International Telecommunication Union

ITU-T   X.1253
TELECOMMUNICATION   (09/2011)
STANDARDIZATION SECTOR
OF ITU

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Cyberspace security – Identity management

Security guidelines for identity management systems

Recommendation ITU-T X.1253

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	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	**X.1250–X.1279**
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1253

Security guidelines for identity management systems

Summary

Recommendation ITU-T X.1253 proposes security guidelines for identity management (IdM) systems. The security guidelines provide how an IdM system should be deployed and operated for secure identity services in a next generation network (NGN) or cyberspace environment. The security guidelines focus on providing official advice on how to employ various security mechanisms to protect a general IdM system and it also provides the required proper security procedures when two IdM systems are interoperated.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1253	2011-09-02	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, 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, 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 TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Recommendation ITU-T X.1253

Security guidelines for identity management systems

1   Scope

The scope of this Recommendation is as follows:

–   general IdM system models and services

–   IdM system related security threats and risks

–   security guidelines for the deployment of IdM systems

–   security guidelines for the operation of IdM systems

–   privacy considerations in IdM systems

The scope of this Recommendation mainly focuses on multi-domain based identity management services. However, the guidelines are also applicable to the centralized identity management system.

NOTE – Implementers and users of the described guidelines shall comply with all applicable national and regional laws, regulations and policies. Some specific regulations and legislation may require the implementation of mechanisms to protect personally identifiable information.

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.1205]   Recommendation ITU-T X.1205 (2008), *Overview of cybersecurity.*

[ITU-T X.1252]   Recommendation ITU-T X.1252 (2010), *Baseline identity management terms and definitions*.

3   Terms and definitions

3.1   Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1   access control [ITU-T X.1252]: A procedure used to determine if an entity should be granted access to resources, facilities, services, or information based on pre-established rules and specific rights or authority associated with the requesting party.

3.1.2   attribute [ITU-T X.1252]: Information bound to an entity that specifies a characteristic of the entity.

3.1.3   (entity) authentication [ITU-T X.1252]: A process used to achieve sufficient confidence in the binding between the entity and the presented identity.

3.1.4   credential [ITU-T X.1252]: A set of data presented as evidence of a claimed identity and/or entitlements.

3.1.5   identity [ITU-T X.1252]: The representation of an entity in the form of one or more information elements which allow the entities to be sufficiently distinguished within context. For

IdM purposes the term identity is understood as contextual identity (subset of attributes) i.e., the variety of attributes is limited by a framework with defined boundary conditions (the context) in which the entity exists and interacts.

NOTE – Each entity is represented by one holistic identity, which comprises all possible information elements characterizing such entity (the attributes). However, this holistic identity is a theoretical issue and eludes any description and practical usage because the number of all possible attributes is indefinite.

3.1.6   identity management [ITU-T X.1252]: A set of functions and capabilities (e.g., administration, management and maintenance, discovery, communication exchanges, correlation and binding, policy enforcement, authentication and assertions) used for:

•   assurance of identity information (e.g., identifiers, credentials, attributes);

•   assurance of the identity of an entity (e.g., users/subscribers, groups, user devices, organizations, network and service providers, network elements and objects, and virtual objects); and

•   supporting business and security applications.

3.1.7   user [ITU-T X.1252]: Any entity that makes use of a resource, e.g., system, equipment, terminal, process, application, or corporate network.

3.1.8   user-centric [ITU-T X.1252]: An identity management (IdM) system that provides the user with the ability to control and enforce various privacy and security policies governing the exchange of identity information, including the users' personally identifiable information (PII), between entities.

3.2   Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1   entity: Anything that has separate and distinct existence and that can be identified in context.

NOTE – An entity can be a physical person, an animal, a juridical person, an organization, an active or passive thing, a device, software application, service etc. or a group of these individuals. In the context of telecommunications, examples of entities include access points, subscribers, users, network elements, networks, software applications, services and devices, interfaces, etc.

