SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

SwA Forum Malware Working Group Update

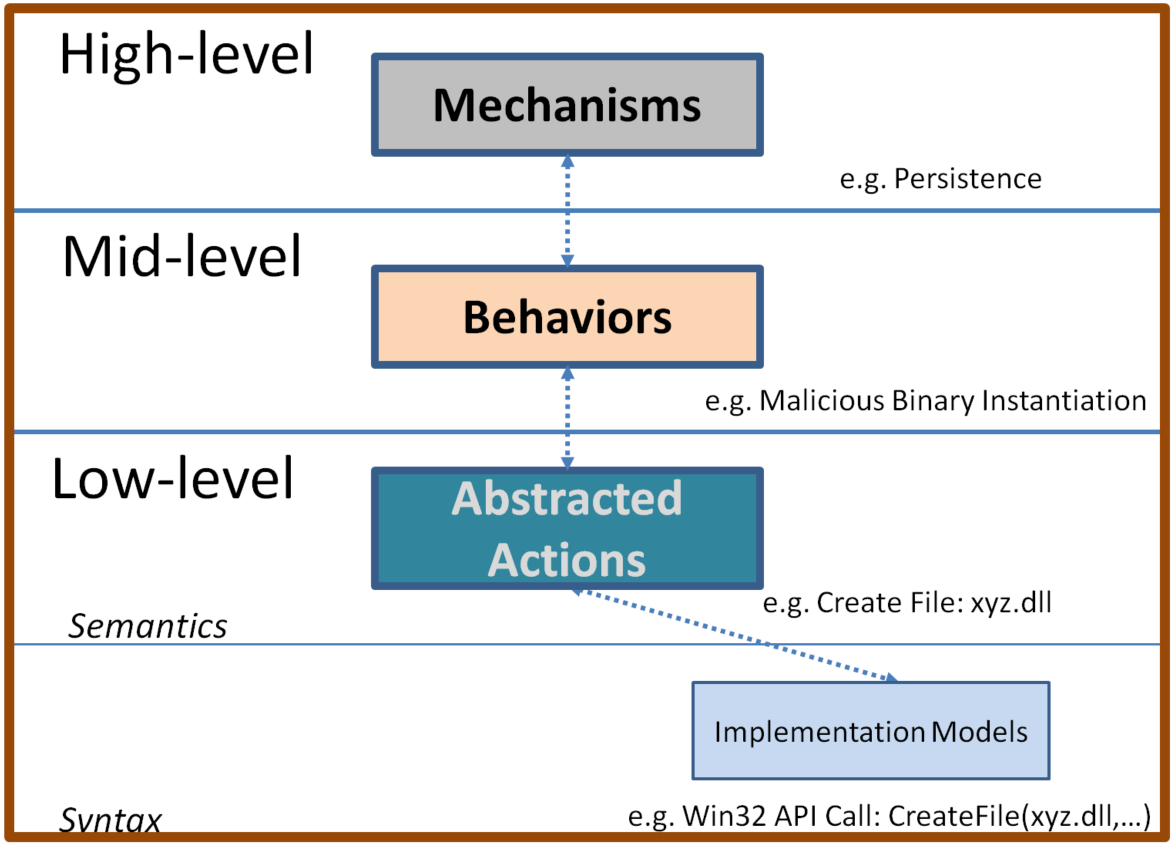
March 2011
Penny Chase

Homeland Security

Malware Working Group Goals

- Improve the analysis, characterization, collection, discovery & knowledge sharing of malware
- Develop standardized language for encoding and communicating high-fidelity information about malware based upon attributes such as behaviors, artifacts, and attack patterns
- Promote software security through balancing secure development (including architecture and deployment) and secure operations

MAEC Overview



Technical Activities

- MAEC Schema v 1.1 released
  - Added static malware triage elements (e.g., PE file attributes)
- Malware Ontology Development
- Collaboration with CAPEC and CEE teams to develop Cyber Observables schema

Technical Activities (Continued)

- Developed translators from dynamic malware triage tools to MAEC:
  - CWSandbox : GFI Software
  - ThreatExpert : Symantec
  - Anubis : International Secure Systems (Isec) Lab
- Developed MAEC → OVAL generator

