State-based models

Attack trees:

do not capture the dependence of security vulnerability on sequences of attaks

State space stochastic methods

Dependence of security vulnerability on sequences of events

state-based methods application in security context

ADversary VIew Security Evaluation - ADVISE

These set of slides are based on the paper:
E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders and C. Muehrcke, "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)," *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, Aachen, 2011, pp. 191-200.

ADversary VIew Security Evaluation - ADVISE

Main objective:
- Compare security strenght of different system architectures
- Analyse threats by different adversaries

1. Executable state-based security model of a system

2. An adversary (how the adversary can attack the system)

3. Results of the attack

Basic point:

attack decision function

how the adversary selects the most attractive next attack step by
- using the adversary attack preferences and the possible attacks

Attack Execution Graph - AEG

Attack execution graph (AEG)

<A, R, K, S, G>

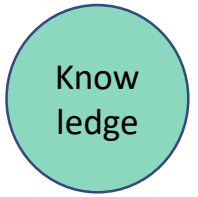
Mobius tool

https://www.mobius.illinois.edu/

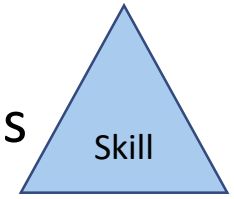
A: set of attack steps

R: set of access domains in the system

K: set of knowledge items relevant to attack the system

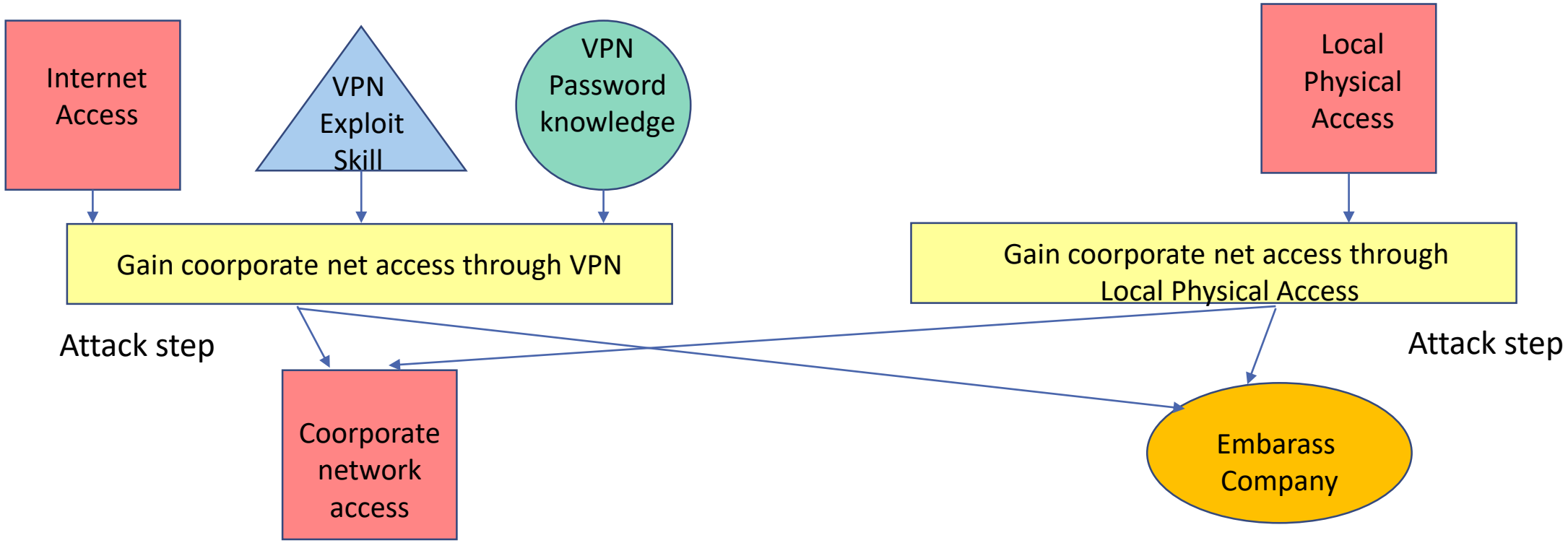


S: set of the adversary attack skills



G: set of adversary attack goals revelan to to the system

ADVISE: AEG



Example of AEG taken from paper

E. LeMay, M. D. Ford, K. Keefe, W. H. Sanders and C. Muehrcke, "Model-based Security Metrics Using ADversary VIew Security Evaluation (ADVISE)," *2011 Eighth International Conference on Quantitative Evaluation of SysTems*, Aachen, 2011, pp. 191-200.

Attack Step

$a_i = <B_i, T_i, C_i, O_i, Pr_i, D_i, E_i>$

X is defined as the set of all reachable model states

$X = \{s1, \ldots, sn\}$

B_i: X ->{true, false}
precondition to check if the attack is enabled
The adversary has the access, the knowledge, and/or skill needed for the attack and the adversary does not have what can be gained when the attack is executed with success

T_i: X x R+ -> [0,1]
time required to execute the attack.
T_i (s) is a random variable defined over a prob. distribution function

C_i: X -> $R^{>=0}$
cost of attempting the attack

O_i:
finite set of outcomes (e.g., success and failure)

Pr_i: X x O -> [0, 1]
prob. of outcome o after the attack
(Σ_o Pr (s, o) = 1)

D_i: X x O -> [0, 1]
