ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

Recommendation

ITU-T X.1220 (11/2023)

SERIES X: Data networks, open system communications and security

Cyberspace security – Cybersecurity

Security framework for storage protection against malware attacks on hosts

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 (1)	X.1100-X.1199
CYBERSPACE SECURITY	X.1200-X.1299
Cybersecurity	**X.1200-X.1229**
Countering spam	X.1230-X.1249
Identity management	X.1250-X.1279
SECURE APPLICATIONS AND SERVICES (2)	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
IMT-2020 SECURITY	X.1800-X.1819

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

Recommendation ITU-T X.1220

Security framework for storage protection against malware attacks on hosts

Summary

Recommendation ITU-T X.1220 provides a framework for the protection of storage against malware attacks on hosts, which bypass network protection and endpoint protection. The framework also considers attacks caused by human errors or social engineering. The framework consists of a host and a storage protection server. The storage protection server works separately from the host, stores data in the storage, and provides a network drive to the host.

When an application on the host requests data, the storage protection server provides real data or fake data depending on whether the application is listed or not in a pre-registered application list that is managed on the storage protection server with the objective of protecting data in the storage against malware attacks that encrypt, tamper, or steal data. The storage protection server allows pre-registered applications to create, modify or delete data in the storage while preventing other applications from performing those operations. It provides pre-registered applications with read-write access to real data from the storage, and non-registered applications with read-only access to fake data. In addition, there is synergy if the framework is applied together with network protection and endpoint protection, as they provide different types of protection.

History [*]

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T X.1220	2023-11-13	17	11.1002/1000/15709

Keywords

Data, malware, protection, storage.

[*] 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, 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 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/.

Table of Contents

Page

Recommendation ITU-T X.1220

Security framework for storage protection against malware attacks on hosts

1 Scope

This Recommendation provides a framework for the protection of storage against malware attacks on hosts, which bypass network protection and endpoint protection. The framework also considers attacks caused by human errors or social engineering.

This Recommendation provides the following:

- definition of the functional architecture and entities of the storage protection framework;
- definition of the operating procedure of the storage protection framework;
- identification of security threats and requirements related to the storage protection framework; and
- use cases of the storage protection framework.

This Recommendation does not address issues related to network protection, endpoint protection or regulation.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 deceptive software [b-ITU-T X.1207]: Software which performs activities on a user's computer without: 1) first notifying the user as to exactly what the software will do on the user's computer; or 2) asking the user whether he consents to the software doing these things. Examples of deceptive software include programs which hijack user configurations, or programs which cause endless pop-up advertisements which cannot be easily clicked out of by the user.

3.1.2 endpoint [b-ITU-T X.1526]: Any computing device that can be connected to a network such as a computer system, server, network appliance, mobile device, etc. Such devices normally are associated with a particular link layer address before joining the network and potentially an IP address once on the network.

3.1.3 firewall [b-ITU-T X.1205]: A system or combination of systems that enforces a boundary between two or more networks. A gateway that limits access between networks in accordance with local security policy.

3.1.4 malware [b-ITU-T X.1218]: Malicious software designed specifically to damage or disrupt a system attacking confidentiality, integrity and/or availability.

NOTE – Examples include viruses, ransomware, spyware, adware and scareware.

3.1.5 unknown malware [b-ITU-T X.1218]: Unknown malware is malware that has not been discovered yet, which means that no signatures or features exist for it in most security systems such as antivirus or antispyware software. There is always a gap period between the time a malware starts spreading across the Internet and the time its signature or feature is available. During this gap period the malware is an unknown malware.

3.2 Terms defined in this Recommendation

This Recommendation defines the following terms:

3.2.1 binary hash: The output of a cryptographic hash function that is used to verify the integrity of an application.

3.2.2 host: A computer that communicates using the Internet protocols.

NOTE – Definition is adapted from [b-ITU-T Y.1545].

3.2.3 mount: A process whereby the operating system of the computer makes storage accessible via the file system of the computer.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

AI	Artificial Intelligence
CCTV	Closed Circuit Television
MFA	Multi-Factor Authentication
PC	Personal Computer

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 Introduction

Malware attacks that encrypt, tamper with, or steal data on hosts are on the rise. To protect data on hosts from such malware attacks, network protection and endpoint protection technologies have been adopted. However, these protection technologies may not be enough to counter such attacks.

