Requirements for the Format for INcident information Exchange (FINE)
<draft-ietf-inch-requirements-03.txt>

Status of this Memo

By submitting this Internet-Draft, we certify that any applicable patent or other IPR claims of which we are aware have been disclosed, or will be disclosed, and any of which we become aware will be disclosed, in accordance with RFC 3668.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than a "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/1id-abstracts.html

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This document is a product of the inch Working Group. Comments should be addressed to the authors or the mailing list at inch@nic.surfnet.nl

This Internet-Draft will expire on August 6, 2005

Copyright Notice

Copyright (C) The Internet Society (2005). All Rights Reserved.
Abstract

The purpose of the Format for Incident report Exchange (FINE) is to facilitate the exchange of incident information and statistics among responsible Computer Security Incident Response Teams (CSIRTs) and involved parties. FINE can be used for reactionary analysis of current intruder activity and proactive identification of trends that can lead to incident prevention. A common and well-defined format will help in the exchange of Incident related information across organizations, regions and countries. This document describes the requirements for an Incident Report Exchange Format.

Table of Contents

1. Introduction ............................................. 3
2. Incident Handling Framework .............................. 3
3. General Requirements .................................... 5
4. Format Requirements ...................................... 6
5. Communication Mechanism Requirements .................. 7
6. Content Requirements ..................................... 7
7. Security Considerations ................................... 8
8. IANA Considerations .................................... 8
9. References ................................................ 9
10. Acknowledgements ....................................... 10
11. Authors’ Addresses ..................................... 10
Full Copyright Statement .................................. 11
Appendix: History of Changes
1. Introduction

Computer security incidents occur across administrative domains, often spanning different organizations and national borders. Hence, a distributed response requiring coordination and collaboration between the involved parties and the responsible Computer Security Incident Response Teams (CSIRTs) are often required to respond to these threats. The basis for this interaction is various data and statistics describing the nature of the incident. This information, referred to as an incident report in this document, supports response activity to the specific incident, but may also inform historical analysis or proactive responses.

This document merely defines the high-level functional requirements for a transport format to exchange incident reports. This abstract data representation, the Format for INCident report Exchange (FINE), is not specified.

The intent of FINE is to decrease the response time to incidents and facilitate by improving the ability of CSIRTs to process incident reports. The definition of a well-defined format will facilitate the exchange of incident reports across organizations, regions and countries by achieving these particular goals:
+ to make the semantics of the report as clear and unambiguous;
+ to ensure that the data has a well defined syntax;
+ to ensure that the structure of the report allows easy categorization and statistical analysis;
+ to ensure the verifiability of the integrity of the report, and the authenticity of the report source.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [RFC2119].

2. Incident Handling Framework

2.1. Descriptive Terms

For the purpose of clarity, certain commonly used terms from the operational domain of CSIRTs are defined here. These are based on related documents [7, 8, 9, 10, 11]

2.1.1. Event

An event is an occurrence in a system or network that may be of interest and warrant attention. An event may or may not be malicious or deliberate.
2.1.2. Attack
An attack is a series of events caused either directly or indirectly by a source that violates a security policy of the target. These violations may include a compromise of a user account, denial-of-service, information theft, etc.

2.1.3. Source
The origin of an attack as described by a host, user account, computer program, network address, person, or organization.

2.1.4. Target
The target of an attack as described by a host, user account, computer program, network address, person, or organization.

2.1.5. Computer security incident
A computer security incident, referred to as incident, is a set of one or more related attacks identified by a CSIRT.

2.1.6. CSIRT
A Computer Security Incident Response Team, CSIRT, is an individual or a group of individuals that coordinate and support the response to incidents in a defined constituency [7]. A CSIRT creates, processes, and maintains incident reports.

2.1.7. Impact
An impact describes the consequence of an incident on a target expressed in terms relevant to a user community.

2.1.8. Incident Report
An incident report is the collection of the information describing an incident.

2.2 The Operational Model
Incident reports are generated, received and updated. For example, an organization may send an incident report to a Computer Security Incident Response Team (CSIRT) when an attack is detected. CSIRTS receive incident reports from customers or from other CSIRTS. The CSIRTS maintain these reports in an Incident Report Database in some format that may be specific to the CSIRT. The CSIRTS may process the reports to generate statistics, or investigate an incident further. As part of the investigation or as part of the reporting, the CSIRT may forward the incident report or parts of it to other CSIRTS. The CSIRTS may also receive results of investigation, or additional information related to currently active incidents from other CSIRTS. In the context of FINE, the incident reports will be handled by a CSIRT via an interface that is capable of converting a FINE formatted
incident report into the internal format used by the CSIRT and vice versa.