probability that the attack is detected when outcome o occurs

E_i: X x O -> X
next state when the outcome o occurs

Attack Step do-nothing

a_{DN} = do-nothing

B_{DN}
precondition is always true

T_{DN}
time between two occurrences of do nothing

C_{DN}
cost is zero

D_{DN}
detectability is zero

$E_{DN}(s,o) = s$
the next state is the same of the current state

$Pr_{DN}(s, o) = 1$
there is only one outcome, with probability 1

Every AEG contains the aDN attack step

there is always at least one attack step in the AEG whose precondition is satisfied

Model state s

A state s in X reflects the progress of the adversary in attacking the system

$s = < R_s, K_s, G_s >$

R_s : set of domains that the adversay has access

K_s : set of knowledge of the adversary

G_s : set of attack goals achieved by the adversary

Adversary Profile

Adversay Profile = $< s_0, L, V, w_C, w_P, w_D, U_C, U_P, U_D, N >$

s_0: initial state of the model

L: attack skill level function

V: attack goal value function

w_C, w_P, w_D : attack preference weights for cost, payoff, detection probability

U_C, U_P, U_D: utility functions for cost, payoff, detection probability

N: planning horizon

Adversary Profile

Adversay Profile = < s_0, L, V, w_C, w_P, w_D, U_C, U_P, U_D, N>

s_0: starting point of the adversary attack
different for insider (more access and knowledge) and outsider adversary

L is the attack skill level function
L : S -> [0, 1] maps each attack skill to a value in [0, 1] (proficiency of the adversary)

V is the attack goal value function
V: G -> $R^{>=0}$, monetary value of each attack goal in the AEG from the adversary viewpoint , more valuable -> larger value

Payoff value P(s) of a state s is a function of the value of all goals V(g) achieved in the model state P(s)= f(V(g))

Adversary Profile

Adversay Profile = < s_0, L, V, w_C, w_P, w_D, U_C, U_P, U_D, N>

Attack preference weight: attactiveness in each of the three criteria when deciding an attack. They are a value in [0,1]

W_C: relative attactiveness of decreasing the cost in attemping the attack step

W_P: relative attactiveness of increasing the payoff for successfully executing the attack step

W_D: relative attactiveness of decreasing the probability of being detected during or after the attack

Adversary Profile

Adversay Profile = < s_0, L, V, w_C, w_P, w_D, U_C, U_P, U_D, N>

Utility functions: map the native value of each attractiveness criterion to a [0, 1] utility scale (higher utility values represent more desirable values)

