Correlation bằng tiền điều kiện và hậu điều kiện có thể phát hiện causal relationship giữa các alert và không bị giới hạn ở known attack scenario.

Framework:

1. Tiền điều kiện và hậu điều kiện

Dùng predicate làm thành phần cơ bản để tạo tiền và hậu điều kiện. Đối với các loại attack có những điều kiện phức tạp thì dùng các predicate có liên kết logical với nhau để diễn tả tiền điều kiện (liên kết or hoặc and). Ở đây chỉ dùng các possible tiền điều kiện và hậu điều kiện chứ không phải actual

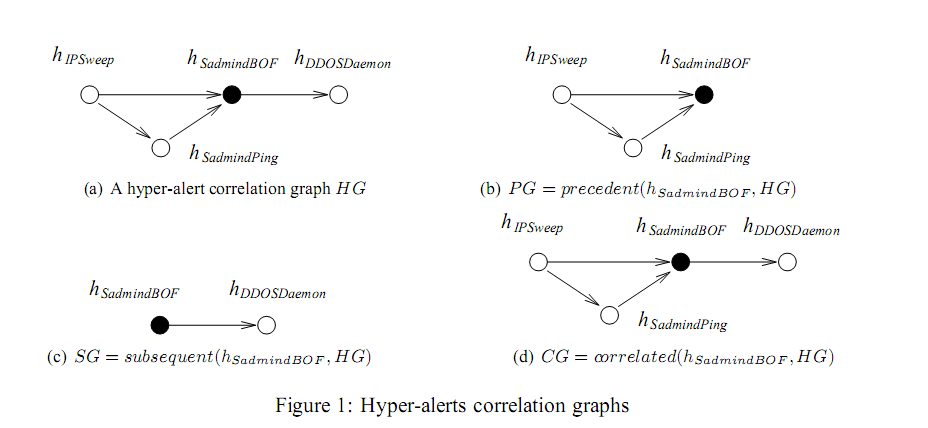
1. Hyper-alert type, hyper-alert and correlation graph

Hyper alert type được dùng để diễn tả tiền điều kiện và hậu điều kiện.

Một hyper alert type gồm fact, prerequisite, consequence. Fact bao gồm tập các attribute cùng với giá trị của nó, prerequisite, consequence là các kết hợp logical của predicates có các biến nằm trong fact. Consequence ở đây là kết quả có thể xảy ra khi tiền điều kiện đạt true.

Một hyper alert là một instance của một hyper alert type khi các tuple trong fact có cùng một interval-base timestamp. Các variable của tiền điều kiện và hậu điều kiện phải nằm toàn bộ trong fact.

Khi correlate các hyper-alert, các consequence của earlier hyper alert và prerequisite của later hyper alert sẽ được phân ra các predicate, và chỉ cần một trong số các predicate này true thì 2 hyper-alert sẽ được correlate (dựa vào time interval để so sánh).



Correlation graph được chia thành các grap nhỏ hơn vì trong thực tế không phải lúc nào toàn bộ các node trong correlation graph cũng miêu tả sự tấn công của attacker

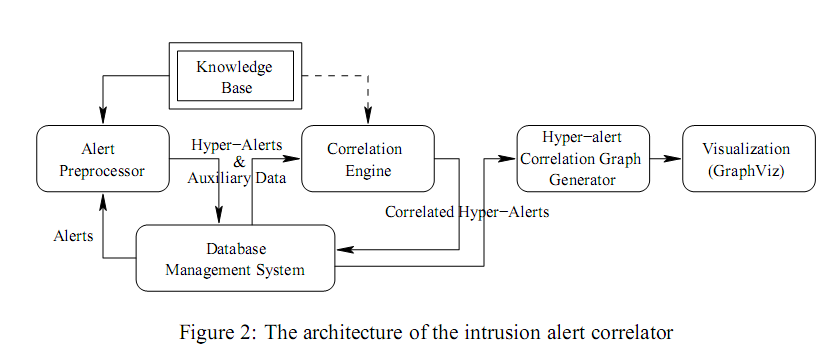
1. Pros and cos:

Dựa vào high level của correlated alerts có thể xây dựng được causal relationships.

Có khả năng giảm tác động của các false alert .

Không phụ thuộc vào các scenario được định nghĩa trước để phát hiện attack. Ngoài ra hệ thống còn có thể correlate alert đối với các fail attack, và miss alert của IDS ( đôi khi correlate các không được chính xác khi một tấn công để chuẩn bị cho một tấn công khác, không thể phát hiện được 2 attack khác nhau của cùng 1 user)

1. Architecture



KB chứa những thông tin cần thiết của hyper-alert types và implication relationship giữa các predicate.

Các predicate được tạo từ string, do dó vấn đề alert correlation được chuyển thành string match.

Áp dụng 2 khái niệm soundness và completeness để xác định độ chính xác, khi gặp nhiều alert giống nhau của cùng một attack, hệ thống sẽ xử lý như là những alert riêng biệt.

Bỏ các false alert bằng cách bỏ các alert ko được correlate lại