These operations are shown in fig. 1

```
+------------------+
|                  |
| +--------+   +---------+              +---------+   +--------+ |
| |        |<--|Interface|<--Incident-->|Interface|-->|        | |
| |Incident|   +---------+    Report    +---------+   |Incident| |
| | Report |       |                          |       | Report | |
| |Database|       |     |===  FINE  ===|     |       |Database| |
| |        |       |                          |       |        | |
| +--------+       |                          |       +--------+ |
|                  |                          |                  |
+------------------+                          +------------------+
```

Fig. 1 Operational Model for FINE

From the operational point of view during the life-cycle of an incident report the following may apply:
+ the report itself evolves. It may exist in one of the following states:
  - handling - the incident report is being handled
  - complete/closed - the incident report has been processed and no further processing is planned
  - waiting - the incident report is waiting on some event;

+ the report is exchanged between CSIRTs and may be investigated/processed by multiple CSIRTs, simultaneously;

+ additions and/or changes to the report may be made by one or more CSIRTs. Therefore, a single CSIRT may not be in a position to vouch for the veracity of all parts of the incident report.

3. General Requirements

3.1 FINE SHALL reference and use previously published RFCs where possible.

3.2 FINE MUST have well defined semantics and provide a standard
mechanism for extensibility.

The values of the various components of FINE should be typed, and the meaning should be well specified. Likewise, there should be a standardized method to deal with the representing data not defined in the data model.

4. Format Requirements

4.1 FINE SHALL support full internationalization and localization.

A significant part of the incident report will be comprised of human readable text. Since some incidents will entail involvement of CSIRTs from different countries and geographic regions, FINE must have provisions for using local character sets and encodings.

In cases where local (non-standard) character sets and encodings are used, the elements that carry encoding sensitive information should be clearly indicated. It should be possible to preserve the content of these elements when transferring an incident report.

4.2 FINE MUST allow multilingual reports.

Different parts of the incident report may be written in a different language. Likewise, multiple versions of the same part of the report may exist, each in a different language.

4.3 FINE MUST support aggregation and filtering of incident report data.

The format of FINE must be structured with components that have a well-defined syntax and semantics. For example, an application may want to generate the number of 'scan’s that originated from a given network. FINE must support such filtering and aggregation.

4.4 FINE MUST be able to document the evolution of an incident.

An incident report may evolve with time, as further investigation is performed on the incident report. Earlier information may be modified and new information may be added. FINE must support the recording of these changes.

4.5 FINE MUST support specifying a granular access restriction policy for the specific elements of the incident report.

Various parts of an incident report will have information of varying degrees of sensitivity and will need to be handled with the appropriate level of confidentiality. It must be possible to specify the degree of confidentiality for the individual components of the
incident report. Applications can then implement different levels of access restrictions for the different components of the incident Report.

4.6 FINE SHOULD allow the application of external mechanisms to support authenticity, integrity, and non-repudiation checks of incident reports.

FINE itself need not guarantee authenticity, integrity, or non-repudiation. However, the specification must detail a standardized mechanism to ensure these properties.

5. Communication Mechanism Requirements

5.1 The communication mechanisms MUST NOT have any bearing on the security of a FINE incident report.

Incident report exchange will normally be conducted using standard communication protocols and exchange mechanisms, for example, e-mail, HTTP, FTP, XML Web Services, etc. FINE must not rely on communication mechanisms or specific applications to ensure authenticity, integrity and/or confidentiality of an incident report. Provisions for authenticity, integrity and confidentiality should be made in FINE.

6. Content Requirements

6.1 FINE MUST be flexible enough to support various degrees of completeness, while still clearly defining the minimal information required for describing an incident.

6.2 FINE MUST support globally unique identifiers for each incident report.

It should be possible to reference an incident report unambiguously using a globally unique identifier. It should be possible to derive the creator of the incident report from this identifier.

