Available online www.jsaer.com

Journal of Scientific and Engineering Research, 2023, 10(1):67-73

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

A Comprehensive Analysis of Common Authentication Errors and Resolution

Prashanth Kodurupati

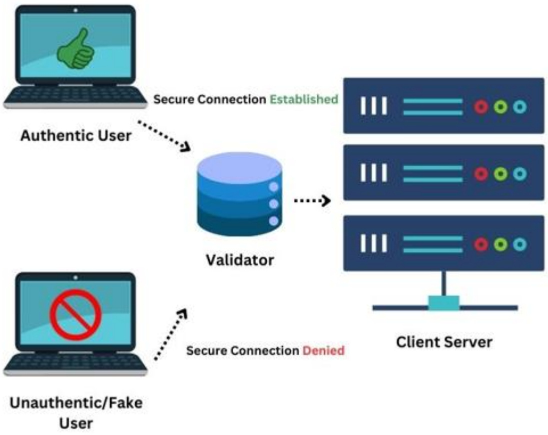
Information Technology, Managed File Transfer Engineer, Minisoft Technologies LLC, Alpharetta, United States of America
Email: prashanth.bachi21@gmail.com

Abstract Authentication is the core of secure online connections and can be applied to multiple layers of an online connection hierarchy and for different levels of permissions in the host system. Password, SSH, certificates, and biometrics are among the most common authentication types currently used and authentication failures and errors they generate may correspond to an individual authentication type. The resolution may or may not require the need to contact the client or client server.

Keywords Authentication error, authentication

1. Introduction

At any given time, there are billions of devices and people online, exchanging data and files in various formats. Most file transfers require both connected end-points to follow a specific set of protocols to ensure the safe delivery of the file from the sender to the receiver.



However, underlying these protocols are the basic internet connectivity and data transfer protocols, processes, and practices that are universally prevalent. One such process is authentication. An overarching definition of authentication would be validating the identity of individuals or devices connecting over the internet [1]. It's used in both public and private networks, and the goal is to ensure that only the individuals or devices that are allowed to access or connect with a specific network can establish a secure connection and unwanted entities are prevented from connecting. It's rarely used as a stand-alone measure when an online connection is established and is often used in conjunction with identification, authorization, and encryption [2]. In most cases, authentication precedes authorization that determines what a user is allowed to do.

Authentication allows a client or client-server to determine whether an individual or device that's attempting to establish a connection is who or what they *say* they are, hence the term - authentication. The entity seeking a connection with a server/client over the internet has to prove its authenticity in order to establish the connection so that further communication or file transfer can happen. If it can't, the authentication fails, and this failure is communicated to the entity seeking to establish the connection via an authentication message.

2. Literature Review

Authentication is something academics and industry experts have been researching and studying since the early days of the internet. Hence, literature on authentication can be found dating back to the late 1980s [3]. The early iterations focused on its logic and implementation, though it was relatively simple owing to the nature of internet/networks in those days [4]. The new century witnessed a significant evolution in authentication protocols, systems, and implementations, and new technologies and authentication processes like biometric authentication and deniable authentication were studied [5][6]. The authentication domain was expanded to cover both private and group authentications [7][8]. A significant number of studies were also conducted on the authentication practices that became necessary in the age of online transactions, predominantly the 2-Factor Authentication 2FA [9]. In conclusion, authentication and authentication failures and its role in the modern internet is a well-studied topic. However, specific authentication errors and their rectification processes is something that formal academic literature is relatively limited in and most of the data/information in this regard comes from organizations that facilitate interconnectivity of various entities on the internet.

3. Problem Statement - Prevalence of Authentication Errors

Before we dive into authentication errors and the factors influencing them, it's a good idea to look into some types of authentication.

3.1 Types of Authentication

The authentication paradigm has expanded significantly thanks to the cloud and the need to establish connections remotely. If we take that into consideration, some of the most common types of authentication types include:

3.1.1 Passwords

Password-based authentication is easily the most prevalent authentication type over the internet, especially for human users [10]. The distinction is important because there are more IoT devices online now than human users, and they rarely use password-based authentication. A combination of username and password ensures a client/client-server that you are who you say you are and have permission to connect to their network. Passwords have their own set of vulnerabilities from an authentication perspective, though most of them lean towards human errors like forgetting a password or sharing it in an unsecured location [11].

