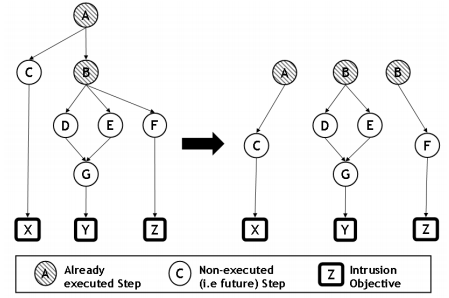
# Success Likelihood of Ongoing Attacks for IDPS

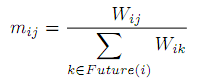
1. Introduction:
   1. Các thành phần của risk analysis (không rõ reference)
      1. Khả năng thành công của attack
         * Hướng đi của paper này
      2. Mức độ ảnh hưởng của attack và các phương pháp counter
         * Nhiều IDS đi theo hướng này
   2. Framework về risk analysis[6]
   3. Ý tưởng: thời gian tấn công cần thiết càng lâu thì khả năng thành công càng thấp.(dựa trên cryptography)
   4. Các bước thực hiện:
      * Xây dựng attack graph cho mỗi sự thay đổi
      * Chia attack graph thành các sub graph dựa trên objective
      * Tạo markow model từ các sub graph
      * Tính toán success likelihood dựa trên markov model
2. Mô hình
   1. Tác giả giới thiệu về các phương pháp correlate
      * Implicit: thống kê
      * Explicit: whole attack scenario
      * Semi-explicit: pre-post
        + Flexible
        + Generic
        + Tác giả dùng LAMBDA (thực ra vì có cùng tác giả là Cuppens)
   2. Ngôn ngữ LAMBDA: chứa các fields
      * Pre
      * Post
      * SK\_Level chỉ kiến thức ít nhất cần thiết để thực hiện step (knows meta-predicate)
        + A dễ hơn B thì SK\_A > SK\_B
      * Dectection
      * Verification
   3. Các hướng để response(không rõ reference)
      * Contextual
        + Không rõ
        + Có vẻ là thiết lập các policy
      * Anti-correlation
        + Chuyển 1 predicate của pre sang false
        + Tác giả chỉ tiếp cận hướng này và nói rằng hướng của tác giả phù hợp với cả 2 cách nhưng xài hướng này vì limited space.
3. Tính toán success likelihood
   1. Chia attack graph tahnh2 các subgraph
      * Tách subgraph dựa trên intrusion objective
      * Subgraph chứa
        + Future node: các node dẫn đến intrusion objective
          - Cách xây dựng không nói rõ
          - Có vẻ là dùng match như trong paper của Cuppens
        + Các node đã thực hiện mà kề với các future node



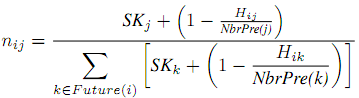
* 1. Chuyển subgraph sang Markov Model
     + Dựa trên assumption: xác xuất để thực hiện 1 elementary attack trong 1 khoảng thời gian < t là 1 phân phối 
     + Cách tính xác suất để chuyển từ 1 node i sang node j(i đã thực hiện, j future node):
       - =0 nếu i và j không nối với nhau trên graph
       - Unified(i,j): số predicate được (có thể ???) unified của Post(i) và Pre(j)
       - NbrPre(j): số predicate của Pre(j)
       - : correlation weight của node i và j
       - Hij số predicate của Pre(j) bị false
       - Future(i) số future node mà kề với node i



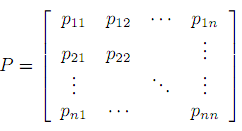
* + - * mij: xác suất thực hiện j trong các future node của i



* + - * nij: xác suất node j dễ hơn các future ndoe khác



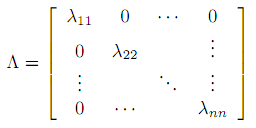
* + - * Từ subgraph có n node sẽ xây dựng transition probabilities matrix



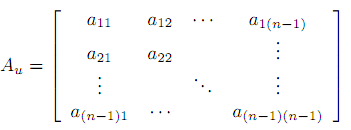
* + - * Tính lamda: exit rate from the state i ???



* + - * Xây dựng ma trận exit rate



* + - * Tính ma trận Markov Model (n x n): 
        + Ma trận này có hàng và cột n = 0 do đây là các giá trị của intrusion objective => bỏ các cột và hàng n => ma trận An



* + - * Tính Mean Time to Intrusion Objective (MTIO)(thời gian trung bình để tấn công tới objective)
        + MTIO của X < MTIO của Y (X và Y là các objective) <=> xác suất thành công của X cao hơn Y
        + 
        + Ma trận S là ma trân 1 hàng n-1 cột: biểu diễn tình trạng của subgraph Markov Model. Tính như sau:

Có 1 step đã được thực hiện: S=[1,0,0,...0]

Có 2 step: S=[1/2,1/2,0,0,0...0]

Tương tự cho 3,4,5...

* 1. Tính toán success likelihood và response
     + Tác giả lấy log của MTIO để xác định (không rõ: tác giả cho là similar như các đại lương vật lý V, I,...)
     + 
     + Lx là giá trị sẽ được dùng.
     + Lx<Ly<Lz thì Z sẽ nguy hiểm nhất được response sớm nhất => Y => X

Các assumptions:

* Các attack đều có cùng impact (thành phần thứ 2 như nhau)
* Các attack đều không intentional cho nên tác giả không cần quan tâm đến ý định của attacker
  + Vì nó là không rõ với cả attacker
  + Có paper nói về việc unintentional

Các lưu ý

* Không rõ cách tác giả xác định future node
* MTIO luôn < 1 : ý nghĩa thực tế của nó ?
* Có nhiều paper về phần risk analysis