6.3 FINE MUST support the naming of the source and target.

6.4 FINE SHOULD support the description of various aspects of the source and target.

6.5 FINE SHOULD contain a description of the methodology used in the attacker.
Well-known classifications or enumeration schemes should be used to describe the attack or exploited vulnerabilities that caused the incident.

6.6 FINE MUST include the identity of the creator of the incident report.

FINE should indicate the source of each component of the incident report if it is different from the creator (e.g., the team handling the incident).

6.7 FINE SHOULD support the including or referencing information external to the incident report.

6.8 FINE MUST support natural language descriptions of the incident.

6.9 FINE SHOULD support references to the appropriate advisories from coordination and analysis centers.

6.10 FINE SHOULD provide for describing the impact of the incident report.

6.11 FINE SHOULD support describing the actions taken during the course of handling an incident.

6.12 FINE SHOULD use a standardized time specification.

Incident reports should represent time in such a way that it is possible to easily compare information reported from different timezones.

Different systems will support different time granularities. FINE should be able to support incident reports from various systems irrespective of their time granularity.

7. Security Considerations

There are no explicit security considerations for this document since no protocol or information model is specified. However, a number of security relevant requirements are outlined for FINE implementers. By its nature, FINE will represent sensitive information. Hence, implementers should ensure support for access restriction (requirement 4.5); transport agnostic security guarantees (requirement 5.1); and confidentiality, integrity, and non-repudiation (requirement 4.8).
8. IANA Considerations

This document requires no action from IANA.

9. References

9.1 Normative References


9.2 Informative References


Acknowledgments.

The precursor of this document is "RFC3067 TERENA’s Incident Object Description Exchange Format Requirements" [2] which is based on the work done at Incident Object Description Exchange Format Working Group at TERENA. Subsequent work and discussion have been carried out in the INCH-WG and in the WIDE-WG on Network Management and Security.

The following individuals, in alphabetic order, have made substantial contribution to this document:
  - Hiroyuki Kido
  - Kathleen M. Moriarty
  - Roman Danyliw

Authors’ Addresses:

Yuri Demchenko
University of Amsterdam, The Netherlands
Email: demch@chello.nl

Hiroyuki Ohno
WIDE Project, Japan
Email: hohno@wide.ad.jp

Glenn Mansfield Keeni
Cyber Solutions Inc.
Sendai, Japan
Email: glenn@cysols.com
Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.
Appendix - non-normative.

Major Changes (reverse count)
Information about changes to the document since publishing -00 version will be documented here.

Major changes in version -03 (Second revision)
1) title changed to
 Requirements for the Format for INCident information Exchange (FINE)
 2) editorial nits
 3) RFC2119 key words used
 4) added description to 4.6
 5) reformatted 4.7 and 5.1 to have single statement requirements followed by description of the requirements.
 6) added an example to 4.2
 7) moved 6.13 to Format requirements as 4.8
 8) updated references #3, #5, #10
 9) updated section 2.2

Major changes in version -03 (First revision)
1) editorial nits
 2) in Security Considerations section an example is added to explain the impact of the contents of the IR on the security and privacy of individuals of organization.
 3) Section 3 is deleted

Major changes in version -02
1) clarified definitions of some terms. Added a few definitions.
 2) in 5.1, added requirement for handling non-standard/local encoding and/or character codes.
 3) in 5.7, added requirement that multiple versions of the report should be consistent.
 4) in 7.5, added requirement that the source of each component of the Incident report must be identified (if different from the creator of the Incident report).
 5) some editorial nits are fixed.

Major changes in version -01
1) clarified definition of some terms - still in the process, needs more discussion with concerned parties.
2) re-written section 2. Operational model

3) added text about multilingual support for non-utf-8 character sets to item "5.1 FINE shall support full internationalization and localization" - results of discussion at IETF-56

4) included clear statement about unique identification of the Incident report to item "5.1 FINE shall support full internationalization and localization."

5) added item about the possibility of Incident description in natural language:

7.7 The FINE may contain a description of the Incident or comprising security events in a natural language.

6) requirement about describing impact of the Incident extended (item 7.9) with recommendation to provide guidelines to describe the impact on the target to ensure a uniform interpretation of the description.

7) item 7.11 about time normalization extended with the possibility to describe time offset when normalization is not possible.