3.2.2   IdM client: The client program that interacts with the IdM server to retrieve identity information.

3.2.3   IdM server: The server that manages the life cycle of an identity for a user.

3.2.4   Mobile IdM client: An IdM client that is installed and used on a mobile device.

4   Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DB   Database

DoS   Denial of Service

FDDI   Fibre Distributed Data Interface

IdM   Identity Management

IdP   Identity Provider

IDS   Intrusion Detection System

IPS   Intrusion Prevention System

LAN   Local Area Network

NGN   Next Generation Network

OS   Operating System

PII   Personally Identifiable Information

PIN   Personal Identification Number

PKI   Public Key Infrastructure

SP   Service Provider

SSL   Secure Socket Layer

TTP   Trusted Third Party

VPN   Virtual Private Network

5   Conventions

None.

6   Background

Over the past decade, the IdM (Identity Management) system has evolved from a silo system to a federated or user-centric IdM system. Most of the IdM systems developed so far have focused on how identity-related services can be provided efficiently and conveniently. Many of the recently developed IdM systems have made some effort to provide security and privacy.

In the early days, the IdM system known as the silo model was deployed in the enterprise domain. Here, each IdM system did not have any connection to any other so it was not possible to share a user's identity information to provide useful services among domains. Furthermore, an identity for one user could be duplicated in several different IdM systems. This makes it difficult for the system administration in the organization to manage a user's identity securely and efficiently.

The next step was to gather all the user's identities in one IdM system and disseminate it whenever it was needed. This approach was known as the centralized model. In this model, too much information for a user is aggregated on a single server. This approach has several drawbacks, as the IdP not only becomes a single point of failure but also may not be trusted by all parties.

The next approach was to let each IdP manage its own identity and decentralize its responsibility to multiple IdPs that could be selected by a user. This approach is known as a federated model. In this model, there exist multiple IdPs that can be trusted by a user and manages the partial identity information of users if required. Identity information of the user in each IdP can be shared using a part of a pseudonym called federated identity. This model avoids the problem of a single point of failure.

As privacy issues for a user becomes more and more important, IdM technology has focused on the users to give them full control over their identity information. This paradigm is known as the user-centric model. In this model, the identity information must pass through the user to give the user a chance to apply his privacy policy when two IdPs share the user's identity information. This model has been adapted by many industry products and embraces other existing IdM technologies.

The convergence of these IdM systems often faces challenging tasks regarding how the security of the converged system is guaranteed and how security and privacy are balanced to provide optimal performance. In addition, most of the security guidelines provided so far usually focused on an identity of providers and relying parties. As security and privacy aspects of a user become mandatory requirements, it is necessary to consider the user-centric part of IdM systems' security to reflect the growing concern about user privacy.

7 Overview of identity management systems

7.1 General model of IdM systems

7.1.1 Application-centric IdM system

In large scale IdM systems, the application-centric IdM system means that identity services and policies are designed to satisfy requirements for identity providers and relying parties and optimized for the requirements of applications, e.g., provisioning a user's account information. There is an identity provider and a relying party in the application-centric IdM system. When an identity service is provided for the user, the identity exchange usually takes place between these two entities. Historically, the identity and access management technologies have focused mainly on the authentication of end users for federated access to applications and services. Therefore, the security requirement is limited to the perimeter of its application domains.

7.1.2 User-centric IdM system

The user-centric IdM is mainly focused on end users and optimized for the requirement of those end users. It means that the main objective of an IdM system is to provide convenient and comprehensive identity services for users. The main feature is to give the user full control over his identity. When a user's identity information is disseminated, it must pass through the user explicitly to give the user a chance to enforce some personal policy if necessary. In the user-centric IdM system, a client program has to be installed in the user's computing environment. Therefore, easy and comprehensive security guidelines are required to guide the user to securely install and deploy any relevant software. The software must manage some of the user's security-related information.

User-centricity distinguishes itself from other models of IdM by emphasizing that the user and not an authority maintains control over how a user's identity attributes are created, disseminated, updated and terminated. It means that the user has full authority for the life cycle of their identity. The level of control can be determined by the user's privacy requirements.

