Beyond attack trees:

Dynamic security modeling with BDMP (Boolean logic Driven Markov Processes)

April 29th 2010

EDCC-8 (2010), Valencia, Spain

Ludovic Pièrre-Cambacédès

Marc Bouissou

EDF R&D

LEADING THE ENERGY CHANGE

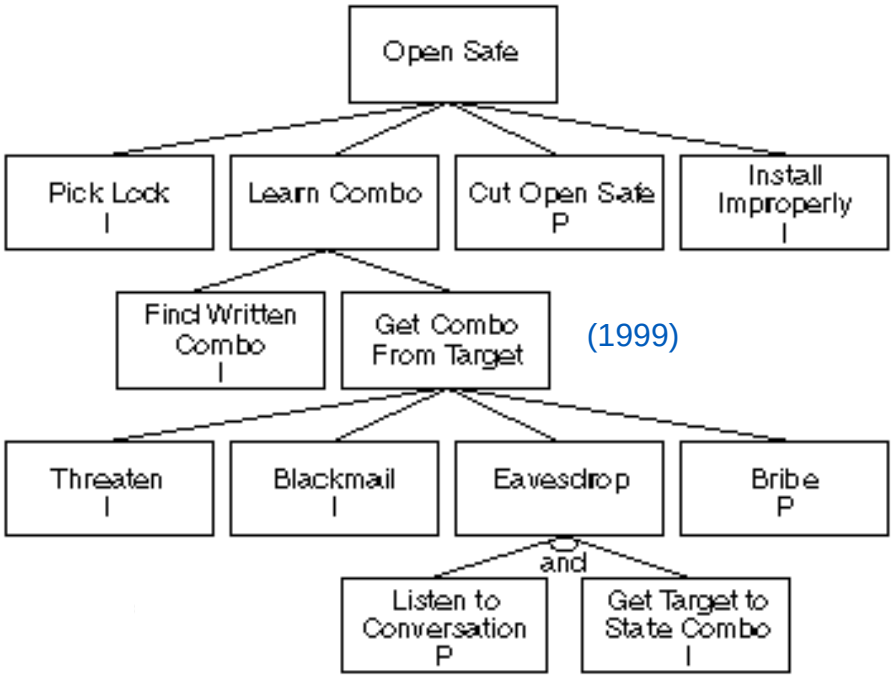
Agenda

- **Introduction**
  - Graphical attack modeling
- **Security modeling with BDMP**
  - Formalism description
  - Example & quantifications
  - Advanced modeling
- **Comparison**
  - Attack trees and Petri-nets
- **Perspectives**

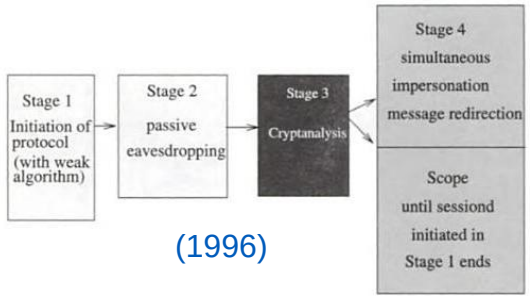
Introduction

Computer attacks graphical modeling (1/2)

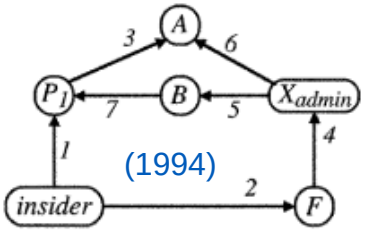
- Graphical representation of an attack process
  - Formalize reasoning
  - Share vision and analysis
  - Support quantification
  - Help security decision
- An active field of research



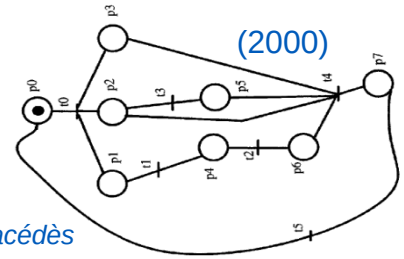
(1999)



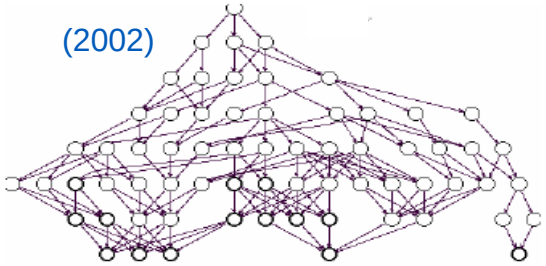
(1996)



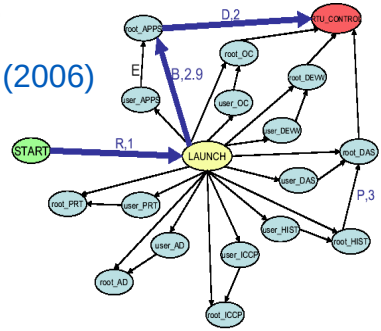
(1994)



(2000)



(2002)



(2006)

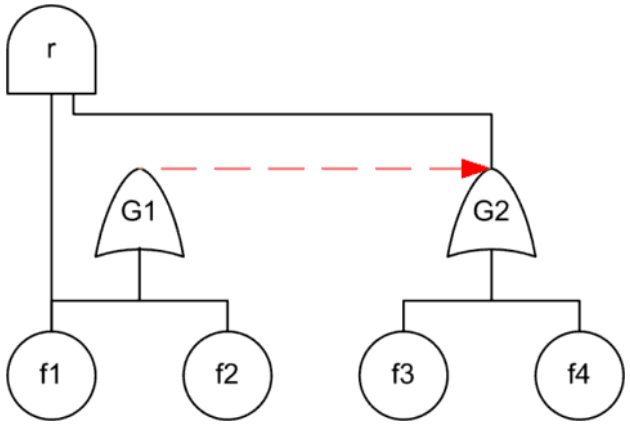
Computer attacks graphical modeling (2/2)

Type	Family	Model names (examples)
Static	Attack trees (A.T.)	Threat tree, Vulnerability tree , Augmented vulnerability tree, Defense tree , Protection tree
	Bayesian networks (BN)	Defense graph, B.N.-attack graph
Dynamic "Low-level" (State-graphs)	*Stochastic models*	*Privilege graph, Compromise graph, State-Space predator model*
	Model-checking enabled	*Attack graph, Logical attack graph, Coordinated attack graph*
Dynamic "High-level" (Compact)	CAD	Phillips *et al*, Goal-inducing attack chain
	Petri net-based	Attack net, PENET (Petri net attack modeling)
	Dynamic BN-based	Frigault *et al*
	DFT-based	Khand *et al*

- Different balances between readability, scalability, modeling power and quantification capabilities

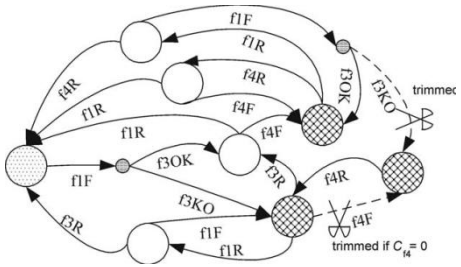
BDMP, the potential for an attractive trade-off

