International Telecommunication Union

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 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/.

Table of Contents

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 capability and an inability to discern a pattern of abnormal application activity or data access from normal activity patterns. For example, bank customers may not even know that a fraud has been committed until they see an account that has not been confirmed on their credit report, or until a debt collector contacts them for payment.

Malware-based attacks against financial customers and company employees cause severe damage to the reputations and finances of their victims. They are rapidly becoming a prevalent tool for attacking customer and corporate accounts, and stealing sensitive information or funds. Therefore, unless business processes and organizations are properly structured to effectively manage fraud detection, important alarms and alerts could be ignored. Finally, malware-based attacks can be used to take over users' accounts, or to perpetrate fraud or theft of server-based assets.

6.2 Role of fraud management

A fraud management system could be applied in three typical fraud cases:

- Detecting account takeover, which typically occurs when user account credentials are stolen, or typically through malicious software (malware). Malware infects a business' computer system not just through infected documents attached to an e-mail, but also simply when an infected website is visited.
- Detecting new account fraud, which typically occurs when user account credentials are stolen, or through malicious software (malware).
- Detecting the use of a stolen (or other's) account, for example, a stolen credit card, when making a purchase, or pretending to be a normal user.

A fraud management system is most commonly used for one or more fraud cases, such as account takeover, internal fraud detection, real-time payment card fraud detection and transaction blocking, and as a specific fraud or misuse management system for the enterprise. In each of these scenarios, it is essential for the enterprise servicing the transaction to verify the legitimacy of the person conducting the transaction.

6.3 Major capabilities for fraud management

When it comes to comprehensively counteracting ID fraud, a fraud detection system requires adhering to three-capabilities to address this problem: monitoring, detection, and incident response. These capabilities include: Steps to be taken in order to find suspicious activity from various event data in the first place; actions to detect fraud earlier in the process when it happens; and actions to take to resolve fraud if suspicious activities are detected.

Monitoring: A fraud detection system can monitor fraud by looking for anomalies in user activity and behaviour at the application level, as well as in the system, database or network level, and watches what transpires inside and across accounts using any channel available to a user. It also monitors and analyses user or account behaviour and associated transactions and identifies anomalous behaviour, using rules or statistical models. It may also (optimally) use continuously updated profiles of users and accounts, as well as peer groups for comparing transactions and identifying the suspect ones. In particular, comprehensive internal fraud monitoring requires the monitoring of privileged information technology (IT) users who are able to modify files and data directly, as opposed to having to go through canned user applications.

Detection: A fraud detection system has the capability to mine, dissect, and analyse large volumes of data using complex relationship and rule screening, defined by the business, to prevent fraud. It can be used for insider (i.e., employee) and external (i.e., customer and business partner) fraud detection. For fraud detection capability support, it can and should profile various entities, such as users, accounts, households, personal computers (PCs), mobile handsets, and kiosks, to spot abnormal transaction behaviour from that entity. Fraud detection uses rule-based policies that are based on human judgment and knowledge and/or predictive mathematical models to score the likelihood of fraud for a given transaction.

Response: After detecting suspicious activity, a fraud management system should respond to the suspicious activity with various precautions, such as an account block or information sharing. A variety of complementary monitoring and detection technologies can help enterprises better detect suspicious user activity, recognize patterns of inappropriate resource access or fraudulent account activity, and investigate and respond to incidents with real-time alerting, incident management, account blocking, or transaction intervention. Therefore, organizations need to determine which combination of monitoring and analysis technologies is the most appropriate for their risk level, as well as determine their security technology implementation and support capabilities.

7 Architecture of fraud detection and response system

7.1 Operation and component

ICT applications can be integrated with fraud detection components to support major capabilities that manage the fraud risk of a transaction from user access to any type of activity. Operation of the fraud detection system should not be transparent to both hackers and users, so that hackers cannot learn the rules of the system, and consequently, legitimate users are not inconvenienced. Suspect user transactions are re-verified by the fraud detection system in real time to assess their legitimacy, or are suspended until the fraud detection system has time to research their legitimacy.

The fraud detection system is composed of several components that process, store, and transfer data for detecting abnormal activity. Operation of the fraud detection system capability is made by data processing between components. Operations and components of the fraud detection system are described in detail in Figure 1. Ideally, the fraud detection system would start to monitor the entire session after the initial log-in. Accordingly, the fraud detection system performs the operations to manage fraud, i.e., from monitoring capability to response capability, as follows:

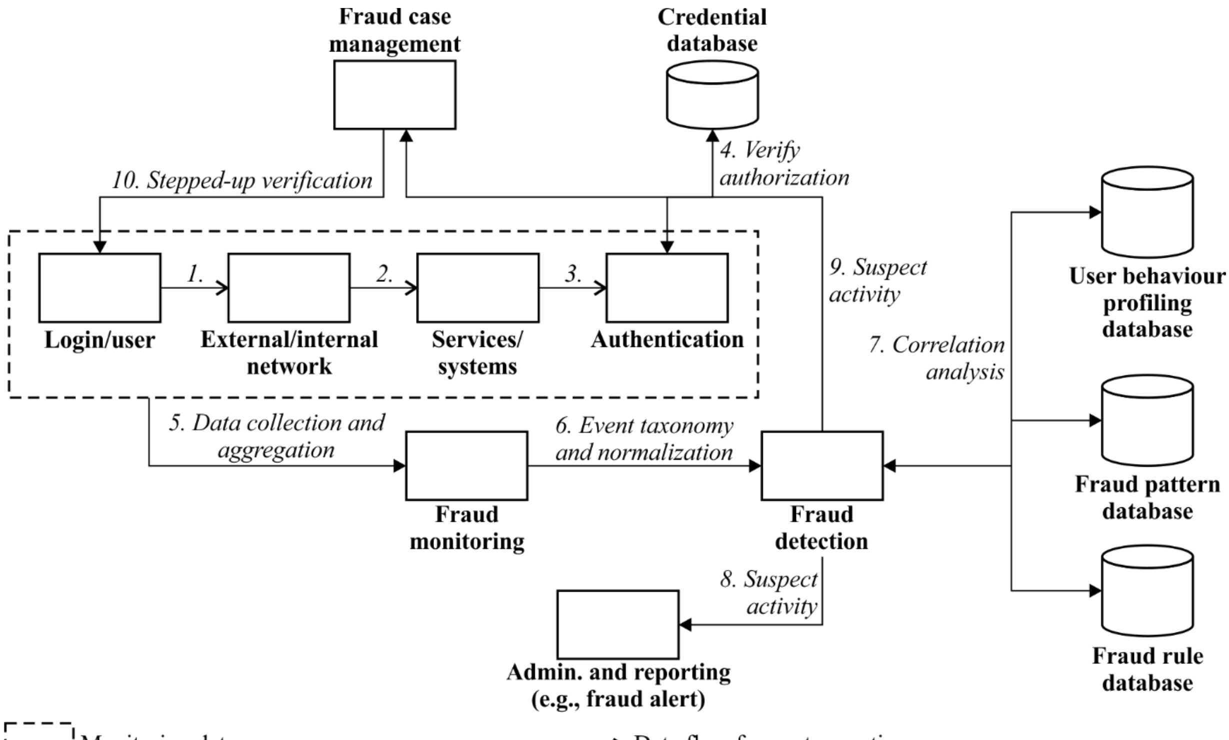
Fraud case management
Credential database
10. Stepped-up verification
4. Verify authorization
9. Suspect activity
User behaviour profiling database
1.
2.
3.
Login/user
External/internal network
Services/ systems
Authentication
7. Correlation analysis
5. Data collection and aggregation
6. Event taxonomy and normalization
Fraud monitoring
Fraud detection
Fraud pattern database
8. Suspect activity
Admin. and reporting (e.g., fraud alert)
Fraud rule database
Monitoring data source
Data flow for next operation
Component of fraud detection system
Request and reponse for operation
X.1157(15)_F01