7.2 Identity services

7.2.1 Identity life cycle management

This is the service that manages identity that is created, released, updated and terminated. The data relating to this service is stored in a database located in a server or a local machine. Therefore, access to this database should be preserved by only authorized users.

7.2.2 Authentication

An authentication service is to verify the legitimate users or entities that request access to the system or resources. Authentication is the key service that IdM systems provide for relying parties. Password crack and masquerading should be prevented at all cost.

7.2.3 Authorization

An authorization service is designed to deal with making decisions regarding the user's access rights and enforcing authorization decisions according to the user's privileges. This service is required to protect the identity system from unauthorized access and usage.

7.2.4 Attribute exchange

This is the service that provides attribute interchange and synchronization. This is one of the most critical services related to security since attributes are exchanged using a communication network. Different levels of security mechanisms are required for communication media varying from wired to wireless.

7.2.5   Security token

A security token service is required to share security or identity information between entities. A security token is usually protected by security and cryptographic mechanisms since it always contains highly confidential information that should not be released.

8   Security threats in IdM systems

Most of the security threats appearing in cyberspace are also supposed to exist in IdM systems, because they operate in a cyberspace. The general security threats in cyberspace are described in [ITU-T X.1205].

In IdM systems, there are various security threats that make the system vulnerable or lead to a security compromise that puts an organization in great danger.

8.1   Systems security

In general, systems security is concerned with protecting users' hardware and data. The intention is that the hardware should be accessed only by authorized users and for the purposes that the owners intend. Furthermore, the system should be utilized for those purposes. Attackers should not be able to dispossess legitimate users of resources.

8.1.1   Unauthorized access and usage

Most systems should not be accessed and used by unauthorized users. IdM systems should be very strict to prevent this type of security vulnerability since any unauthorized access to identity in an IdM system can lead to further security threats such as identity theft and masquerading.

8.1.2   Inappropriate usage

Inappropriate usage means that a user can use an IdM system to process or carry out a certain job that is not intended originally. An authorized user should have some limitation to using parts of the IdM system without proper privileges. Some services are restricted to authorized users, some to specific users, and some services are generally forbidden to all but administrators.

8.1.3   Denial of service

Usually an IdM system is the first entrance for a user to visit to use application services. Therefore, IdM systems are very likely to be a target for attack to stop providing services. A broad variety of attacks are possible on IdM systems to deny services. Denial of service attacks are often very easy to execute and difficult to stop. Many such attacks are designed to consume huge computing resources, making it difficult or impossible to serve legitimate users.

8.2   Passive security threats

In passive security threats, the attacker reads packets off the network but does not write them. The simplest way to implement such an attack is to simply be on the same LAN as the victim. On most common LAN configurations, including Ethernet, 802.3, and FDDI, any machine on the wire can read all traffic destined for any other machine on the same LAN.

Wireless communication channels deserve special consideration, especially with the recent and growing popularity of wireless-based LANs, such as those using 802.11. Since the data is simply broadcast on well-known radio frequencies, an attacker simply needs to be able to receive those transmissions. Such channels are especially vulnerable to passive attacks. Although many such channels include cryptographic protection, it is often the case that such security technology is not used with proper configuration.

8.2.1 Confidentiality violations

The confidentiality attack is to violate any private conversion or communication that is carried out on a communication line. In the Internet, there are still many cases that confidential information is transmitted in clear form. Any credential that is obtained through this attack can be reused for further attacks.

8.2.2 Password sniffing

Password sniffing is to collect user passwords that are transmitted over the network to obtain unauthorized use of resources. An attacker who can read this traffic can therefore capture the password and replay it. In other words, the attacker can initiate a connection to the IdM system to steal a user's identity information.

8.3 Active security threats

When an attack involves writing data to the network or the system, it is referred to as an active attack. Active attacks are an intrusion into a computer network which attempts to delete or modify the data stored on the IdM systems which form part of the network. This is one of the most serious forms of attack since many companies' operations critically depend on this data.

8.3.1 Replay attacks

In this attack, the attacker records a sequence of messages off the wire and plays them back to the corresponding party which originally received them. Note that the attacker does not need to be able to understand the messages. He or she merely needs to capture and retransmit them.

