Network Working Group
Internet Draft
Expires: April 27, 2003

Glenn M Keeni
Cyber Solutions Inc.
Hiroyuki Ohno
WIDE Project
October 28, 2002

INCH Requirements
<draft-glenn-inch-req-00.txt>

Status of this Memo

Copyright Notice

Abstract

The purpose of the Incident Report Format is to facilitate the exchange of incident information and statistics among involved parties and responsible Computer Security Incident Response Teams (CSIRTs) 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 retrieving, archiving and exchanging Incident Reports across organizations, regions and countries.

This document describes the requirements for an Incident Report format.

Table of Contents

1. Introduction

Computer security incidents occur across administrative domains often spanning different organizations and national borders. Therefore, the exchange of incident information and statistics among involved parties and the responsible Computer Security Incident Response Teams (CSIRTs) is crucial for both reactionary analysis of current intruder activity and proactive identification of trends that can lead to incident prevention.

In the following we refer to the information pertaining to an incident as an Incident Report (IR).

This document defines the high-level functional requirements of the format of an IR to facilitate collaboration between CSIRTs and parties involved when handling computer security incidents.

2. The Information.

To make the information useful for search, retrieval, aggregation and analysis related processing the semantics of the contents should be well defined. It should be noted that there is a generic difference between "alerts" [Cite idwg-requirements-doc] and incident reports. The IDMEF alerts are generated by "sensors" and processed by managers (applications). On the other hand the incident reports will be generated by human beings and will also be consumed by human beings. In the case of incident reports, the intent is

- to make its semantics as clear and unambiguous as possible even across regional and national boundaries.
- to have a well defined syntax (atleast for parts of it),
- to enable categorization and statistical analysis
- to make it possible to ensure integrity of the message, and the authenticity of the message source authenticated

3. General Requirements

3.1. The Incident Report Format (IRF) shall reference and use previously published RFCs where possible.

4. Format Requirements

4.1 A major part of the IR will comprise of human-readable text. The IRF must support full internationalization and localization,

so that all users of the Internet can use their own language and its standard character set to express themselves. This will require compliance with the IETF Character Set Policy [RFC2277].

4.2 IRF must be structured to support search and retrieval,

filtering and aggregation. The structure will contain several components and some components may be structures themselves. Each component of a structure will have a well defined semantics.

4.3 **An IR may evolve with time. As investigation proceeds more information about an incident may be revealed and parts of the** earlier information will be refined/obsoleted. The IRF must be able to support an accurate record of the evolution of the IR with appropriate timestamps identifying the epochs in the lifetime of an IR..

4.4 **All time references in the IR should** be interpreted in an unambigious manner. It should be possible to transform the time references to any of the standard time references e.g. UTC.

4.5 **An IR may contain sensitive information. The IRF must support an access control mechanism. It must be possible to define** the access control for the individual components of the IR and for individual accessing entities.

4.5 **An IR must be globally uniquely identifiable. It should be possible to map the origin of an IR from its globally unique** identifier.

4.6. **The IRF itself must be extensible.** The extension will be in terms of addition of components and/or extending the components.

5. Communications Requirements

5.1. **IR generation and exchange will normally be initiated by humans using standard communication protocols, for example, e-mail,** HTTP, FTP, etc. The communication mechanism must have no bearing on the authenticity, integrity, confidentiality of the IR itself.

6. Content Requirements

The IRF must be flexible enough to support various degrees of completeness. At the same time it must clearly state the minimal information without which the information in the IR will be seriously degraded.

6.1 **An IR will generally refer to one or more entities. The entity may be an attacker, a victim or an observer. There are several** facets of an entity involved in an IR. The entity may have zero or more network addresses and names as well as zero or more location names, organizational name, person names, machine names etc. The IRF should support various facets describing the entities

involved.

6.2 **There may be different rules and conventions for naming entities in different regions and networks. The IRF must be able** to accomodate these rules and conventions. The format must be able to identify the rule or convention that is used in the naming.

6.3 **And IR must contain information based on which globally uniquely identifier for the IR will be formed.**

6.4 **The IR should contain a classification of the attack. The IRF must support well known classification/enumeration** schemes.

6.5 **The IR must contain information about the originator of the various components of the report.**

6.6 **The IR should contain information about the attacker and victim, if known.**

6.7 **The IR should contain reference to advisories corresponding to the IR e.g. CERT/CC, CVE,**

6.8 **The IR should contain a description of the incident.**

6.9 **The IR should contain additional references/pointers/information This information should include IDMEF [4] messages which** may have been generated by security devices.

6.10 **The IR should describe the Impact on the target, if known. There should be guidelines to describe the impact on the target** to ensure a uniform interpretation of the description.

6.11 **The IR should decribe the actions taken since the occurance of the incidence.**

6.12 **The IR should carry information whereby its authenticity, integrity can be verified and non-repudiation can be guaranteed.**

6.13 **The semantics of the IRF must be well defined. The various components of the IRF should have a well defined** semantics. [Cant say the same about the contents of all components]

7. Intellectual Property

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF's procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

8. Acknowledgments.

The precursor of this document is "IODEF Requirements" [RFC3067] which is based on the work done at Incident Taxonomy and Description Working Group at TERENA. Subsequent work and discussion has been carried out in the INCH-BOF and in the WIDE-WG on Network Management and Security.

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

8. Security Considerations

This does not describe a protocol by itself memo it describes the requirements for an Incident Report. It reports themselves are about security incidents. The contents of the Incident Reports will have significant direct and/or indirect impact on the security and privacy of a network and/or individuals. Protocol designers should take care to analyze and implement the requirements stated in 4.5 and 6.12.

Authors' Addresses

Glenn Mansfield Keeni
Cyber Solutions Inc.
Sendai
Japan

EMail: glenn@cysols.com

Hiroyuki Ohno
WIDE Project, Japan

Email: hohno@wide.ad.jp

Full Copyright Statement

Acknowledgement

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