International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.1209

(12/2010)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

Cyberspace security – Cybersecurity

Capabilities and their context scenarios for cybersecurity information sharing and exchange

Recommendation ITU-T X.1209

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	**X.1200–X.1229**
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

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

Recommendation ITU-T X.1209

Capabilities and their context scenarios for cybersecurity information sharing and exchange

Summary

Recommendation ITU-T X.1209 describes high level scenarios and supporting capabilities for cybersecurity information sharing and exchange. This Recommendation provides capabilities important for supporting interoperability between applications for the sharing and exchange of cybersecurity information.

Capabilities are described which may be used in scenarios/situations supporting previously independent acting entities to participate in various coordinated efforts, such as the prevention or halting of targeted behaviour or the coordination of analysis and determination efforts.

The goal of the capabilities listed and described is to support more efficient and effective security operations by supporting the interoperable sharing and exchange of information between trusted parties working together to monitor, maintain and generally manage the security of systems and networks.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X.1209	2010-12-17	17

Keywords

Cybersecurity information, information exchange, information sharing.

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/.

CONTENTS

Recommendation ITU-T X.1209

Capabilities and their context scenarios for cybersecurity information sharing and exchange

1 Scope

This Recommendation provides capabilities important for supporting interoperability between applications for the sharing and exchange of cybersecurity information. Accordingly, clause 7 contains descriptions of high level use capabilities scenarios which are used to set the context for the capabilities found in clause 8. To further clarify the purpose of the capabilities, clause 9 contains descriptions of which capabilities are more likely to be needed in which situations.

The intended audience for this Recommendation are those involved in authorized security operations.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 cybersecurity [b-ITU-T X.1205]: Collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- availability
- integrity, which may include authenticity and non-repudiation
- confidentiality.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 cybersecurity information: Structured information or knowledge which may include but is not limited to: the "state" of equipment, software or network systems; forensics related to incidents or events; parties implementing the information exchange capabilities in terms of cybersecurity; specifications for the exchange of information in terms of cybersecurity, including modules, schemas and assigned numbers; identities and trust attributes for all of the preceding and implementation requirements, guidelines and practices.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

DDoS Distributed Denial of Service

FTP File Transfer Protocol

HTTP HyperText Transfer Protocol

HTTPS Secure HyperText Transfer Protocol (HTTP over SSL)

IPS Intrusion Prevention System

5 Conventions

None.

6 Introduction

Cyber attacks involving viruses, worms, etc., are shortening their propagation speeds through networks using various techniques, ever evolving into more threatening forms. Various kinds of security solutions including anti-virus, spyware detection, firewall, virtual private network, intrusion detection and protection, etc., have been developed, so that security incidents due to such threatening attacks may be countered by a rapid response system through the taking of effective countermeasures.

Security managers' most common line of defense against exploits, viruses, worms and botnets has primarily been in the form of various discussion forums that many security professionals subscribe to. Usually within a couple of days to a week, holes are plugged, vulnerabilities patched and things can return back to normal.

Unfortunately, the exploitation of vulnerabilities by viruses, worms and botnets could propagate across networks very quickly. Within seconds, entire networks can be significantly affected.

The exchange of cybersecurity information within a given organization may be accomplished quickly. However, the exchange of a broad range of information between organizations is not well supported using current methods. The lack of effective communication means may turn each organization into an island of security.

Therefore, it is important to share cybersecurity information among many organizations, including telecom operators, telecom service providers and centers of security operations. To make such an information exchange possible, what is needed are:

- trusted and secure methods for participants to exchange information more quickly,
- methods to ensure the protection of privacy.

This Recommendation provides considered scenarios and supporting capabilities for the exchange of cybersecurity information among participants in a secure, trusted and reliable manner.

7 Capabilities scenarios

To be able to put the capabilities listed in clause 8 into a proper context for the understanding of this Recommendation, high level usage scenarios are presented in five different settings to help explain the five logical groups of capabilities which follow.