- Interest proven in reliability and safety engineering



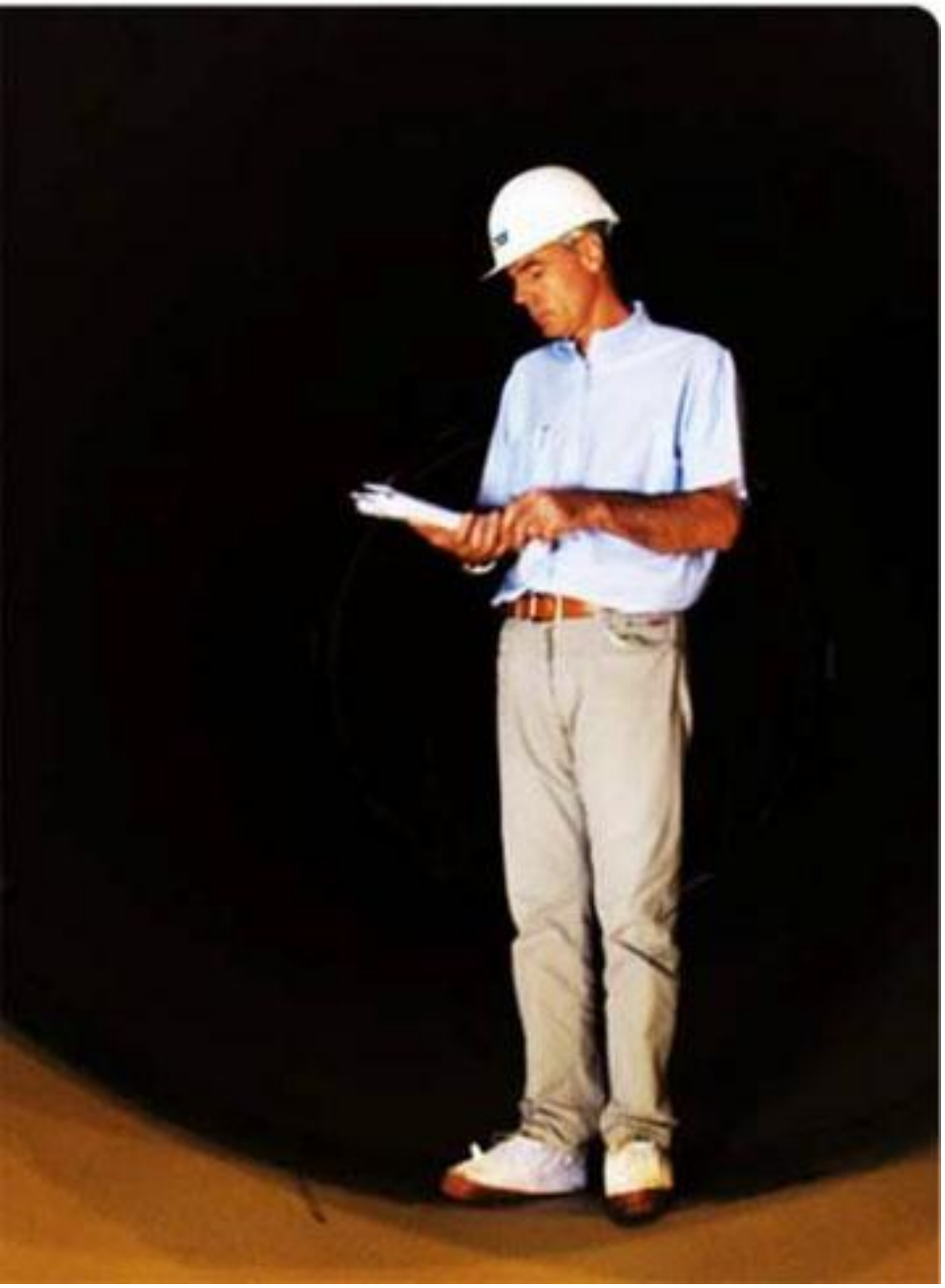
- ✓ Dynamic
- ✓ Readable
- ✓ Tractable

A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov Processes *Reliability Engineering and System Safety*, Vol. 82, Issue 2, Nov. 2003, pp.149-163



- Invented and used at EDF (NPP safety, substations, data centers reliability,…)
- Complete theory and software framework

⇒ Adaptation to security modeling



Theoretical basis & Attack modeling

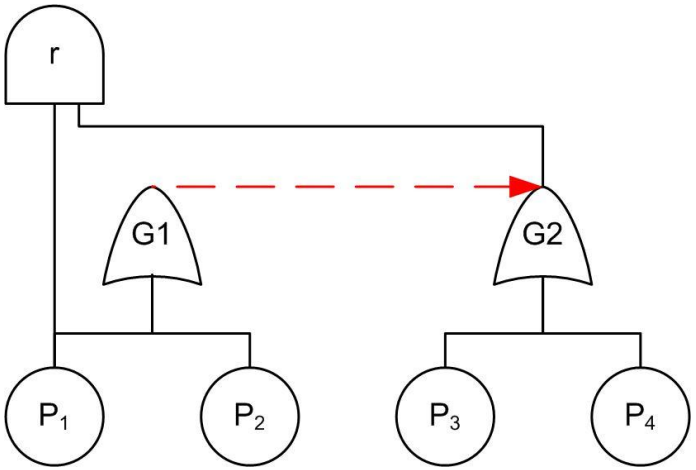
BDMP in a nutshell – Original definition

- Main ideas
  - New semantics to the graphical representation of fault trees
  - Markov processes are associated to the leaves (components)
    - Two modes (“required” and “not required”)
    - Mode of a leaf = f (states of some selected other leaves)
  - Dynamic, model dependencies
- Graphical elements
  - BDMP = $\{\mathcal{F}, r, T, \{P_i\}\}$

$\mathcal{F}$ = Fault tree, r = top event,

G1 = secondary top, T = trigger,

P_i =“triggered” Markov processes



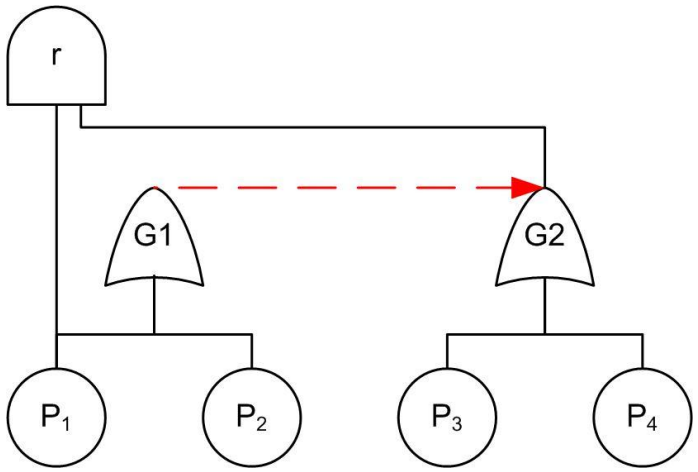
BDMP - Application to attack modeling

- Main ideas
  - New semantics to the graphical representation of attack trees
  - Markov processes are associated to the leaves (actions/events)
    - Two modes, “Active” and “Idle”
    - Mode of a leaf = f (states of some selected other leaves)
  - Dynamic, model attack sequences
- Graphical elements
  - BDMP = $\{\mathcal{A}, r, T, \{P_i\}\}$

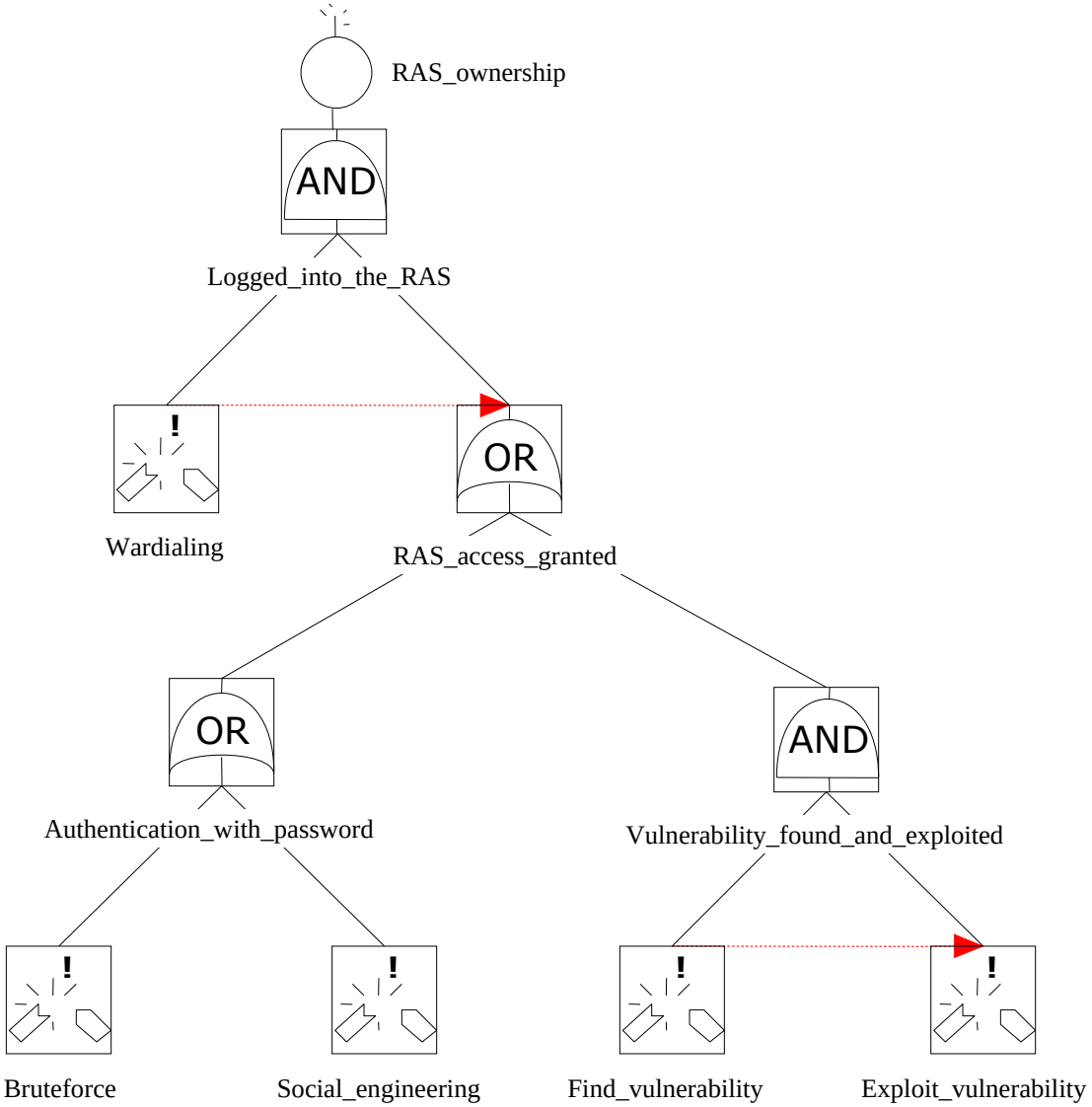
$\mathcal{A}$ = Attack Tree, r = top event,

