Internet Engineering Task Force
INTERNET-DRAFT

Nevil Brownlee
John White
The University of Auckland
September 1995

Framework for Security Incident Response
<draft-ietf-grip-framework-irt-00.txt>

Status of this Memo

This document is an Internet Draft. 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. This Internet Draft is a product of the Internet Accounting Working Group of the IETF.

Internet Drafts are draft documents valid for a maximum of six months. Internet Drafts may be updated, replaced, or obsoleted by other documents at any time. It is not appropriate to use Internet Drafts as reference material or to cite them other than as a 'working draft' or 'work in progress.'

Please check the I-D abstract listing contained in the Internet-drafts Shadow Directories on nic.ddn.mil, nnsc.nsf.net, nic.nordu.net, ftp.nisc.sri.com or munnari.oz.au to learn the current status of this or any other Internet Draft.

Abstract

This document provides guidelines for Internet Security Incident Response Teams (IRTs), and recommends a "template" through which every IRT should describe itself and its functions. It was produced by the GRIP Working Group of the IETF.

Contents

1 Introduction

The Working Group group was formed to provide guidelines and recommendations to facilitate the consistent handling of security incidents in the Internet community.

Security incidents and potential threats of them usually extend beyond institutional or local community boundaries. "Consistent handling" implies that any group calling itself an Incident Response Team (IRT) must react to security incidents or to threats of them in ways which the general Internet community agrees to be in its general interest.

The "Framework for Security Incident Response" is seen as resting on the

work of individual IRTs and the cooperation between them.

This document therefore recommends a "template" through which every IRT should describe itself and its functions. It further recommends that templates should be accessible among teams, to make possible a fully effective cooperative response framework for incidents or threats across the entire domain affected by them.

1.1 Template Repository

If templates are to be accessible between IRTs, a central repository will be needed for them. The GRIP Working Group believe that some of the existing Internet archive areas could be used for this purpose.

Each team should be responsible for ensuring that its own template is available to at least its constituency and its co-operating partner teams. Digital signatures should be used to protect the completed templates against modifications. The keeper of each template repository will be responsibly for verifying the identity of each IRT loding a template in the repository.

--- (Future drafts will present more specific recommendations
concerning the sharing of Template information) ---

The Template is summarized in the section immediately below, and the remainder of the document describes its components.

2 Description Template: Security Incident Response Team

Contact Information
---
* name of the team
* address
* telephone
* telefax
* other telecommunication like STU-III
* electronic mail
* encryption methods for communication: PGP, PEM, MOSS, ..
* actual list of members on demand (optional)

* Date of last update
* Distribution of template updates

Charter

* mission statement
* constituency
* sponsor / affiliation
* authority

Policies

* types of incidents
* level of support
* disclosure
  - of compromised site's information
  - the compromise of IRT site to constituency
* cooperation & interaction with
  - incident response teams
  - vendors
  - investigative agencies
  - involved sites
  - press
* communication & authentication
* point of customer contacts
* incident reporting requirements

Services

* incident response
  - verification
  - understanding
  - coping
  - notification
* proactive activities

Incident Reporting Forms

Disclaimers

3 Purpose of the Template

The Template which this document proposes is expected to be used by a response team to describe what it does, and in the process create criteria against which its performance can be measured. The Template does not attempt to specify a "correct" way for the team to operate, but does recommend on specific policies and functions seen as necessary for such a team to play a consistent role in the overall security framework. It also comments on additional roles a team might include in the ambit of its operations.

The primary purposes of the Template are:

- to help IRTs improve the way they operate;
- to improve interactions between different IRTs, and between IRTs and other organizations such as vendors and law-enforcement agencies;
- to note necessary interactions with their constituencies in setting expectations and defining policies;
- to help new groups understand what it takes to "be" an IRT.

A Template might appear to provide a marketing tool for comparing different teams, but this kind of marketing use (or abuse) is strongly discouraged by the GRIP Working Group.

3.1 Other Related Material

This 'Framework for Response Teams' document is the first produced by the GRIP Working Group. A second document will set out guide-lines for technology vendors to help them handle security incidents. The definition of terms given in the next section applies to both documents.

Another relevant IETF document is RFC 1244, the Site Security Handbook, produced by (and being updated by) the Site Security Handbook Working Group (SSH). Site requirements and recommendations are covered by the Handbook, while response team expectations and procedures are addressed by the GRIP documents.

Other documents of interest for the discussion of incident response teams and their tasks are available by anonymous FTP. A collection can

be found on:

* ftp://ftp.nic.surfnet.nl/surfnet/net-security/cert-nl/docs/reports/R-92-01

Some especially interesting documents are:

* CERT-NL Framework
  ftp://ftp.cert.dfn.de/pub/csir/docs/cert-nl.opframe.txt

* FIRST potential members
  ftp://ftp.first.org/pub/first/newmemlt.txt
  ftp://ftp.first.org/pub/first/profile.txt
  ftp://ftp.first.org/pub/first/op`frame.txt

* Bibliography
  http://www.cert.dfn.de/eng/team/kpk/certbib.html

4 Definitions

This section defines terms used in describing security incidents and response teams. For the purpose of the GRIP documents only a limited list is really needed. This should help maintain focus on the purpose of the documents, and prevent a duplication of other definitions or - even worse - a proliferation of competing definitions.

