Network Working Group
Request for Comments: 3067
Category: Informational

J. Arvidsson
Telia CERT
A. Cormack
JANET-CERT
Y. Demchenko
TERENA
J. Meijer
SURFnet

February 2001

TERENA's Incident Object Description and Exchange Format Requirements

Status of this Memo

Copyright Notice

Abstract

The purpose of the Incident Object Description and Exchange Format is to define a common data format for the description, archiving and exchange of information about incidents between CSIRTs (Computer Security Incident Response Teams) (including alert, incident in investigation, archiving, statistics, reporting, etc.). This document describes the high-level requirements for such a description and exchange format, including the reasons for those requirements. Examples are used to illustrate the requirements where necessary.

1. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [1].

2. Introduction

This document defines requirements for the Incident object Description and Exchange Format (IODEF), which is the intended product of the Incident Taxonomy Working Group (ITDWG) at TERENA [2]. IODEF is planned to be a standard format which allows CSIRTs to exchange operational and statistical information; it may also provide a basis for the development of compatible and inter-operable tools for Incident recording, tracking and exchange.

Another aim is to extend the work of IETF IDWG (currently focused on Intrusion Detection exchange format and communication protocol) to the description of incidents as higher level elements in Network Security. This will involve CSIRTs and their constituency related issues.

The IODEF set of documents of which this document is the first will contain IODEF Data Model and XML DTD specification. Further discussion of this document will take place in the ITDWG mailing lists <incident-taxonomy@terena.nl> or <iodef@terena.nl>, archives are available correspondently at http://hypermail.terena.nl/incident-taxonomy-list/mail-archive/ and http://hypermail.terena.nl/iodef-list/mail-archive/

2.1. Rationale

This work is based on attempts to establish cooperation and information exchange between leading/advanced CSIRTs in Europe and among the FIRST community. These CSIRTs understand the advantages of information exchange and cooperation in processing, tracking and investigating security incidents.

Computer Incidents are becoming distributed and International and involve many CSIRTs across borders, languages and cultures. Post-Incident information and statistics exchange is important for future Incident prevention and Internet security improvement. The key element for information exchange in all these cases is a common format for Incident (Object) description.

It is probable that in further development or implementation the IODEF might be used for forensic purposes, and this means that Incident description must be unambiguous and allow for future custody (archiving/documentation) features.

Another issue that is targeted by developing IODEF is a need to have higher level Incident description and exchange format than will be provided by IDS (Intrusion Detection Systems) and the proposed IDEF (Intrusion Detection Exchange Format). Compatibility with IDEF and other related standards will be satisfied by the IODEF requirement on modularity and extensibility. IODEF should vertically be compatible with IDMEF, IODEF might be able to include or reference IDMEF Alert message as initial information about Incident.

2.2. Incident Description Terms

A definition of the main terms used in the rest of document is given for clarity.

Where possible, existing definitions will be used; some definitions will need additional detail and further consideration.

Taxonomy of the Computer Security Incident related terminology made by TERENA's ITDWG [2] is presented in [12].

2.2.1. Attack

An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.

Attack can be active or passive, by insider or by outsider, or via attack mediator.

2.2.2. Attacker

Attacker is individual who attempts one or more attacks in order to achieve an objective(s).

For the purpose of IODEF attacker is described by its network ID, organisation which network/computer attack was originated and physical location information (optional).

2.2.3. CSIRT

CSIRT (Computer Security Incident Response Team) is used in IODEF to refer to the authority handling the Incident and creating Incident Object Description. The CSIRT is also likely to be involved in evidence collection and custody, incident remedy, etc.

In IODEF CSIRT represented by its ID, constituency, public key, etc.

2.2.4. Damage

An intended or unintended consequence of an attack which affects the normal operation of the targeted system or service. Description of damage may include free text description of actual result of attack, and, where possible, structured information about the particular damaged system, subsystem or service.

2.2.5. Event

An action directed at a target which is intended to result in a change of state (status) of the target. From the point of view of event origination, it can be defined as any observable occurrence in a system or network which resulted in an alert being generated. For example, three failed logins in 10 seconds might indicate a brute-force login attack.

2.2.6. Evidence

Evidence is information relating to an event that proves or supports a conclusion about the event. With respect to security incidents (the events), it may include but is not limited to: data dump created by Intrusion Detection System (IDS), data from syslog file, kernel statistics, cache, memory, temporary file system, or other data that caused the alert or were collected after the incident happened.

Special rules and care must be taken when storing and archiving evidence, particularly to preserve its integrity. When necessary evidence should be stored encrypted.