Network protection technologies, such as firewall work based on whitelist-based and behaviour-based detection mechanisms. Whitelist-based detection works by comparing all traffic on the network with the whitelist and inspecting every packet. If the attack starts with the approved network or encrypted data packets, it easily bypasses the whitelist-based detection mechanism. To overcome the limitations of whitelist-based mechanisms, behaviour-based detection mechanisms including artificial intelligence (AI) technology have been adopted, but these are resource-intensive and inevitably less accurate.

If the network protection is compromised, endpoint protection should protect data on hosts. However, endpoint protection technologies, such as antivirus technology work based on blacklist-based and behaviour-based detection mechanisms. Blacklist-based detection works by comparing application binary hashes running on the hosts with the blacklist so unknown malware can bypass the blacklist-based detection mechanism. Endpoint protection technologies have also adopted behaviour-based detection mechanisms to overcome the limitations of blacklist-based mechanisms, but they require more computing power on the hosts and work less accurately. It is difficult to accurately decide whether a process running on the host is malware or a normal application if it is malware running in a new way. This is especially so if the malware or deceptive software includes user deception techniques that induce user consent, it then is more difficult to protect data in the storage only using endpoint protection technologies.

If malware attacks bypass network protection and endpoint protection, then data in the storage mounted on the host can be encrypted, tampered with, or stolen. It is not possible to determine whether applications requesting the data are normal applications used by the user or malware from the storage perspective since general storages provide data according to requests by applications on the host.

Figure 1 illustrates limitations of network protection and endpoint protection.

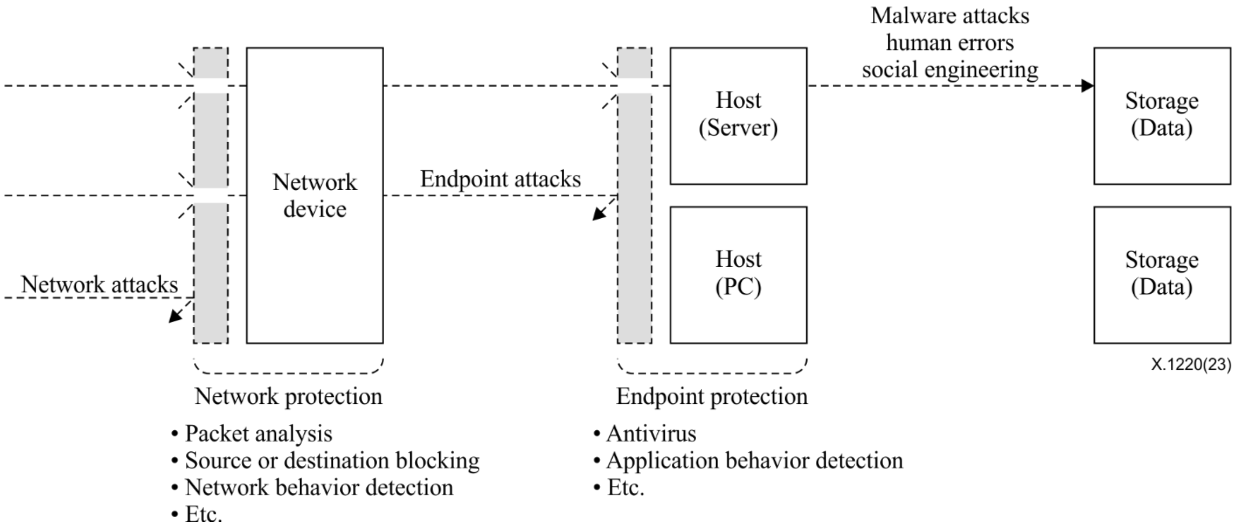


Figure 1 – Limitations of network protection and endpoint protection

Therefore, a security framework may be needed for storage protection against malware attacks on hosts, which bypass network protection and endpoint protection, and would also counter attacks caused by human errors or social engineering.

The framework consists of a host and a storage protection server. The storage protection server works separately from the host, stores data in the storage, and provides a network drive to the host.

When an application on the host requests data, the storage protection server provides real data or fake data to the application after comparing it with the pre-registered application list managed on the storage protection server for protecting data in the storage from malware attacks which encrypt, tamper with, or steal data.

The storage protection server allows pre-registered applications to create, modify or delete data in the storage while preventing other applications from performing those operations. It provides pre-registered applications with read-write access to real data from the storage, and non-registered applications with read-only access to fake data.