8.3.2 Man-in-the-middle attack

An attacker subverts the communication stream in order to pose as the sender to the receiver and the receiver to the sender. This kind of attack is serious because it masquerades as both a sender and a receiver. Consequently, many techniques which provide integrity of the communication stream are insufficient to protect against man-in-the-middle attacks. Man-in-the-middle attacks are possible whenever a protocol lacks peer entity authentication.

8.4 IdM system related security threats

These are the threats that are particularly concerned with IdM systems. The threats listed below are the main security weaknesses for which any IdM system should provide proper countermeasures.

8.4.1 Password related threats

One of the password related threats is due to the use of a weak password. If a user chooses a weak password, i.e., a guessable password, for the authentication, then the password can be subject to dictionary attack. Another problem occurs when the user keeps using the same weak password to several websites for login. In this case, any website that has a security weakness can be attacked to reveal its user passwords and the attacker simply tries to login to the other websites using the stolen passwords.

The other one is password sniffing by spyware in a computer. Any computer can be infected by spyware that can hijack a user or administrator password.

8.4.2 Unauthorized access

Unauthorized access is a term that can refer to a number of different kinds of attacks. The ultimate goal of the attacker is to gain access to resources illegitimately [ITU-T X.1205].

An IdM system providing authentication and identity services has to be available and accessed by all the parties that need to consume the user's identity to provide application services. Therefore, a fine-grained access control mechanism is necessary to protect the system from unauthorized access.

8.4.3 Eavesdropping

Eavesdropping is a difficult threat to detect. The aim of the attacker here is to listen and mostly record raw data on the enterprise LAN. This attack uses a "promiscuous mode" of the off-the-shelf Ethernet adaptors that are sold on the market. This mode allows an attacker to capture every packet on the network. There are plenty of free network sniffers on the web today that an attacker can use for eavesdropping [ITU-T X.1205].

IdM systems usually communicate with users and other entities to share credentials and identity information that is often confidential using wired or wireless networks. Therefore, any information that is picked up by an eavesdropper can lead to identity theft.

8.4.4 Phishing

This is an attempt by a third party to solicit confidential information from an individual, a group, or an organization by mimicking, or spoofing, a specific, usually well-known brand, usually for financial gain. An attacker attempts to trick users into disclosing personal data, such as credit card numbers, online banking credentials, and other sensitive information, that he/she may then use to commit fraudulent acts. A phishing website is a site designed to mimic the legitimate website of the organization whose brand is being spoofed. In IdM systems, phishing is a serious threat because the victim's authentication information or other personally identifiable information can be used in identity theft or other fraudulent activity once that information is captured by an attacker.

8.4.5 Identity theft

This is a high-profile security issue, particularly for organizations that store and manage large amounts of personal identity information. Not only can compromises resulting in the loss of personal data undermine customer and institutional confidence and result in costly damage to an organization's reputation, but data breaches can also be financially costly to organizations.

9 Security guidelines for IdM systems

Security guidelines of clauses 9.1 and 9.2 specify how to manage security when a general IdM system is deployed and operated. These guidelines provide baseline security requirements for an IdM system that can be securely deployed and operated in various computing environments. Clauses 9.3, 9.4 and 9.5 are devoted to the entities of IdM systems, which are IdM server, client and mobile client. Clause 9.6 describes privacy considerations in IdM systems.

9.1 Security guidelines for deployment of IdM systems

This clause provides security guidelines for when an IdM system is installed and deployed. In most cases, the preparation for trust and key management will be an issue.

9.1.1 Trust management

Every authorization made using IdM systems is dependent on trusting that an identity and its attributes are authentic and correct. Therefore, an identity is only useful when it has been authorized. The authority is established on the basis of trust. The plan of trust management is the first step for IdM systems to be deployed and operated successfully.