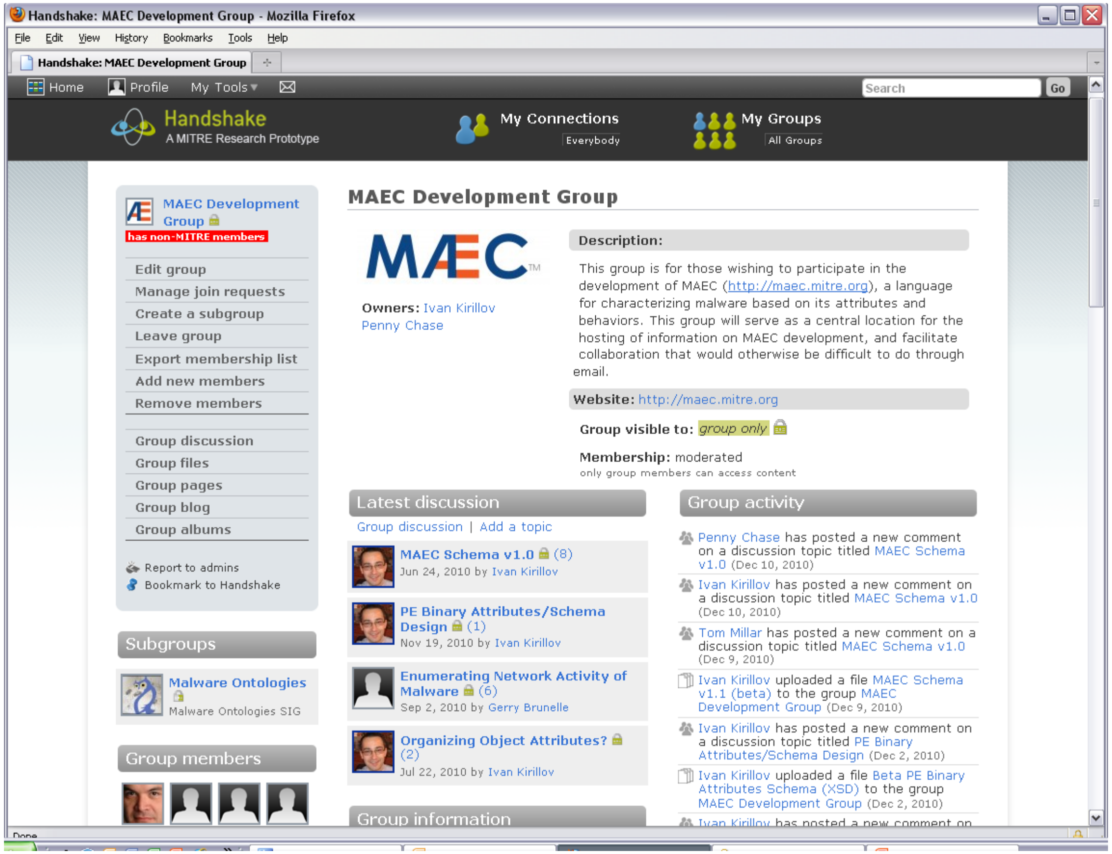
Community Engagement

- IEEE ICSG Malware Working Group
  - Developed Malware Metadata Exchange Schema to facilitate sharing samples between AV vendors
  - MAEC currently imports the IEEE ICSG Malware Metadata exchange schema
  - The MAEC team has been invited to join the WG and develop the next version of the schema
    - MAEC and Malware Metadata Exchange Schemas will refer to each other

Community Engagement (Continued)

- Dynamic Malware Triage tool vendors supported translator development
  - Some are planning on native MAEC support
- Working with Mandiant to incorporate openIOC in MAEC (this will now be done through Cyber Observables schema)
- Executing NDAs with vendors to discuss opportunities for MAEC

MAEC Development Handshake Group



MAEC Development Group

Owners: Ivan Kirillov
Penny Chase

Description:

This group is for those wishing to participate in the development of MAEC (http://maec.mitre.org), a language for characterizing malware based on its attributes and behaviors. This group will serve as a central location for the hosting of information on MAEC development, and facilitate collaboration that would otherwise be difficult to do through email.

Website: http://maec.mitre.org

Group visible to: *group only*

Membership: moderated
only group members can access content

Latest discussion

Group discussion | Add a topic

MAEC Schema v1.0 (8)
Jun 24, 2010 by Ivan Kirillov

PE Binary Attributes/Schema Design (1)
Nov 19, 2010 by Ivan Kirillov

Enumerating Network Activity of Malware (6)
Sep 2, 2010 by Gerry Brunelle

Organizing Object Attributes? (2)
Jul 22, 2010 by Ivan Kirillov

Group information

Group activity

Penny Chase has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 10, 2010)

Ivan Kirillov has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 10, 2010)

Tom Millar has posted a new comment on a discussion topic titled MAEC Schema v1.0 (Dec 9, 2010)

Ivan Kirillov uploaded a file MAEC Schema v1.1 (beta) to the group MAEC Development Group (Dec 9, 2010)

Ivan Kirillov has posted a new comment on a discussion topic titled PE Binary Attributes/Schema Design (Dec 2, 2010)

Ivan Kirillov uploaded a file Beta PE Binary Attributes Schema (XSD) to the group MAEC Development Group (Dec 2, 2010)

Ivan Kirillov has posted a new comment on

- MITRE hosts a social networking collaboration environment: https://handshake.mitre.org
- Supplement to mailing list to facilitate collaborative schema development
- Malware Ontologies SIG Subgroup

Future Plans

- MAEC Schema Development
  - Additional low-level attributes (e.g., Netflow, Layer 7 protocols)
  - Behaviors and mechanisms
  - Signature and Indicators of Compromise (IOCs) management
  - Mitigation and response support
  - Expressiveness (operators, constraints, relationships)