3.1.2 Secure Shell (SSH)

Secured Shell or SSH integration gained traction thanks to remote connectivity requirements since it allows devices/users to connect with their desired clients/websites/servers/applications even over an insecure network [12]. The SSH authentication protocol relies upon two sets of keys - private and public, and it's the combination of these keys that allows a user or device to connect with the desired client/client server remotely. The keys are generated using mathematical algorithms, and once a secure connection is established via an SSH protocol, where first the server and then the client are authenticated, communication and file transfer can take place [13].

3.1.3 Certificate-Based Authentication

Apart from these two, there is also certificate-based authentication [14]. Digital certificates issued Certificate Authorities (CAs) can portray an individual, organization, or even a website as authentic and trust-worthy to servers and clients. The Secure Sockets Layer (SSL) certificates fall into this category and they trigger a browser-level authentication process, which prevents users from connecting to websites with expired or flagged certificates.

3.1.4 Biometric Authentication

Biometric authentication [15], is gaining more traction since mobile devices capable of face recognition and equipped with fingerprint scanners have become more common. While its primary uses are still at device level, biometric authentication *can* be implemented on more comprehensive levels, but regardless of the scope of the connection it helps establish, biometric authentication is inherently user-centric/human-centric.

Another way to classify different authentication types is the layer they are implemented at. The broadest classification here is establishing a secure connection between two entities online, where either entity can be a human user, an online account, a server, a website, etc. However, separate authentication requirements can be enforced to safeguard how entities interact and behave online. For example, a user representing an organization may be allowed to connect with a client server using merely their username and password. But if they want to transfer files or change something in a database, they may have to prove their authenticity in another way as well.

From an implementation perspective, authentication can be applied to different layers of a network connection hierarchy, including application, transport, and network layers.

3.2 Authentication Errors - Definition, Classification, and Causes

3.2.1 Definition

Authentication errors [16] are generated whenever authentication fails, and it can happen even if a legitimate user or device is trying to connect with a client/server. There are several reasons for that, and each may result in different authentication errors.

3.2.2 Password-Based Authentication Errors

Password-related authentication errors are typically generated when you use the wrong name, wrong password, wrong combination of user and password, or if you do not follow all of the entry protocols besides username and password, like solving a CAPTCHA. These can also be classified as authentication errors associated with credentials and can also be time-based, i.e., temporary passwords or expired passwords.

While password-related authentication errors are common in both B2C and B2B user connections, there are other types of authentication failures, resulting in authentication errors that typically take place when client and host servers are in B2B connections. This includes SSH authentication errors.

3.2.3 SSH Authentication Error

When it comes to SSH authentication failures, the most common reason is that the address to the private key is wrong, so when the client/server requests it, they don't get a matching pair for their public key, resulting in the generation of an authentication error. However, the errors may also be generated when the client is using the wrong identifier or doesn’t have the right private key in place to match with the public key.

3.2.4 Certificate-Based Authentication Error

If other authentication measures are in place like certificate-based authentication, it may generate authentication errors unique to the protocols and may have its own set of triggers/driving factors. The most common reason behind an error when certificate-based authentication is in place is expired certificates, but there are other reasons as well.

For example, a client may fail to recognize or trust the certificates in place. Many clients/servers clearly define which certificates they accept and recognize, and if the user certificates are from a different source, it may result in an error. Another reason is that like the SSH key, the client server may not be able to find your certificate.

3.2.5 Biometric Authentication Error

When it comes to biometric authentication, the failures are usually device-related, like the front camera not taking the depth of the face accurately enough for recognition or an oil film on the thumb-print scanner preventing it from being read properly by the device.

3.2.6 Other Authentication Error Triggers and Scenarios

It's important to note that authentication failures don't just occur when a user or device is trying to connect to another. They may also occur when files are being transferred from one end-point to another, even if the device/user authentication has already taken place. We can call them transfer authentication errors. Some systems may have additional authentication layers and safety protocols to ensure that only the right type/files are transferred, and they may result in file-transfer authentication errors.

Most servers have security measures in place to prevent unauthorized users from establishing a connection, and in some cases, they may trigger an authentication error. For example, if you are trying to log into a client-server with a different device or from a different location than you usually do (different IP address), it may result in an authentication error. In some cases, account restrictions/user restrictions may be conveyed via an authentication error. For example, the client-server may have barred entry to some specific accounts or accounts hailing from a specific organization or sharing the same certificate. This may result in an authentication error when you attempt to establish a connection.

4. Resolving Authentication Errors

The solutions to different authentication errors will depend upon the error itself or the factors that triggered it.