G1 = secondary top, T = trigger,

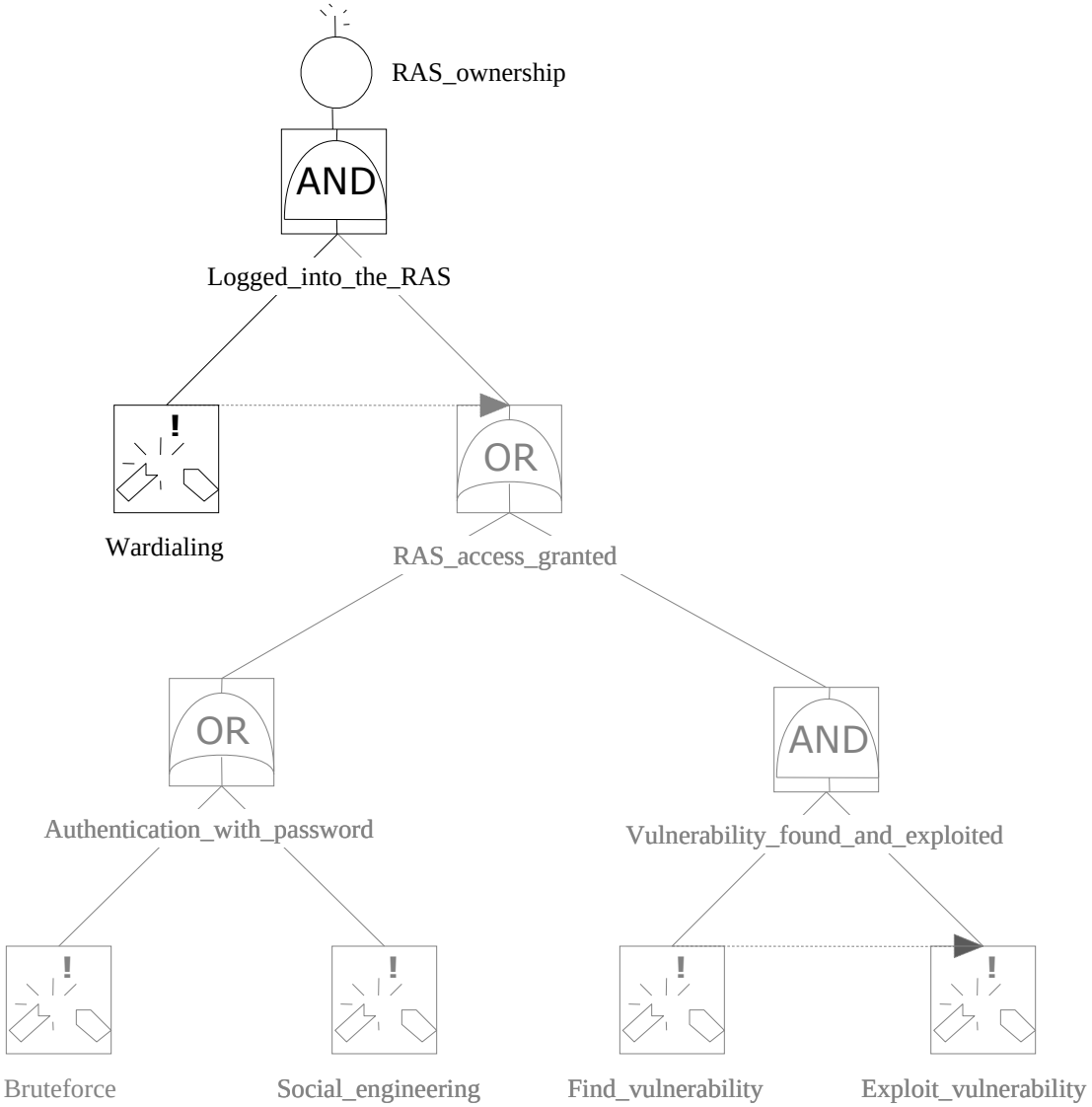
P_i =“triggered” Markov processes



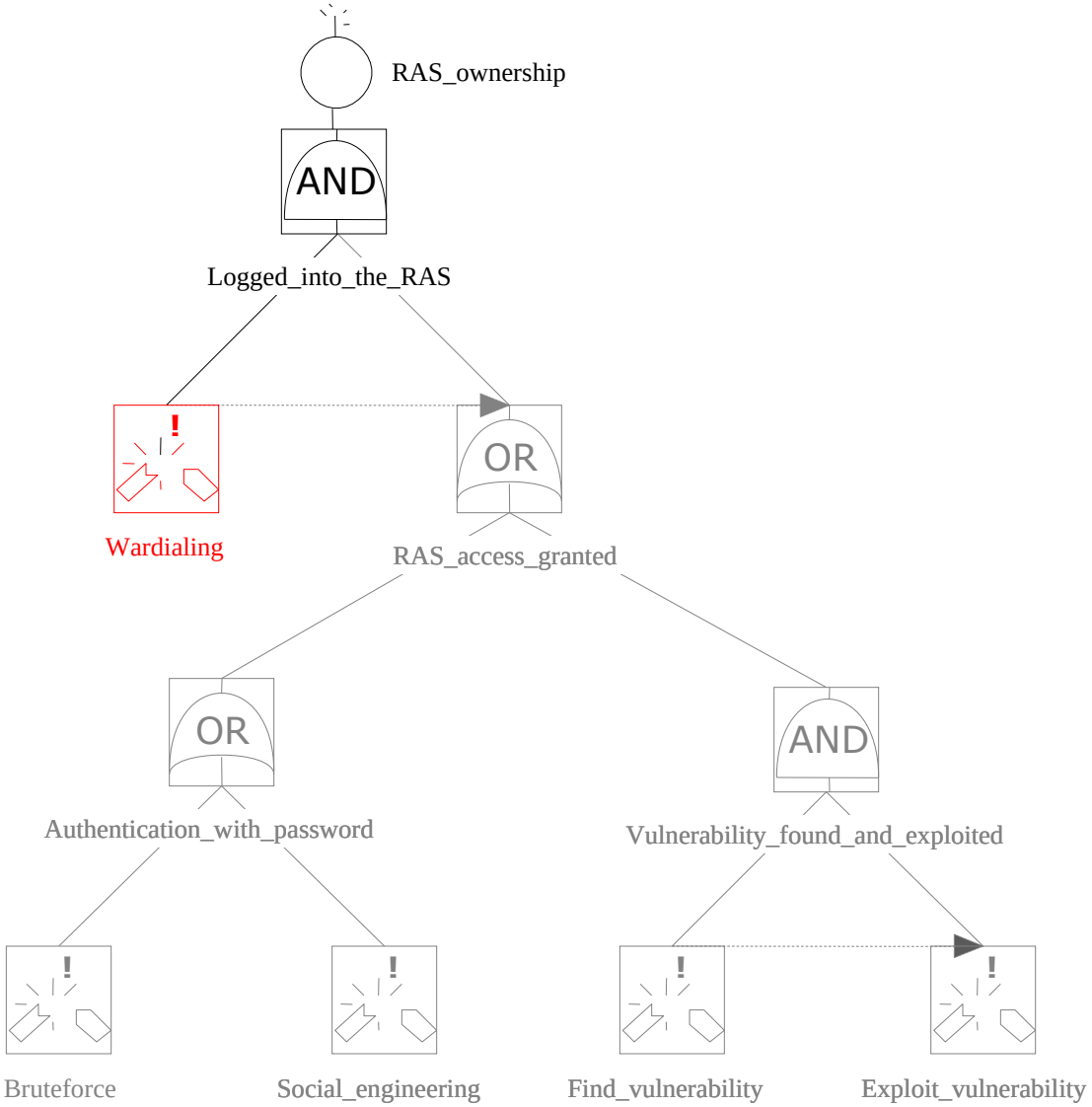
A first feel: a simple Remote Access Server attack



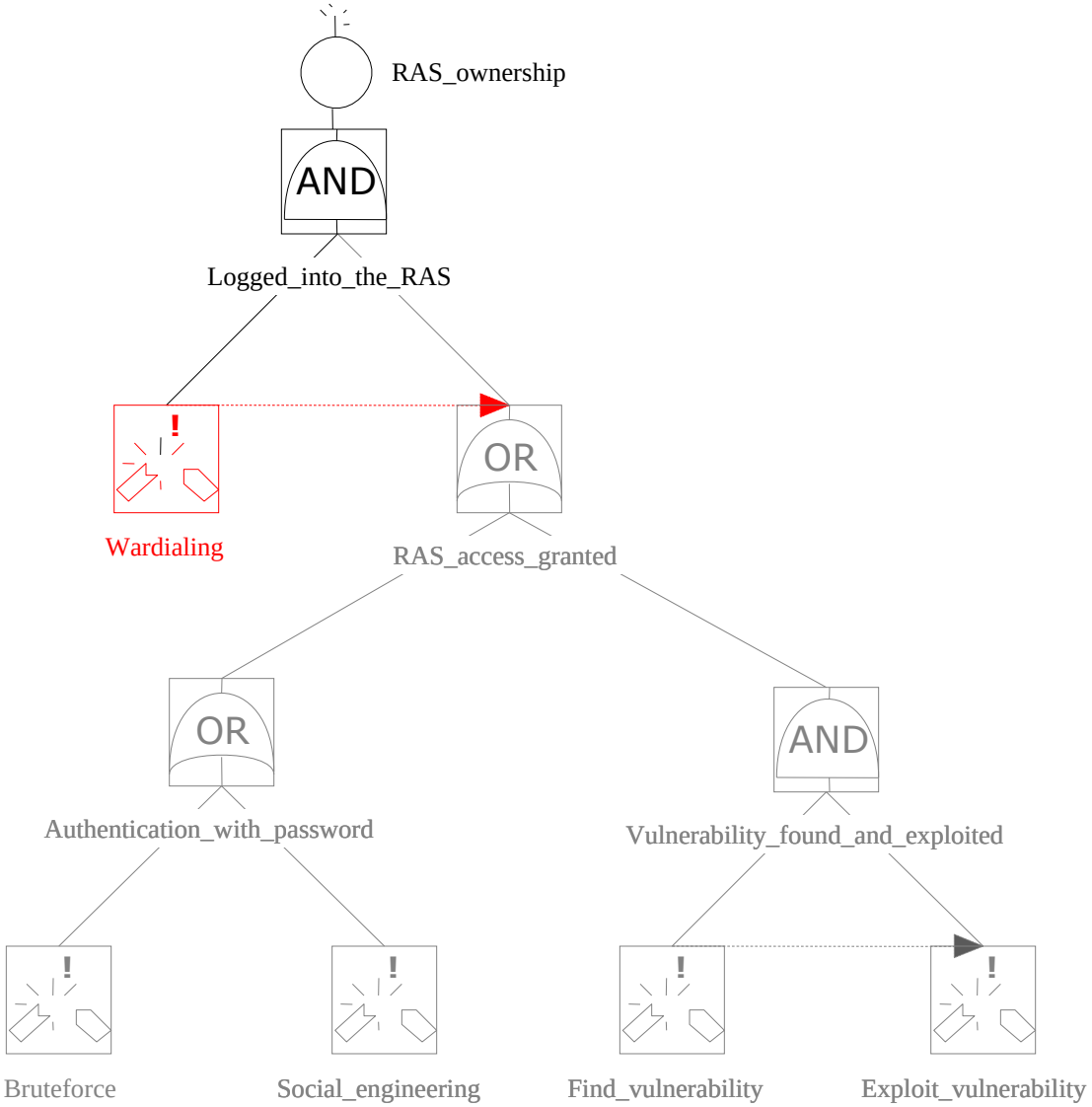
RAS attack BDMP – Step 0 (attack just started)