7.1 General scenario

This general scenario applies to all subsequent scenarios.

Scenario: Information exchange partners share security event and incident related information useful to identify and prevent adversarial attacks on their respective networks.

The important aspect of this scenario is that the two parties may collect similar types of data but from different sources and/or in different formats and/or slightly different contents of similar types of data.

7.2 Operational policies

This scenario describes a situation where different information exchange partners have different restrictions for access to different elements of information being shared.

Scenario: Information exchange partners have a business agreement to share security event and incident-related information.

One important aspect of this scenario is that access to each information exchange partners' information may be restricted with access granted based on a pre-existing trust relationship. Another important aspect is that the trust placed in the information received may be associated with the trust relationship that exists.

7.3 Regional policies

This scenario describes a multiple information exchange partner situation where different respective partners have different legal and/or regulatory restrictions on different elements of the same type of information being shared. Similar to the previous scenario, this scenario also highlights the possibility that one may be allowed to share information that one's self may not actually be allowed to access or view.

This scenario differs from the previous scenario due to the source of restrictions placed on the exchange of information. The source of restrictions in the previous scenario is operational policies decided by each information exchange partner, while restrictions in this scenario are due to operational policies imposed externally, such as by regional jurisdictions.

Scenario: Two parties operating in different regions may exchange information under different requirements placed on them by the respective regions.

The important aspect of this scenario is that in addition to parties having different operational policies, there may also be policies associated with the region in which the information is exchanged.

7.4 Exchange format

Scenario: One information exchange partner delivers information, which includes ports or port ranges involved, to a second partner concerning a troublesome behaviour pattern of traffic. The information shared is used to identify instances of a specific attack.

The important aspect of this scenario is that the contents of the information exchanged needs to be easily understood by and agreed to by all information exchange partners involved.

7.5 Privacy protection

The scenarios included in this clause highlight different privacy related issues, whether the "privacy" is corporate or personal. In addition, they highlight the need for the ability to ensure the privacy of information exchanges themselves.

- Scenario: A security operations centre collects information related to a malicious attack against one of its managed networks, systems or more generally, a managed asset. This information is then provided to a network service provider to identify the source or sources of the given malicious attack.

  The important aspect of this scenario is that the network service provider has the ability to personally identify the suspected source(s) of the attack but does not need to divulge that information to the security operations centre.
- Scenario: The complete set of information collected by one information exchange partner may contain elements which the information exchange partner may wish to reveal to exchange partners within their organization or operations but do not wish to reveal to those outside of their operations.

  The important aspect of this scenario is that parties involved in the exchange of information may choose to share all of the information available or only a subset or, may obfuscate in some way some or all of the information it shares.
- Scenario: Two parties exchange sensitive information over "public" networks.

  The important aspect of this scenario is that the privacy of the information exchanged needs to be able to be ensured no matter the communication method used.

7.6 Access granularity

This scenario highlights the situation where different types or elements of security information may be shared under and depending on different conditions.

Scenario: A service publishes advisories and warnings on both a free and a subscription basis delivering differing levels of information dependant on a given subscription's definition of services.

An example of differences between levels could be making only raw data available at one level, while at a different level raw and analysed data are made available.

The important aspect of this scenario is that although all the information made available may be of a given type, there may be different "levels" of information made available to different second parties.

7.7 Source verification

This scenario highlights the need for authentication of information exchange partners.

Scenario: An information exchange partner receives information from a second partner and verifies that the information did indeed come from the second partner.

The important aspect of this scenario is that parties exchanging information with each other need to verify that the information came from the actual intended sender and not a third party attempting to masquerade as the intended sender.

7.8 Multichannel distribution

This scenario, although similar to "access granularity", highlights the situation where different levels of information may be made available using different methods.