4.1 Resolving Password Authentication Failures and Errors

Most password-related authentication errors are straightforward, and once you enter the right combination of credentials, you can log in. But you may also trigger errors like too many login attempts, in which case you may have to wait for a predefined time to access the server again. All of these may technically fall under the same authentication failure and error-generation class, i.e., passwords, but both the error and resolution may have a different dimension.

4.1.1 Login Conditions

It’s important to understand that authentication errors may be generated when you are attempting to establish the connection for the first time using new credentials. These errors may refer to specific rules regarding the username and passwords that you may have to follow. For example, you may not be allowed to use any special characters in the name and the user name you choose must be unique. The requirements/rules for the password may be more complex. They may require you to include special characters, both capital and small characters, and numbers. The goal is to create a complex password [17] that may not be easy to hack using brute force attacks that attempt to guess your password by running all possible combinations.

4.2 Resolving SSH Authentication Failures and Errors

The solution for authentication errors related to SSH protocol may be different. As we mentioned, the most common reason an SSH authentication fails is that the private key is not accessible to the client-server, and the solution is usually to rectify the address in the established connection and make sure the address to the private key is accurate. Even a single mistake in the path to the key may result in a repeat error. But there can be other reasons as well, especially on on-site connections. This may be because a switch/router has not been configured to accept the first-time public key. In this case, reconfiguring it to accept this key can be the solution.

4.3 Resolving Certificate and Biometric Authentication Failures and Errors

For certificate-based authentication errors, refreshing/updating the certificates or ensuring that you have certificates that are from a source the client-server recognizes and trusts can solve the issue.

For biometric authentication errors, the solution may range from simple to complex based on where the problem lies. If it’s a simple issue of reconfiguring the device or cleaning the input surfaces (camera or fingerprint reader), then attempting that may solve the issue. However, if the fingerprint scanner or camera is damaged, then repairing them may be the only option to get rid of the authentication errors.

In addition to simple connection-related authentication errors, you may also be faced with file-transfer errors/data-transfer errors when you attempt to transfer a file that's either not in the right format, too large, or not safe from your device to a client-server. The authentication errors, in this case, usually specify what transfer rule you are violating, and resolving that issue may get rid of the error.

Authentication Error Classification	**Resolution Measures**	**Client Communication**
Establishing Secure Connection	Following error message directions. Adhering to client server requirements Updating certificates. Ensuring availability and right address of SSH keys. Device maintenance/repair (for biometric).	Conditional
File Transfer	Checking and validating permissions from the clients.	Conditional
Insufficient Permissions	Reaching out to the client to ensure sufficient permissions have been granted to the user.	Necessary
Time-Based Errors	Waiting through the block time.	Not Required

5. Essential Responsibilities

The responsibility of identifying the cause of authentication failure, deciphering the error code, and taking steps to resolve the issue, typically fall on the entity initiating a connection, even if the error and failed attempt to establish a secure connection or transferring files is communicated to both entities involved in the connection. If the issue can be resolved without contacting the client or client server, it remains the responsibility of the entity that initiated the connection. However, if they have followed all the necessary authentication protocols and the error persists, the responsibility may be shifted to client/client server and they may have to resolve the issue on their end.

6. Good Authentication Practices

One important factor to consider is that, in many cases, authentication errors enforce good authentication practices, so they are not necessarily a bad thing to encounter. They ensure that the connection established is safe and secure for both you and the client and that any communication and data transfer that takes place does not violate any standard safety protocols. Understanding, implementing, and navigating good authentication practices don't just benefit you from a safety perspective; they may also reduce the frequency of authentication errors.

This may include creating strong passwords and enforcing and following the rules of strong passwords. If a client server has established these rules and has added multiple "checks" on each new password, like specific password length, using special characters and numbers, then you have to follow these rules in order to ensure that your attempt to establish a connection doesn't result in an error.

However, one of the best authentication practices by far is the implementation of Multi-Factor Authentication (MFA). MFA [18] allows a client-server/server to add another layer over the existing authentication measure, usually credential-based, to ensure that the right individuals or devices can connect to them and no one else. This usually includes receiving a temporary message or a one-time password on your personal phone number or email. Using that to log in in addition to your credentials assures the client-server without a shadow of a doubt that you are who you say you are.

7. Limitations and Recommendations

This is an overarching overview of some of the most common authentication types, and authentication failures and errors associated with each type. But each server administrator and communication and other platforms (ERP, CRM, etc.) may have their repository of authentication errors and the steps that can be taken to get past these errors. The lack of standardization prevents us from building a more comprehensive guide on authentication errors and their resolution.