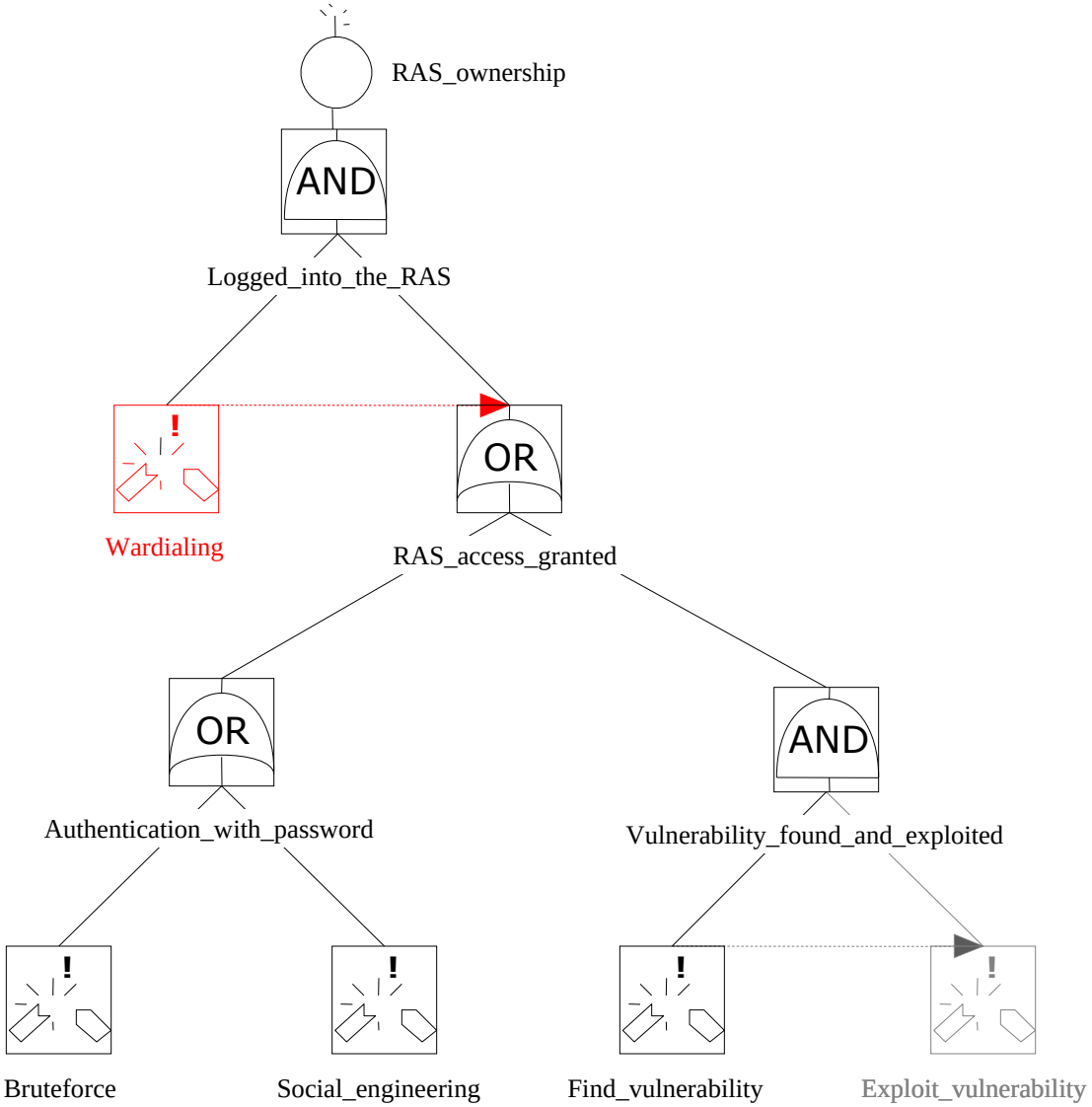
RAS attack BDMP – Step 1



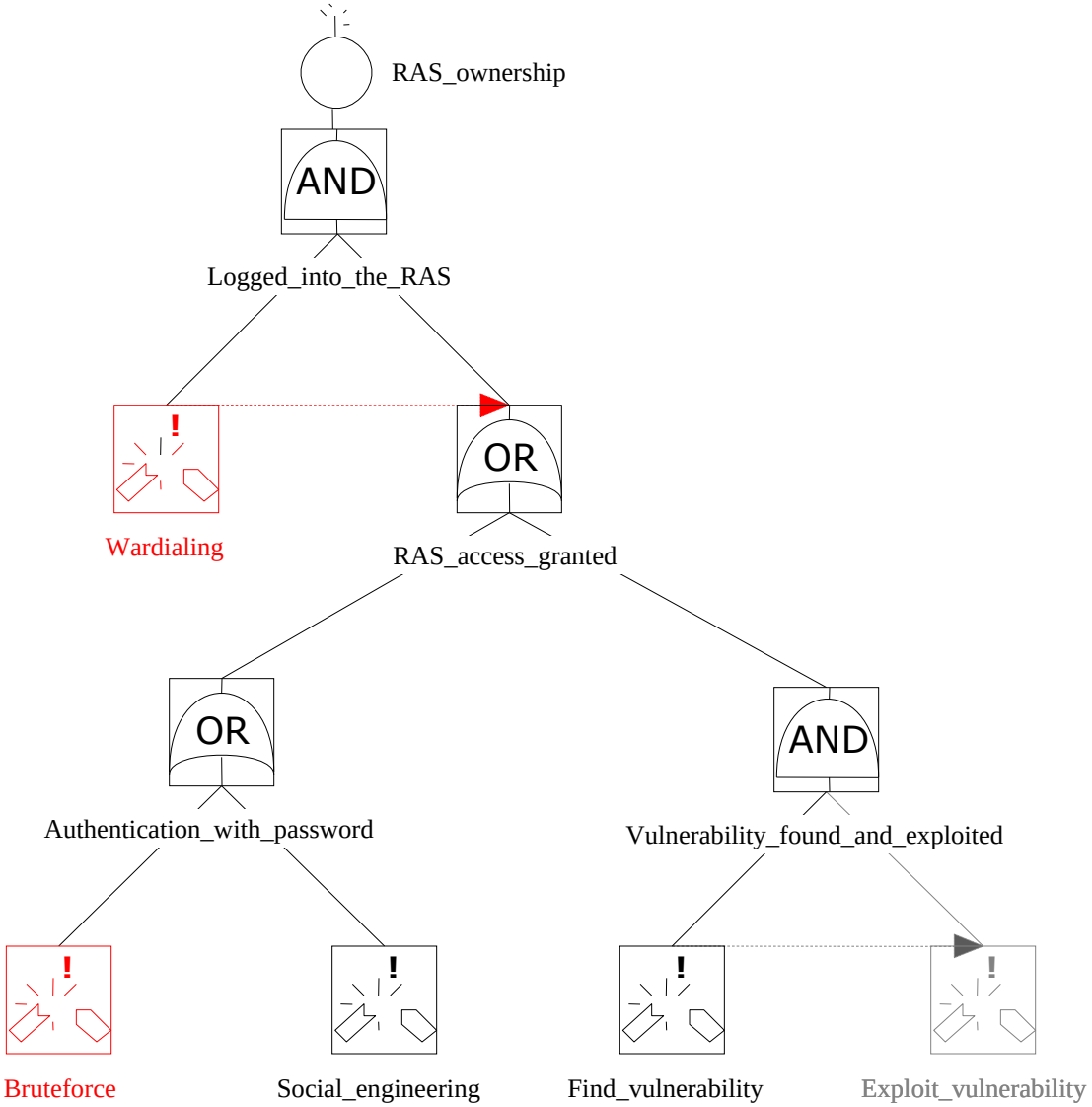
RAS attack BDMP – Step 1



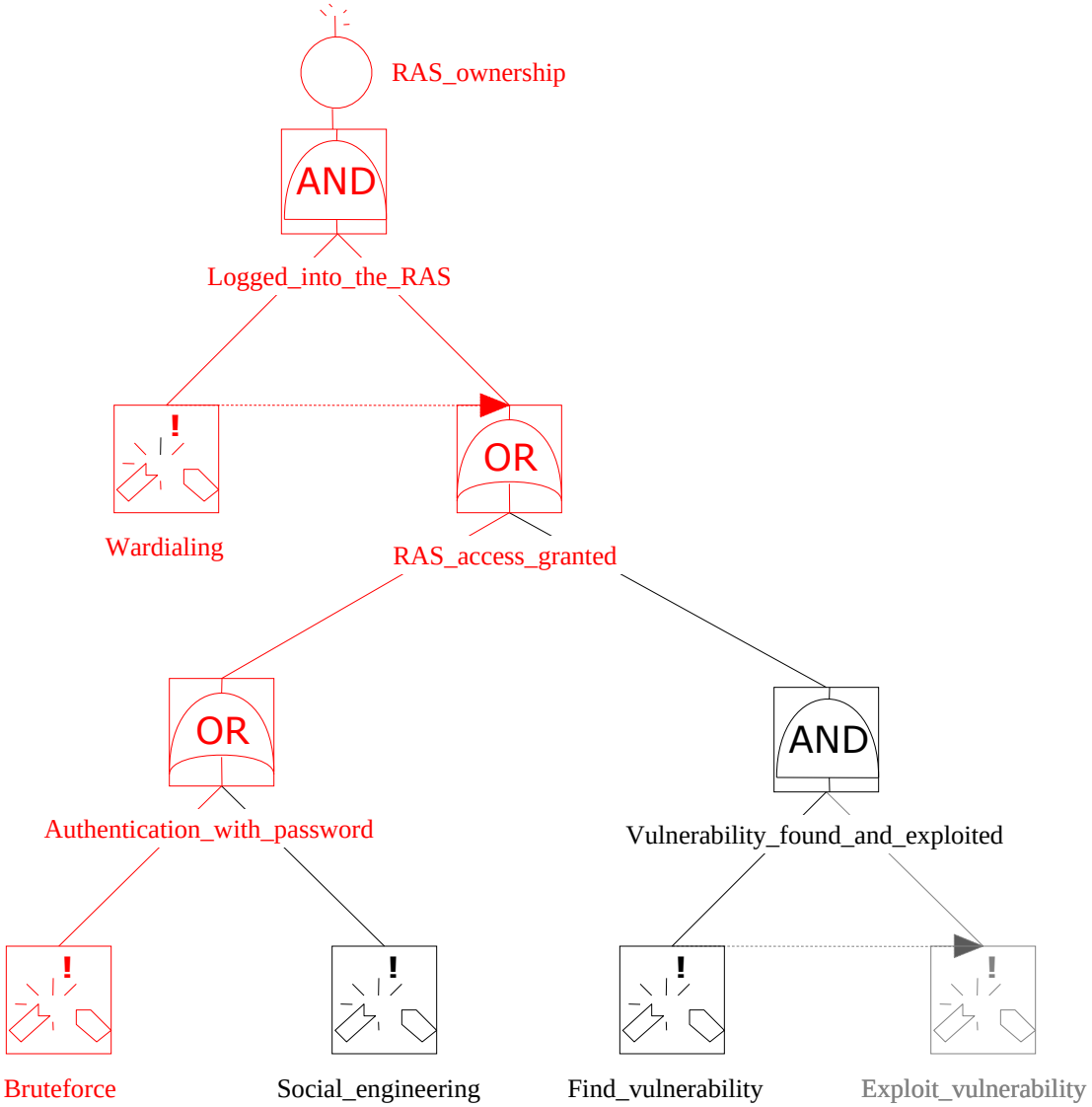
