such as the Internet and wireless communication networks, with mobile phones or computers serving as collection or reception terminals. To ensure the security of news information collection and transmission, this paper adopts a PKI/CA-based multi-factor authentication system to issue digital certificates to legitimate users. Through flexible and diverse authentication methods, it satisfies different types of terminal users, effectively reducing security risks associated with single factors and providing enhanced authentication security. Single sign-on enables one-time login with secure access throughout. The system also fully considers data transmission security in complex network environments, implementing targeted data security protection measures against potential security risks such as information interception, content leakage, or content tampering during transmission.

This paper proposes a multi-factor authentication system based on the Xinhua News Agency's news information collection platform. Architecturally, it comprises cryptographic infrastructure, a security support platform, and upper-layer applications, forming an integrated security service platform. A monitoring and auditing system provides real-time and effective monitoring of the platform's security service capabilities and its ability to secure upper-layer applications, with operational status visualized through reports and charts for detailed analysis.

3.1 Overall Framework

The overall security framework based on PKI technology in this paper is illustrated below:

[Figure 1: see original paper] Overall Framework Diagram

The user identity verification component consists of a CA issuance system, RA registration system, KM key management system, encryption machines, and LDAP directory service system. As the infrastructure of the PKI/CA certificate authentication system, it is responsible for issuing and managing digital certificates and publishing user certificates and blacklist information to the LDAP directory service. USB intelligent password keys can serve as digital certificate storage media for user identity identification through digital certificates. Encryption machines provide secure key storage and high-speed cryptographic operations for the CA issuance system and RA registration system.

Unified identity authentication provides multiple authentication methods for

the news information collection platform through a multi-factor authentication platform. Users can select different authentication methods based on their terminal login approach, such as fingerprint recognition or dynamic passwords. By integrating with identity authentication gateways, it provides platform users with high-strength identity authentication based on digital certificates. The mobile certificate download portal enables mobile certificate download services, while mobile middleware facilitates certificate authentication on mobile devices.

Digital signature services employ digital signature technology combined with timestamp technology to achieve content confidentiality, integrity, and non-repudiation of operations during manuscript transmission at specific time nodes.

The digital certificate comprehensive statistics and query system provides a unified display platform for certificate issuance and usage statistics, enabling data analysis on digital certificates and behavior audit data based on digital certificates.

To ensure standardized certificate issuance operations and clarify the responsibilities of certificate administrators, a series of certificate management measures have been formulated. To meet the secure application of certificates, certificate format specifications for the industry and enterprise have been established to ensure that certificate information can be conveniently recognized and invoked by application systems.

3.2 Logical Architecture

This paper fully considers the current status of news information collection operations and security requirements such as unified identity management, unified identity authentication, and data transmission security. Through in-depth analysis of business usage scenarios, the logical architecture of the security design for the PKI-based news information collection platform is illustrated below:

[Figure 2: see original paper] Logical Architecture Diagram

4. Summary and Outlook

The new media revolution presents both opportunities and challenges for identity authentication. Every stage of news information—from generation, transmission, and storage to utilization—carries the risk of information leakage. Therefore, employing multi-factor identity authentication technology to implement strong encryption throughout this process is the most conventional and effective security measure. With biometric recognition technology, we can effectively ensure that information about identified biological entities is secure and reliable, enabling effective control of news information from the source and establishing national identity authentication authority in cyberspace.

References

[1] Hong Jiewen, Gui Weixia. New Media Technology [M]. Chongqing: Southwest China Normal University Press, 2016.

[2] Yang Xijing. How to Promote the Integrated Development of Traditional Publishing and New Media [J]. Science-Technology & Publication, 2014(11): 8-10.

[3] Lin Yuanming. Research and Implementation of Identity Authentication System Based on Mobile Token [D]. Xiamen: Xiamen University, 2009.

[4] Fan Liangyun. Research and Implementation of Identity Authentication System Based on 121 Token, Mobile Token and Biometric Features [D]. Xiamen: Xiamen University, 2010.

[5] Alfred J. Menezes, Paul C. van Oorschot, Scott A. Vanstone. Handbook of Applied Cryptography [M].

[6] Ji Xiaoyu. Research and Implementation of Two-Way Identity Authentication System with Dynamic Password [D]. Dalian: Dalian University of Technology, 2008.

[7] Wang Yunhong, Tan Tieniu. Modern Identity Authentication New Technology: Biometric Recognition Technology [J]. China Basic Science, 2000, 9(1): 4-10.

[8] Bolle R M, Connell J, Pankanti S, et al. Biometrics 101 [R]. Report RC22481. IBM Research, 2002.

[9] Maltoni D, Maio D, Jain A K, et al. Handbook of Fingerprint Recognition [C]. New York: Springer-Verlag, Inc., 2003.

[10] Cai Wandong. Network and Information Security [M]. Beijing: Northwestern Polytechnical University Press, 2004.

(Author's affiliation: Communication Technology Bureau, Xinhua News Agency)

Note: Figure translations are in progress. See original paper for figures.