According to the Guidelines for Evidence Collection and Archiving (Evidence) evidence must be strictly secured. The chain of evidence custody needs to be clearly documented.

It is essential that evidence should be collected, archived and preserved according to local legislation.

2.2.7. Incident

An Incident is a security event that involves a security violation. An incident can be defined as a single attack or a group of attacks that can be distinguished from other attacks by the method of attack, identity of attackers, victims, sites, objectives or timing, etc.

An incident is a root element of the IODEF. In the context of IODEF, the term Incident is used to mean a Computer Security Incident or an IT Security Incident.

However we should distinguish between the generic definition of 'Incident' which is an event that might lead to damage or damage which is not too serious, and 'Security Incident' and 'IT Security Incident' which are defined below:

a) Security incident is an event that involves a security violation. This may be an event that violates a security policy, UAP, laws and jurisdictions, etc. A security incident may also be an incident that has been escalated to a security incident.

   A security incident is worse than an incident as it affects the security of or in the organisation. A security incident may be logical, physical or organisational, for example a computer intrusion, loss of secrecy, information theft, fire or an alarm that doesn't work properly. A security incident may be caused on purpose or by accident. The latter may be if somebody forgets to lock a door or forgets to activate an access list in a router.

b) An IT security incident is defined according to [9] as any real or suspected adverse event in relation to the security of a computer or computer network. Typical security incidents within the IT area are: a computer intrusion, a denial-of-service attack, information theft or data manipulation, etc.

2.2.8. Impact

Impact describes result of attack expressed in terms of user community, for example the cost in terms of financial or other disruption

2.2.9. Target

A computer or network logical entity (account, process or data) or physical entity (component, computer, network or internetwork).

2.2.10. Victim

Victim is individual or organisation which suffered the attack which is described in incident report.

For the purpose of IODEF victim is described by its network ID, organisation and location information.

2.2.11. Vulnerability

A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Most systems have vulnerabilities of some sort, but this does not mean that the systems are too flawed to use. Not every threat results in an attack, and not every attack succeeds. Success depends on the degree of vulnerability, the strength of attacks, and the effectiveness of any countermeasures in use. If the attacks needed to exploit a vulnerability are very difficult to carry out, then the vulnerability may be tolerable. If the perceived benefit to an attacker is small, then even an easily exploited vulnerability may be tolerable. However, if the attacks are well understood and easily made, and if the vulnerable system is employed by a wide range of users, then it is likely that there will be enough benefit for someone to make an attack.

2.2.12. Other terms

Other terms used: alert, activity, IDS, Security Policy, etc. - are defined in related I-Ds, RFCs and standards [3, 6, 7, 8, 9, 10].

3. General Requirements

3.1. The IODEF shall reference and use previously published RFCs where possible.

Comment:
The IETF has already developed a number of standards in the areas of networks and security that are actually deployed in present Internet. Current standards provide framework for compatibility of IODEF with other related technologies necessary to operate /implement IODEF in practice. Another issue of compatibility for the IODEF is its general compatibility with IDEF currently being developed by IETF IDEWG. In the interest of time and compatibility, defined and accepted standards should be used wherever possible.

In particularly, IODEF specification proposals SHOULD rely heavily on existing communications, encryption and language standards, where possible.

4. Description Format

4.1. IODEF shall support full internationalization and localization.

Comment:
Since some Incidents need involvement of CSIRTs from different countries, cultural and geographic regions, the IODEF description must be formatted such that they can be presented to an operator in a local language and adhering to local presentation formats.

Although metalanguage for IODEF identifiers and labels is considered to be English, a local IODEF implementation might be capable to translate metalanguage identifiers and labels into local language and presentations if necessary.

Localized presentation of dates, time and names may also be required. In cases where the messages contain text strings and names that need characters other than Latin-1 (or ISO 8859-1), the information preferably should be represented using the ISO/IEC IS 10646-1 character set and encoded using the UTF-8 transformation format, and optionally using local character sets and encodings [13].

4.2. The IODEF must support modularity in Incident description to allow aggregation and filtering of data.

Comment:
It is suggested that Incident description with IODEF might include external information, e.g., from IDS, or reference externally stored evidence custody data, or such information might be removed from current IODEF description, e.g., in purposes of privacy or security. Another practical/real life motivation for this requirement is to give possibility for some CSIRTs/managers to perform filtering and/or data aggregation functions on IODEF descriptions for the purposes of statistics, reporting and high level Incident information exchange between CSIRTs and/or their constituency and sponsors.