Figure 1 – Operations and components of a fraud detection system

Login, authentication, and verifying authorization operation (data flows 1, 2, 3, and 4)

Under normal circumstances, the initial log-in is analysed and assigned a risk score when the credential collected during the log-in is compared with data residing in the user's credential database (username and password), the IP, the user behaviour profile database, etc. The verifying authorization is guided by the authentication rules defined in the credential database, which is typically configurable by the institution and is extensible to allow new rules.

Fraud monitoring, detection, and case management operation (data flows 5, 6, 7, 9, and 10)

The fraud detection system collects data from various sources (i.e., networks, services/systems, and authentication) after user login. The fraud detection system analyses the collected data from the fraud monitoring component. For example, if there is any questionable activity identified by the authentication, the fraud detection system sends the suspected fraud information to the fraud detection component. Then, the fraud detection component sends a query request of data to analyse correlation in fraud related databases (i.e., user behaviour profiling data, fraud pattern data, and fraud rule data). Fraud cases are prioritized based on the risk level derived from the fraud detection component and provide a complete picture of risk associated with those interactions with high risk scores. In a fraud case of high risk level, the fraud case management component requests stepped-up verification to the login-user. The resolution of cases can and should be fed back into the databases to create a self-learning loop to improve future performance.

Administration and reporting operation (data flow 8)

The administration and reporting component should also be available for the institution to better understand and control the fraud detection system. This component allows the system users to easily analyse and report on system performance, identify scoring or access inconsistencies and areas for improvement, and track system users' actions and performance. Furthermore, reporting tools provide an easy way to present detailed performance information to senior management and fraud analysts.

7.2 Architecture considerations

When implementing the fraud detection system for ICT applications, one of the three following architectures should be considered: Fraud-detection modules built into the application server (e.g., the web), listening and/or monitoring of the online application, and programmatic interfaces into the legacy application. Business rules and processes are more important determinants of an application's effectiveness.

A fraud-detection module placed inside the application server

Rules maintained by the enterprise are applied by the filter to any hypertext transfer protocol (HTTP) request (for example, log-in or payment) before the transaction hits the application. Transactions can be stopped and/or redirected to a transaction-verification routine in real time through the execution of the module's fraud rules. Several vendors provide plug-ins to application servers which are directly embedded with a pre-processor.

Listening and/or monitoring of the ICT application (listening mode)

In this mode, the application listens to or "sniffs" input files or HTTP network traffic (for example, log-in), or reads data using application server plug-ins installed on each server. Data is read in real time (network "sniffer" approach) or in near real time (application server listener approach) and is either fed to another fraud management application or reconstructed into a format on which fraud rules can be applied. In the latter case, suspect transactions are queued for fraud analyst follow-up. Customized application programming interfaces (APIs) can be integrated so that transactions are redirected to challenge/response verification.

Programmatic interfaces into the legacy application (in-line integration mode)

In this case, APIs are used to pass all transactions through the fraud detection system before a transaction is processed. Transaction flow is controlled, and a user can be challenged in real time if a suspect transaction is detected. Changes in business rules require changes to the core application. APIs are mainly based on web services. In addition, APIs make it harder to switch vendor-specific solutions.

Generally, using APIs for fraud detection gives enterprises/organizations direct control over the transaction flow, but requires significant integration work, and must be constantly updated when the core application changes. Application servers which do not require intervention in real time in user transactions will prefer the second approach, which is the easiest to pull out and replace.

8 Technical capabilities of fraud detection and response

8.1 Monitoring capabilities

The monitoring capability establishes user and data context needed for early attack and breach detection and enables data access and activity monitoring. Privileged user and sensitive data access monitoring is also a common requirement for compliance reporting.

The fraud detection system needs to implement security information and event management capability to gain broad-scope monitoring of user activity and resource access across the network, systems, databases, and applications. The fraud detection system also needs to augment event data with context about users, assets, threats, and vulnerabilities to improve the effectiveness of security monitoring for breach detection. Furthermore, it needs to selectively augment general security monitoring with additional capabilities, such as advanced threat monitoring, based on the level of risk and capability to implement and effectively operate the fraud detection and response system.

The fraud detection system also collects event data in near real time in a way that enables immediate analysis. The real-time monitoring capability is important for threat management to track and analyse the progression of an attack across components and systems, and for user activity monitoring to track and analyse the activity of a user across applications, or to track and analyse a series of related transactions or data access events. Finally, the real-time monitoring capability should support batch data collection for cases where real-time collection is not practical or is not needed.

