Incident Taxonomy and Top-Level Classification

Presented at 3rd CERT-COORD meeting 11-12 May 2000, Vienna

Coordinator(s):
Andrew Cormack <Andrew.Cormack@ukerna.ac.uk>
Jan Meijer <jan.meijer@surfnet.nl>

Secretary:
Yuri Demchenko <demch@terena.nl>

Liaison(s):
CERT/CC - Kevin Houle <kjh@cert.org>
AusCERT - Rob McMillan <rob@auscert.org.au>

Mailing List:
incident-taxonomy@terena.nl

Description of Working Group:

Security incidents are becoming more common and more serious. Since incidents are often distributed over multiple sites, it is likely that different aspects of a single incident will be visible to different CSIRTs and systems. Thus there is an increasing need for classification of incidents to facilitate useful systemised analysis (rather than ad-hoc), ensure completeness and minimal confusion in operations, provide a uniform reporting scheme that is widely understood (and not open to misinterpretation) and take advantage of economies of scale.

CSIRTs require the scheme to fully describe items including such information as victim class, vulnerability classification, target software component, target system type and so on. All this implies to the top-level classification that must allow qualitative reporting of an individual incident, within the bounds of acceptable information.

There is also a clear need for meaningful analysis. CSIRTs must also be able to report trends, such as:
(a) important victim classes (commercial, education, government, other) and how attacks against those victims have changed over some period.
(b) the shift in appearance and exploitation of vulnerabilities.

The audience for the taxonomy and reporting protocol will be CSIRTs, particularly CSIRTs within FIRST as step to global Incidents information exchange. The secondary audiences for the data reported under such a scheme will include non-CSIRT technical and user audience.

The Incident Taxonomy and Top-Level Classification Working Group will coordinate its efforts with other CSIRT related Working Groups and activities and particularly, CERT/CC and AusCERT.

The working group intends to develop its classification and information exchange framework that should satisfy operational needs of CSIRTs. The first step to this will be taxonomy of Best Current practice. Subsequent iterations can be developed within a wider FIRST framework and after pilot implementation among selected CSIRTs.

Information exchange framework should support future extensions and events by being flexible enough to allow easy expansion as events evolve. Relation to existing tools and Databases is foreseen. Special extension format should allow to use internal classification (extensions) for internal needs of CSIRTs

Top-Level Incident Classification framework

Proposed classification scheme/framework must/will/should answer general question ***"What type of site was attacked to what level and with what vulnerability?"*** and provide support the following common information:

1. Incident description

1.1. What was targeted? Was it a person (what class?), or networking/communication component (which one?), or something else?
1.2. What software or network component was targeted?
1.3. What generic vulnerability class was used?
1.4. Optionally, what tool was used? - This less important than the other two because tools change daily.

2. Incident/attack target description:

2.1. What generic types of system were targeted: Authentication, Access control, Mail hubs, Network control devices and so on?
2.2. What level of penetration was achieved: none, network-read, network-write, host-read, host-write (or whatever)?

3. Victim identity description. It's not about to report specific sites, although generic industry sectors are important (Example: education, Commercial, Government, Other). The scheme should not include intruder identity. Local policy for information disclosure should be applied here.

4. Additional information may be included to specify geographical location or origination of the Incidents. insofar as target audience is concerned about whether an incident is purely domestic or international in nature.

The outputs of this working group will be:

1. Taxonomy of Best Current Practice based on existing classification and reporting schemes used by active CSIRTs.
2. Top-level Incident classification satisfying CSIRTs operational needs

3. Framework and Language for Incident Statistics exchange that will also allow future and local extension.

Goals and Milestones:

April 2000 - Draft document on Top-Level Incident Classification
April 2000 - Draft document on Taxono my of Best Current Practice
June 2000 - Draft document on Framework and Language for Incident Statistics exchange
June 2000 - Version 1 document on Top-Level Incident Classification proposed to CERT/CC
September 2000 - Version 2 document on Top-Level Incident Classification
September 2000 - Version 1 of Taxonomy of Best Current Practice
November 2000 - Version 1 of Framework and Language for Incident Statistics exchange
December 2000 - Pilot implementation and update

Documents available:

Proposed list of incident categories (Draft proposal by UKERNA and SURFnet - http://www.terena.nl/tech/task-forces/tf-csirt/pre-meeting3/TLversion0_2.html)

Mailing list archive - http://hypermail.terena.nl/incident-taxonomy-list/mail-archive/.