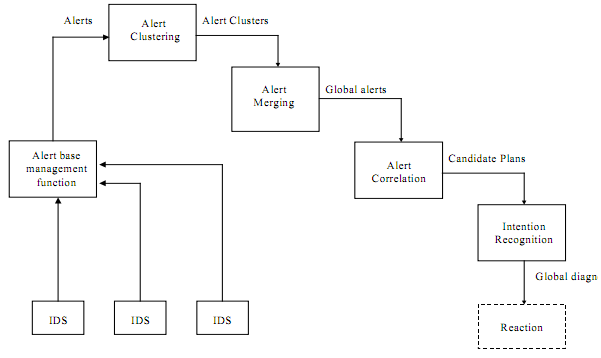
## Alert correlation in a Cooperative Intrusion Detection Framework

1. Giới thiệu:
   * Các phương pháp phát hiện xâm nhập
     + Anomaly detection (Behavorial approach)
     + Signature analysis (Misuse detection)
     + Đều tạo ra nhiều false positive
   * Giải pháp:
     + Kết hợp nhiều IDS lại và tổng hợp alert
     + Các alert được kết hợp vẫn còn ở mức đơn giản => correlate
2. Các khái niệm
   * Kiến trúc CRIM



* + - Alert base management function
      1. Nhận alert từ các IDSes
      2. Alert ở dạng IDMEF
      3. Chuyển sang dạng relational
    - Alert clustering
      1. Chuyển các alert ở trong DB sang cluster
    - Alert merging
      1. Sử dụng similarity (đọc rõ hơn trong [3])
      2. Mỗi cluster sẽ có 1 representative
    - Alert Correlation
  + Alert Modeling
    - Dùng IDMEF sau đó chuyển sang biểu diễn ở dạng logic
  + Attack specification
    - Dùng LAMBDA (trc đây nhóm mình đề xuất dùng CAML)
    - Attack sẽ có 5 fields
      1. Pre condition
         1. Chứa các predicate

Predicate để biểu diễn access\_level

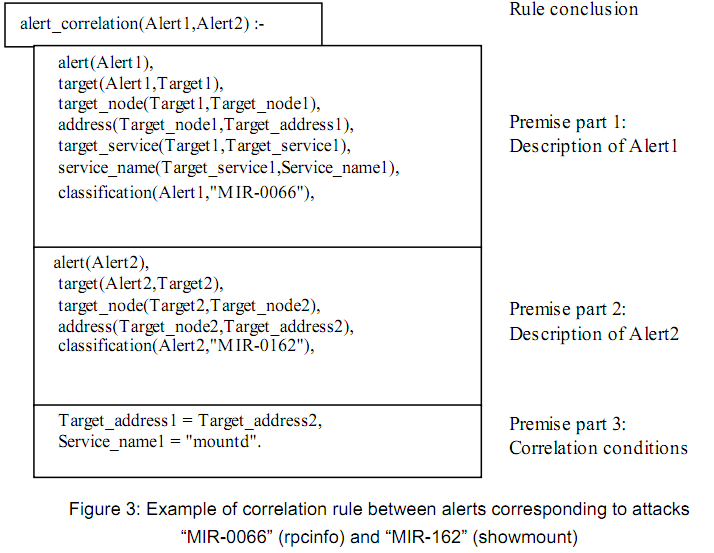
Predicate để biểu diễn effect của attack

Predicate biểu diễn tình trạng của hệ thống

Meta predicate: knows(x,y)

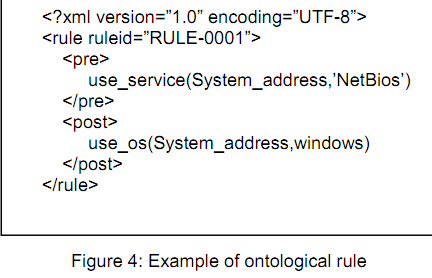
* + - * 1. Phép toán được sử dụng not và conjunction
      1. Post condition
         1. Chứa các predicate
         2. Phép toán được sử dụng not và conjunction
      2. Attck scenario: các event mà attacker dùng để tấn công. Thường ở dạng script
      3. Detection scenario: các sự kiện thể hiện sự tấn co6gn của attacker
         1. Sử dụng event calculus algebra
      4. Verification: nếu attack thành công thì có thể thực hiện để kiểm tra thành công hay không
         1. Sử dụng event calculus algebra

1. Explicit correlation
   * Tác giả cho rằng có 2 cách để correlate
     + Explicit: admin sẽ chỉ ra những sự kiện nào có liên quan
       1. Có thể áp dụng cho hệ thống của mình: admin chỉ ra giữa 2 node có liên quan
     + Implicit: sử dụng thống kê để xác định những sự kiện có liên quan
   * Cách biểu diễn
     + Dùng predicate: attack\_correlation(alert1,alert2)



* + Tác giả đề xuất cách tạo các correlation này 1 cách tự động gọi là semi-explicit correlation

1. Semi-explicit correlation
   * Ý tưởng chính: do đã biết trc các predicate có thể tạo được mapping alert nào sẽ thực hiện trc alert nào.
   * Phương pháp: có 3 trường hợp
     + Attack A có thể unified với Attack B thông qua mgu (most general unifier)
     + Chỉ có 1 số pre và post của attack A và B có thể unify thông qua mgu
     + Post của attack A có thể unify với pre của attack B gián tiếp thông qua 1 ontological rule



* + Sau đ1o tạo các correlation rules.
    - Các rules được tạo offline
    - Việc correlate sẽ thực hiện online

1. Một số ghi chú
   * Tác giả cho rằng nếu 1 node không được correlate thì là false positive
   * Tác giả cũng đề xuất 1 phương pháp prediction
     + Tương tự như cách nhóm mình đề xuất
   * Đối với các event mà alert không phát hiện được, tác giả dựa vào thông tin correlate để thêm vào (abductive correlation)