4.1 Constituency

Implicit in the purpose of a Security Incident Response Team is the existence of a constituency. This is the group of users, sites, networks or organizations served by the team.

4.2 Partner Teams

Implicit in the purpose of the Template proposed here is the existence of Partner Teams which are its primary audience, and which share in the responsibility for addressing security incidents or threats common to their separate constituencies.

4.3 Security

After considerable discussion, the Working Group decided not to attempt a definition of "security", but instead to rely on intuition, or on definitions in other documents such as the Site Security Handbook.

4.4 Incident

For the purpose of this document:

'A computer security incident is any event which compromises some aspect of computer or network security.'

The definition of an incident may vary between organizations, but at least the following categories are generally applicable:

* loss of confidentiality,
* compromise of integrity,
* denial of service,
* misuse,
* damage.

These are very general categories. For instance the forging of an electronic mail message and a successful password attack are two examples of 'compromise of integrity.'

Within the definition of an incident the word 'compromised' is used. Sometimes an administrator may only 'suspect' an incident. During the handling of a call it must be established whether or not an incident really occurred.

4.5 Security Incident Response Team

Based on two of the definitions given above:

'A Security Incident Response Team is a group authorized to deal

with security incidents that occur within its defined constituency.'

It should provide a channel for receiving reports about suspected incidents and for disseminating incident-related information to its constituency and to other related parties; it should also provide assistance to members of its constituency in handling these incidents.

4.6 Vendor

A 'vendor' is any entity that produces networking or computing technology, and is responsible for the technical content of that technology. Examples of 'technology' include hardware (routers, switches, etc), and software (operating systems, mail forwarding systems, etc).

Note that the supplier of a technology is not necessarily the 'vendor' of that technology. As an example, an Internet Services Provider (ISP) might supply routers to each of its customers, but the 'vendor' is the manufacturer, being the entity responsible for the technical content of the router, rather than the ISP.

4.7 Vulnerability

A 'vulnerability' is a characteristic of a piece of technology which can be exploited to perpetrate a security incident. For example, if a program allowed ordinary users to execute operating system commands in privileged mode, this "feature" would be a vulnerability.

5 The Security Incident Response Team Template

This material which follows is addressed to those responsible for Security Incident Response Teams.

5.1 Template Updates

Details of an IRT change with time, so the template must indicate when it was last changed, who will be informed of future changes, and (by implication) who will not. Without this, it is inevitable that misunderstandings and misconceptions will arise over time.

5.1.1 Date of last update

This should be sufficient to allow anyone interested to evaluate the currency of the template.

5.1.2 Distribution of Template Updates

Persons on this list are notified automatically whenever the template is changed. The list might normally cover the constituency and immediate Partner IRTs. Readers not on the list can then recognise that they should check the central repository (above) for possible updates.

Digital signatures should be used for update messages sent by an IRT to those on its distribution list.

5.2 Charter

Every IRT must have a charter which specifying what it is to do, and the authority under which it will do it. The charter should include at least the following:

* mission statement
* constituency
* sponsor / affiliation
* authority

5.2.1 Mission Statement

The mission statement should focus on the team's core activities, already stated in the definition of an IRT. In order to be considered a Security Incident Response Team, the team MUST provide incident response, by definition.

The goals and purposes of a team are especially important, and require clear, succinct definition.

5.2.2 Constituency

An IRT's constituency (as defined above) can be determined in many ways. For example it could be a company's employees or its paid subscribers,

or it could be defined in terms of a technological focus, such as the users of a particular operating system.

The definition of constituency should create a perimeter around the group to whom the team will provide service. The policy section (below) should explain how requests from outside the perimeter will be handled.

Constituencies might overlap, as when an ISP supports an IRT, but delivers services to customer sites which also have IRTs. The Authority section (below) should make such relationships clear.

People within the constituency have to learn that there is an IRT for their purposes; the building of a trusted relationship with the constituency is an on-going process which never ends.

5.2.3 Sponsoring organization / affiliation

The sponsoring organization, which authorises the actions of the IRT, should be given next. Defining the affiliation amounts to stating: "Who is your God?".

5.2.4 Authority

IRTs may not have authority to intervene in the operation of all the systems within their perimeter. They should identify the scope of their control as distinct from the perimeter of their constituency; if other IRTs operate hierachically within their perimeter, these should be identified.

--- (Responsibility should be covered here) ---

5.3 Policies

5.3.1 Types of incidents and level of support

The types of incident which the team is authorised to address and the level of support the team will contribute in assisting with each type of incident should be summarized here in list form. The Services section (later) provides opportunity for more detailed definition.