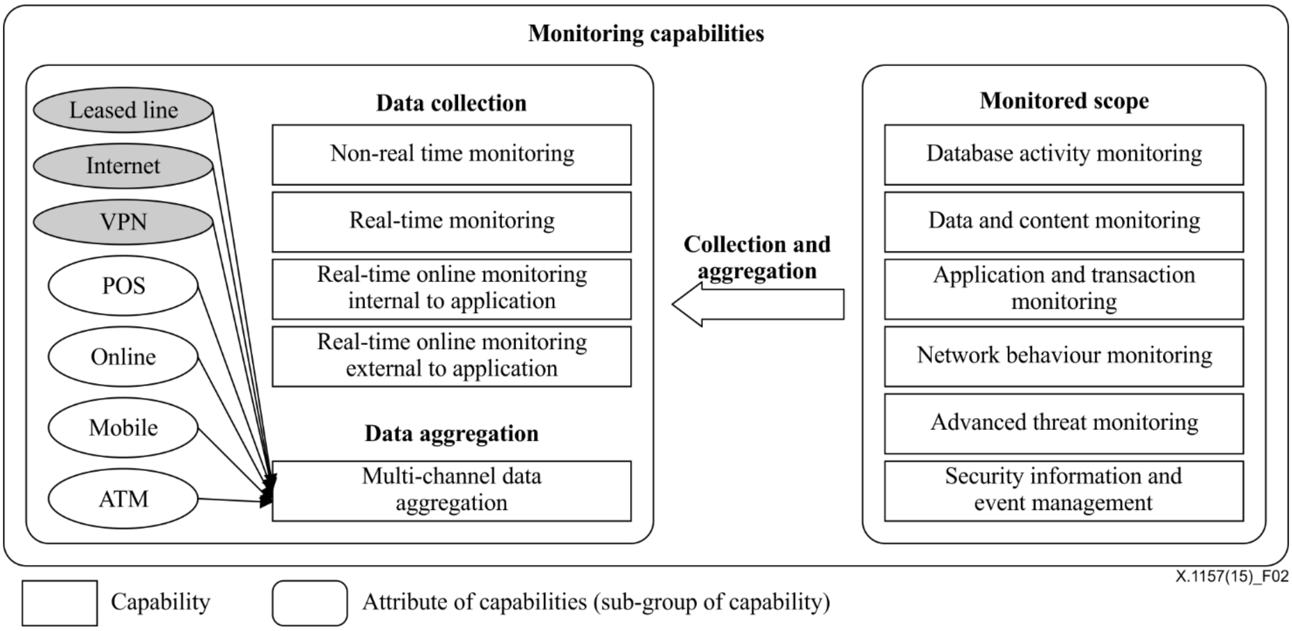
Monitoring capabilities
Leased line
Internet
VPN
POS
Online
Mobile
ATM
Data collection
Non-real time monitoring
Real-time monitoring
Real-time online monitoring internal to application
Real-time online monitoring external to application
Data aggregation
Multi-channel data aggregation
Collection and aggregation
Monitored scope
Database activity monitoring
Data and content monitoring
Application and transaction monitoring
Network behaviour monitoring
Advanced threat monitoring
Security information and event management
X.1157(15)_F02
Capability
Attribute of capabilities (sub-group of capability)

Figure 2 – Monitoring capabilities of a fraud detection system

8.1.1 Data aggregation and collection

Data aggregation and collection are supported for a wide variety of log data sources, including network and security devices, server, database and application logs, output of security-relevant applications such as vulnerability assessment and database activity monitors, and the output of relevant ID and access management technologies such as enterprise directories, user provisioning, and access management systems.

Non-real time monitoring

Non-real time monitoring requires manual or automated reviewing of log files. It may provide a rapid deployment option for post-transaction analysis with longer clearance periods and can remove the ability to stop transactions at the point of completion. It should support batch data collection for cases where real-time collection is not practical or is not needed.

Real-time monitoring

Real-time monitoring monitors all transactions (e.g., HTTP) in real time using a web server filter. This function can monitor without additional hardware by using a low impact web server filter. There is no need to implement any application changes to see real-time transaction data.

Real-time online monitoring internal to the application function

Real-time online monitoring internal to the application function monitors all HTTP web transactions in real time via internal application integration. This function can be costly and time-consuming to deploy and maintain because it needs extensive application modifications to monitor the specific transaction points.

Real-time online monitoring external to the application

Real-time online monitoring external to the application monitors all HTTP web transactions in real time via an external application filter. This function has no impact on the application for sniffer and web filter approaches, but the external application filter is in-line to the application, which may introduce a risk to application reliability. There is no need to implement any application changes required to see real-time transaction data.

Multi-channel data aggregation

Multi-channel data aggregation means that transaction data from other channels can be fully incorporated in the monitoring and fraud detection processes. In addition, multi-channel data aggregation looks for suspect user or account behaviour and at the same time offers the benefit of looking across channels and products and correlating alerts and activities for each user, account or entity. Multi-channel data aggregation enables the analysis of relationships among internal and/or external entities and their attributes (for example, users, accounts, account attributes, machines, and machine attributes) to detect abnormal activities or misuse.

8.1.2 Monitored data source

The fraud detection system can detect malicious activity in a constant stream of discrete events that are usually associated with an authorized user and are generated from multiple networks, system, and application sources. The monitoring capabilities include integration with multiple sources to obtain suspicious and incident events.

Database activity monitoring

Database activity monitoring helps maintain the separation of duties for users that have privileged database access by monitoring administrator activity. This capability also improves database security by detecting policy violations and unusual activity. Database event aggregation, correlation, and reporting provide a database audit capability without the need to enable native database audit functions.

This capability supports the ability to find alterations to the structure and content of the database and data access by privileged users through local or remote log-ins. Because it operates at the database and file layer, it lacks context of any information access and navigation that is not tied to the database or associated files. Network monitoring components (in-line or out-of-band) can be used to monitor structured query language (SQL) queries and administrative access from the network.

Data and content monitoring

Data and content monitoring capabilities are often used to limit information leaks, such as credit card numbers, personally identifiable information, and document- or database-based intellectual property, with functions supporting content monitoring, filtering, and data loss prevention (DLP). The purpose of this capability is to enable the enterprise to monitor its internal content to detect suspicious activities. Content monitoring and filtering are used to protect content in motion (through network monitoring or filtering), at rest (via storage scanning), and in use (through endpoint agents). Most functions also include the capabilities to scan stored content on the network for policy violations (for example, a credit card number on an unapproved server) and find violations of corporate policies on the appropriate use of content and data.

DLP tools can discover, monitor, and actively block the movement or access to sensitive data by using content inspection and contextual analysis techniques to apply one or more policies at the time of use. DLP is limited by an organization's ability to define sensitive content, its structures or other identifying characteristics.

Although these functions are extremely useful in limiting accidental exposure or those caused by bad business processes, there are many non-monitored activities that can be used by a malicious attacker or insider (such as camera phones, voicemail, paper and pen) to circumvent content-aware solutions.

Application and transaction monitoring

The application and transaction monitoring capability includes application monitoring because application weaknesses are frequently exploited in targeted attacks, and abnormal application activity may be the only signal of fraudulent activity or a successful breach. The ability to parse activity streams from packaged applications enables application-layer monitoring of those components; moreover, the ability to define and parse activity streams for custom applications enables application-layer monitoring for in-house developed applications.

The monitoring capability also watches out for suspect user activity in an application within a given access channel (for example, web, phone, in person, or across applications and access channels) or even organizations where black-listed IP addresses are shared across organizations. This can range from detecting abnormal access (for example, simultaneous access by one device from two disparate geographic locations) to a suspect transaction sequence (for example, a change in address followed by a high-value money transfer). By default, it can also spot unauthorized employee activities if carried out in an application that is monitored by the fraud detection application.

Network behaviour monitoring

The network behaviour monitoring capability provides visibility into the network operations based on traffic flows between systems, including the: source, destination, port, protocol, volume of data exchanged, and user ID. This capability has applicability for security- and operations-related analysis. In addition, this capability uses a combination of signature and anomaly detection to provide visibility into the state of the network and to identify deviations from baselines, which may indicate abnormal or suspicious behaviour. The purpose of this capability is so that the enterprise can monitor its internal network behaviour to detect suspicious activities.