PKI (public key infrastructure) is one of the fundamental trust mechanisms for identity management systems. The main purpose of PKI is to provide a public key certificate that can be used for authentication and a secure channel. In a large scale IdM system, it is strongly recommended to establish a TTP (trusted third party) using PKI. The certificate that is issued from PKI can be used to authenticate a user to the IdM system and encrypt a communication channel in SSL. The digital signature is another key application of the certificate.

9.1.2 Network security

It is an essential requirement that a network environment should be secured using various means. First of all, the network perimeter should be secured using a firewall. Any IdM system must reside within the perimeter of the firewall. In addition, more sophisticated network security mechanisms such as VPN and IDS/IPS can be employed to provide more secure network environments.

9.1.3 Secure hosting environment

A hosting environment is where an IdM system is installed and operated. In servers or workstations where the IdM system component is installed, anti-virus programs and keyboard protection programs are required to be installed before the IdM system is installed. It should be guaranteed that the hosting environment is not compromised by any security attacks before any IdM system is installed and deployed.

9.1.4 Secure storage

Many important and sensitive data are kept in storage such as a database or directory server. During set-up, the storage server should be installed on a secure computer and an admin account should be established based on the proper installation guideline to exclude the case that any rogue account can be opened and later be used to compromise the system.

9.2 Security guidelines for operation of IdM systems

This clause provides security guidelines for when an IdM system is operated. Authentication and access control is one of the main issues to handle.

9.2.1 Digital signature

Digital signature is the security mechanism that can guarantee authenticity and integrity of a message that is signed. In the IdM system, there are many situations where a user has to demonstrate his willingness or consent for digital transactions. In this case, the digital signature that is employed can be used as evidence to verify its integrity.

9.2.2 Encryption

The IdM system requires encryption at various levels of its operation. First of all, messages that are exchanged between entities need to be encrypted, as confidentiality is required. Depending on the IdM operation policy, some of the data stored on a database is required to be encrypted for confidentiality and unauthorized access. The encryption will provide a maximum level of confidentiality for IdM systems and it will ultimately ensure the privacy of a user and his identity information.

9.2.3 Authentication

Authentication is a gate function to prevent unauthorized access to the system from illegitimate users. With the Internet, simple id/password authentication is widely used but it has many weak points in security measures. Therefore, strong authentication is recommended whenever it is necessary to assure high confidence of a user who accesses the system. Phishing and pharming attacks can be mitigated if mutual authentication is employed.

9.2.4 Secure communication

Most of the information that is exchanged between a user and the IdM system is privacy-concerned and confidential in nature. Moreover, the protocol messages among entities can carry sensitive and confidential information that needs to be encrypted over communication lines. Secure communication can be achieved by using existing technologies such as SSL and VPN.

9.2.5 Access control

Various entities such as administrators and users can access an IdM system for particular services and day-to-day maintenance. Any proper access control mechanism is needed to prevent system penetration from malicious third parties. In most cases, a discretionary access control (i.e., access control lists) model should be sufficient. However, as a role-based access control model can provide more elaborate and fine-grain control, it can be applied where a more secure and flexible access control model is required.

9.3 Security guidelines for IdM servers

This clause provides security guidelines which are specific to an IdM server installed and operated in large workstations or servers.

9.3.1 Securing the operating system

Most commonly-available IdM servers operate on a general-purpose OS (operating system). Many security issues can be avoided if the OS used by the IdM server is configured appropriately. Since an IdM server is installed on the existing OS, its security is mostly dependent on that of the OS. The techniques for securing different OS vary greatly; therefore, this clause includes the generic procedures common in securing most OS. The more basic security management in OS can be found in [ITU-T X.1205] and [b-NIST SP 800-123].

In order to secure IdM servers, the following basic steps are necessary to secure the OS:
– patch and update the OS
– harden and configure the OS to address security adequately
– install and configure additional security controls, if needed
– test the security of the OS to ensure that the previous steps adequately addressed all security issues.

