

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1157

(09/2015)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

Secure applications and services – Security protocols

Technical capabilities of fraud detection and response for services with high assurance level requirements

Recommendation ITU-T X.1157

ITU-T

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
PKI related Recommendations	X.1340–X.1349
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
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Recommendation ITU-T X.1157

Technical capabilities of fraud detection and response for services with high assurance level requirements

Summary

Recommendation ITU-T X.1157 provides capabilities required to support fraud detection and response in security sensitive information and communication technology (ICT) application services. Fraud detection and response services support the detection, analytics, and management of fraud across users, accounts, products, processes and channels. It monitors and analyses user activity and behaviour at the application level (rather than at the system, database, or network level) and watches what transpires inside and across accounts, using any channel available to a user. It also analyses behaviour among related users, accounts, or other entities, looking for abnormal activity, corruption or misuse. It is most commonly used in verticals managing customer money, such as e-finance, enterprise remote access, etc., but is equally commonly used to detect internal fraud and other types of unauthorized activities.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X.1157	2015-09-17	17	11.1002/1000/12353

Keywords

Fraud detection system, fraud management.

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

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/>.

© ITU 2016

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	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	General aspects of fraud detection and response	3
	6.1 Problem statements.....	3
	6.2 Role of fraud management	4
	6.3 Major capabilities for fraud management.....	4
7	Architecture of fraud detection and response system	5
	7.1 Operation and component.....	5
	7.2 Architecture considerations	6
8	Technical capabilities of fraud detection and response	7
	8.1 Monitoring capabilities.....	7
	8.2 Detection capabilities	10
	8.3 Response capabilities.....	15
	Appendix I – Sensitive ICT application services.....	18
	I.1 E-finance services.....	18
	I.2 E-healthcare services	19
	I.3 Enterprise remote access services	19
	Bibliography.....	22

Recommendation ITU-T X.1157

Technical capabilities of fraud detection and response for services with high assurance level requirements

1 Scope

This Recommendation provides guidelines on technical capabilities for fraud management in services with high assurance level requirements. The objective of this Recommendation is to provide a system capable of detecting fraud activities. This Recommendation is applicable to many commercial and enterprise sectors using security sensitive information and communication technology (ICT) applications through the deployment of a fraud detection and response system. This Recommendation is also applicable to the management of internal fraud in an organization as well as external fraud by remote access or commercial service. This Recommendation covers the following areas:

- capabilities for fraud detection and response service;
- operations and components for fraud detection and response system; and
- considerations for incident defence and response service.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 assurance level [[b-ITU-T X.1252](#)]: A level of confidence in the binding between an entity and the presented identity information.

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

NOTE – Use of the term authentication in an identity management (IdM) context is taken to mean entity authentication.

3.1.3 authentication assurance [[b-ITU-T X.1252](#)]: The degree of confidence reached in the authentication process that the communication partner is the entity that it claims to be or is expected to be.

NOTE – The confidence is based on the degree of confidence in the binding between the communicating entity and the identity that is presented.

3.1.4 end user [[b-ITU-T X.1141](#)]: A natural person who makes use of resources for application purposes.

3.1.5 identity [[b-ITU-T X.1252](#)]: A representation of an entity in the form of one or more attributes that allow the entity or entities to be sufficiently distinguished within context. For identity management (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 that 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 assurance [b-ITU-T X.1252]: The degree of confidence in the process of identity validation and verification used to establish the identity of the entity to which the credential was issued, and the degree of confidence that the entity that uses the credential is that entity or the entity to which the credential was issued or assigned.

3.1.7 identity proofing [b-ITU-T X.1252]: A process which validates and verifies sufficient information to confirm the claimed identity of the entity.

3.1.8 identity verification [b-ITU-T X.1252]: The process of confirming that a claimed identity is correct by comparing the offered claims of identity with previously proven information.

3.1.9 service provider [b-ITU-T X.1141]: A role donned by a system entity where the system entity provides services to principals or other system entities.

3.2 Terms defined in this Recommendation

This Recommendation uses the following terms:

3.2.1 fraud detection system: Software as an application that supports monitoring, detection, and management of fraud or other misuse across users (e.g., customers), accounts, channels, products and other entities (e.g., kiosks).

NOTE – To deploy the fraud detection system, enterprise applications could integrate with a fraud detection engine that assesses the fraud risk of a transaction, from user navigation and application access, to any type of activity, such as a change of address, payment or retrieval of sensitive information.

3.2.2 fraud management: A whole range of activities, which include early warning systems, signs and patterns of different types of fraud, profiles of users and their activities, incident response etc., to mitigate security risk using a fraud detection system.

NOTE – There are a number of issues that make the development of fraud management systems necessary including: the huge volume of data involved; the requirement for fast and accurate fraud detection without inconveniencing business operations; the ongoing development of new fraud to evade existing techniques; and the risk of false alarms.

3.2.3 security sensitive information and communication technology (ICT) application: Application that requires very high security assurance level for protecting an information asset of individuals, secret information, organization, and/or enterprise.

NOTE – When security sensitive ICT applications are compromised and controlled by the attacker, the exposure of sensitive information, i.e., personal or financial information, causes massive harmful effects to users, organizations, telecommunication infrastructure, and services, which may include applications for e-finance, e-healthcare, and enterprise remote access.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

API	Application Programming Interface
ATM	Automated Teller Machine
DLP	Data Loss Prevention
DNS	Domain Name System
DSL	Digital Subscriber Line
GSM	Global System for Mobile Communications
HTTP	HyperText Transfer Protocol
ICT	Information and Communication Technology
ID	Identity

IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IT	Information Technology
MITM	Man-in-the-Middle
NAC	Network Access Control
OS	Operating System
PC	Personal Computer
PIN	Personal Identity Number
SMS	Short Message Service
SP	Service Provider
SQL	Structured Query Language
SSL	Secure Socket Layer
TAN	Transaction Authentication Number
WiMAX	Worldwide Interoperability for Microwave Access

5 Conventions

The words "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The words "is recommended" indicate a requirement which is recommended but is not absolutely required. Thus, this requirement need not be present to claim conformance.

The words "is prohibited from" indicate a requirement which must be strictly followed and from which no deviation is permitted if conformance to this Recommendation is to be claimed.

The words "can optionally" indicate an optional requirement which is permissible without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option and the feature can be optionally enabled by the network operator/service provider (SP). Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 General aspects of fraud detection and response

6.1 Problem statements

In telecommunication-based application services, malware-based attacks have been responsible for targeted attacks in many types of companies and vertical industries (e.g., e-transportation, e-hospital, and other types of e-industries). These attacks are becoming a major concern and are increasingly delivered through targeted spear-phishing e-mails and through malware-infected objects like advertisements that inexperienced users click on. These methods have been used to infect multiple organizations.

Organizations in many commercial and enterprise sectors face significant risks of data loss, inappropriate account access, and transaction activity from external and internal sources. Targeted malware can often bypass existing protection technologies, and the resulting data breaches are not detected until after a long time and significant data exfiltration has occurred. The evidence of malicious activity is usually hiding in plain sight, and is undetected because of a lack of monitoring