Security use cases include monitoring to detect the spread of worms, the unauthorized installation of applications, and suspicious system access activity. Operation use cases include capacity planning and traffic analysis, including the capability to bind a user ID to traffic flow, or to address auditor requirements to track user access to critical systems. This capability has little visibility beyond layer 3, so it cannot directly detect system, database, content, file system, or other access issues.

Advanced threat monitoring

Targeted malware bypasses the current generation of network Internet service providers (IPSs), network firewalls, and web security gateway technologies. Some small, specialized vendors have network-based products for detecting advanced threats. These tools generally work by analysing executables to detect malicious capabilities (often using virtual environments), by monitoring communications (including domain name system (DNS) queries) to and from known or suspected botnet command-and-control centres, or by a combination of both techniques. These capabilities can quickly identify a potential compromise by an advanced threat (e.g., advanced persist threat), but many of the same capabilities are being added to next-generation firewalls, IPSs, and web security gateways.

Other functions specialize in detecting threats against an enterprise in the external environment, including the "darknet," in the Internet relay chat channels, in chat rooms, in social networks, etc. These functions can be conducted by detecting activity against a domain, a set of IP addresses, or key words.

Security information and event management

The capabilities of security information and event management are the broad scope of event collection and the ability to correlate events across disparate information sources for early breach detection. The capability improves threat management and security incident response through the collection and analysis of security events from a wide variety of data sources in real time. These sources include network and security devices, server, database, and application logs, the output of security relevant applications, such as security management and database activity monitors, and the output of relevant identity and access management technologies such as enterprise directories, user provisioning, and access management systems. Furthermore, the capability supports security policy compliance monitoring and incident investigation through analysis and reporting on historical data from these sources.

For fraud detection, the capability aggregates and analyses the event data that is produced by devices, systems, and applications. The primary data source is log data, but the capability can also process other forms of data. The data is normalized so that events from disparate sources can be correlated and analysed according to rule sets that are designed for specific purposes, such as network security event monitoring or user activity monitoring because the monitoring and analysis are totally dependent on event data that is produced by other sources. Activity that is not externalized as an event or in an activity log is not visible to the capability.

8.2 Detection capabilities

Fraud detection uses background server-based processes (transparent to users) that examine user access and behaviour. The fraud detection then compares this information to a profile of what is expected and considered "normal." It simultaneously evaluates a combination of risk factors to surface real fraud and keep false detection rates low. Suspect user transactions are re-verified in real time to assess their legitimacy or are suspended until fraud analysts have time to research their legitimacy.

Since fraud detection operates in the context of an application, it cannot detect rogue and potentially fraudulent processes that are external to the application. Fraud detection cannot detect or suspect behaviour that is not defined to its engine because the rules are not aware of the activity pattern, the model has not learned enough to single it out, or the application integration is not providing enough relevant data to the fraud risk assessment engine. For the detection to be effective, the analysis requires embedded knowledge for specific use cases, or the customer needs to provide this knowledge in the form of customized correlation rules and reports. Therefore, the fraud detection system needs capabilities such as a fraud pattern update, a predefined rule library support, and real-time rule processing.

Most capabilities require extensive model tuning, profile tuning, or detection rule development before the applications are fully functional. These capabilities include monitoring all transactions, automated risk analysis and risk rating, user behaviour profiling and learning, application service specific- and intelligent-fraud decision, and a cross-channel risk assessment.

Transaction capture

Transaction capture are the capabilities which match and extract key attributes from transactions and which require detailed behaviour profiling for each user automatically upon first access.

Event normalization and taxonomy

Event data needs to be normalized so that events from disparate sources can be correlated and analysed according to sets of rules that are designed for specific purposes such as network security event monitoring or user activity monitoring. This is a mapping of information from heterogeneous sources to a common event classification scheme. Taxonomy aids in pattern recognition, and it also improves the scope and stability of correlation rules. When events from heterogeneous sources are normalized, they can be analysed by a smaller number of correlation rules, which reduces deployment and support labour. In addition, normalized events are easier to work with when developing reports and dashboards.

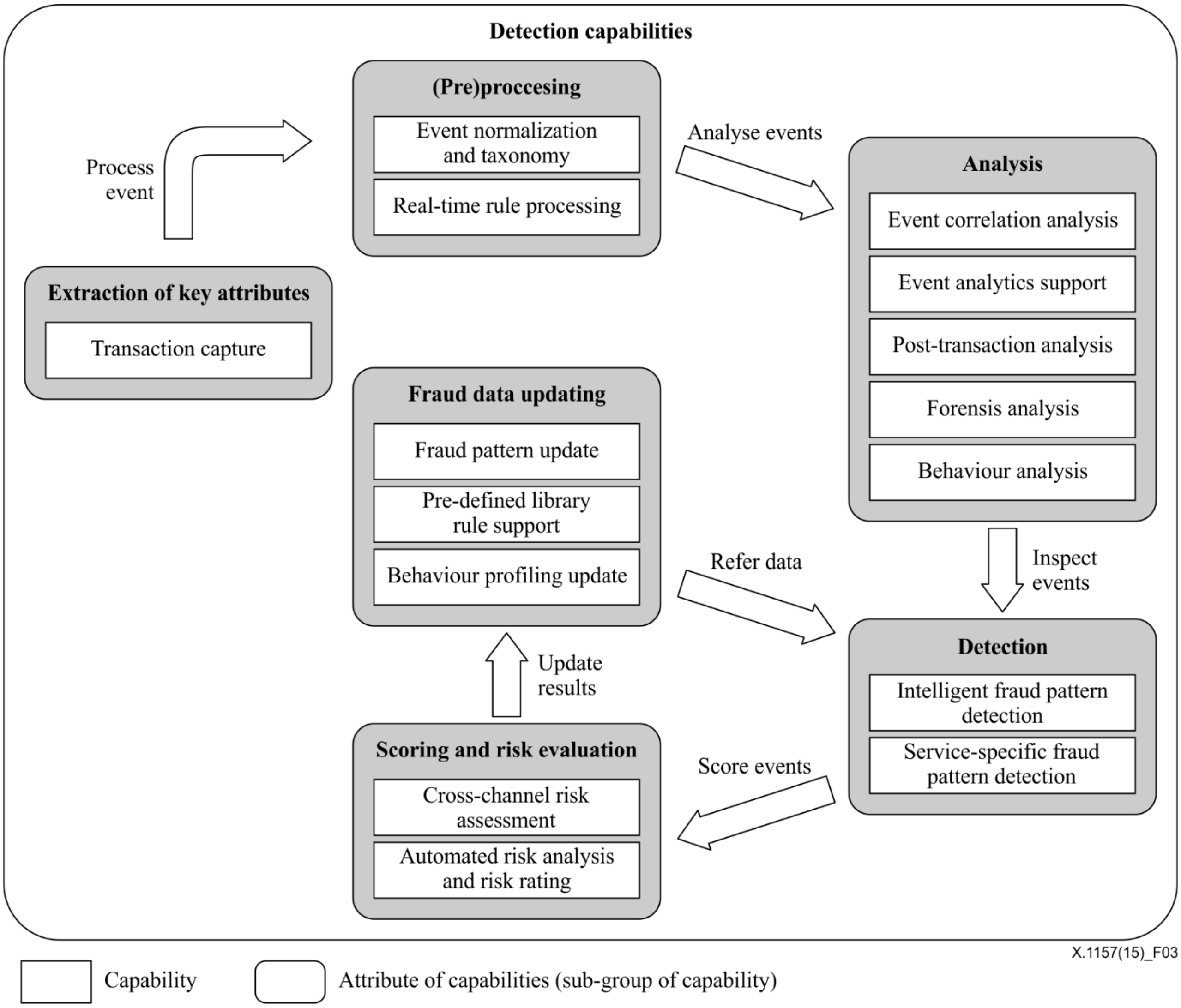
Detection capabilities
(Pre)proccesing
Event normalization and taxonomy
Real-time rule processing
Process event
Analyse events
Analysis
Event correlation analysis
Event analytics support
Post-transaction analysis
Forensis analysis
Behaviour analysis
Extraction of key attributes
Transaction capture
Fraud data updating
Fraud pattern update
Pre-defined library rule support
Behaviour profiling update
Refer data
Inspect events
Detection
Intelligent fraud pattern detection
Service-specific fraud pattern detection
Update results
Scoring and risk evaluation
Cross-channel risk assessment
Automated risk analysis and risk rating
Score events
X.1157(15)_F03
Capability
Attribute of capabilities (sub-group of capability)