Thus, data in the storage is protected from malware attacks on hosts, and even attacks caused by human error or social engineering, which bypass network protection and endpoint protection.

In addition, there is synergy if the framework is applied together with network protection and endpoint protection, as they provide different types of protection.

Figure 2 illustrates the concept of storage protection against malware attacks on hosts.

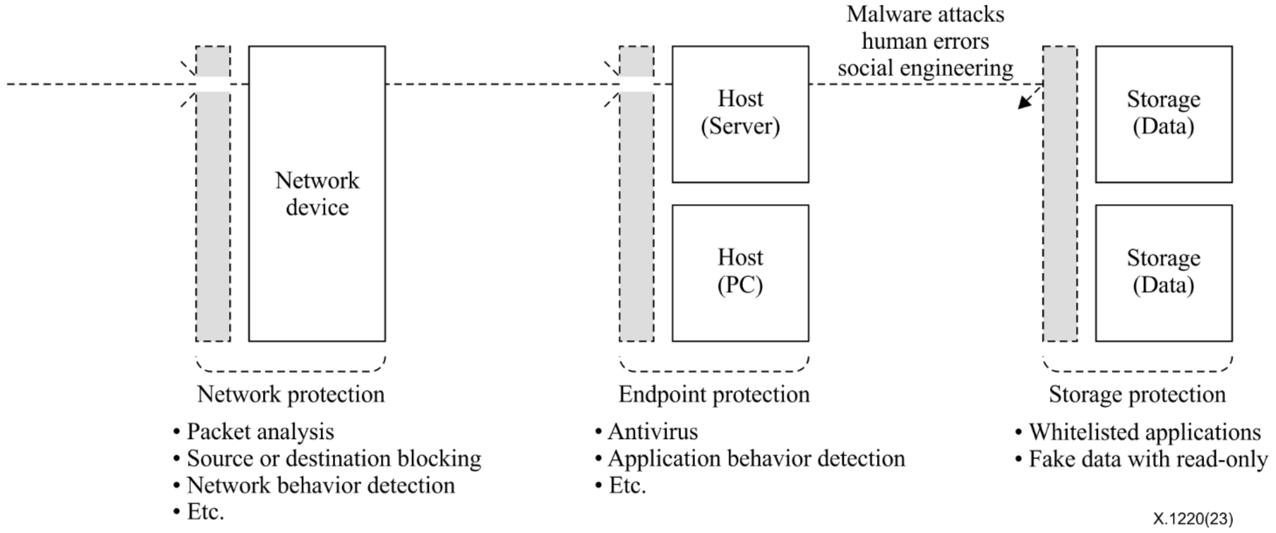


Figure 2 – Concept of storage protection against malware attacks on hosts

7 Storage protection framework

7.1 Functional architecture

This clause defines the functional architecture of the storage protection framework, which protects storage against malware attacks on hosts.

Figure 3 illustrates the functional architecture of the storage protection framework.

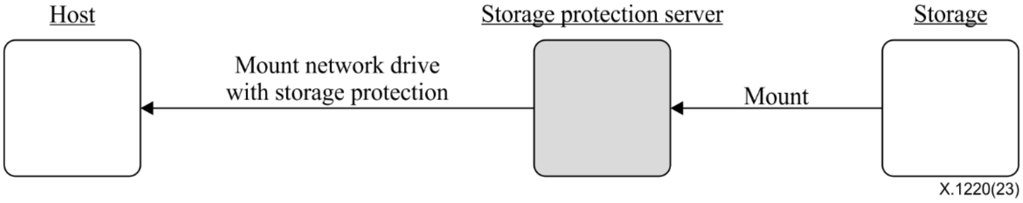


Figure 3 – Functional architecture of storage protection framework

The storage protection framework consists of hosts and a storage protection server.

The host mounts the storage protected by a storage protection server as a network drive and requests data from the storage protection server through the network drive.

The storage protection server stores data on mounted local storage or external storage and provides the data to the host through a network drive.

When an application running on the host requests data in the storage protected by the storage protection server through a network drive, the storage protection server provides real data or fake data depending on whether the application is listed or not in a pre-registered application list that is managed on the storage protection server. It provides pre-registered applications with read-write access to real data from the storage, and non-registered applications with read-only access to fake data.

Since the storage protection server provides data to the host through a network drive, data can be protected even if the host is completely taken over by malware attacks. Even if malware tries to attack data through a network drive, it is difficult to attack beyond data creation, reading, writing, and deletion requests because it is mounted as a storage device on the host.