Therefore the IODEF descriptions MUST be structured to facilitate these operations. This also implies to strong IODEF semantics.

4.3. IODEF must support the application of an access restriction policy attribute to every element.

Comment:
IODEF Incident descriptions potentially contain sensitive or private information (such as passwords, persons/organisations identifiers or forensic information (evidence data)) and in some cases may be exposed to non-authorised persons. Such situations may arise particularly in case of Incident information exchange between CSIRTs or other involved bodies. Some cases may be addressed by encrypting IODEF elements, however this will not always be possible.

Therefore, to prevent accidental disclosure of sensitive data, parts of the IODEF object must be marked with access restriction attributes. These markings will be particularly useful when used with automated processing systems.

5. Communications Mechanisms Requirements

5.1. IODEF exchange will normally be initiated by humans using standard communication protocols, for example, e-mail, WWW/HTTP, LDAP.

Comment:
IODEF description is normally created by a human using special or standard text editors. The IODEF is targeted to be processed by automated Incident handling systems but still must be human readable, able to be viewed and browsed with standard tools (e.g., browsers or electronic table processors or database tools like MS Excel or Access). Incident information exchange will normally require authorisation by an operator or CSIRT manager so is not expected to be initiated automatically. The role of Incident handling system is to provide assistance and tools for performing the exchange.

It is important to distinguish the purposes of the machine readable and exchangeable IDEF Intrusion message format and the human oriented and created IODEF Incident description.

Communications security requirements will be applied separately according to local policy so are not defined by this document.

6. Message Contents

6.1. The root element of the IO description should contain a unique identification number (or identifier), IO purpose and default permission level

Comment:
Unique identification number (or identifier) is necessary to distinguish one Incident from another. It is suggested that unique identification number will contain information at least about IO creator, i.e. CSIRT or related body. The classification of the Incident may also be used to form a unique identification number. IO purpose will actually control which elements are included in the IODEF object Purposes may include incident alert/registration, handling, archiving, reporting or statistics. The purpose, incident type or status of Incident investigation may require different levels of access permission for the Incident information.

It is considered that root element of the IODEF will be <INCIDENT> and additional information will be treated as attributes of the root element.

6.2. The content of the IODEF description should contain the type of the attack if it is known.

It is expected that this type will be drawn from a standardized list of events; a new type of event may use a temporary implementation-specific type if the event type has not yet been standardized.

Comment:
Incident handling may involve many different staff members and teams. It is therefore essential that common terms are used to describe incidents.

If the event type has not yet been standardized, temporary type definition might be given by team created IO. It is expected that new type name will be self-explanatory and derived from a similar, existing type definition.

6.3. The IODEF description must be structured such that any relevant advisories, such as those from CERT/CC, CVE, can be referenced.

Comment:
Using standard Advisories and lists of known Attacks and Vulnerabilities will allow the use of their recommendations on Incident handling/prevention. Such information might be included as an attribute to the attack or vulnerability type definition.

6.4. IODEF may include a detailed description of the attack that caused the current Incident.

Comment:
Description of attack includes information about attacker and victim, the appearance of the attack and possible impact. At the early stage of Intrusion alert and Incident handling there is likely to be minimal information, during handling of the Incident this will grow to be sufficient for Incident investigation and remedy. Element <ATTACK> should be one of the main elements of Incident description.

6.5. The IODEF description must include or be able to reference additional detailed data related to this specific underlying event(s)/activity, often referred as evidence.

Comment:
For many purposes Incident description does not need many details on specific event(s)/activity that caused the Incident; this information may be referenced as external information (by means of URL). In some cases it might be convenient to store separately evidence that has different access permissions. It is foreseen that another standard will be proposed for evidence custody [5].

6.6. The IODEF description MUST contain the description of the attacker and victim.

Comment:
This information is necessary to identify the source and target of the attack. The minimum information about attacker and victim is their IP or Internet addresses, extended information will identify their organisations allowing CSIRTs to take appropriate measures for their particular constituency.

6.7. The IODEF description must support the representation of different types of device addresses, e.g., IP address (version 4 or 6) and Internet name.

Comment:
The sites from which attack is launched might have addresses in various levels of the network protocol hierarchy (e.g., Data layer 2 MAC addresses or Network layer 3 IP addresses). Additionally, the devices involved in an intrusion event might use addresses that are not IP-centric, e.g., ATM-addresses. It is also understood that information about the source and target of the attack might be obtained from IDS and include the IP address, MAC address or both.

6.8. IODEF must include the Identity of the creator of the Incident Object (CSIRT or other authority). This may be the sender in an information exchange or the team currently handling the incident.