U_C: $R^{>=0}$ -> [0, 1] map the monetary value of the attack step cost to a [0, 1]
lower cost - higher utility value

U_P: $R^{>=0}$ -> [0, 1] map the monetary value of the attack step payoff to a [0, 1]
higher payoff - higher utility value

U_D: [0, 1] -> [0, 1] map the probability of attack step detection to a [0, 1]
lower detection probability - higher utility value

ADVISE model: execution

A_s is the set of available attack steps a_i in state s:
the attack steps whose precondition is satisfied ($B_i(s)$=True)

The attractiveness of the all available attack steps is evaluated from the viewpoint of the adversary with the criteria

- Cost
- Detectability
- Expected payoff in the next state

Attack preference weights in the adversary profile are used

ADVISE model: execution

Short sighted adversary

$$attr(a_i, s) = w_C\, C_i(s) + w_P\, P_i(s) + w_D\, D_i(s)$$

linear combination of adversary preferences weights with the data about attack step

$$P_i(s) = \Sigma_o\, (P(E_i(s,o)) \,.\, Pr_i(s, o)) \qquad D_i(s) = \Sigma_o\, (D_i(s,o) \,.\, Pr_i(s, o))$$

$P_i(s)$: expected payoff

$P(E_i(s,o))$: Payoff in the next state reached by outcome o (Ei(s,o))

$\beta(s)$ best next attack step

$$\{a^* \text{ in } A_s \mid attr(a^*, s) = \max\ attr(a_i, s) \text{ forall } a_i \text{ in } As\ \}$$

one of the maximally attractive steps is chosen uniformely

ADVISE model: execution

Utility function U_C U_P U_D are not shown in attr(a_i, s) for semplicity
They should be applied to move towards a common unit of utility.

$C_i(s)$ ---- U_C ($C_i(s)$)
$P_i(s)$ ---- U_P ($P_i(s)$)
$D_i(s)$ ---- U_D ($D_i(s)$)

Ci(s) =2.01 million
Ci(s')=2.05 million
Better mapped -> same utility value

Ci(s) =10.000
Ci(s')=50.000
better mapped -> two distinct utility values

An attack step outcome is randomly generated using the probabilities distributions

The attack step outcomes determine the sequence of state transitions

ADVISE execution algorithm

ADVISE model execution algorithm

Time <- 0
State <- 0
while Time < τ do
    $Attack_i$ <- β(State)
    Outcome <- o,
    Time <- Time +t,
    State <- Ei (State, Outcome)
end while

ADVISE metrics specification

State metrics $< \tau, \lambda, \sigma >$

τ is the end time $[0, \tau]$

λ is the type of state metrics :

EndProb: state occupacy probability at time τ with $\sigma(s)$=True

AvgTime : average amount of time spent in state such that $\sigma(s)$= True in the interval $[0, \tau]$

σ is the state indicator function: s= <R, K, G>

$\sigma(s)$ returns True, for states of interest

e.g., $\sigma(s)$ = true if goal g1 has been achieved

ADVISE metrics specification

Event metrics $< \tau, \delta, \varepsilon >$

τ is the end time $[0, \tau]$

δ is the type of event metrics : let ε a set of events

Freq: the number of occurrences of events in ε in the interval $[0, \tau]$

ProbOcc : prob. that all the events in ε occur at least once in the interval $[0, \tau]$

ε is a set of events in the model
(attack steps, attack step outcomes, access domains, knowledge or goals)

Example
Frequency of attack step a_i in the interval $[0, \tau]$
ε is equal to $\{a_i\}$

ADVISE model

In the paper:

- more sophisticated adversary decision with a long range planning attack decision function are shown (State Look-Ahead Tree)

- A case study on a SCADA (Supervisory Control and Data Acquisition) architecture is analysed: 2 variants of the architecture and 4 different profiles of adversaries.