RAS attack BDMP – Step 1



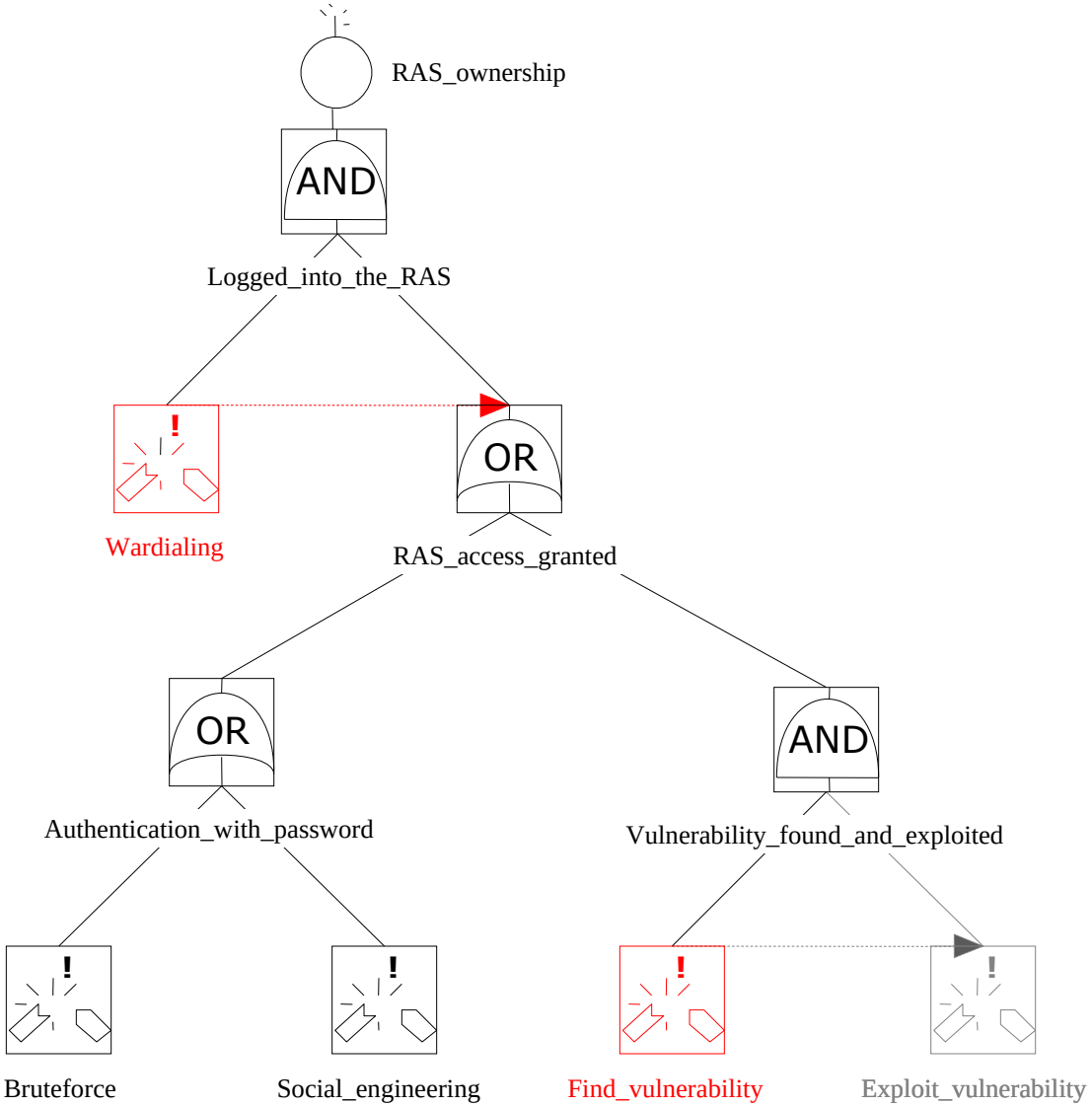
RAS attack BDMP – Step 2



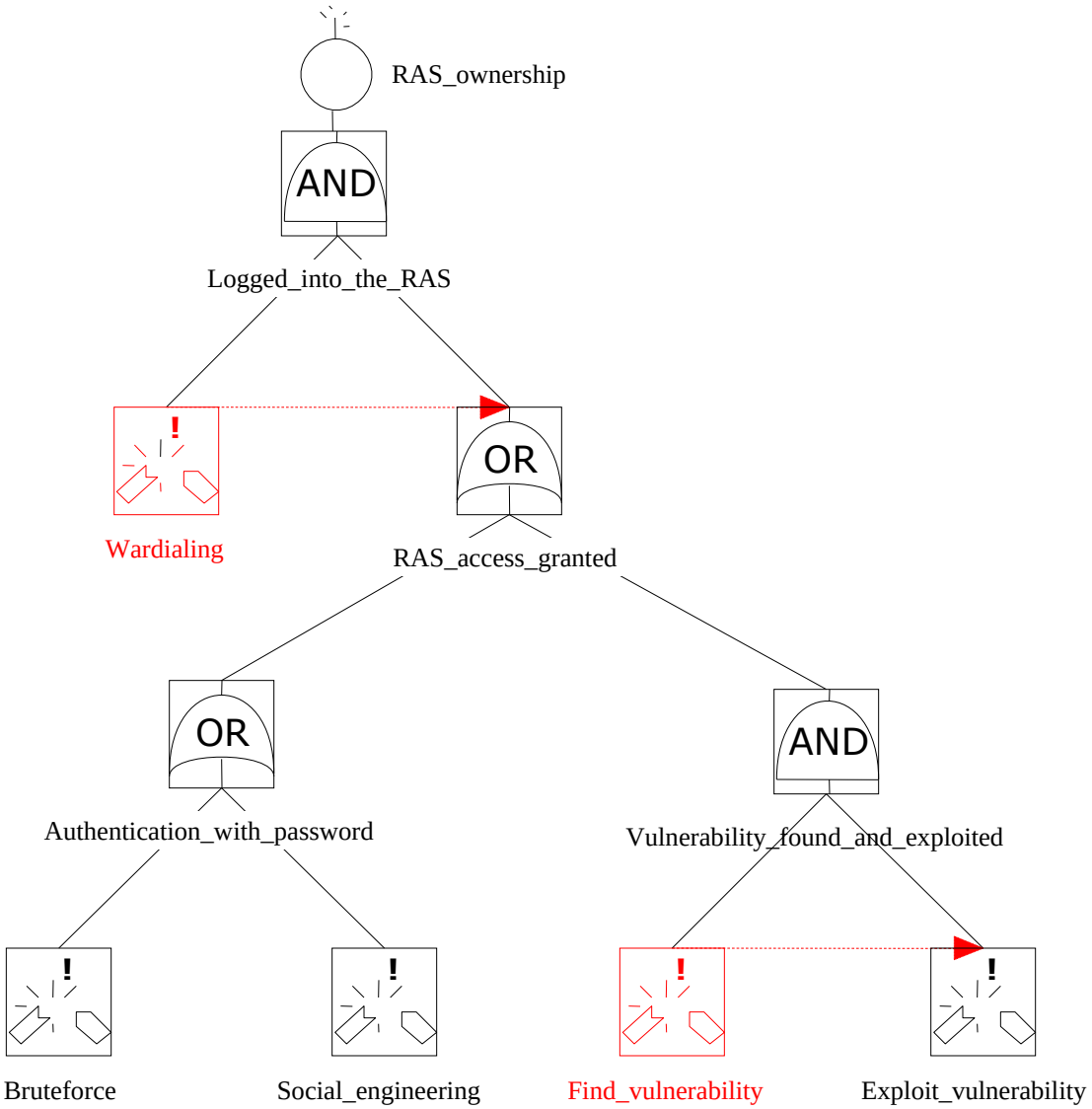