Comment:
The identity of Incident description creator is often valuable information for Incident response. In one possible scenario the attack may progress through the network, comparison of corresponding incidents reported by different authorities might provide some additional information about the origin of the attack. This is also useful information at post-incident information handling/exchange stage.

6.9. The IODEF description must contain an indication of the possible impact of this event on the target. The value of this field should be drawn from a standardized list of values if the attack is recognized as known, or expressed in a free language by responsible CSIRT team member.

Comment:
Information concerning the possible impact of the event on the target system provides an indication of what the attacker is attempting to do and is critical data for the CSIRTs to take actions and perform

damage assessment. If no reference information (Advisories) is available, this field may be filled in based on CSIRT team experience.

It is expected that most CSIRTs will develop Incident handling support systems, based on existing Advisories (such as those from CERT/CC, CVE, etc.) that usually contain list of possible impacts for identified attacks.

This also relates to the development of IDEF which will be implemented in intelligent IDS, able to retrieve information from standard databases of attacks and vulnerabilities [3].

6.10. The IODEF must be able to state the degree of confidence in the report information.

Comment:
Including this information is essential at the stage of Incident creation, particularly in cases when intelligent automatic IDS or expert systems are used. These normally use statistical engines to estimate the event probability.

6.11. The IODEF description must provide information about the actions taken in the course of this incident by previous CSIRTs.

Comment:
The IODEF describes an Incident throughout its life-time from Alert to closing and archiving. It is essential to track all actions taken by all involved parties. This will help determine what further action needs to be taken, if any. This is especially important in case of Incident information exchange between CSIRTs in process of investigation.

6.12. The IODEF must support reporting of the time of all stages along Incident life-time.

Comment:
Time is important from both a reporting and correlation point of view. Time is one of main components that can identify the same Incident or attack if launched from many sites or distributed over the network. Time is also essential to be able to track the life of an Incident including Incident exchange between CSIRTs in process of investigating.

6.13. Time shall be reported as the local time and time zone offset from UTC. (Note: See RFC 1902 for guidelines on reporting time.)

Comment:
For event correlation purposes, it is important that the manager be able to normalize the time information reported in the IODEF descriptions.

6.14. The format for reporting the date must be compliant with all current standards for Year 2000 rollover, and it must have sufficient capability to continue reporting date values past the year 2038.

Comment:
It is stated in the purposes of the IODEF that the IODEF shall describe the Incident throughout its life-time. In the case of archiving this duration might be unlimited. Therefore, implementations that limit expression of time value (such as 2038 date representation limitation in "Unix time") MUST be avoided.

6.15. Time granularity in IO time parameters shall not be specified by the IODEF.

Comment:
The time data may be included into IODEF description by existing information systems, retrieved from incident reporting messages or taken from IDS data or other event registration tools. Each of these cases may have its own different time granularity. For the purposes of implementation, it should be possible to handle time at different stages according to the local system capabilities.

6.16. The IODEF should support confidentiality of the description content.

The selected design should be capable of supporting a variety of encryption algorithms and must be adaptable to a wide variety of environments.

Comment:
IODEF Incident descriptions potentially contain sensitive or private information (such as forensic data (evidence data), passwords, or persons/organisations identifiers) which would be of great interest to an attacker or malefactor. Incident information normally will be stored on a networked computer, which potentially may be exposed to attacks (or compromised). Incident information may be transmitted across uncontrolled network segments. Therefore, it is important that the content be protected from unauthorised access and modification. Furthermore, since the legal environment for privacy

and encryption technologies are varied from regions and countries and change often, it is important that the design selected be capable of supporting a number of different encryption options and be adaptable by the user to a variety of environments. Additional measures may be undertaken for securing the Incident during communication but this issue is outside of IODEF scope as it implies more strict rules for IO archiving and storing in general.

6.17. The IODEF should ensure the integrity of the description content.

The selected design should be capable of supporting a variety of integrity mechanisms and must be adaptable to a wide variety of environments.

Comment:
Special measures should be undertaken to prevent malicious IO changes.

Additional measures may be undertaken for securing the Incident during communication but this issue is outside of IODEF scope.

6.18. The IODEF should ensure the authenticity and non-repudiation of the message content.

Comment:
Authenticity and accountability is needed by many teams, especially given the desire to automatically handle IOs, therefore it MUST be included in the IODEF. Because of the importance of IO authenticity and non-repudiation to many teams and especially in case of communication between them, the implementation of these requirements is strongly RECOMMENDED.