Figure 3 – Detection capabilities of a fraud detection system

Fraud pattern update

A fraud pattern update is an automatic update of fraud incident data from the network. The fraud incident data includes geographical IP data for location analysis of the source of transactions including a city, a country and Internet service provider (ISP), as well as host reputation data for identifying transactions from known suspicious sources and anonymizer data for transactions from someone attempting to hide the origination point. The fraud pattern update should have the capability to apply the fraud detection system to other fraud use cases throughout the enterprise and to customize it to meet the specific enterprise business requirements. For example, the fraud detection system could integrate results from external fraud detection, credit scoring, and shared-intelligence systems, such as blacklists.

For the deployment of a fraud pattern update, intelligence about the current threat environment exists in a variety of sources, including open-source lists, the threat and reputation content developed and maintained by security research teams within the security vendors, and data developed by managed security and other SPs. Threat intelligence data can be integrated in a fraud detection system in the form of watch-lists, correlation rules, and queries in ways that increase the success rate of early breach detection.

Up-to-date information on threats and attack patterns can help an organization recognize abnormal activity. For example, a small amount of outbound activity to an external IP address might appear normal and could be easily overlooked. However, that changes if there is a threat intelligence system which indicates that the destination is associated with botnet control. This information can be compared with the machine learning algorithms of expected behaviour, or with the more generic rules as to what constitutes "normal" behaviour, to detect fraud.

Predefined library rule support

Predefined library rule support means that the fraud detection system supports the available proven rules to address fraud. Typically, the function of the fraud detection system includes a range of proven rules for deployment and should also be included to easily create/modify new rules. Additionally, this function may include the ability to share rules with other organizations. This function enables the fraud detection system to quickly update and test rules as well as new fraud scenarios, and to easily view and analyse data and fraud detection results. It can also make a specific set of rules to manage fraud or misuse at the customer level, at the group of customers' level, or of any other user.

Most credit card fraud detection systems enable enterprises to manage the business rules that each of their transactions runs against, so that the businesses can detect fraud patterns particular to their situations.

This library rule could define a set of rules based on security and contextual information:

- User context: The business roles of a user;
- Asset context: Ownership, related applications, or business processes;
- Information security context: Vulnerabilities present at the operating system (OS), application, web or database layer, and configuration status;
- External threat context: Known bad actors and attack patterns;
- Data context: Business-critical or legal and regulatory compliance requirements;
- Application context: The business use of the application and the boundaries for normal data access.

Event correlation analysis

Event correlation establishes relationships among messages or events that are generated by devices, systems, or applications, based on characteristics such as the source, target, and protocol or event type. There should also be a library of predefined correlation rules and the ability to easily customize those rules. By event correlation analysis, a security event console should provide the real-time presentation of security incidents and events.

Event analytics support

Event analytics is accomplished through real-time event correlation and through query-based analysis of historical events. Security event analytics is composed of dashboard views, reports, and ad hoc query functions to support the investigation of user activity and resource access in order to identify a threat, a breach, or the misuse of access rights. When suspect activity is surfaced by security monitoring or activity reporting, it is important to be able to analyse user and resource access. This process can be achieved by using an iterative approach to start with a broad query about an event source, user, or target, and to then initiate increasingly focused queries to identify the source of the problem. Event analytics uses behavioural analysis functions to augment rule-based correlation.

Real-time rule processing

Real-time rule processing is the processing ability of fraud rules against the transaction stream in real time to generate user/session risk scores and detailed incident alerts. This function needs to consider unusual user behaviour, common fraud patterns, black/whitelists and fraud incident data. This function can support rule syntax such as unusual user behaviour with grace periods, client device ID, common fraud patterns, black/whitelists, geographical IP data, and host reputation data. Additionally, the fraud detection system can perform a risk score for each session and a cumulative risk score for each user; it can also enable risk-based authentication which provides the user and session risk scores in real time to the authentication system to determine if additional authentication is necessary.

Management tool support

The management tool support function supports the cost-effective storage and analysis of a large amount of information that includes the collection, indexing, and storage of all log and event data from every source, as well as the capability to search and report on that data. Reporting capabilities should also include predefined reports, as well as the ability to define ad hoc reports or use third-party reporting tools. The management tool function generally includes predefined and modifiable reports for user activity, resource access, and model reports for specific and periodic management purposes. Typically, the management tool is available through the web supporting case assignment and workflow, including user-specific views, such as known fraud incident status, current activities and new flagged items, and configurable alerting mechanisms, including e-mail and web service notifications.

Post-transaction analysis

Post-transaction analysis is the ability to capture and store all data elements for future analysis. Afterwards, the data warehouse contains a full transaction history for all users up to a period of time. This function requires sophisticated capture and formatting of data for real-time storage and rapid retrieval and evaluation. The fraud detection system uses the behaviour profile for each individual user for post-traction analysis and can store transactions classified by session, user, and time stamp for retrieval and analysis.

Forensic analysis

The forensic analysis function is to search, filter, and drill into the details of the transaction data warehouse. The capability includes the ability to filter, search, and do detailed analysis of transactions and access patterns. It supports the identification of emerging fraud patterns which merit real-time detection rules.