9.3.2 Configure user authentication

For IdM servers, the authorized users who can configure the server should be limited to a small number of designated server administrators. To enforce policy restrictions, if required, the server administrator should configure the server to authenticate a user by requiring proof that the user is authorized for such access. In the case of IdM servers that are required to provide high levels of confidence and trust, organizations may also use temper-resistant authentication hardware, such as tokens or one-time password devices. In this case, use of authentication mechanisms where authentication information is reusable (e.g., passwords) and transmitted in the plaintext form over an untrusted network is strongly discouraged because the information can be intercepted and used by an attacker to masquerade as an authorized user.

The default configuration of the OS often includes guest accounts with or without passwords. The administrator should remove or disable unused guest accounts to eliminate their use by attackers.

9.3.3 Configuring access control

Most IdM servers provide the capability to specify access privileges individually for the credentials of identity information. Any user who accesses an IdM server should not be allowed to access other users' identity information. The proper setting of access controls can help prevent the disclosure of sensitive or restricted identity information that is not intended for public dissemination. In addition, access controls can be used to limit resource use in the event of a DoS (denial of service) attack against the server.

9.3.4 Logging

Logging is an essential part of a sound security counter-measure. It is very important that the correct data is captured in the logs and then later those logs are monitored closely. Network and system logs are important, especially system logs in the case of encrypted communications, whereas network monitoring is less effective.

Reviewing logs is a mandatory and effective way to find suspicious activity. In many cases, log files are often the only record of suspicious behaviour. Enabling the mechanisms to log information allows the logs to be used to detect failed and successful intrusion attempts, and to initiate alert mechanisms when further investigation is needed. Procedures and tools need to be in place to process and analyse the log files and to review alert notifications.

It should be ensured that access controls can enforce separation of duty by ensuring server logs cannot be modified by server administrators and potentially ensure that the server process is only allowed to append to the log files.

9.4 Security guidelines for IdM clients

This clause provides security guidelines for when an IdM client program is operated. In the case that a web browser is used as an IdM client, security vulnerability is dependent on the browser itself. Nevertheless, some of the guidelines still can be followed to ensure the security of its client environment.

9.4.1 Secure distribution of a client program

These days most of the browser-dependent plugins are downloaded from a website. If a user accidently downloads a wrong IdM client program that can potentially harm a system of the user, then no strong security mechanisms will be able to protect the user from malicious activity. Therefore, a provider of the IdM client program must ensure that a disseminated client program is integrity protected and provides a secure way to validate its integrity.

9.4.2 Integrity of a client program

To provide integrity of a client program, a digital signature is a key solution for the candidate. If the client program is signed by a provider and a signing certificate is provided for validation, then the user can securely download and verify the integrity of the program code. There is an alternative method that uses a hash algorithm to ensure the integrity of a code. The client code is the input to the hash algorithm to produce a hash value, which is the digest of the client code. If the hash value is published on the web in a secure way, the user can validate his client program by calculating a hash value of the downloaded client program. However, the former is more secure than the latter.

9.4.3 Client DB file

Client DB (database) files should be stored securely. Access to the DB should strictly be limited to authenticated users. In most cases, an IdM client manages user credential information including passwords and security tokens that should be kept in an encrypted form for confidentiality. Also the DB file itself should be protected from illegal alteration and modification for its integrity. When the DB file is removed from a system, there should be no trace on the hard disk for later recovery.

9.4.4 Secure password

Most of the security mechanism is ultimately dependent on an authentication password to access the system. If a user uses a weak password that can be cracked by a brute force attack, then no other security mechanisms can protect the system from malicious users. Therefore, it is the most important task for an IdM service provider to ensure a user uses a strong password for the login.

9.4.5 Uninstalling a client program

When a client program is uninstalled in a user system, any password, credential and identity information should be deleted permanently and personal configuration for the client program should be erased as well.

9.5 Security guidelines for mobile IdM clients

This clause provides security guidelines for mobile IdM clients, which are installed and operated on a mobile device. The mobile device has exclusive characteristics such as portability and mobility. However, these characteristics can be security weak points if an attacker exploits it.

