Análisis Forense Informático

Automatización de Procesamiento de Evidencia Digital

Martín Barrere Cambrún
CIBSI 2009 - Montevideo - Uruguay

TUTORES
Gustavo Betarte - Alejandro Blanco - Marcelo Rodríguez

Grupo de Seguridad Informática - Instituto de Computación - Facultad de Ingeniería
Universidad de la República - Montevideo - Uruguay

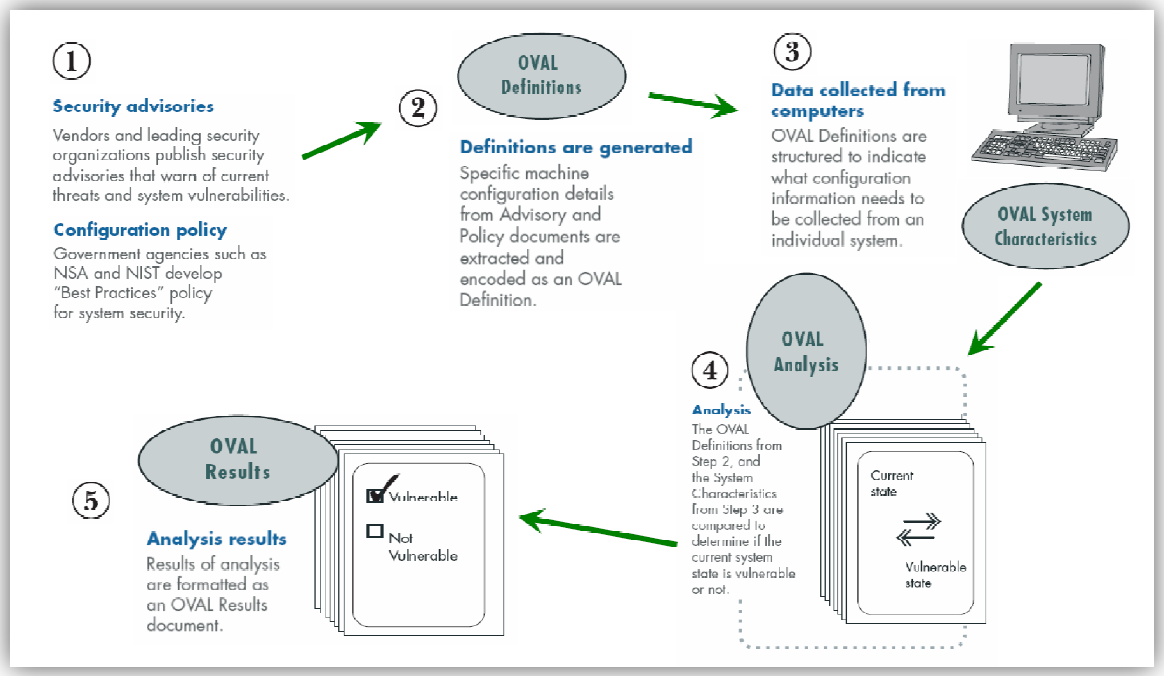
Análisis Forense Informático

- Objetivos.
  - Facilitar reconstrucción de eventos delictivos en un modo legalmente aceptable.
  - Anticipar acciones no autorizadas que puedan perturbar el curso normal de las operaciones.
- Etapas de una investigación.

- Tipos de evidencia.
  - Volátil. Es extremadamente importante; es necesario el uso de herramientas adecuadas; el procedimiento es muy ¨artesanal¨.
  - No volátil. Recuperación a más largo plazo, clonación de medios.

OVAL - Ovaldi

- OVAL (Open Vulnerability Assessment Language) es una colección de esquemas XML para representar información de sistemas; expresando estados de máquinas específicos y reportando resultados de evaluación.

