IODEF Forensics Extension

Chris Inacio
inacio@cert.org
authors

• Other contributors more than welcome
• More points of view welcome as well
Source materials

• Current (rough outline) draft based on the following:
  
  • DEXF - draft submission to ITU-T for handling forensic information
  
  • DFXML - Simson Garfinkle work on defining a forensics interchange format ([http://www.forensicswiki.org/wiki/Category:Digital_Forensics_XML](http://www.forensicswiki.org/wiki/Category:Digital_Forensics_XML))
  
• Alternatives / More Standards
  
  • CybOX ([http://cybox.mitre.org](http://cybox.mitre.org))
schema design

- Captures
  - Information about who did the initial forensics diagnosis
    - Who, what, where
  - The tools used to do the initial diagnosis
  - (DEXF & DFXML)

- Data items of interest
  - Notes them as byte-runs (DFXML)
  - Offset + length into data source
  - Wraps most things in a hash for integrity
Initial proposal schema

- Version
  - Major, Minor
- Site Name
- Examiner Name
- Evidence ID
- Creation Time
- Tool Name
- Tool Version
- Host Operating System

- Device
  - Device Type
  - Device Model
  - Device Serial
  - Sector Size
  - Device Sectors
  - Hash
    - Hash Type
initial schema continued

- File Object
  - Name
  - ID
  - Size
  - Partition
  - Mode
  - ACL
  - mtime
  - atime
  - ctime

- byte run
  - hash
    - hash type
    - hash size
    - hash value
cybox v0.7

- CybOX - Cyber Observables (http://cybox.mitre.org)
- Originally designed to support to other standards
- CAPEC - Common Attack Pattern Enumeration and Classification
- MAEC - Malware Attribute Enumeration
cybox v0.7 more observables

• Abstract file
  • unix file
  • windows file
• Semaphore
  • unix
  • windows
• Disk
• Disk Partition
• Windows
• Computer Account, Critical Section, Driver, Event Log, Event, Executable File, Kernel Hook, …
cybox object model

• Borrowed heavily from OpenIOC
• Contains lots of hints for malicious code (MAEC) and intrusions (CAPEC)
  • e.g. Ease of Obfuscation. Obfuscation Techniques
• Large underlying model for many SCAP / Making Security Measurable standards /
Cybox v1.0

- Being worked on now
- Working with Simson Garfinkle to extend CybOX v0.7 with DFXML
- Still basing many models on OpenIOC for data representation
Packaging and Transport Encapsulation for Exchange of Incident Data (IODEF)
- Incident & Exchange Context
- Additional Data

Packaging and Integrity Encapsulation for Exchange of Forensics Data (DEXF)
- Integrity mechanisms
- Ability to split and merge data across multiple files for transport

Forensic Data Analysis Contextual Packaging (DFXML)
- Analysis process-related data
- Forensic domain-specific data
- References to or inclusion of the raw evidence

Forensic Data Analysis Characterization (CybOX)
- Forensic data properties and context
- Granular analysis source context
Questions

• Does the working group want to adopt this?
• Other Authors?
• Do we want to wait on CybOX?
  • If so, what does that mean, how does that work?
• What model should forensics exchange