9.5.1 Device lost or stolen

Since a mobile device is portable, it is very likely to be lost or stolen. There are many ways to penetrate the mobile device to extract personal information for identity fraud. Therefore, a mobile client in the device should be prepared for any security attack that might cause unauthorized use or identity fraud. When the device is lost or stolen, the incident is reported to a mobile communication provider and, based on the situation; the operator can lock the device remotely to block any access to the device. This is appropriate when the device is lost in a friendly environment such as home or the workplace. In any other cases, the operator should be able to erase any personal information or identity record stored on the device if the owner thinks that the device is permanently lost or stolen and there is no way of getting it back.

9.5.2 Device authentication

If a mobile device has a small size display for input, then it is very difficult for a user to login to the device using an alphanumeric-based password every time the device is used. In this case, a PIN (personal identification number) is used as a password, but on many occasions it is not used for the sake of convenience. To overcome this situation, the mobile client of IdM should provide user-friendly but secure enough authentication mechanisms suitable for the mobile device. The mobile client must enforce password-based authentication in the case of the device not using any authentication mechanisms for user login.

9.5.3 Database backup

Most identity information is collected and processed within a mobile device for various services. However, many of those identities are sensitive and privacy-concerned personal information which need to be protected for integrity and confidentiality. As indicated earlier, the device easily tends to be lost or stolen. Therefore, the mobile client of IdM needs to provide a way to back up the database of identity information. This can be done in two ways. The first way is to back up the database in secondary storage such as on an SD (secure digital) memory card if available. The second way is to use an external backup server to provide a database backup service for the client. In this case the user's database can always be restored even if the device is lost or stolen.

9.5.4 Mobile communication security

A mobile device most of the time uses mobile communications to communicate with other devices. However, it is recognized that mobile communications are very vulnerable to active and passive attacks. The mobile client of IdM usually transmits sensitive personal information over the mobile link. Therefore, any communication with a mobile client using mobile links needs to be protected by transport layer security for integrity and confidentiality.

9.6 Privacy considerations in IdM systems

Privacy is a very important issue in the context of IdM security. However, there are many rules and regulations for each individual country when privacy guidelines are to be practically applied. Therefore, in this clause, some privacy issues for IdM systems are explored and provided as information.

9.6.1 User consent

When identity is collected from a user and used by an IDP or SP, the consent from a user should be obtained explicitly for clarification. It would be best if user consent is obtained by a form of digital signature, which can be verified later if necessary.

9.6.2 Identity choice

IdM systems explicitly provide a way for an individual to choose whether or not to allow the collection, usage, transfer, storage, archiving, or disposal of identity. Privacy for the user is enhanced because the user is in control of managing their identity and privacy policy. This user-centric approach should be considered in the phase of IdM system design.

9.6.3 Purpose of identity

The IdM system should notify a user of all the purposes for which personal information is collected and used, in a readily understandable manner, prior to collecting their identity. In addition, the system should make a reasonable effort to use identity for the purpose that is notified.

9.6.4 Identity limitation and minimization

IdM systems that collect identities should only collect those necessary to fulfil the purposes that they have identified except with the consent of the individual or as permitted or required by law.

The IdM system that collects identities should carefully consider and document procedures that state clearly which identity is needed for which purpose and how it ensures that all identity processing involves collecting only the minimal identities necessary for their purpose.

9.6.5 Disposal of identity

IdM systems should dispose of the identity after its stated purpose has been fulfilled and no other legal or regulatory obligations require a longer retention period. When an identity is disposed of, it should be ensured that all identity information stored in related systems such as backup and archive systems are deleted as well.

9.6.6 Privacy policy set-up

Before the IdM system is operated, privacy policies such as privacy preference and privacy authorization policies may be set up. This policy governs the usage of the identity that is submitted to the system by a user.

9.6.7 Anonymity

Anonymity can be the ultimate objective to be achieved in a privacy enhanced IdM system. However, it is a very difficult and complex function to provide at a reasonable cost. Therefore, in most cases, a pseudonym can be applied to satisfy the privacy requirement of an IdM system.

Bibliography

[b-NIST SP 800-123] Scarfone, K.A., Jansen, W., and Miles, T. (2008), *Guide to General Server Security*, NIST Special Publication SP-800-123.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems