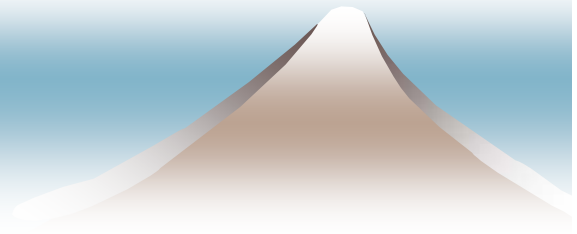
INCH Requirements

<draft-ietf-inch-requirements-03.01.txt>

IETF-60 SanDiego,
August, 2004



Issues Status:

Req-Issue-001:{01-12} Editorial nits

~~02 use of MUST SHOULD etc.~~	~~TBD~~
~~04 overall edit~~	~~TBD~~
~~06 sec-2 citations~~	~~TBD~~
~~06 sec-10 update citations 3,5,8~~	~~TBD~~
06 sec-10 citations style 10, 11	TBD

Issues Status:

Req-Issue-002:01

- Section 2.1.1:
  - what is meant by the fact that an attack is active or passive?

citation[8] RFC2828 says

- Active vs. passive: An "active attack" attempts to alter system resources or affect their operation. A "passive attack" attempts to learn or make use of information from the system but does not affect system resources. (E.g., see: wiretapping.)

Understood. Please cite the source in the text.
Done. [Closed]

Issues Status:

Req-Issue-003:01

- what is been implied by the text "an attack may be successful"?

Not all attacks are successful.
An attack is not necessarily a breach. An attempted breach is an attack.

TBD

Issues Status:

Req-Issue-004:01

- what is the relationship between an Attack (2.1.1) and an Event (2.1.5)?

2.1.5. Event

An occurrence in a system or network, which may be of interest and/or warrants attention. An event may indicate an attack. An event may also indicate an error, a fault, or be the result of a deliberate act that is not an attack. For example, the occurrence of three failed logins in 10 seconds is an event. It might indicate a brute-force login attack. A program failure, network fault, and system shutdown are other examples of an event.

TBD

Issues Status:

Req-Issue-005:01

- Section 2.1.2 and Section 2.1.9 what is the difference between an Attacker and Source. In both cases, it is said that this word is not referrning to a person but either a "network ID" or "computer".

"Source" is more generic and in some cases may include "Attacker" (the computer/network ID)

Are you trying to distinguish between the actual box on which the offending packets originated and the actor that ran the tool?

Yes. .

Issues Status:

Req-Issue-006:01

- Section 2.1.10 and Section 2.1.11 what is the difference between an Target and Victim.

"Target" is more generic and in some cases may include "Victim" (the computer/network ID)

Issues Status:

Req-Issue-007:01

- Section 2.1.3 : A CSIRT is an encompassing term to refer to anyone having a security responsibility that entails coordination or cooperation.

  Is it necessary to change the definition of CSIRT or, would it do to say that FINE applies to CSIRTs and "anyone with a security responsibility" or something similar to that.

  [TBD]

Issues Status:

Req-Issue-008:01

- Section 2.1.7: what is the relationship between an Attach (2.1.1) and an incident? .

  2.1.7 A Computer/Network Security Incident, referred to as incident in this work, is a set of one or more events. The events in the incident may indicate attacks. There may also be incidents which comprise of events which are not indicative of attacks.
  We may have an incident about which we are not sure whether it is attack. Also, there may be incidents like network faults, power outages, disk crashes.

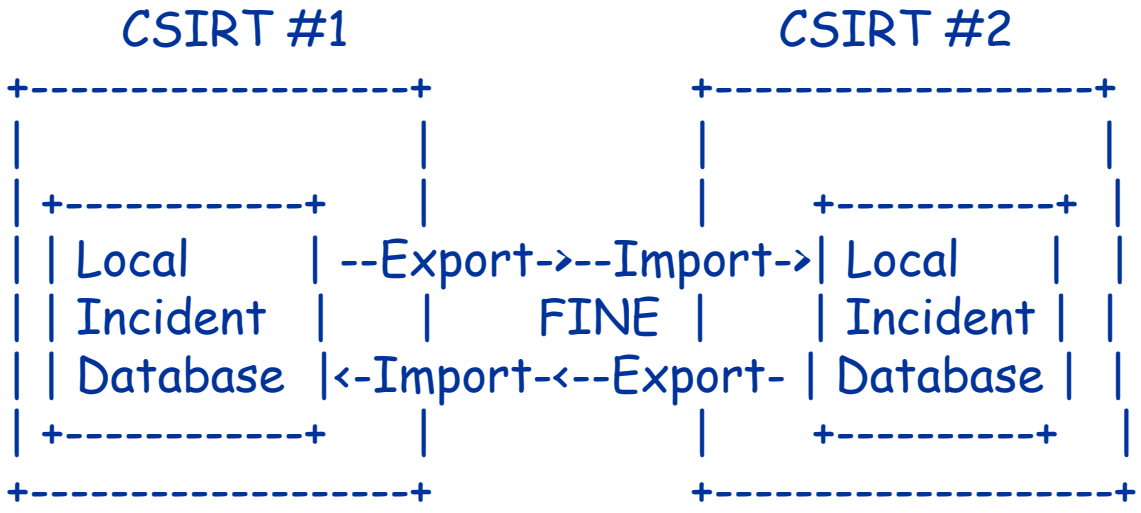
  We need to distinguish between security operations and general IT helpdesk outages.

  We are not concerned with IT helpdesk. But, from the security operations point of view, it may not always be possible to know whether an event is an attack or not.
  [TBD]

Issues Status:

Req-Issue-009:01

Change Fig. 1 "Operational Model for FINE "



Do we change the operational model?. In the above diagram FINE operates only between CSIRT's. In the current draft - FINE operates between a CSIRT and any other entity that wants to exchange/query IR data e.g. CSIRTsm Customers, Collaborators, involved parties. [TBD]