Behaviour analysis

The fraud detection system requires transactions with behaviour profiles for all users and supports more sophisticated systems to track the behaviour of individual users. It builds a profile of normal activity and uses a behaviour analysis function to send alerts on deviations. Behaviour profiling employs a learning phase that builds profiles of normal activity for discrete event sources collected by monitoring capabilities.

The fraud detection system automatically starts profiling a user from the first time they are seen by the system. The system can then build up a profile of what is considered "normal" behaviour for that user and then check for "unusual" behaviour as it happens. The detection phase alerts on deviations from normal behaviour. When abnormal conditions are well defined, it is possible to define correlation rules that look for a specific set of conditions. The capability must automatically detect, track, translate, and understand patterns and anomalies that may be harmful and yet avoid interruption of legitimate customer experience. Finally, behaviour profiling can enable risk decisions based on deviation from normal behaviour.

Following initial profiling, more time is needed for the system to learn what constitutes abnormal behaviour or for enterprises to implement the right rules to detect abnormal behaviour or sessions. This approach can improve the ability to discover a targeted attack but will still require extensive tuning by domain experts to control false positives.

Intelligent fraud pattern detection

Not all fraud can be detected through network and application logs and discrete data fields. Unstructured data analysis must be included through the use of various data mining logic that can evaluate the appropriateness of the information entered.

Enterprises should look for the data mining logics that learn on their own, with minimal data, and for systems where they can easily and quickly update rules for known or newly discovered fraud parameters. It can check a new online user's ID against an ID-scoring service provided directly by ID-scoring vendors. These scores ascertain the likelihood that an online user is a fraudster.

Service-specific fraud pattern detection

A fraud detection system requires the ability to define rules that look for patterns of transactions that correspond to known fraud patterns and service-specific fraud patterns. In other words, the system looks for a specific sequence of transactions and conditions that are suspicious according to business/work logic in the application service. This pattern could be carried out within a single session, or span multiple sessions and multiple users according to the specific application service.

Finally, if not tuned properly, fraud detection systems can generate too many false positives. In environments such as electronic trading, where real-time execution is imperative, a high false positive rate is clearly unacceptable.

Cross-channel risk assessment

Fraud detection systems only operate in a given application and a given channel, and are not checked across channels (for example, phone, web, or in person) or account types (for example, deposit or credit). In addition, fraud detection systems do not know about fraudulent activity outside of the application, and they are not integrated in systems that know about such activity (for example, network-based and system-based fraud detection). Therefore, they cannot detect rogue and potentially fraudulent processes that are external to the application.

Accordingly, fraud detection requires watching for suspect user activity in an application within a given access channel (for example, web, phone, or in person), or across applications, access channels, or even organizations (where, for example, "blacklisted" IP addresses are shared across organizations). This can range from detecting abnormal access (for example, simultaneous access by one device from two disparate geographic locations) to a suspect transaction sequence (for example, a change in address followed by a high-value money transfer).

To detect more fraud, the fraud detection system requires integration of the scores from the fraud detection modules into cross-channel risk scoring modules that look across user channels (for example, call centres or automated teller machines (ATMs)).

Automated risk analysis and risk rating

This requires the ability to assess, evaluate, and automatically rate the security risks. Detecting fraud and scoring transaction risk is driven by models or rules, or a combination of both. To find suspicious activity from various gathered data, it can use various modelling techniques such as Bayesian, neural networks, and other data mining technologies, which need data in order to calculate fraud probabilities.

Neural networks that work well in the present credit card space do not work well in the Internet space because they need large amounts of data to detect fraudulent patterns. Therefore, for web-based transactions, the fraud detection system uses alternative modelling techniques, such as Bayesian, which needs less data to calculate fraud probabilities or just rule-based detection. Fraud detection models generate risk scores, which can be fed into the application's rule sets and then maintained and updated by the enterprise organization.

8.3 Response capabilities

The fraud detection system requires automatic triggering of fraud alerts, account blocks, and a stepped-up applicant verification of a particular transaction that has been tagged as suspect for incident response. All online account applications or high-risk anonymous transactions should go through a set of initial screening procedures, starting with authentication events as the result of the initial ID-proofing procedure, to the application usage and application logs. The initial screening procedure includes basic fraud detection, such as client device identification and verification of basic ID data, such as name, e-mail address, geo-location analysis, telephone number validation, credit card fraud detection, credit bureau report validation and/or ID scoring.

The suspect transactions that do not pass the initial ID-proofing steps should be routed to a fraud investigation team and queued for manual or automated additional screening. Afterwards, the fraud detection system can use a risk-based and layered ID-proofing approach that steps up the ID vetting if suspect users and high-risk transactions are prompted for additional screening.

Stepped-up applicant verification

The fraud detection system can integrate the authentication mechanism so that the risk score generated by the fraud system determines the strength for the authentication of the user or the verification of the user's transactions. It presents the steps that can be taken to weed out suspect transactions or other high-risk transactions that require ID proofing. In order to minimize costs and maximize customer convenience, enterprises can take a risk-based approach, where the strength of the ID-proofing solution is commensurate with the risk of the transaction. For this, the fraud detection system can use combined multiple ID-proofing applications, which is described in [b-ITU-T X.1154].

In general, there is no singular, all-encompassing ID-proofing application available on the market. However, there are a number of commercially available ID-proofing mechanisms that can be combined to provide an effective deterrent against fraudsters.