RAS attack BDMP – Step 2



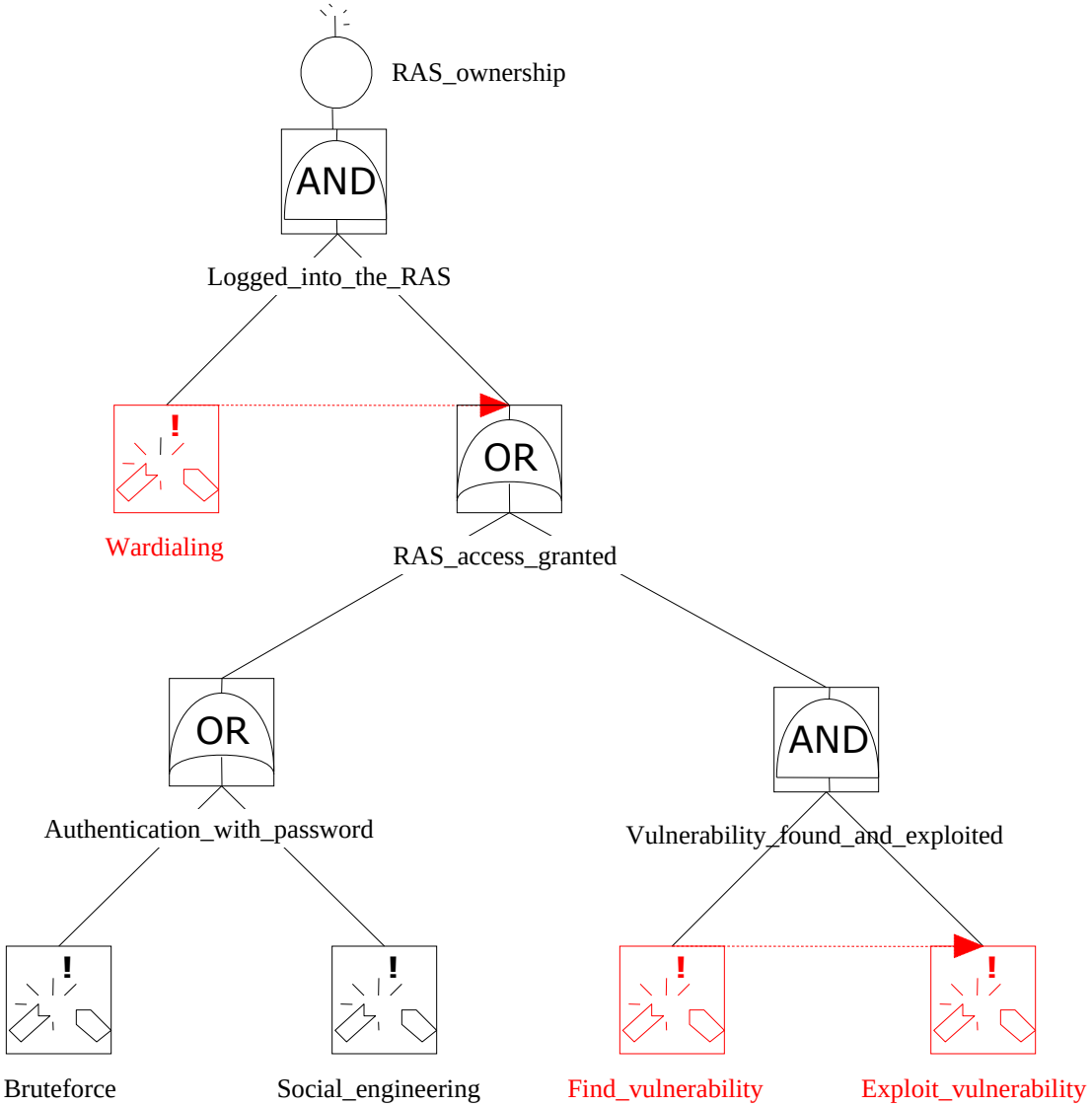
RAS attack BDMP – Step 2’



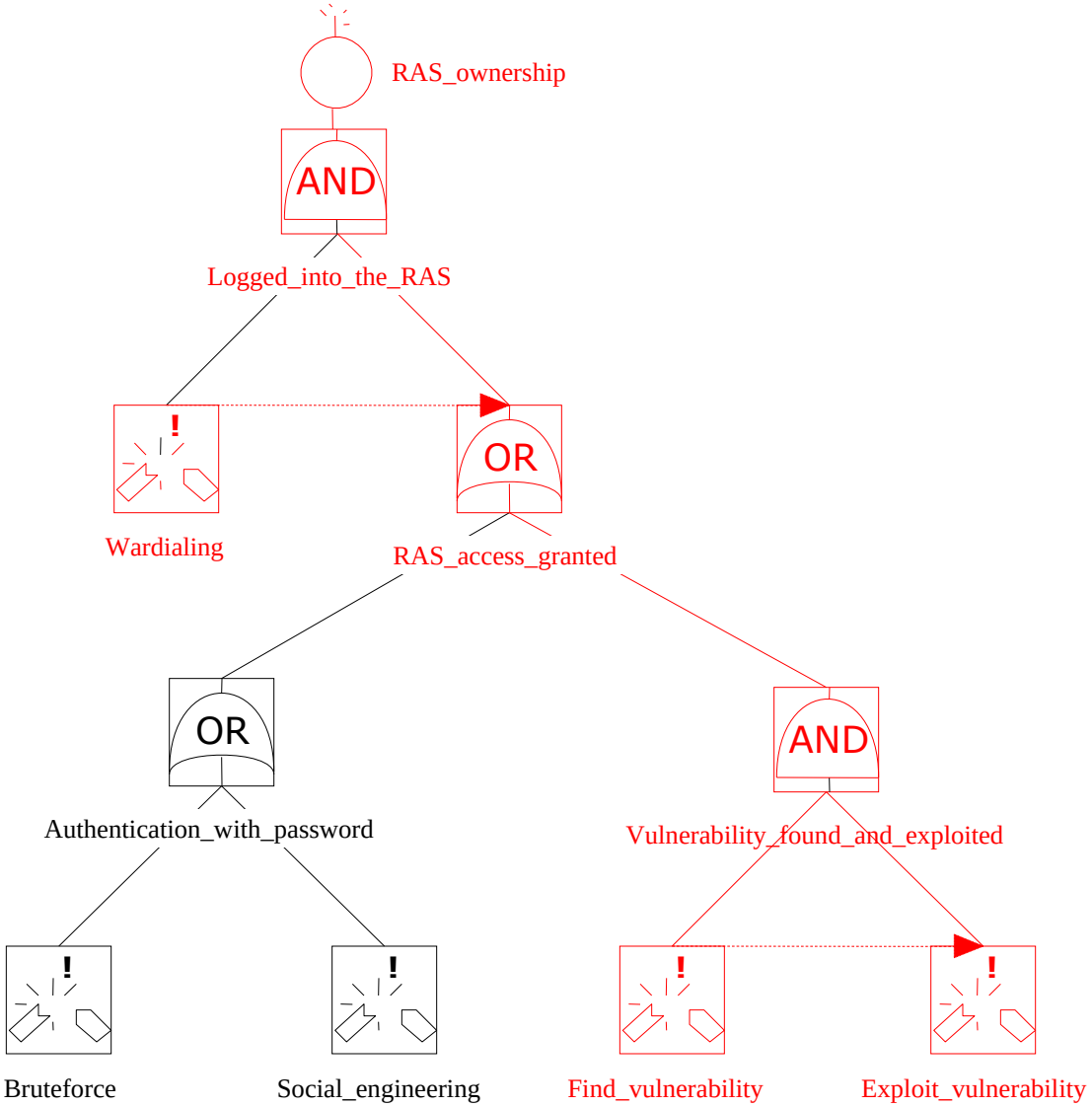
RAS attack BDMP – Step 2’



