

Recommendation

ITU-T X.1283 (09/2024)

SERIES X: Data networks, open system communications
and security

Cyberspace security – Identity management (IdM) and
Authentication

Threat analysis and guidelines for securing password and passwordless authentication solutions

ITU-T X-SERIES RECOMMENDATIONS

Data networks, open system communications and security

PUBLIC DATA NETWORKS	X.1-X.199
OPEN SYSTEMS INTERCONNECTION	X.200-X.299
INTERWORKING BETWEEN NETWORKS	X.300-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	X.850-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999
INFORMATION AND NETWORK SECURITY	X.1000-X.1099
SECURE APPLICATIONS AND SERVICES (I)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	X.1200-X.1229
Countering spam	X.1230-X.1249
Identity management (IdM) and Authentication	X.1250-X.1299
SECURE APPLICATIONS AND SERVICES (II)	X.1300-X.1499
CYBERSECURITY INFORMATION EXCHANGE	X.1500-X.1599
CLOUD COMPUTING SECURITY	X.1600-X.1699
QUANTUM COMMUNICATION	X.1700-X.1729
DATA SECURITY	X.1750-X.1799
INTERNATIONAL MOBILE TELECOMMUNICATIONS (IMT) SECURITY	X.1800-X.1839
METaverse AND DIGITAL TWIN SECURITY	X.2000-X.2199
SOFTWARE SUPPLY CHAIN SECURITY	X.2150-X.2199
ARTIFICIAL INTELLIGENCE (AI) / MACHINE LEARNING (ML) SECURITY	X.2200-X.2249

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T X.1283

Threat analysis and guidelines for securing password and passwordless authentication solutions

Summary

The security community is undertaking a significant movement to replace password authentication with alternative solutions that are collectively known as passwordless authentication. Unfortunately, many of the passwordless solutions proposed suffer from the same limitations as current password authentication solutions. These proposed passwordless authentication solutions are vulnerable to man-in-the-middle and phishing attacks among others.

Recommendation ITU-T X.1283 presents security and threat analysis of authentication solutions that are based on the use of shared secrets and closely examines security risks associated with password authentication systems and emerging passwordless authentication solutions.

The Recommendation considers threat analysis, and develops guidelines and best practices for the protection of users and accounts based on these methods. This Recommendation can be used by adopters to support legacy solutions as they migrate to stronger authentication methods based on public key infrastructure (PKI) technology as presented in for example Recommendation ITU-T X.1277 and Recommendation ITU-T X.1278.

History*

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1283	2024-09-06	17	11.1002/1000/15889

Keywords

Password authentication, passwordless authentication.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, and information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definition.....	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	1
4	Abbreviations and acronyms	2
5	Conventions	2
6	Security overview	2
	6.1 User authentication	3
	6.2 Password security risks.....	3
	6.3 Password maintenance guidelines	5
7	Measures to protect password authentication	6
	7.1 Preventions	6
	7.2 Risk-based authentication.....	9
	7.3 Risk based authentication (RBA) advantages	12
8	Passwordless authentication	12
	8.1 Security risks and guidelines for passwordless authentication.....	13
	8.2 Steps towards passwordless authentication	18
	8.3 Phishing-resistant multi-factor authentication (MFA)	22
	8.4 Threats and mitigation measures for passwordless solutions.....	23
	Bibliography.....	25

Recommendation ITU-T X.1283

Threat analysis and guidelines for securing password and passwordless authentication solutions

1 Scope

This Recommendation presents threat analysis, identifies risks associated with password and passwordless solutions, and specifies the following:

- Definition of passwordless authentication.
- Threat analysis of password and passwordless solutions and their vulnerabilities for web and mobile solutions.
- Guidelines to protect passwords and passwordless solutions.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T X.509] Recommendation ITU-T X.509 (2019), *Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*.
- [ITU-T X.1254] Recommendation ITU-T X.1254 (2020), *Entity authentication assurance framework*.
- [ITU-T X.1278.2] Recommendation ITU-T X.1278.2 (2023), *Client to authenticator protocol*.

3 Definition

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 relying party (RP) [ITU-T X.1254]: Actor that relies on an identity assertion or claim.

3.1.2 security domain [b-NIST-1]: A domain that implements a security policy and is administered by a single authority.

3.1.3 federated authentication [b-NIST]: A process that allows for the conveyance of identity and authentication information across a set of networked systems.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 passwordless authentication: A method of verifying an entity's claimed identity without relying on shared secrets, but instead utilizing alternative factors such as biometrics, public-key cryptography, or registered devices.

3.2.2 phishing-resistant multi-factor authentication: Use of authentication methods that are specifically designed to mitigate the risk of phishing attacks.