Scenario: An information exchange partner makes security notifications and alerts available via different means and under different conditions. Their data may be available for download from a searchable directory for free, selectively delivered via email for one level of service or available in machine readable and accessible form for yet another level of service.

The important aspect of this scenario is that the same or different types of information may be made available via a variety of means and under a variety of conditions.

7.9 Backwards compatibility

Scenario: Two information exchange partners have already been exchanging specific information using specific formats and protocols. A new standard supporting their current methods of exchange becomes available which provides new and additional functionality.

The important aspect of this scenario is that existing applications need to be supported to the greatest extent possible while, at the same time, providing them with an upgrade path should new standards become available.

8 Capabilities

The following clauses list various capabilities which support the types of scenarios listed above in clause 7.

8.1 Format/encoding capabilities

- The format and structure of the security information needs to be known and understood by both parties.
  - Security information exchanged is of a heterogeneous nature, such as firewall, or other network security appliance messages and signatures as well as different types of application-specific information such as event and incident reporting, analysis and response, forensic data exchange, etc.
  - The format of information exchanged represents various types of security information generated by and applicable to heterogeneous system environments.
- A variety of types of security related information needs to be able to be shared. Examples include, but are not limited to, traffic behaviour signatures, system access signatures, source IP address(es), source and/or target port ranges, etc.
- Parties need to be able to include various levels of information, from a single packet's contents up to all packets involved in a network wide DDoS attack.
- The contents of the security information need to be known and understood by both parties.
- The subject matter, usability and applicability of the information need to be identifiable.

8.2 Transfer/exchange capabilities

- Parties need to be able to transfer, deliver and receive security information across a wide and extensible range of distribution and transmission mediums.
- Applications may need to support synchronous and asynchronous exchanges among parties during the sharing and exchange of security information.
- Applications may need to support push, pull and subscription based information delivery.
- Applications need to support stable operation during the exchange and processing of large amounts of security information.

- Exchange protocols used need to use and/or build upon existing protocols already in wide usage.

8.3 Security capabilities

- Cybersecurity information involved in sharing and exchange needs to be able to be authenticated and verified.
- Applications need to support reliability, confidentiality, integrity and availability of information and services.
- Involved parties need to be identifiable in an authenticated and verifiable manner.
- Applications need to prevent attacks against a cybersecurity information sharing and exchange due to forging and/or falsifying of contained information or the source/destination of the contained information.
- Source parties need to be able to ensure that only authorized parties are able to access sensitive information. This is to provide for privacy of communications and applies whether privacy is required for personally identifiable information or private corporate information or whatever is deemed important to remain private and accessible only to those authorized.
- Source parties need to be able to control access at a granular level such that only parties authorized to access specific elements of a given piece of security information are able to do so and not access elements for which they are not authorized.
- Parties need to be able to secure security related information against access by unauthorized parties even in an open environment where the security related information is available to all, including unauthorized parties.

8.4 Policy capabilities

- Parties need to be able to individually define and declare applicable policy, local and/or regional, with regards to the provisioning and/or accessing of provided cybersecurity information. An example of this could be not revealing routing information that may be disclosed in destination addresses as being a "policy" issue.
- Parties need to be able to provide and access security information in a manner consistent with their respective applicable policies with regards to the provisioning and/or accessing of security information.
- Parties need to be able to declare within which jurisdiction a given set of policy declarations apply.
- Parties need to be able to individually define and declare possible jurisdictional requirements and limitations with regards to the provisioning and/or accessing of security information within their respective jurisdictions.
- Parties need to be able to provide and access security information in a manner consistent with their respective jurisdictional requirements.

8.5 Vendor neutrality capabilities

To support the sharing and exchange of as wide a range of cybersecurity information as possible, applications need to provide services with as little dependence on any one specific vendor's system or vendor specific data as possible. At the same time, it is better if no specific vendor's systems or data is excluded either.