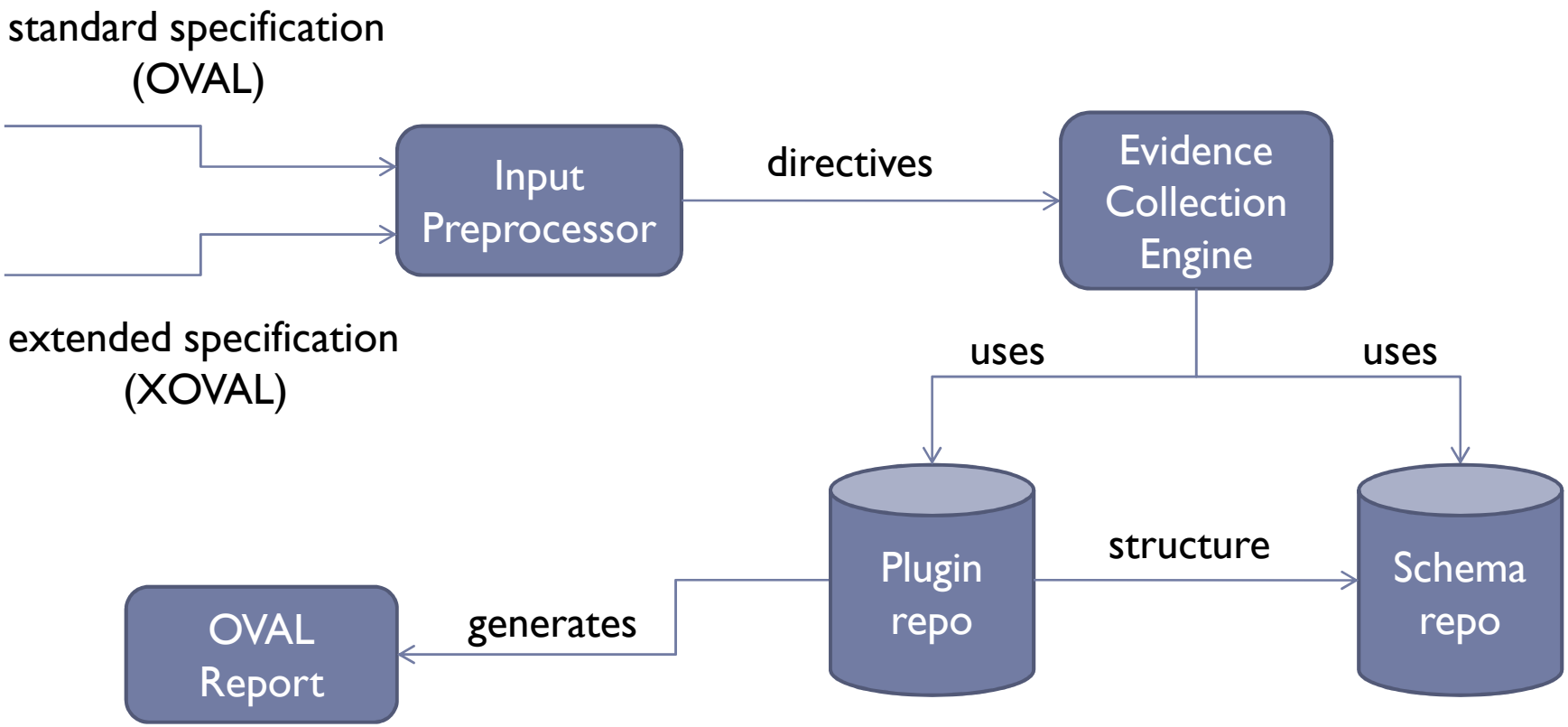


- Ovaldi. Intérprete de código abierto utilizado como implementación de referencia en la evaluación de definiciones OVAL.

Propuesta

- ¿Por qué OVAL?
  - Lenguaje desarrollado sobre un marco formal, altamente expresivo y poderoso.
  - Estándar orientado a la divulgación de contenido vinculado a la seguridad informática.
- Enfoque
  - Utilizar infraestructura OVAL para especificación de evidencia digital.
  - Un ataque puede ser visto como un proceso que afecta a un conjunto de componentes sobre un sistema operativo y un procedimiento forense como un conjunto de primitivas forenses que inspeccionan cada uno de los componentes afectados.
  - Queremos utilizar el mecanismo de definiciones y tests de OVAL para especificar Procedimientos Forenses.
- Objetivos
  - Extensión del lenguaje OVAL (XOval).
    - Aumentar el espectro de objetos o evidencia de interés soportada por OVAL.
  - Proveer un intérprete escalable(XOvaldi) que se adapte a la evolución del lenguaje OVAL y XOval.
  - Relevar impacto de la herramienta en el marco general de la actividad forense automatizada.

Arquitectura XOvaldi



Conclusiones

- ¿Dónde estamos?
  - Etapa de diseño de la herramienta.
- ¿Hacia dónde vamos?
  - Desarrollo de una herramienta de recolección de evidencia digital basada en especificaciones XOval para Linux y Windows.
- Trabajo a futuro
  - Mecanismo simple para generación de especificaciones XOval.
  - Recolección de evidencia remota mediante plugins (SNMP, Nagios).
  - Evaluación de la salida de la herramienta como entrada para componentes de análisis de evidencia.

Referencias

- DFRWS. A Road Map for Digital Forensics Research.
  - Digital Forensics Research Workshop, August 2001, Utica, New York.
  - http://www.dfrws.org/2001/dfrws-rm-final.pdf
- A Formalization of Digital Forensics
  - R. Leigland and A.W. Krings. International Journal of Digital Evidence, Vol. 3, Issue 2, Fall 2004.
- OVAL - Mitre
  - http://oval.mitre.org/