4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

2FA	2 Factor Authentication
ID	User Identifier
KBA	Knowledge-Based Authentication
MFA	Multi-Factor Authentication
MITM	Man In The Middle
OTP	One Time Password
PIN	Personal Identification Number
PKI	Public Key Infrastructure
QR	Quick Response code
RBA	Risk-Based Authentication
RP	Relying Party
SMS	Short Message Service
U2F	Universal 2 nd Factor

5 Conventions

This Recommendation applies the following verbal forms for the expression of provisions:

- a) "shall" indicates a requirement;
- b) "should" indicates a recommendation;
- c) "may" indicates a permission;
- d) "can" indicates a possibility or a capability.

6 Security overview

Passwords are susceptible to a wide range of attacks, limiting their ability to effectively protect high-value systems. Typing a password on a mobile device introduces additional friction for the user, without providing adequate security for the underlying system.

Username and password login flow is neither user-friendly nor inherently secure, especially for accounts protected by knowledge-based authentication (KBA) systems used in account recovery processes. To enhance password security, many relying parties (RPs) are implementing multi-factor authentication (MFA) solutions. These solutions fall into a minimum of four categories:

- 1) **Something you know:** This includes passwords or personal identification numbers (PINs), but these are vulnerable. Additional factors are needed for improved security.
- 2) **Something you have:** Involves possession of a physical device or security token, such as hardware tokens, mobile devices, or smart cards.
- 3) **Something you are:** Encompasses biometric factors like fingerprints, facial recognition, or other unique physiological or behavioural characteristics.
- 4) **Something you do:** Involves behavioural factors, such as the way a user interacts with an application or device, including patterns of mouse movements or typing speed.

Implementing multifactor authentication by combining factors from different categories adds an extra layer of security, making it more challenging for attackers to gain unauthorized access. Multi-factor authentication, sometimes also called 2FA (two factor authentication when two factors are used), is

an authentication method requiring the use of more than one authentication factor each belonging to a different authentication category before a user is granted access. The use of factors of non-overlapping risk profile is preferable to enhance the security of the authentication. For example, when a user enters a password to logon to a web site, the relying party can check if the device has been seen before and send a one-time password (OTP) [ITU-T X.1254] to the user who enters it as part of the authentication process. MFA improves the security of a transaction but is not immune to phishing and other form of attacks. MFA tends to increase friction to the rightful user and not necessarily to the hacker when it comes to phishing-based attacks.

Strong authentication protocols based on a public key infrastructure (PKI) [ITU-T X.509] solution can help in protecting online access while reducing friction to users. This technology is being used by the industry to promote passwordless authentication.

Not all passwordless solutions are secure, some implementations are replacing passwords with techniques such as quick response (QR) code [ITU-T X.1278.2] which suffers from the same vulnerabilities as password authentication.

6.1 User authentication

Users create accounts at relying parties (RP). These accounts are generally composed of a username and password. User authentication is a security process to provide an answer to a relying party at login in order to verify you are who you claim to be. Once a user is authenticated, the relying party authorization policy will determine what the user is allowed to access and which services he/she can use.

The task of authenticating a user consists of presenting a login dialogue to the user where the username and password are entered, if the relying party matches the credential details, then the system can approve access. Authentication relies on the use of authentication factors to validate the claimed identity of the user. As stated above, there are multiple categories of authentication factors that can be combined in an MFA system.

6.2 Password security risks

Passwords themselves are often the subject of attacks. Repositories or databases of passwords are subject to attacks. Some password security risks are considered in clauses 6.2.1 to 6.2.9.

6.2.1 Brute force attack

Hackers can attempt to crack a user password by performing a brute force attack. In this method, a hacker utilizes a program to login to a victim's account with all possible password combinations. These attacks usually start with a list of commonly used passwords, known hacked passwords or the easiest passwords to guess.

6.2.2 Dictionary attack

A dictionary attack uses a more customized form of brute force attack. A hacker focuses on using combinations of passwords that are more likely to succeed. Dictionary attacks can have a great success rate if the attacker is aware of victim's habits and behaviour. Hackers can customize dictionary attacks if they have some information about the user.

6.2.3 Phishing attack

This is the most effective attack method to compromise a user's credentials. In this attack, the hacker entices the user to logon to the hacker site under false pretences. The hacker manages to convince the user to log on to what looks like a legitimate relying party site. The hacker will then be able to steel the unsuspecting victim's credentials.

Most successful phishing attacks are disguised using well-crafted emails that look legitimate to the target victim. The hacker's emails take users to fake login sites that look like the legitimate relying

party web sites. The victims can be tricked into providing their credentials to the hacker. Studies have shown that hackers act very quickly to maximize on the stolen credentials to takeover the victim's account.