9 Applicability of capabilities

The scenarios and capabilities described in this Recommendation provide a set of discrete "tools" that one can choose to mix and match their use to create one's application. Some applications, which are less complex, such as simple data aggregation and/or information search, may need only a few of the capabilities listed; while others, which are feature rich and provide more extensive services, may need to combine and implement more of the capabilities.

What follows is a discussion of when specific types of capabilities may be more necessary and when they may be of a more optional nature.

9.1 Format/encoding capabilities

For any cybersecurity information sharing and exchange to take place, both sender and receiver of information need to be able to understand exactly what the contents are that they are exchanging. Accordingly, the format and encoding capabilities apply to any and all scenarios within which cybersecurity information is shared and/or exchanged.

9.2 Transfer/exchange capabilities

Similar to the importance of format and encoding capabilities, two or more information exchange partners need a method for getting the information from the sending side to the receiving side.

9.3 Security capabilities

There is very little point in exchanging security related information without at least some level of security assurance involved in the identification of exchange partners and securing of any communication channel between them.

However, different situations and applications will have different security requirements, so it is important that adopters and implementers well consider their specific application's needs.

For example, in an application where two exchange partners have a dedicated communication line that implements security measures of its own, there may be little or no need at all for special security considerations beyond what the exchange environment already provides.

On the other hand, if information is made available using publicly accessible channels of communications, a broad spectrum of security measures will likely be needed.

9.4 Policy capabilities

Not all applications supporting cybersecurity information sharing and exchange functionality will need to make use of the ability to declare restrictions, limitations and/or authorizations. However, the ability to declare such types of policy related information is important in many business and personal situations.

As with security capabilities, where conditions or situations in which policy related functionality is provided for outside of a given application, possibly due to operational or contractual agreements, the ability to declare and enforce policy within an application itself may not be needed.

9.5 Vendor neutrality capabilities

Vendor neutrality is very situation dependent. If one is sharing or exchanging data generated by a given vendor's product using the given vendor's exchange format and/or exchange protocols, vendor neutrality does not really apply.

On the other hand, if a given application's goal is the broadest application and support of information exchange, maintaining a neutral stance with regards to vendor specific methods and/or information is considered important.

Appendix I

Introduction to cybersecurity information sharing and exchange

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

This appendix describes the conceptual structure of an example of a cybersecurity information application as shown in Figures I.1 and I.2. The pair of diagrams shows two different views of the application topology enabled by the capabilities listed in clause 7. Although other topologies are possible, the topology shown includes the use of all capabilities, while other possible topologies and applications may need only a sub-set of the described capabilities.

The first diagram describes the scenario of numerous information sharing partners, each with different functionalities, applications and information shared. It shows different methods for how information from a given node may be accessed by applications making use of the information.

It should be noted though that this appendix does not proscribe exactly how or for what purpose the information is used, only that it may be accessed via a variety of means. Also, the first diagram shows that all exchanges between nodes are supported via the use of a standardized message format.

The second diagram is a third dimension perspective view of the first diagram showing two example information exchange partners and describes the capabilities each is likely to need to implement to participate in the exchange process. Again, as with the first diagram, actual implementations or applications may not need all of the functionalities supported by all the capabilities listed, and so are free to choose which functionalities are actually included in a given implementation/application.