RAS attack BDMP – Step 3

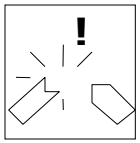
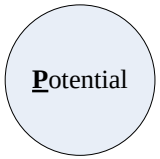
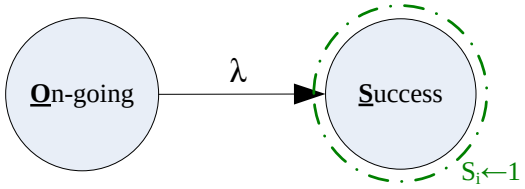
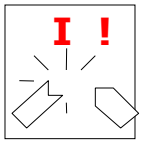
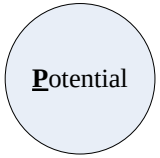
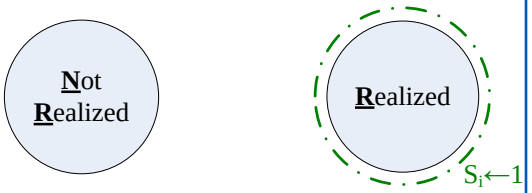


RAS attack BDMP – Step 3



The two basic security leaves

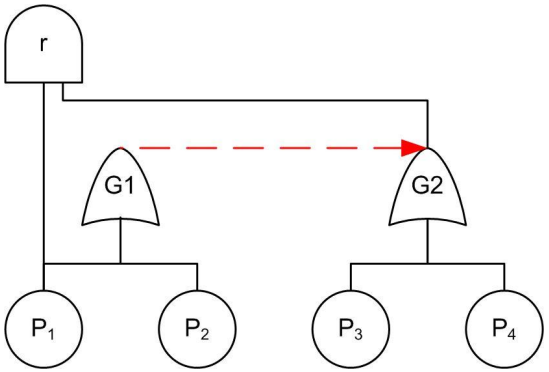
- A subset and adapted version of the original leaves
  - Two kinds of leaves: Attack Step & Instantaneous Security Event
  - No notion of “repairable” systems, simpler Markov models

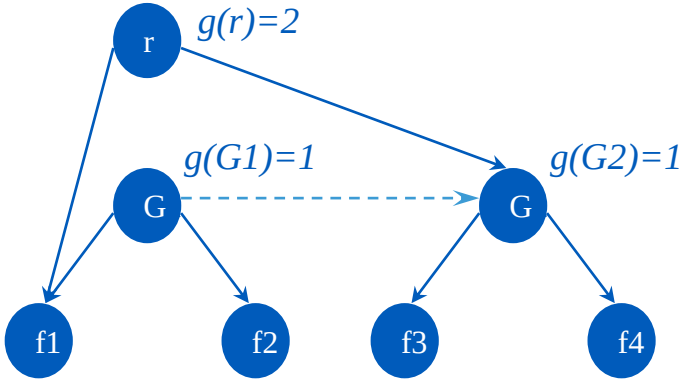
Symbol	“Idle” mode	Transfer between modes	“Active” mode
 Attack Step		P⇔ O (with $Pr = 1$) S ⇔S (with $Pr = 1$)	
 I.S.E		P ⇨NR (with $Pr= 1-\gamma$) P ⇨ R (with $Pr = \gamma$)	

Formal foundations – snapshot 1/5

A (security-oriented) BDMP $(\mathcal{A}, r, T, \{P_i\})$ is made of

- An attack tree $\mathcal{A} = \{E, L, g\}$
  - a set $E = G \cup B$, where G is a set of gates and B a set of basic events
  - (E, L) a directed acyclic graph, with L a set of oriented edges (i, j)
  - a function g, defining the gates ($g: G \rightarrow N^*$, with $g(i)$ the gate parameter k)





- A main top objective r
- Set of triggers T is a subset of $(E - \{r\})x(E - \{r\})$ such that

$$\forall (i, j) \in T,\ i \neq j \text{ and } \forall (i, j) \in T, \forall (k, l) \in T, i \neq k \Rightarrow j \neq l$$

Formal foundations – snapshot 2/5

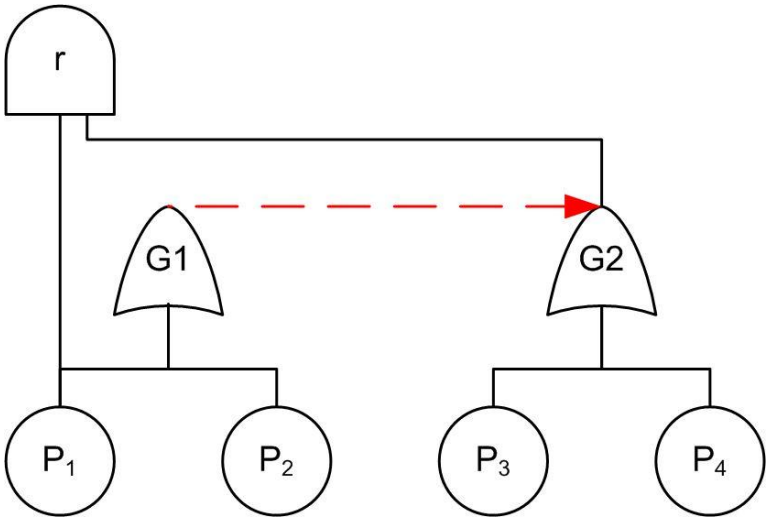
- $P=\{P_i\}_{i\in E}$, triggered Markov Processes $\{Z_0^i(t), Z_1^i(t), f_{0\to1}^i, f_{1\to0}^i\}$
  - $Z_0^i(t)$ and $Z_1^i(t)$ two homogeneous Markov process
  - $f_{0\to1}^i(x)$ and $f_{1\to0}^i(x)$ two "probability transfer functions"
    - For k in $\{0, 1\}$ (modes), A_k^i state-space of $Z_k^i(t)$
    - $S_k^i \subset A_k^i$, subset that generally corresponds to attacker action successes states (or event realization states)
    - For any $x \in A_0^i$, $f_{0\to1}^i(x)$ is a probability distribution on A_1^i such that if $x \in S_0^i$, then $\sum_{j\in S_1^i}(f_{0\to1}^i(x))(j)=1$
    - For any $x \in A_1^i$, $f_{1\to0}^i(x)$ is a probability distribution on A_0^i such that if $x \in S_1^i$, then $\sum_{j\in S_0^i}(f_{1\to0}^i(x))(j)=1$

Formal foundations – snapshot 3/5

- Three families of Boolean functions of the time (1/3)
  - Structure functions $(S_i)_{i \in E}$

$$\forall i \in G,\ S_i \equiv \sum_{j \in sons(i)} S_j \geq g(i)$$

$$\forall j \in B,\ S_j \equiv Z^j_{X_j} \in S^j_{X_j}$$, with $X_j = 0$ or 1, indicating the mode in which P_j is at time t



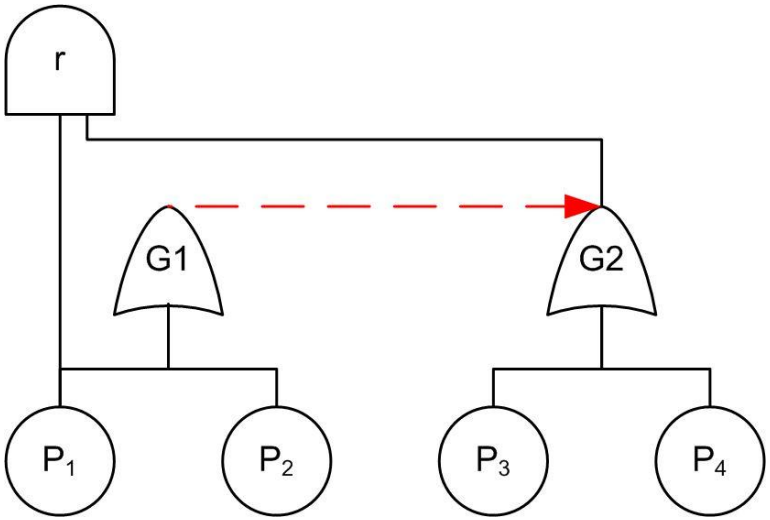
S_i (Structure functions)
$S_r = S_{f1} \wedge S_{G2}$
$S_{G2} = S_{f3} \vee S_{f4}$
$S_{G1} = S_{f1} \vee S_{f2}$
$S_{f1} = 1 \Leftrightarrow P_{f1}$ *in success state*
$S_{f2} = 1 \Leftrightarrow P_{f2}$ *in success state*
$S_{f3} = 1 \Leftrightarrow P_{f3}$ *in success state*
$S_{f4} = 1 \Leftrightarrow P_{f4}$ *in success state*

Formal foundations – snapshot 4/5

- Three families of Boolean functions of the time (2/3)
  - Process selectors $(X_i)_{i \in E}$

If i is a root of $\mathcal{A}$, then $X_i = 1$ else

$$X_i \equiv \neg\left[\left(\forall x \in E, (x,i) \in L \Rightarrow X_x = 0\right) \vee \left(\exists x \in E \,/\, (x,i) \in T \wedge S_x = 0\right)\right]$$



X_i (Process selectors)
$X_r = 1$
$X_{G2} = S_{G1}$
$X_{G1} = 1$
$X_{f1} = X_{G1} \vee X_r = 1$
$X_{f2} = X_{G1} = 1$
$X_{f3} = X_{G2} = S_{G1}$
$X_{f4} = X_{G2} = S_{G1}$