The storage protection can eliminate the need to implement unnecessary protection technologies or mechanisms by providing fake data with a read-only attribute when applications that have not been pre-registered request data.

Typical protection methods that block requests from applications and block providing data to applications can cause continuous request events, which can be resource-intensive for both the host and storage while storage protection can be lightweight by just providing fake data with a read-only attribute.

7.2 Entities

The entities constituting the storage protection framework are composed of hosts and a storage protection server.

A storage protection agent is installed and runs on the host. It communicates with the storage protection server through the storage protection agent.

A storage protection engine is installed and runs on the storage protection server. It responds to requests from the storage protection agent.

7.2.1 Host

The host requests data from the storage protection server through the network drive. Applications that require data access and the storage protection agent are installed and run on the host.

The storage protection agent consists of the application registration module and the network drive module. Figure 4 illustrates the components and functions of the host.

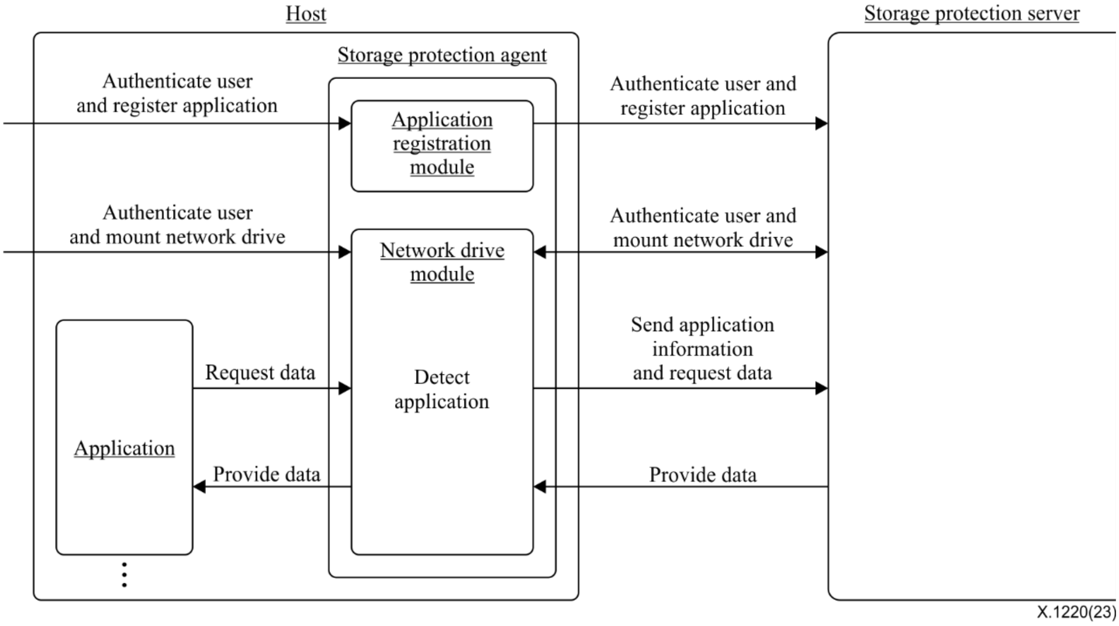

Host
Storage protection server
Storage protection agent
Authenticate user and register application
Application registration module
Authenticate user and register application
Authenticate user and mount network drive
Network drive module
Authenticate user and mount network drive
Send application information and request data
Application
Request data
Detect application
Provide data
Provide data
X.1220(23)

Figure 4 – Components and functions of host

Component and functions of the host are described in Table 1.