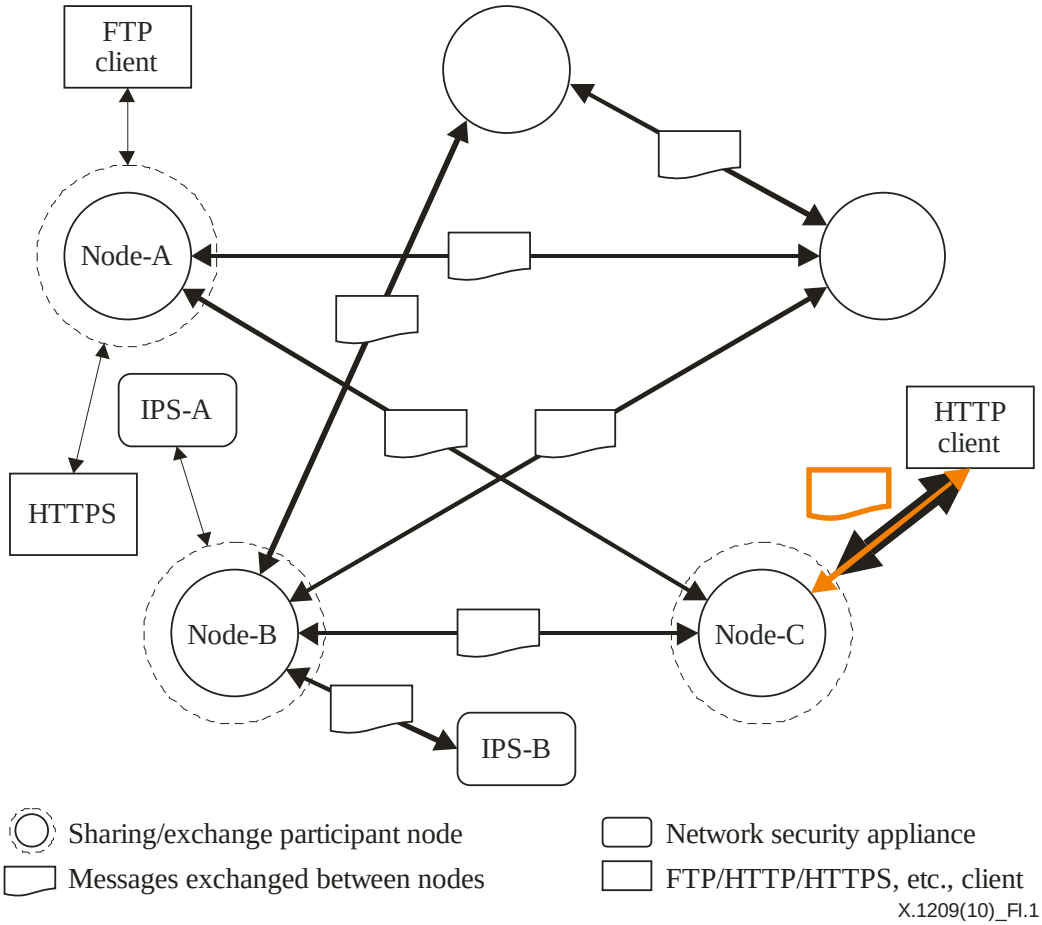

Figure I.1 – Example of cybersecurity information sharing and exchange deployment

- All participant nodes communicate with each other via standardized messages.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)
  – Transfer/exchange capabilities (clause 8.2)

- Data requested from one node may actually be provided by another.

  The following capabilities are important in support of this functionality:

  – Security capabilities (clause 8.3)
  – Policy capabilities (clause 8.4)

- A given node may implement framework protocols only, or it may make framework data available through other protocols/services, e.g., as FTP or HTTP are used to access framework data from Node-A.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)
  – Transfer/exchange capabilities (clause 8.2)
  – Vendor neutrality capabilities (clause 8.5)

- Security appliances, e.g., an intrusion prevention system (IPS-A) and another intrusion prevention system (IPS-B) connecting to Node-B may access cybersecurity information either directly, e.g., IPS-B, or via a wrapper service, e.g., IPS-A, allowing devices to make use of sharing and exchange functionality either in cybersecurity information sharing and exchange standardized manner, or using device dependant/proprietary methods.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)
  – Transfer/exchange capabilities (clause 8.2)
  – Vendor neutrality capabilities (clause 8.5)

- A security appliance may use any protocol or protocol layer supporting the carriage of messages, e.g., TCP/IP, HTTP, HTTPS, SSL used by clients requesting services from Node-C.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)
  – Transfer/exchange capabilities (clause 8.2)
  – Vendor neutrality capabilities (clause 8.5)

