INCH Requirements

draft-ietf-inch-requirements-02.txt

Changes since -01.txt

Glenn M. Keeni/Yuri Demchenko

INCH-WG@IETF-58,
November 13. 2003

Clarified definitions

2.1.1. Attack

One or more steps taken by an attacker to achieve an unauthorised result. An Attack can be active or passive. An attack may be successful.

2.1.2. Attacker

Attacker is an entity that attempts one or more attacks. An attacker may be an insider, an outsider, or an entity acting via an attack mediator. ◦ ◦ ◦

Clarified definitions

2.1.5. Event

An occurrence in a system or network, which maybe of interest and/or warrants attention. An event may indicate an attack. An event may also indicate an error or a fault or 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, system shutdown are other examples of event.

Clarified definitions

2.1.7. Computer/Network Security Incident
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 be incidents which comprise of events which are not indicative of attacks.

Definition added

2.1.9. Source

The source of an attack. This can be a logical entity (e.g. a user account, a computer process or data, a logical network or inter-network) or a physical entity (e.g. a computer interface, a router etc.)

Non-standard/local encoding

- Sec 5.1 – added requirement for handling non-standard/local encoding and/or character codes.

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.

Multilingual versions

In Sec 5.7, added requirement that multiple versions of the report should be consistent

5.7. FINE must allow multilingual reports. In case there are multiple language versions of a component of the report, the versions should be consistent and, and FINE must provide a way to identify which version is authentic.

Source of information

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).

7.5 FINE must include the identity of the creator of the Incident Report (CSIRT or other authority). FINE should indicate the source of each component of the Incident Report if it's different from the creator.
The source of a component of the Incident Report may be the creator of the Incident Report, the team handling the incident or, some other party.

Other Changes

- Editorial nits

Requirements implementation in IODEF Schema

- Current IODEF Datamodel and XML Schema implement all requirements except:
  - Req#5.7 – marking up authenticity of the language version in case of many versions in different languages
  - Req.#7.5 – documenting source of information by elements
    - Currently only source of the whole Incident Report or Event is described by the Contact element

Required changes after v02

- Technical
  - Explicitly state goal of the FINE; currently ambiguous
- Editorial
  - Further explanation of certain requirements
  - Re-ordering of certain requirements
  - Full content “polish”

Summary

- WG Last Call in December 2003 on the mailing list