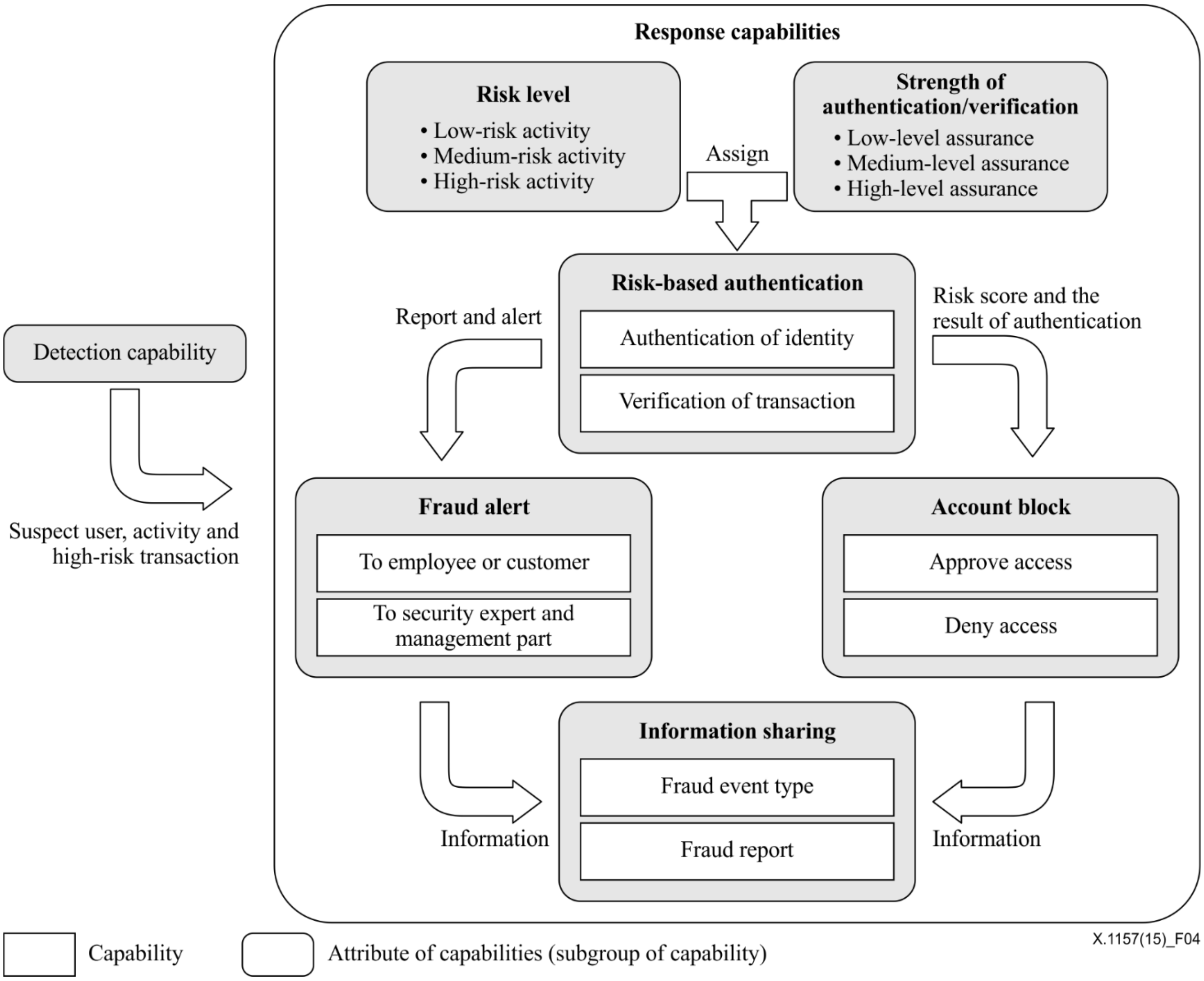

Figure 4 – Response capabilities of fraud detection system

Risk-based authentication

The higher the risk, as determined, for example, by a fraud detection system, the more costly and inconvenient to the customer the ID-proofing measures are required. Several approaches are available where stronger authentication is needed, for example:

- The initial account access is set up to enable low-risk activity, such as read-only access to public information requiring very basic ID proofing. For example, the ID proofing mechanism can check the user's name and mailing address against a secondary source;
- Higher-risk activity, such as updating a mailing address, is delayed until stronger ID proofing (see [b-ITU-T X.1254]) along with fraud detection is undertaken. This includes authentication providing a higher assurance level;
  - The ID proofing mechanism can verify personal information against a public source database using knowledge-based authentication. This verification combines publicly available information, such as demographic data, driver's license records, and credit bureau data;
  - The ID proofing mechanism can require the user to respond to one or more challenge questions that either have been pre-answered or stored in the user profile or are based on information that the genuine account holder should know;
  - The ID proofing mechanism can use alternative channel authentication methods, such as cellular phone or e-mail, to contact the account holder. The ID proofing mechanism can also send a one-time-password to a new online user via a voice call or short message

service (SMS) message to a phone number already on record at the enterprise or that was input on a new account application or payment page by the user;

- The riskiest activities, such as money transfers to a linked external bank account, are prohibited until the user can be contacted for validation, however, because many transactions are executed in batch mode (rather than real time), this approach may not alter the timing of the transaction execution.

Fraud alerts

Fraud alerts mean automatic/manual alert generation when suspicious activity is detected. Fraud alert is typically the result of a combination of a risk score and some rules that act on that score. Detailed alerts include transaction attributes and activity description, and can be notified via e-mail, or pager; configurable by rule, severity and administration user. Fraud alerts can be sent to a security expert or a customer/user according to measured risk level. The security expert can then investigate the perceived risk in more detail, while the fraud alert to the customer/user can be used to alert potential lenders that their ID may have been stolen.

Account block

An account block is applied to user accounts when suspicious activity is detected. The user can be approved or denied access based on the assigned score and the institution's tolerance limits. Users who do not score adequately to warrant full access can be allowed limited access or be required to provide stronger authentication to gain full access or be permitted to perform certain high-risk transactions. If users do not meet those requirements, they can re-start the stepped-up verification procedure or are promptly blocked.

Information sharing

Fraud detection systems should ensure that the systems effectively coordinate portions of their incident response activities with the appropriate partners of organization.

The most important aspect of incident response coordination is information sharing, where different organizations share threats, attacks, and vulnerability information with each other so that each organization's knowledge benefits the other. Also, information sharing can take place directly between the enterprise and the customers or between the organization and the employee because the same threats and attacks often affect multiple organizations or services simultaneously. The purpose of information sharing is to enable any organization that has detected fraud to share this information, either internally or with other potential victim organizations.

The receiving organization can use this information, for example, to institute a manual review of transactions initiated from suspicious IP addresses. A fraud report can describe a particular transaction that is known to be, or believed to be, fraudulent, or it may describe a pattern of behaviour that is believed to be indicative of fraud.

Appendix I

Sensitive ICT application services

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

I.1 E-finance services

I.1.1 E-banking and security issues

Online banking (or Internet banking or e-banking) allows customers of a financial institution to conduct financial transactions on a secure website operated by the institution, which can be a retail or virtual bank, credit union, or building society. To access a financial institution's online banking facility, a customer having personal Internet access must register with the institution for the service and set up a password (under various names) for customer verification. To access online banking, the customer goes to the financial institution's website and enters the online banking facility using their customer number and password. Some financial institutions have set up additional security steps for access, but there is no consistency to the adopted approach.

Though single password authentication is still in use, it by itself is not considered secure enough for online banking in some countries. There are two different security methods in use for online banking:

- The personal identity number/transaction authentication number (PIN/TAN) system where the PIN represents a password used for the log-in and TANs represent one-time passwords to authenticate transactions. TANs can be distributed in different ways; the most popular one is to send a list of TANs to the online banking user by postal letter. The most secure way of using TANs is to generate them by need using a security token. These token-generated TANs depend on the time and a unique secret, stored in the security token (two-factor authentication). Online banking with PIN/TAN is usually done via a web browser using a secure socket layer (SSL) secured connections, so that there is no additional encryption needed;
- Another way to provide TANs to an online banking user is to send the current bank transaction's TAN to the user's global system for mobile communications (GSM) mobile phone via SMS. The SMS text usually quotes the transaction amount and details; TAN is only valid for a short period of time. Banks in many countries, particularly in Germany, Austria, and the Netherlands, have adopted this "SMS TAN" service, as it is considered very secure;
- Signature-based online banking where all transactions are signed and encrypted digitally. The keys for the signature generation and encryption can be stored on smartcards or any memory medium, depending on the concrete implementation.