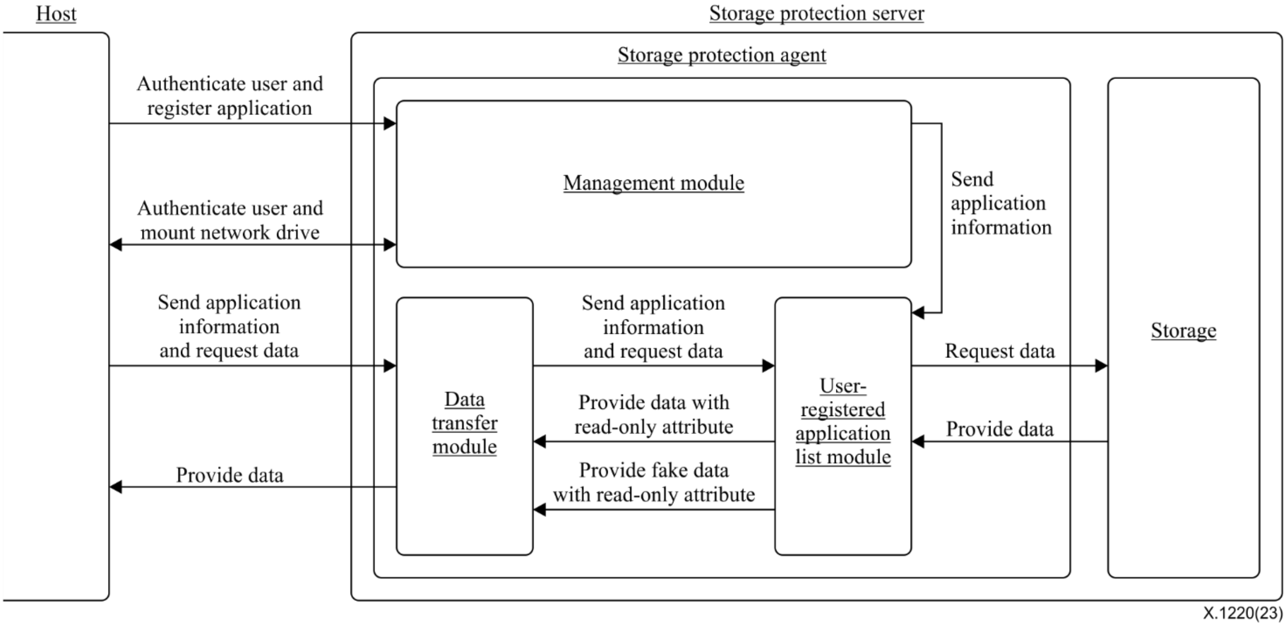
Table 1 – Descriptions of components and functions of host

Component		Function	Description
Application		Data request	Requests data in the storage protected by the storage protection server through the network drive module to create, read, modify, and delete data, such as documents and images.
Storage protection agent	Application registration module	Application registration	Registers the application information such as binary hash and name of the executable file after user authentication. Once registered, the application is allowed to create, view, modify, and delete data in the storage protected by the storage protection server.
	Network drive module	Network drive mount	Connects the storage of the storage protection server to the host as a network drive after user authentication.
		Application detection	Detects applications attempting to create, view, modify, or delete data in the storage protected by the storage protection server.
		Data request	Requests data in the storage protected by the storage protection server through the storage protection server to create, view, modify, or delete data when an application requests it. Sends the detected application information to the storage protection server.
		Data process result provision	Provides data with a read/write attribute or fake data with read-only attribute received from the storage protection server to the application which requested data to read. Provides the result of creation, modification, or deletion received from the storage protection server to the application which requested creation, modification, or deletion of data, or the result of blocking the request.

7.2.2 Storage protection server

The storage protection server is mainly composed of the storage protection engine and the storage.

The storage protection engine is composed of the management module, data transfer module, and the user-registered application list module. Figure 5 illustrates the components and functions of the storage protection server.



Host
Storage protection server
Storage protection agent
Authenticate user and register application
Management module
Send application information
Authenticate user and mount network drive
Send application information and request data
Send application information and request data
Data transfer module
Provide data with read-only attribute
User-registered application list module
Request data
Provide data
Storage
Provide data
Provide fake data with read-only attribute
X.1220(23)

Figure 5 – Components and functions of storage protection server

The components and functions of the storage protection server are described in Table 2.

Table 2 – Descriptions of components and functions of storage protection server

Component		Function	Description
Storage protection engine	Management module	Application management	Manages the application registration. Provides application information to the user-registered application list module.
		User management	Manages user accounts and user authentication.
		Mount management	Manages and provides a network drive to the hosts after user authentication.
		Storage management	Manages storages used by the storage protection server for data storage.
	Data transfer module	Data request	Requests data and sends the requesting application information received from a host through the network drive to the user-registered application list module.
		Data provision	Provides the data provided from the user-registered application list module to the host through the network drive.
	User-registered application list module	Pre-registered application verification	Verifies whether the requesting application is a pre-registered application when data request and requesting application information are received from the data transfer module.
		Fake data creation	Creates fake data when not registered applications request data.
		Data request	Request data in the storage protected by the storage protection server when a pre-registered application requests data.