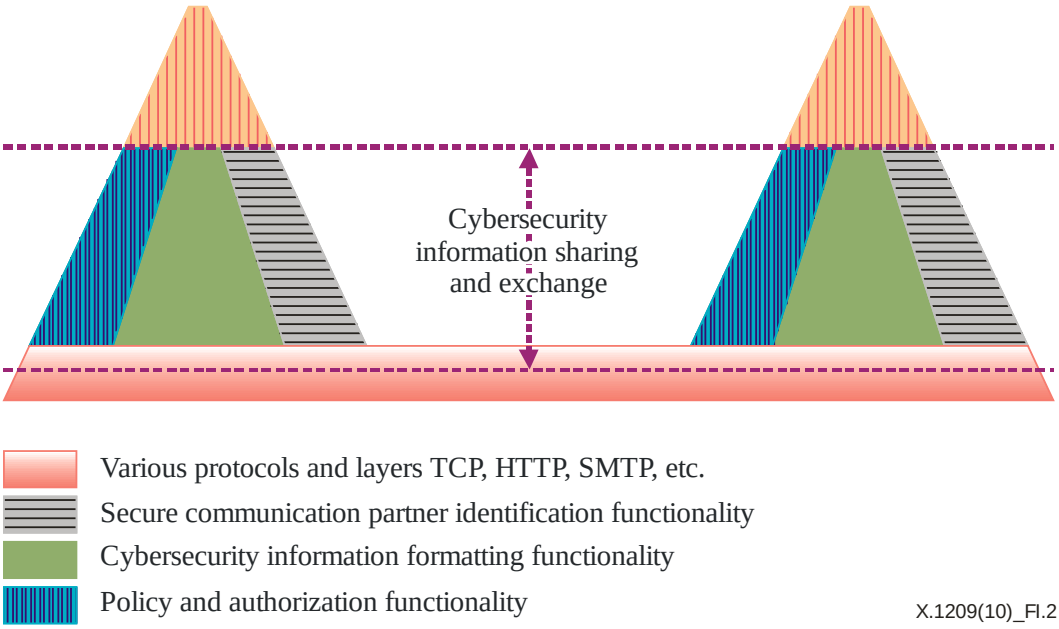

Figure I.2 – Two-node perspective

- Participating nodes exchange requests and responses through various protocols and layers of protocols.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)

  – Transfer/exchange capabilities (clause 8.2)

- For many applications, trusted methods of identifying communication partners will be needed.

  The following capabilities are important in support of this functionality:

  – Security capabilities (clause 8.3)

  – Policy capabilities (clause 8.4)

- Nodes acquire and make use of data provided by other nodes.

  The following capabilities are important in support of this functionality:

  – Format/encoding capabilities (clause 8.1)

  – Security capabilities (clause 8.3)

  – Policy capabilities (clause 8.4)

  – Vendor neutrality capabilities (clause 8.5)

- Applications make use of various authorization verification functionalities to satisfy various security related requirements as needed based on the application.

  The following capabilities are important in support of this functionality:

  – Policy capabilities (clause 8.4)

- Applications at different nodes may need to make use of identity information from other nodes for various reasons, e.g., client of Node A requests access to cybersecurity information available at Node B.

  The following capabilities are important in support of this functionality:

  – Policy capabilities (clause 8.4)

- The core functionalities of a given participant node are:
  - Receiving cybersecurity information.
  - Storing/archiving cybersecurity information.
  - Serving requests for cybersecurity information.

  The following capabilities are important in support of the mentioned functionalities:
  - Format/encoding capabilities (clause 8.1)
  - Transfer/exchange capabilities (clause 8.2)
  - Policy capabilities (clause 8.4)
- Applications use related tools, e.g., authentication and authorization verification to handle access related issues.