We recommend that the topic be studied from various different perspectives. From platform/server side perspective when it comes to the full range of authentication errors they have classified and the remediation steps they recommend, to analyzing a specific authentication failure category and accompanying error from the perspective of different vendors like IBM Sterling, Amazon, etc.

8. Conclusion

While it's not common, it certainly happens that you may receive an authentication error without guidance or directions on how to rectify it. For example, if a client-server is sending the message over and over that the password you have set is not acceptable without telling you *why* it's not acceptable. When that happens, you may have to reach out to your client/client-server to learn why you are receiving this message. However, in most cases, the error provides the necessary information you need to ensure that the authentication error goes away.

References

[1]. G.J. Simmons; A survey of information authentication, *Proceedings of the IEEE Volume: 76, Issue: 5, pp: 603 - 620* (1988), https://ieeexplore.ieee.org/abstract/document/4445

[2]. Michael Burrows, Martin Abadi, Roger Needham; A logic of authentication, *ACM Transactions on Computer Systems, Volume 8, Issue 1, pp 18–36* (1990), https://dl.acm.org/doi/abs/10.1145/77648.77649

[3]. James Wayman, Anil Jain, Davide Maltoni & Dario Maio; An Introduction to Biometric Authentication Systems, *Biometric Systems pp 1–20* (2005), https://link.springer.com/chapter/10.1007/1-84628-064-8_1

[4]. Mario Di Raimondo, Rosario Gennaro; New approaches for deniable authentication, *CCS '05: Proceedings of the 12th ACM conference on Computer and communications security Pages 112–121* (2005), https://dl.acm.org/doi/abs/10.1145/1102120.1102137

[5]. Martín Abadi, Cédric Fournet; Private authentication, *Theoretical Computer Science Volume 322, Issue 3, Pages 427-476* (2004), https://www.sciencedirect.com/science/article/pii/S0304397504001380

[6]. Lein Harn; Group Authentication, *IEEE Transactions on Computers, Volume: 62, Issue: 9*, (2013), https://ieeexplore.ieee.org/abstract/document/6331482

[7]. Thanasis Petsas, Giorgos Tsirantonakis, Elias Athanasopoulos, Sotiris Ioannidis; Two-factor authentication: is the world ready?: quantifying 2FA adoption, *EuroSec '15: Proceedings of the Eighth European Workshop on System Security, Article No.: 4 Pages 1–7* (2015), https://dl.acm.org/doi/abs/10.1145/2751323.2751327

[8]. Eric Grosse; Mayank Upadhyay; Authentication at Scale, *IEEE Security & Privacy (Volume: 11, Issue: 1)*, (2013), https://ieeexplore.ieee.org/abstract/document/6381399

[9]. Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Jean-Jacques Schwartzmann; A Review on Authentication Methods, *Australian Journal of Basic and Applied Sciences* (2013), https://hal.science/hal-00912435/

[10]. Amanpreet A. Kaur, Khurram K. Mustafa; A Critical appraisal on password-based Authentication, *International Journal of Computer Network and Information Security (IJCNIS)* vol. 11 (2019), https://www.mecs-press.org/ijcnis/ijcnis-v11-n1/v11n1-5.html

[11]. Mohammadreza Hazhirpasand Barkadehi, Mehrbaksh Nilashi, Othman Ibrahim, Ali Zakeri Fardi, Sarminah Samad; Authentication systems: A literature review and classification, *Telematics and Informatics Volume 35, Issue 5* (2018), https://www.sciencedirect.com/science/article/abs/pii/S0736585318301400

[12]. Network Working Group; The Secure Shell (SSH) Authentication Protocol (2006), https://www.rfc-editor.org/rfc/rfc4252.html

[13]. Tim Callan; SSH Keys Explained: Generation, Authentication, Key Pair Info & More (2020), https://www.sectigo.com/resource-library/what-is-an-ssh-key

[14]. IBM; Certificate-based authentication, https://www.ibm.com/docs/en/ztpf/2020?topic=certificates-certificate-based-authentication

[15]. Biometric Authentication, Science Direct, https://www.sciencedirect.com/topics/computer-science/biometric-authentication

[16]. Authentication Error Codes, *Oracle*, https://docs.oracle.com/cd/E19528-01/819-4671/adsrr/index.html

[17]. Bhaveer Bhana, Stephen Vincent Flowerday; Usability of the login authentication process: passphrases and passwords, *Information and Computer Security* (2021), https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2021-0093/full/html

[18]. Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, Yevgeni Koucheryavy; Multi-Factor Authentication: A Survey, *MDPI Cartography* (2018), https://www.mdpi.com/2410-387X/2/1/1