I.1.2 E-payment and security issues

E-payment is the electronic exchange or transfer of money from one account to another, either within a single financial institution or across multiple institutions, through computer-based systems.

An unsecured e-payment system may not get trust from its users. Trust is very critical to ensure acceptance from users. E-payment applications represent a security challenge as they highly depend on critical ICT systems that create vulnerabilities in financial institutions and businesses and can potentially harm customers. A secure electronic financial transaction has to meet the following requirements:

- Integrity and authorization: Integrity is defined as the accuracy, completeness, and validity of information in accordance with business values and expectations. Integrity of payment systems means that no money is taken from a user unless a payment is authorized by them.

In addition, users might require from a financial institution to not receive any payment from them without their explicit consent;

- Confidentiality: Confidentiality is defined as the protection of sensitive or private information from unauthorized disclosure. Some parties involved may wish confidentiality of transactions. Confidentiality in this context means the restriction of the knowledge about various pieces of information related to a transaction such as the ID of payer/payee, purchase content, amount, etc. In most cases, the participants involved want to ensure that communications are private;
- Availability and reliability: Availability is to ensure that information systems and data are ready for use when they are needed. This is often expressed as the percentage of time that a system can be used for productive work. All parties require the ability to make or receive payments whenever necessary.

I.2 E-healthcare services

Electronic healthcare, or e-healthcare, for paperless management of all activities within large healthcare establishments, promises much in speeding up the typical bureaucracy of healthcare in medical centres and hospitals. However, the realities that face the proper implementation of e-healthcare involve many security issues. For widespread adoption of e-healthcare by hospitals, it is essential to perform a detailed evaluation of security issues to set the stage for standardization of various components for the proper implementation of e-healthcare. A typical e-healthcare system can consist of many components and subsystems, such as: appointments and scheduling; admission, discharge, and transfer; prescription order entry; dietary planning; routine clinical notes; lab and radiology orders; picture archiving; and smart card sign-on. Each of these subsystems is vulnerable to security threats.

I.2.1 Security issues in e-healthcare services

- Threats to information privacy and security: The extant knowledge base on information security risks identifies different types of threats to privacy and security of health information. Yet, the current ad hoc taxonomy alone may not be useful for this practice;
- Privacy concerns among healthcare consumers: With increasing reliance on web-based systems for managing health information and the deployment of personal health banks, privacy concerns of healthcare consumers have come to the forefront;
- Data interoperability and information security: The basic premise of data interoperability is to facilitate accurate and seamless data exchange within and between organizations to support timely healthcare;
- Information security issues of e-health: The healthcare sector has experienced significant growth in the use of mobile devices and web-based applications. Contemporaneously, information security research has focused on the development of frameworks and protocols to address security issues in e-health.

I.3 Enterprise remote access services

Many organizations' employees and contractors use enterprise remote access technologies to perform work from external locations. Most telecommuters use enterprise remote access technologies to interface with an organization's non-public computing resources. The nature of enterprise remote access technologies – permitting access to protected resources from external networks and often external hosts as well – generally places them at a higher risk than similar technologies only accessed from inside the organization, as well as increasing the risk to the internal resources made available to telecommuters through enterprise remote access.

I.3.1 Security issues in enterprise remote access

The most common security objectives for enterprise remote access technologies are as follows:

- Confidentiality: Ensure that remote access communications and stored user data cannot be read by unauthorized parties;
- Integrity: Detect any intentional or unintentional changes to remote access communications that occur in transit;
- Availability: Ensure that users can access resources through remote access whenever needed.

To achieve these objectives, all of the components of enterprise remote access solutions, including client devices, remote access servers, and internal servers accessed through remote access, should be secured against a variety of threats. Enterprise remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats than technologies only accessed from inside the organization.

Major security concerns for enterprise remote access are as follows:

- Lack of physical security controls: Enterprise remote access client devices are used in a variety of locations outside the control of the organization, such as employees' homes, coffee shops, hotels, and conference rooms. The mobile nature of these devices makes them likely to be lost or stolen, which places the data on the devices at increased risk of compromise. Even if a client device is always in the possession of its owner, there are other physical security risks, such as an attacker looking over an enterprise remote access worker's shoulder at a coffee shop and viewing sensitive data on the client device's screen;
- Unsecured networks: Because nearly all enterprise remote access occurs over the Internet, organizations normally have no control over the security of the external networks used by clients. Communication systems used for enterprise remote access include telephone and digital subscriber line (DSL) modems, broadband networks such as cable and wireless mechanisms (see [b-IEEE 802.11]), worldwide interoperability for microwave access (WiMAX), and cellular networks. These communication systems are susceptible to eavesdropping, which places sensitive information transmitted during enterprise remote access at risk of compromise. Man-in-the-middle (MITM) attacks may also be performed to intercept and modify communications. Risk from use of unsecured networks can be mitigated, but not eliminated, by using encryption technologies to protect the confidentiality and integrity of communications, as well as using mutual authentication mechanisms to verify the identities of both endpoints;
- Infected devices on internal networks: Client devices, particularly laptops, are often used on external networks and then brought into the organization and attached directly to the organization's internal networks. An attacker with physical access to a client device may install malware on the device to gather data from it and from networks and systems that it connects to. If a client device is infected with malware, this malware may spread throughout the organization once the client device is connected to the internal network. In addition to using appropriate anti-malware technologies from the organization's secure configuration baseline, such as anti-malware software on client devices, organizations should consider the use of network access control (NAC) solutions that verify the security posture of a client device before allowing it to use an internal network. Organizations should also consider using a separate network for telecommuter client devices, instead of permitting them to directly connect to the internal network;

- External access to internal resources: Enterprise remote access provides external hosts access to internal resources, such as servers. If these internal resources were not previously accessible from external networks, making them available via remote access will expose them to new threats, particularly from untrusted client devices and networks, and significantly increase the likelihood that they will be compromised. Each form of enterprise remote access that can be used to access an internal resource increases the risk of that resource being compromised.

Bibliography

[b-ITU-T X.1141] Recommendation ITU-T X.1141 (2006), *Security Assertion Markup Language (SAML 2.0).*

[b-ITU-T X.1154] Recommendation ITU-T X.1154 (2013), *General framework of combined authentication on multiple identity service provider environments.*

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

[b-ITU-T X.1254] Recommendation ITU-T X.1254 (2012), *Entity authentication assurance framework.*

[b-IEEE 802.11] IEEE 802.11, *IEEE Standard for Information technology – Telecommunications and information exchange between systems, Local and metropolitan area network – Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.*

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	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	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

Printed in Switzerland
Geneva, 2016