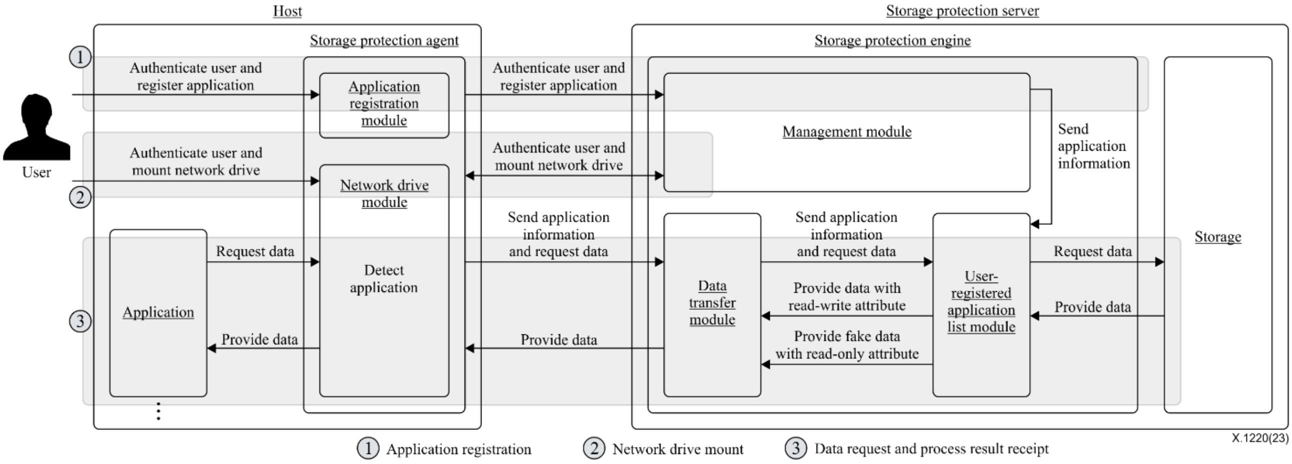
Table 2 – Descriptions of components and functions of storage protection server

Component		Function	Description
		Request process	Provides data with a read/write attribute when a pre-registered application requests to read. Processes data when a pre-registered application requests to write, modify, or delete, and then sends the result to the data transfer module. Provides fake data created by itself with a read-only attribute when a not registered application requests to read. Blocks processing data when a not registered application requests to write, modify, or delete, and then sends the result to the data transfer module.
Storage		Data storage	Stores data created by pre-registered applications.

8 Operating procedure

The operating procedures of the storage protection framework, which can protect data stored in the storage even when the malware runs on the host are shown in Figure 6.

The operating procedures are divided into application registration, network drive mount, and data request and process result receipt. Figure 6 illustrates the operating procedures of the storage protection framework based on the overall components and functions.



Host
Storage protection agent
Storage protection server
Storage protection engine
User
1
Authenticate user and register application
Application registration module
Authenticate user and register application
Management module
Send application information
2
Authenticate user and mount network drive
Network drive module
Authenticate user and mount network drive
3
Application
Request data
Provide data
Detect application
Send application information and request data
Provide data
Data transfer module
Send application information and request data
Provide data with read-write attribute
Provide fake data with read-only attribute
User-registered application list module
Request data
Provide data
Storage
X.1220(23)
1 Application registration
2 Network drive mount
3 Data request and process result receipt

Figure 6 –Operating procedures of storage protection framework

8.1 Application registration

The user requests to register the application after being authenticated as a legitimate user through the application registration module of the storage protection agent installed in the host.

When requesting application registration to the storage protection server, the binary hash of the application executable file, executable file name and path, etc., are provided.

The application registration module performs user authentication and application registration with the management module of the storage protection engine installed in the storage protection server.

When an authenticated user registers an application, the management module sends application information to the user-registered application list module of the storage protection engine.

When the binary hash of a registered application is changed by authorized methods such as regular software updates, the application information needs to be updated or re-registered.

8.2 Network drive mount

The user requests the network drive mount with the storage protected by the storage protection server after being authenticated as a legitimate user through the network drive mount module of the storage protection agent installed in the host.

The network drive module performs user authentication and network drive mount with the management module of the storage protection engine installed in the storage protection server.