  The following capabilities are important in support of this functionality:
  - Security capabilities (clause 8.3)
  - Policy capabilities (clause 8.4)
- Applications use a common data model to handle access related issues between nodes.

  The following capabilities are important in support of this functionality:
  - Format/encoding capabilities (clause 8.1)
  - Transfer/exchange capabilities (clause 8.2)
  - Vendor neutrality capabilities (clause 8.5)
- Applications use trusted identifiers both in communications between nodes as well as between nodes and clients.

  The following capabilities are important in support of this functionality:
  - Security capabilities (clause 8.3)
  - Policy capabilities (clause 8.4)
- Node-to-node requests and responses are considered the "norm", while applications may provide an application layer interface between node-to-client requests and responses for those clients not implementing the standardized methods and/or protocols used between nodes.

  The following capabilities are important in support of this functionality:
  - Format/encoding capabilities (clause 8.1)
  - Transfer/exchange capabilities (clause 8.2)
  - Vendor neutrality capabilities (clause 8.5)
- The framework supports both push and pull modes of operations as well as state-full and stateless modes of operation.

  The following capabilities are important in support of this functionality:
  - Transfer/exchange capabilities (clause 8.2)
- Application architectures may provide the "hooks" into trusted identification and identification data models that applications require.

  The following capabilities are important in support of this functionality:
  - Security capabilities (clause 8.3)
  - Policy capabilities (clause 8.4)

Appendix II

Related activities

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

II.1 Common security information

Common security information is open security information provided by non-profit organizations such as CERT/CC, MITRE or open project. For example, there is the information of common vulnerabilities and exposures (CVE), common weakness enumeration (CWE), common malware enumeration (CME) and common attack pattern enumeration and classification (CAPEC), open source vulnerability database (OSVDB), signatures which [b-Snort] or [b-Bro] provide, and so on.

In the case of MITRE, CVE is a directory of publicly known information security vulnerabilities and exposures. It is being used as the basis for the National Vulnerability Database (NVD) developed by the U.S. National Institute of Standards and Technology. CWE provides a unified, measurable set of software weakness that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems. CME provides single, common identifiers to new virus threats and to the most prevalent emerging virus threats to reduce public confusion during malware incidents. It is not an attempt to replace the vendor names used for viruses and other forms of malware, but rather to facilitate the adoption of a shared, neutral indexing capability for malware. CAPEC provides a publicly available catalog of attack patterns along with a comprehensive schema and classification taxonomy.

In the case of OSVDB, this project is an independent and open source database created by and for the security community. It is to provide accurate, detailed, current, and unbiased technical information on security vulnerabilities. Also it will promote greater, more open collaboration between companies and individuals, eliminate redundant works, and reduce expenses inherent with the development and maintenance of in-house vulnerability databases.

Snort is an open source network intrusion prevention and detection system utilizing a rule-driven language, which combines the benefits of signature, protocol and anomaly based inspection methods. The rules of Snort have been rigorously tested against the same standards the VRT (Vulnerability Research Team) uses for customers.

Finally, Bro is an open source project based on network intrusion detection that passively monitors network traffic and looks for suspicious activity. The rules of Bro might describe activities, what activities are worth alerting, or signatures describing known attacks or access to known vulnerabilities.

II.2 Novel security information

Novel security information is automatically generated signatures for novel threats or attacks, abnormal traffic, unknown worm, etc. Attack signature generation has been a hot research topic recently, and a couple of experimental solutions such as "Early bird" and "Polygraph" have been proposed. The main role of these solutions is to detect cyber attacks and capture byte sequences, which represent the identity of the attack. The FirstLight Signature Service or Active Malware Protection of Endeavor Security and ZASMIN (Zero-day Attack Signature Management INfrastructure) of ETRI provide new signatures that are constantly being updated, revised and extended. These developing advanced pattern generation technology enable us to automatically generate signatures based on attack traffic. Although there has been an advance in improving the quality of signatures, sharing of the signatures is still in its infancy.

