# An ontology-based intrusion alerts correlation system

Keywords: Alert Correlation, Intrusion detection, Ontology, System integration and implementation.

Phân loại về kĩ thuật intrusion alert correlation: có 3 loại chính

* Nhóm các alert vào các cụm khác nhau dựa trên sự tương đồng giữa các alert.
  + Nhanh + kết hợp các tấn công không biết trước.
  + Tuy nhiên, dựa trên các thông số được chọn lựa bởi chuyên gia, và không phù hợp để tìm ra được mối quan hệ nhân quả giữa các alert.
* Nhóm các alert dựa trên các kịch bản tấn công được định nghĩa trước.
  + Tự động xây dựng mô hình kết hợp cảnh báo.
  + Cần phải training cho mỗi lần triển khai, và mô hình kết quả có thể bị overfit bởi các kịch bản không có trong dữ liệu training.
* Mô hình cuộc tấn công bằng cách dựa vào tiền và hậu điều kiện.
  + Cần phải hiểu rõ về tất cả các cuộc tấn công khá kĩ để có thể hiểu được tiền và hậu điều kiện, phụ thuộc khá nhiều vào kinh nghiệm của chuyên gia và khó đáp ứng yêu cầu với các kiểu tấn công mới.

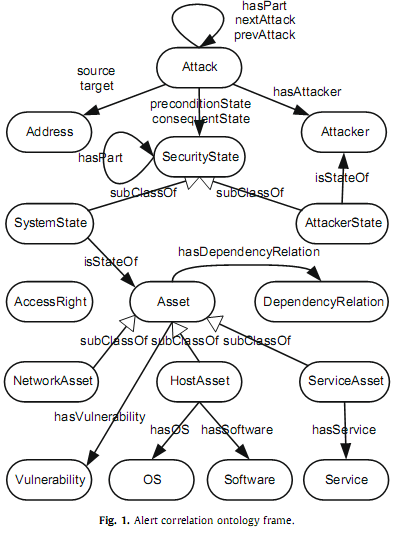
Paper này trình bày về Mô hình phân cấp kết hợp cảnh báo (*hierarchical compound alert correlation knowledge model HCACKM*) dựa trên 2 loại sau (kịch bản + tiền/hậu điều kiện) sử dụng Ontology và tập trung hiện thực hệ thống kết hợp cảnh báo.

Một vài kiến thức:

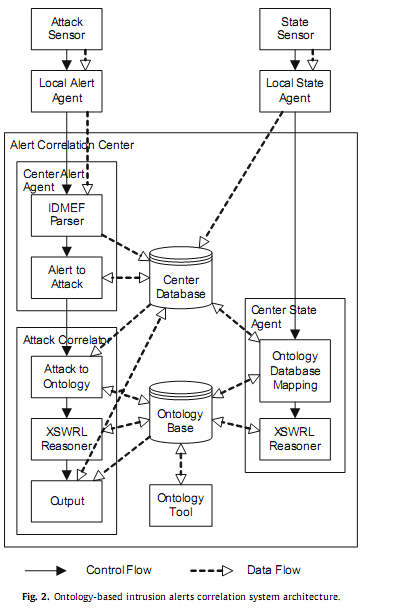
* OWL (We Ontology Language) dựa trực tiếp trên Desciption Logic (DL), gồm các thành phần cơ bản: class, property, restriction và individual.
* SWRL (Semantic Web Rule Language): kết hợp OWL và Rule Markup Language.
* XSWRL (Extended Semantic Web Rule Language): trong SWRL các biến có lượng từ là với mọi. Trong XSWRL giới thiệu thêm về lượng từ tồn tại 🡪 biểu diễn một số tri thức mới.

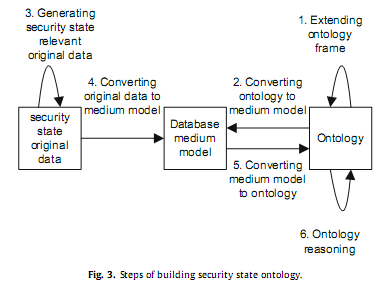
Ex: LeftShoe(?x) ^ RightShoe(?y) ^ color(?x, ?z) ^ color(?y; ?z) 🡪 Shoes(!a)^ hasPart(!a; ?x)^ hasPart(!a; ?y).

Khung sườn kết hợp cảnh báo dựa trên ontology này dựa trên HCACKM và biểu diễn bằng OWL, định nghĩa một số class, thuộc tính và ràng buộc cơ bản. Khi mở rộng các class và thuộc tính cơ bản này có thể thu được Knowledge Base về Alert Correlation Ontology.



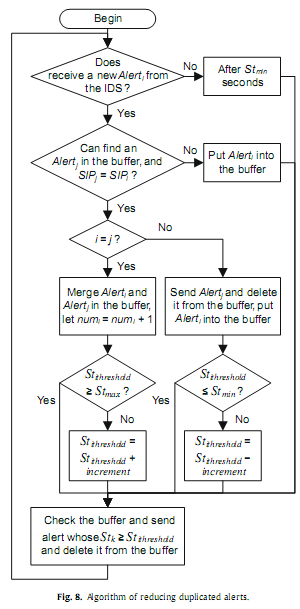
Từ trên hướng này, họ phát triển hệ thống kết hợp cảnh báo tấn công dựa trên ontology.





Tiền xử lý cảnh báo:

* Local Alert Agent: thực hiện các công việc sau:
  + Chuyển các cảnh báo IDS sang IDMEF
  + Gom cụm cảnh báo và merge các cảnh báo trùng nhau



* + Gửi các cảnh báo dạng IDMEF rút gọn về cho Center Alert Agent
* IDMEF parser: sử dụng dom4j để parse các đặc tả về IDMEF alert