8.3 Data request and process result receipt

When an application running on the host accesses the storage protected by the storage protection engine of the storage protection server through the network drive module of the storage protection agent and requests to read data, the network drive module detects the application, and then sends the application information such as executable file binary hash, executable file name and path to the data transfer module of the storage protection engine installed in the storage protection server.

The data transfer module requests data to the user-registered application list module of the storage protection engine along with the application information.

The user-registered application list module provides data with a read/write attribute from the storage protected by the storage protection server to the data transfer module when a pre-registered application requests, but provides fake data with a read-only attribute created by itself to the transfer module when the other applications request.

The user-registered application list module processes data creation, modification, or deletion when a pre-registered application requests to create, modify, or delete data but blocks the requests from non-registered applications. After the data are either processed or blocked, the result is sent to the data transfer module.

The data transfer module sends the data or the process result, which is received from the user-registered application list module to the network drive module of the host, and then the network drive module provides the data or process result to the application.

9 Security threats

In this clause, potential security threats that may arise from the storage protection framework are identified.

9.1 Storage protection server administrator credentials leak

If the credentials of the administrators of the storage protection server are leaked, an attacker can directly access the storage protection server to encrypt, tamper with, or steal data in the storage or to change the application information in the user-registered application list module.

Furthermore, malware can be registered to the user-registered application list, or legitimate application information can be removed from the list, potentially affecting the host system while accessing data.

9.2 User credential leak

If the credentials of the users are leaked, malware can be registered in the user-registered application list module by an attacker.

9.3 Applications tampering

After an application installed on the host is registered in the user-registered application list, it can be tampered with via the same executable file name by injecting malicious code into it to attack data in the storage.

9.4 Malware registration by inducing users

Malware can imitate legitimate applications and be installed on the host. It can then be registered in the user-registered application list by deceiving or tricking users.

9.5 Application changes

When an application installed on the host is updated, typically its binary hash is changed, potentially interrupting access to data.

10 Security requirements

In this clause, the security requirements are described in response to potential security threats that may arise from the storage protection framework. The relationship between each security threat and security requirement is described in Appendix I.

10.1 MFA for storage protection server administrator accounts

Multi-factor authentication (MFA) such as one-time password should be applied to the administrator accounts of the storage protection server.

10.2 MFA for user accounts

Multi-factor authentication such as one-time password should be applied to the user accounts when registering applications to the storage protection server.

10.3 Hash-based application registration

The storage protection server shall manage the application information in the user-registered application list module based on the hash of the executable file to verify whether the requesting application is legitimate even if it has the same file name.

10.4 Binary hash management

Before registering an application in the user-registered application list, its binary hash should be compared to the genuine binary hash that is managed separately in the management module.

The genuine binary hash should be added to the module from a trusted environment based on the applications installed on hosts to perform an integrity check. For updated applications, their binary hashes should be pre-added to the module to ensure uninterrupted access to data.

Annex A

Relationship between security requirements and threats

(This annex forms an integral part of this Recommendation.)

Table A.1 describes the relationship between security requirements and potential security threats that may arise from the storage protection framework.

Table A.1 – Relationship between security requirements and threats

Security requirements	**Security threats**				
	Administrator credentials leak	**User credentials leak**	**Application tampering**	**Malware registration by inducing users**	**Application changes**
MFA for storage protection server administrator accounts	o	–	–	–	–
MFA for user accounts	-	o	–	–	–
Hash-based application registration	–	–	o	–	–
Binary hash management	–	–	–	o	o

Appendix I

Use cases of storage protection framework

(This appendix does not form an integral part of this Recommendation.)

I.1 CCTV storage protection

A storage protection server can be used to prevent attacks on video data from cyber security incidents which encrypt, tamper with, or steal the data.

To protect the storage, applications that create and play the video data need to be registered in the storage protection server and set the data location to a network drive provided by the storage protection server.

Video data is only able to be created or played through the applications. The video data is also protected even if the administrator of the closed circuit television (CCTV) server tries to delete, modify, or steal the data through the network drive.

I.2 Blockchain wallet storage protection

A storage protection server can be used to prevent attacks on the private key of a blockchain wallet from cyber security incidents which may encrypt, tamper with, or steal the private key.

To protect the storage, the wallet application needs to be registered in the storage protection server and the private key location set to a network drive provided by the storage protection server.

The private key is only able to be accessed through the applications, and it remains protected even if someone attempts to delete, modify, or steal the data through the network drive.