The team should state whether it will act on information it receives about vulnerabilities which create opportunities for future incidents.

A commitment to act on such information on behalf of its constituency is regarded as an optional pro-active service policy rather than a core service requirement for an IRT.

5.3.2 Co-operation and interaction with other organizations

This section should make explicit the related groups with which the IRT interacts:

* incident response teams
* vendors
* law-enforcement agencies
* press

5.3.3 Reporting and Disclosure

The default status of any and all security-related information which a team receives can only be 'confidential,' but rigid adherence to this makes the team a 'black hole.' Its template should define what information it will report or disclose, to whom, and when.

Different teams are likely to be subject to different legal restraints requiring or limiting disclosure, especially if they work in different jurisdictions. Each team's template should specify any such restraints, both to clarify users' expectations and to inform other teams.

Conflicts of interest, particularly in commercial matters, may also restrain disclosure by a team; the present Draft does not recommend on how such conflicts should be addressed.

An explicit policy concerning disclosure to the Press can be helpful, particularly in clarifying the expectations of an IRT's constituency.

'Disclosure' includes:

- reporting incidents within the constituency to other teams;

- handling incidents occurring within the constituency, but reported from outside it.

- reporting observations from within the constituency indicating suspected or confirmed incidents outside it;

- acting on reports of incidents occurring outside the constituency;

- passing information about vulnerabilities to vendors, to Partner IRTs or directly to affected sites lying within or outside the constituency;

- feed-back to parties reporting incidents or vulnerabilities;

- the provision of contact information relating to members of the constituency, members of other constituencies, other IRTs or law-enforcement agencies.

The reporting and disclosure policy should make clear who will be the recipients of an IRT's reports in each circumstance. It should also note whether the team will expect to deal through another IRT or directly with a member of another constituency over matters directly involving that member.

A team will normally collect statistics. If they are distributed, the template's reporting and disclosure policy should say so, and should list the recipients.

5.3.4 Communication and authentication

Methods of secure and verifiable communication should be established. This is necessary for communication between IRTs and between an IRT and its constituents. The template should include public keys or pointers to them, including key fingerprints, together with guidelines on how to use this information to check authenticity.

At the moment it is recommended that every IRT have, as a minimum, a PGP key available, since PGP is available world-wide. Teams may also make other mechanisms available, for example PEM.

For comunication via telephone or facsimile an IRT may keep secret authentication data for parties with whom they may deal, such as an agreed password or phrase.

5.4 Services

Services should be defined in two sections, as listed below.

* direct incident response
  + verification of incident
  + technical assistance analysis to understand compromise

+ notification of other involved parties

    + eradication
    + recovery

 * optional
    + information provision
       - vunerablility archive
       - patches and resolutions
    + tools
    + education
    + audit and consulting
    + product evaluation

5.5 Incident reporting Forms

Samples of reporting forms used by the IRT (or pointers to them) should be included at this point in a template.

5.6 Disclaimers

Although the template does not constitute a contract, liability might conceivably result from its descriptions of services and purposes. The inclusion of a disclaimer at the end of the template is recommended.

It should be noted that some forms of reporting or disclosure relating to specific incidents or vulnerabilities can imply liability, and IRTs should consider the inclusion of disclaimers in such material.

In situations where the original version of a template must be translated into another language, the translation should carry a disclaimer and a pointer to the original. For example:

> Although we tried to carefully translate our German template into English, we can not be certain that both documents express the same thoughts in the same level of detail and correctness. In all cases, where there is a difference between both versions, the German version is the binding version for our operation.

6 Appendix: Note on procedure definitions

Policies and statements of services in the template have to be implemented as procedures, but descriptions of those procedures should not be included in the template.

The following notes are intended to assist those seeking to form or to improve their IRTs.

```
 * External
    + identify other response teams
    + define supported clients:
        - by domain, through registration system, other means
    + establish secure communication practices
        - use of network, cell-phones, etc
    + define information that a client site must/should provide
        - use of reporting forms


* Internal
  + secure the team's infrastructure
  + protect information servers
  + protect sensitive data
  + define expiry of sensitive data
  + define disposal practice for sensitive data
  + establish methods for gathering and keeping statistics
  + establish 'knowledge base' of lessons learned from past incidents
  + create practical implementations of disclosure policies
  + document explicit practices for disclosure to the Press
```

The Site Security Handbook is a first resource to consult in securing a team's infrastructure. IRT-specific security measures may evolve later.

7 Security Considerations

This document discusses the operation of Security Incident Response Teams, and is therefore not directly concerned with the security of protocols or network systems themselves.

Nonetheless, it is vital that IRTs establish secure communication channels with other teams, and with members of their constituency. They must also secure their own systems and infrastructure.

8 Author's Addresses

Nevil Brownlee
The University of Auckland

Phone: +64 9 373 7599 x8941
E-mail: n.brownlee@auckland.ac.nz

John White
The University of Auckland

Phone: +64 9 373 7599 x8946
E-mail: j.white@auckland.ac.nz