6.19. The IODEF description must support an extension mechanism which may be used by implementers. This allows future implementation-specific or experimental data. The implementer MUST indicate how to interpret any included extensions.

Comment:
Implementers might wish to supply extra data such as information for internal purposes or necessary for the particular implementation of their Incident handling system. These data may be removed or not in external communications but it is essential to mark them as additional to prevent wrong interpretation by different systems.

6.20. The semantics of the IODEF description must be well defined.

Comment:
IODEF is a human oriented format for Incident description, and IODEF description should be capable of being read by humans. The use of automatic parsing tools is foreseen but should not be critically necessary. Therefore, IODEF must provide good semantics, which will be key to understanding what the description contains. In some cases the IODEF description will be used for automatic decision making, so it is important that the description be interpreted correctly. This is an argument for using language-based semantics. The metalanguage for IODEF identifiers and labels is proposed to be English, a local IODEF implementation might be able to translate metalanguage identifiers and labels into local language and presentations if necessary.

7. IODEF extensibility

7.1. The IODEF itself MUST be extensible. It is essential that when the use of new technologies and development of automated Incident handling system demands extension of IODEF, the IODEF will be capable to include new information.

Comment:
In addition to the need to extend IODEF to support new Incident handling tools, it is also suggested that IODEF will incorporate new developments from related standardisation areas such as IDEF for IDS or the development of special format for evidence custody. The procedure for extension should be based on CSIRT/IODEF community acceptance/approval.

8. Security Considerations

This memo describes requirements to an Incident Object Description and Exchange Format, which intends to define a common data format for the description, archiving and exchange of information about incidents between CSIRTs (including alert, incident in investigation, archiving, statistics, reporting, etc.). In that respect the implementation of the IODEF is a subject to security considerations. Particular security requirement to access restriction indication is discussed in section 4.3, requirements to Incident description confidentiality, integrity, authenticity and non-repudiation are described in sections 6.16, 6.17, 6.18.

9. References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Incident Taxonomy and Description Working Group Charter - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/

[3] Intrusion Detection Exchange Format Requirements by Wood, M. - December 2000, Work in Progress.

[4] Intrusion Detection Message Exchange Format Extensible Markup Language (XML) Document Type Definition by D. Curry, H. Debar - February 2001, Work in Progress.

[5] Guidelines for Evidence Collection and Archiving by Dominique Brezinski, Tom Killalea - July 2000, Work in Progress.

[6] Brownlee, N. and E. Guttman, "Expectations for Computer Security Incident Response", BCP 21, RFC 2350, June 1998.

[7] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, May 2000.

[8] Establishing a Computer Security Incident Response Capability (CSIRC). NIST Special Publication 800-3, November, 1991

[9] Handbook for Computer Security Incident Response Teams (CSIRTs), Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski. - CMU/SEI-98-HB-001. - Pittsburgh, PA: Carnegie Mellon University, 1998.

[10] A Common Language for Computer Security Incidents by John D. Howard and Thomas A. Longstaff. - Sandia Report: SAND98-8667, Sandia National Laboratories - http://www.cert.org/research/taxonomy_988667.pdf

[11] Best Current Practice of incident classification and reporting schemes currently used by active CSIRTs. - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/BCPreport1.rtf

[12] Taxonomy of the Computer Security Incident related terminology - http://www.terena.nl/task-forces/tf-csirt/i-taxonomy/docs/i-taxonomy_terms.html

[13] Multilingual Support in Internet/IT Applications. - http://www.terena.nl/projects/multiling/

Acknowledgements:

This document was discussed at the Incident Taxonomy and Description Working Group seminars (http://www.terena.nl/task-forces/tf-csirt/tf-csirt000929prg.html#itdwg) in the frame of TERENA Task Force TF-CSIRT (http://www.terena.nl/task-forces/tf-csirt/). Incident Taxonomy and Description Working Group at TERENA can be contacted via the mailing lists <incident-taxonomy@terena.nl> or <iodef@terena.nl>, archives are available correspondently at http://hypermail.terena.nl/incident-taxonomy-list/mail-archive/ and http://hypermail.terena.nl/iodef-list/mail-archive/

Authors' Addresses

Jimmy Arvidsson
Telia CERT

EMail: Jimmy.J.Arvidsson@telia.se

Andrew Cormack
JANET-CERT

EMail: Andrew.Cormack@ukerna.ac.uk

Yuri Demchenko
TERENA

EMail: demch@terena.nl

Jan Meijer
SURFnet

EMail: jan.meijer@surfnet.nl

Full Copyright Statement

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.