I.3 Email server storage protection

A storage protection server can be used to prevent attacks on email data from cyber security incidents which may attempt to encrypt, tamper with, or steal the data.

To protect the storage, applications that create and read the email data need to be registered in the storage protection server and the data location set to a network drive provided by the storage protection server.

The email data is only able to be created or read through the applications. The email data is also protected even if the administrator of the server tries to delete, modify, or steal the data through the network drive.

I.4 Backup storage protection

A storage protection server can be used to prevent attacks on the backup data from cyber security incidents which attempt to encrypt, tamper, or steal the data.

To protect the storage, applications that create and restore the backup data need to be registered in the storage protection server and the data location set to a network drive provided by the storage protection server.

Backup data is only able to be created or restored through the applications. The data is also protected even if the administrator of the backup server tries to delete, modify, or steal the data through the network drive.

I.5 General storage protection

A storage protection server can be used to prevent the data in general storages from cyber security incidents which attempt to encrypt, tamper with, or steal the data.

To safely use the large-capacity general storage currently in use, the storage protection server is constructed as shown in Figure I.1, then the existing general storage is mounted as an external storage of the storage protection server.

Even if large amounts of data are stored in the existing general storage, data can be immediately protected through the storage protection server without any data migration.

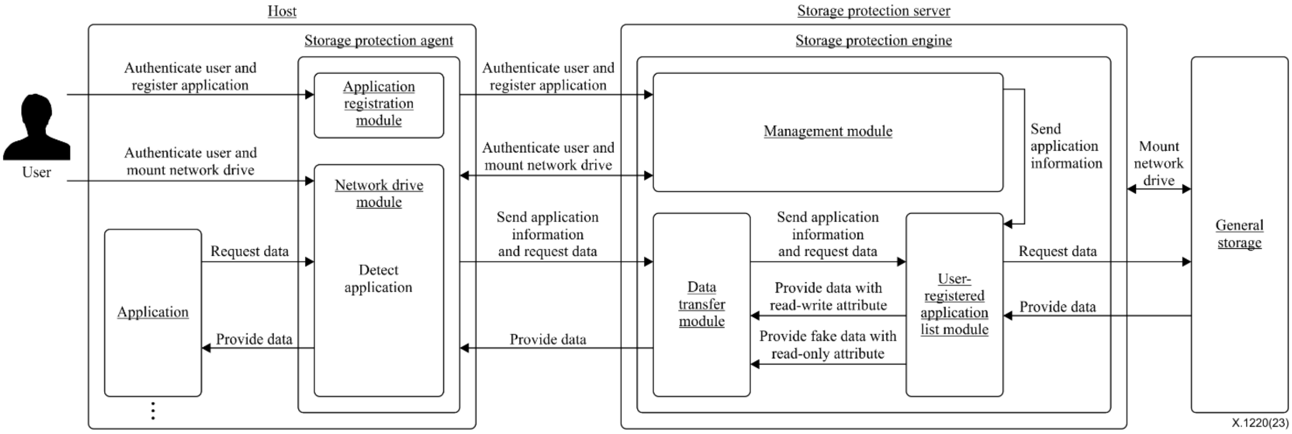

Host
Storage protection agent
User
Authenticate user and register application
Application registration module
Authenticate user and mount network drive
Network drive module
Detect application
Application
Request data
Provide data
Storage protection server
Storage protection engine
Authenticate user and register application
Authenticate user and mount network drive
Send application information and request data
Provide data
Management module
Send application information
Data transfer module
Send application information and request data
Provide data with read-write attribute
Provide fake data with read-only attribute
User-registered application list module
Request data
Provide data
Mount network drive
General storage
X.1220(23)

Figure I.1 – Operating procedure of the storage protection framework with general storages

Bibliography

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

[b-ITU-T X.1207] Recommendation ITU-T X.1207 (2008), *Guidelines for telecommunication service providers for addressing the risk of spyware and potentially unwanted software.*

[b-ITU-T X.1218] Recommendation ITU-T X.1218 (2020), *Requirements and guidelines for dynamic malware analysis in a sandbox environment.*

[b-ITU-T X.1526] Recommendation ITU-T X.1526 (2014), *Language for the open definition of vulnerabilities and for the assessment of a system state.*

[b-ITU-T Y.1545] Recommendation ITU-T Y.1545 (2013), *Roadmap for the quality of service of interconnected networks that use the Internet Protocol.*

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2023