IODEF datamodel issues

IETF 55, 21 November 2002 Jan Meijer <{}jan.meijer@surfnet.nl>{}
INCH datamodel issues

- Linkage between attacker/victim
- Degree of IDMEF compatibility
- General unclarity of the datamodel
- Readability of the document
- Sanitization techniques
- Purpose and Restriction attribute definition
- Items on enumerated lists
- readability of the document

Linkage Attacker/Victim and Source/Target (1)

- Attacker/Victim:

"The Attacker class augments information found in the Source class with further details related to the entity(ies)/person(s) identified as the source(s) of the incident activity."

- Source/Target:

"The Source class contains information about the possible source(s) of the incident event(s). An event may have more than one source (e.g., in a distributed denial of service attack). For the purpose of compatibility, the Source class has been reused from the IDMEF."
Linkage Attacker/Victim and Source/Target (2) +———-+ +———+ +————-+ +———-+ |} Incident |}<{}>{} -|} Attack |}<{}>{} -|} Source |}<{}>{} -|} Node |} +———-+ +———+ +————-+ +———-+ |} |} |} |} |} |} +———-+ |} |} |} |} |} |}<{}>{} -|} User |} |} |} |} |} |} |} +———-+ <{}SNIP>{} |} |} |} |} +————-+ +———-+ |} |} |} |}<{}>{} -|} Target |}<{}>{} -|} Node |} |} |} |} |} +————-+ +———-+ |} |} |} |} |} |} +———-+ |} |} |} |} |} |}<{}>{} -|} User |} |} |} |} |} |} |} +———-+ <{}SNIP>{} |} |} +———+ +————-+ |} |}<{}>{} -|} Method |}<{}>{} -|} Classification |} |} |} +———+ +————-+ |} |} |} |} +————-+ |} |} |} |}<{}>{} -|} Description |} |} |} +———+ +————-+ |} |} +———+ +————-+ |} |}<{}>{} -|} Attacker |}<{}>{} -|} Contact |} |} |} +———+ +————-+ |} |} |} |} +————-+ |} |} |} |}<{}>{} -|} Location |} <{}SNIP>{} |} |} +———+ +————-+ |} |}<{}>{} -|} Victim |}<{}>{} -|} Contact |} |} |} +———+ +————-+ |} |} |} |} +————-+ |} |} |} |}<{}>{} -|} Location |}
Linkage Attacker/Victimand Source/Target <{}IODEF-Description>{} <{}Incident>{} <{}Attack>{} <{}Source>{} <{}Node>{} ... <{}/Node>{} <{}Node>{} ... <{}/Node>{} ... <{}/Source>{} <{}Source>{} <{}Node>{} .. <{}/Node>{} ... <{}/Source>{} <{}Target>{} <{}Node>{} ... <{}/Node>{} ... <{}/Attack>{} ... <{}Attacker>{} <{}Contact>{} ... <{}/Contact>{} <{}/Attacker>{} <{}Attacker>{} <{}Contact>{} ... <{}/Contact>{} <{}/Attacker>{} <{}Victim>{} <{}Contact>{} ... <{}/Contact>{} <{}/Victim>{} ... <{}/Incident>{} <{}/IODEF-Description>{} IDMEF compatibility

- " One of the design principles in the IODEF is compatibility with the Intrusion Detection Message Exchange Format (IDMEF) [3] developed for intrusion detection systems. For this reason, IODEF is heavily based on the IDMEF and provides upward compatibility with it."

- IODEF != IDMEF
- IDMEF classes have been adopted both semantically and syntactically where sometimes only adoption of syntax would be appropriate (impact)
- Strict compatibility maintenance created complex and unclear constructions
- And problems that can not easily be solved

Other issues

- Datamodel unclear and too complex

General feeling of overcomplexity, unclarity and basically not fulfilling the needs for exchanging incident coordination data between CSIRTs (and other entities!)

- Readability of the document
- Sanitization techniques

Need to express that a particular item is available but can not be shared

- Purpose and Restriction attribute semantics
- Items on enumerated lists
- readability of the document

Reordered datamodel (1)

- " One of the design principles in the IODEF is compatibility with the Intrusion Detection Message Exchange Format (IDMEF) [3] developed for intrusion detection systems. For this reason, IODEF is heavily based on the IDMEF and provides upward compatibility with it."
- IODEF != IDMEF
-
-

Reordered datamodel (2)

- Looking at the datamodel: two main areas
- Incident meta-data ('fuzzy', human interpretation)
- Data that can be 'measured', objective data
- Example: incident-impact vs. attack impact

<u>First result of restructuring:</u>
Incident Report
Incident meta-data Incident data Event —-0..*- Attacker/Victim —0..*- Source/Target Authority Record IncidentImpact Impact History AdditionalData

- Folded Source/Target into one class
- Folded Attacker/Victim into one class