There are some variations of these attacks whereby the hacker calls the victim and convinces them to provide their credentials under false pretences.

For most phishing attacks, the use of MFA cannot stop the attack since the user's second factor could also be captured by the hacker and passed back to the relying party.

6.2.4 Rainbow table attack

Passwords are usually stored hashed in data stores to minimize the impact of a data breach at an identity provider. A hashing function performs a one-way transformation of the password into a fixed size string that in theory cannot be converted back into clear text by an attacker. The objectives of the hashing step are to prevent an attacker that has compromised the password store from acquiring the text version of the password.

Attackers have learned to perform inverse lookup of the hashed strings of passwords using rainbow tables. Rainbow tables have hashes of popular passwords already computed and as such the inverse operation can be done quickly. The viability of a rainbow table is a function of the hashing algorithm used and the coverage provided in those tables in terms of leaked or compromised passwords.

6.2.5 Credential stuffing

In this type of attack the hacker can obtain the user credentials through a data hack. This is possible because users tend to re-use passwords. The attacker will try a user's compromised credentials from one site on other sites. In this regard the attacker will use lists of stolen usernames and passwords in combination on various accounts. The process is repeated until an account is taken over.

Credential stuffing works because users tend to reuse passwords on many sites.

6.2.6 Key logger attack

Key logger is a form of malware attack, in which an attacker installs a program on a victim's machine to track keystrokes. The attack can be conducted when a user logs on to a malicious site or a site that has been compromised. The attack can affect mobile and web-based devices.

As the victim types in their logon credentials (username and password), the attacker records the information for later use. This attack can bypass any protection that is offered using long and strong passwords.

6.2.7 Password recovery

Attackers can trick the relying party or the identity provider to reset the victim's password. This can be done through taking advantage of online support for a forgotten password feature in online systems. Attackers can take advantage of systems that rely on knowledge-based authentication (KBA) to takeover a user's account [ITU-T X.1254]. In some cases, attackers can fool helpdesk operators into performing a password reset on an account. On-line systems that rely on secret questions are very easy to circumvent since this information can be easily guessed or found on social media.

6.2.8 Default passwords

Device equipment and software vendors often ship their products with default passwords. These passwords are common and can be known by hackers. Many deployments do not force the users to change the password after first use.

6.2.9 Password storage risks

When a password is created by the user during the credentialing process, the system stores a copy of the hashed password in a secure database. This step is needed so that the system can validate subsequent logins based on the same password. For such systems it is important to secure the password database through proper salting and hashing of these passwords.

For organizations that rely on passwords for user authentication it is crucial that they follow a strict and comprehensive strategy for storing the passwords in data stores. The following steps can help enhance the security of password storage:

- Passwords hashing: This step helps to transform user passwords into strings of fixed size composed of random bits. In general, this step is one way and is difficult to reverse. When a user logs on, the system computes the hash of the entered password with the stored hash and authenticates the user when a match is confirmed.
- Salting passwords. Salting a password enhances the randomness of the hashed version of the password. For the salt to be useful, it needs to be unique to each password. Salting reduces the effectiveness of using rainbow tables to find the password from its hash. In general, salting is performed after a password has been hashed.

6.3 Password maintenance guidelines

Improving the security of passwords requires an organization to develop flexible password policies that allow users to select and protect their passwords. In this regard, [ITU-T X.1254], [b-NIST] guidelines are presented to help organizations advise their users on how to choose secure passwords:

- 1) Passwords should be of sufficient complexity that it would be impractical for an attacker to discover the correct secret value.
- 2) An effective password policy should address more than the quality of a given password. The policy should also address the behaviour of users that interact with the service provider.
- 3) From the user angle, the application interface should enable password show so that the user can be sure that the password as entered is the correct one. This step reduces data exposure risks due to incorrectly typed passwords.
- 4) Password managers should be used as these can help people to select and use stronger passwords. Password managers should be used in the workplace and at the consumer level.
- 5) When processing requests to establish and change passwords, service providers should compare user entered passwords against a list that contains values known to be commonly used, expected, or compromised passwords. For example, the list may include, but is not limited to:
 - a) Passwords obtained from previous breaches.
 - b) Dictionary words.
 - c) Repetitive or sequential characters.
 - d) Context-specific words, such as the name of the service, the username, etc.
- 6) Organizations should protect their users' passwords data stores. Passwords should be salted and hashed before they can be stored. Using salted hashes to store password data ensures that hackers do not get access to raw password data.
- 7) Locking a user out of a password protected application if they use an incorrect password a few times is important. Policies should be set to ensure logon attempts are logged and a locking policy is applied to restrict or restore access to an account.