II.3 Related activities to share security information

II.3.1 Computer incident response teams (CIRTs)

CIRTs study network security vulnerabilities, research long-term changes in network systems, and develop information and training to help improving security. They continue to respond to major security incidents and analyse product vulnerabilities. Along with the rapid increase in the size of the Internet and its use for critical functions, there have been progressive changes in intruder techniques, increased amounts of damage, increased difficulty of detecting an attack, and increased difficulty of catching the attackers.

II.3.2 European Network and Information Security Agency

European Network and Information Security Agency (ENISA) presented the first feasibility study on an EISAS (European Information Sharing and Alert System) to inform SMEs (Small and Medium Enterprises) and citizens in the European Union on threats, vulnerabilities, and attacks. The feasibility study concluded that the most optimal way for the EU to facilitate information sharing is to assume the role of facilitator, moderator of discussion and a 'keeper of good practice' between national information sharing and alert system, rather than taking a central, operational function by itself. In order to carry out the study, the feasibility of an EISAS was assumed and had to be verified. EISAS suggested a general model consisting of three main components, and this model was intended to identify functional areas in which an EISAS could add value to existing information sharing activities in the member states and address gaps in coverage with NIS information (network and information security). The three components are IGC (information gathering component), IPC (information processing component) and IDC (information dissemination component).

II.3.3 Forum of Incident Response and Security Teams

Forum of Incident Response and Security Teams (FIRST) is the premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents – reactive as well as proactive. This forum brings together a variety of computer security incident response teams from government, commercial, and educational organizations. This forum aims to foster cooperation and coordination in incident prevention, to stimulate rapid reaction to incidents, and to promote information sharing among members and the community at large.

II.3.4 Asia Pacific Computer Emergency Response Team

Asia Pacific Computer Emergency Response Team (APCERT) cooperates with Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to ensure Internet security in the Asia Pacific region, based around genuine information sharing, trust and cooperation. They facilitate information sharing and technology exchange, including security information, viruses and malicious code among its members. Also, they promote collaborative research and development on subjects of interest to its members, and provide recommendations to help address legal issues related to security information and emergency response across regional boundaries.

II.3.5 Information sharing and Analysis Center for Telecommunications

The Internet and other telecommunication networks form the base of a social economic structure on a world scale. Ensuring the information security becomes the urgent issue in social economic life. Information sharing and Analysis Center for Telecommunications (Telecom-ISAC) aims at collecting, analysing and sharing information on incidents and takes timely measures to ensure trouble free and stable operations of telecommunications services. Furthermore, the ISAC creates a forum with wide variety of collaborative members to share their insights and experiences including information on security risks, vulnerabilities, security solutions, and so on.

Appendix III

Related activities

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

[APCERT] Asia Pacific Computer Emergency Response Team. http://www.apcert.org

[CERT] Computer Emergency Response Team. http://www.cert.org

[ENDEAVOR] Endeavor Security, http://www.endeavorsecurity.com

[FIRST] Forum of Incident Response and Security Team. http://www.first.org

[MITRE] MITRE, http://makingsecuritymeasurable.mitre.org/

[Telecom-ISAC] Telecom information sharing and Analysis Center. https://www.telecom-isac.jp

[WIKI] Wikipedia. http://en.wikipedia.org

Bibliography

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

[b-Bro] Bro (November 2004), *Quick Start Guide Manual*.

[b-EISAS] European information sharing and Alert System (2006/2007), *A feasibility study*.

[b-OSVDB] Open Source Vulnerability DataBase. *Project Aims and Objectives.*

[b-Snort] Snort (May 2008), *Snort User Manual 2.8.2*.

[b-ZASMIN] Information Security Research Division of ETRI, *Zero-day Attack Signature Management Infrastructure.*

SERIES OF ITU-T RECOMMENDATIONS

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

Printed in Switzerland
Geneva, 2011