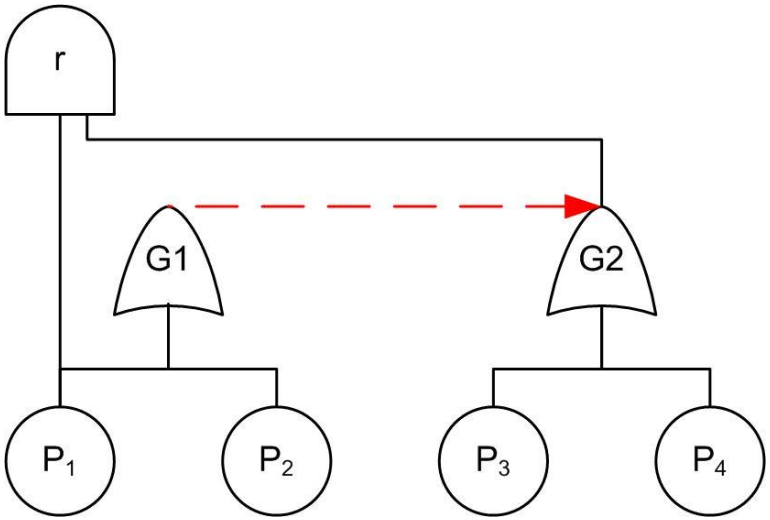
Formal foundations – snapshot 5/5

Three families of Boolean functions of the time (3/3)

- Relevance indicators $(Y_i)_{i \in E}$

If $i = r$ (finale objective), then $X_i = 1$ else

$$Y_i \equiv \left(\exists x \in E / (x,i) \in L \wedge Y_x \wedge S_x = 0\right) \vee \left(\exists y \in E / (i,y) \in T \wedge S_y = 0\right)$$



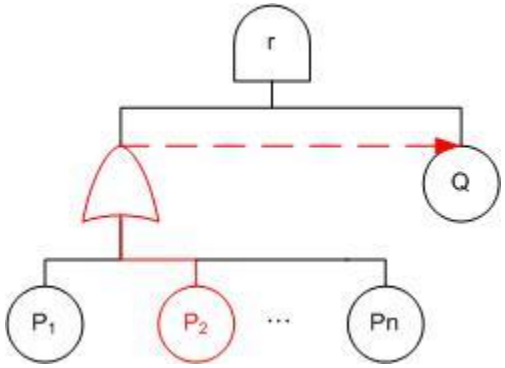
Y_i (Relevance indicators)
$Y_r = 1$
$Y_{G2} = \neg S_r$
$Y_{G1} = 1$
$Y_{f1} = \neg S_{G1} \wedge Y_{G1}$
$Y_{f2} = \neg S_{G1} \wedge Y_{G1}$
$Y_{f3} = Y_{G2} \wedge \neg S_{G2}$
$Y_{f4} = Y_{G2} \wedge \neg S_{G2}$

Mathematical properties

Robustness

- Theorem 1: $(S_i)(X_i)(Y_i)_{i\in E}$ are computable whatever the BDMP structure
- Theorem 2 : Any BDMP, defined at time t by the modes and the P_i states, is a valid homogeneous Markov process

Combinatory reduction by relevant event filtering

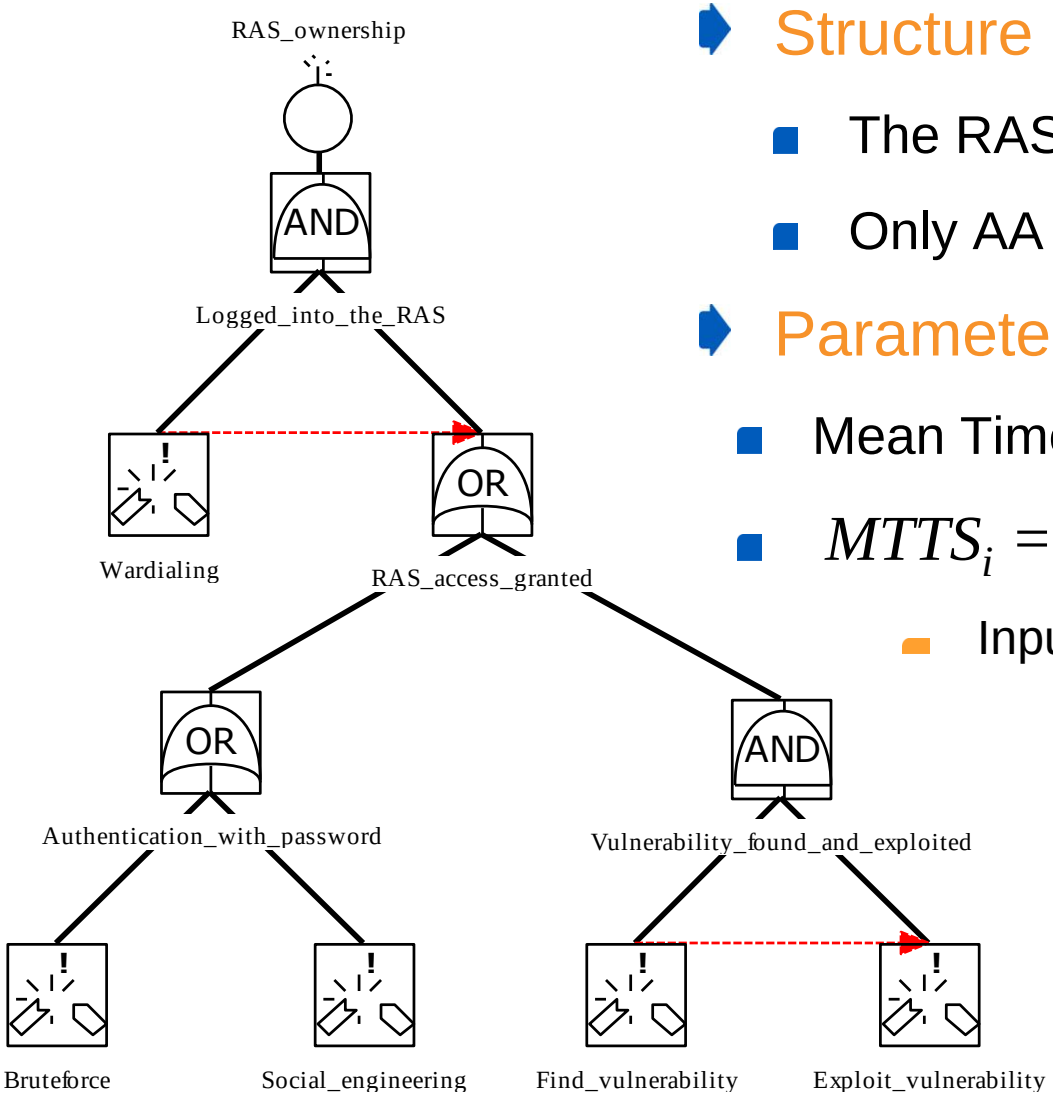


- After attack step P_2, all the others P_i are not relevant anymore: nothing is changed for “r” if we inhibit them
- The number of sequences leading to the top objective is
  - n, if we filter the relevant events $(\{P_1,Q\},\{P_2,Q\},\ldots)$
  - exponential otherwise $(\{P_1,Q\},\{P_1,P_2,Q\},\{P_1,P_3,Q\},\ldots)$

- Theorem 3: if the P_i are such that $\forall i \in B, \forall t, \forall t' \geq t, S_i(t)=1 \Rightarrow S_i(t')=1$* $Pr(S_r(t)=1)$ is unchanged whether irrelevant event ($Y_i=0$) are trimmed or not

* This is always the case in our framework (~ non-repairable in reliability studies)

Enough of theory – back to the use-case

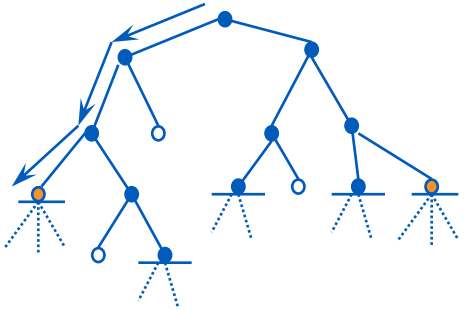


- Structure
  - The RAS attack again
  - Only AA leaves, AND/OR gates, triggers
- Parameters (success rates λ_i)
  - Mean Time To Success
  - $MTTS_i = 1/\lambda_i$
    - Input from the security analyst

- Bruteforce, Find_vuln., Exploit_vuln.: $\lambda = 10^{-4}$, i.e. MTTASR ~ 2,8h
- Wardialing: $\lambda = 10^{-5}$, i.e. MTTASR ~ 28h,
- Passwd_by_social_engineering: $\lambda = 5.10^{-6}$, i.e. MTTASR~55h

Quantification (1/2) – Time-domain analysis

- Taking advantage of the BDMP framework
  - Quantification tools, algorithms and optimizations
  - Efficient sequence exploration with trimming
    - Probability to reach the objective in a given time
    - Overall mean time to the attack success
    - Probability of each explored sequence
    - Ordered list of sequences



0.55
1.07×10^5 s
Cf. hereunder

Sequences ***Attack steps***	**Probability in mission time**	**Average duration after init.**	**Contribution**
[Wardialing, Bruteforce]	0.2717	4.878×10^3	0.4877
[Wardialing, Find_vuln, Bruteforce]	0.1272	9.7561×10^3	0.2329
[Wardialing, Find_vuln, Exploit_vuln]	0.1272	9.7561×10^3	0.2329
[Wardialing, Social_eng.]	0.0136	4.8780×10^3	0.0249
[Wardialing, Find_vuln, Social_eng.]	0.0064	9.7561×10^3	0.0116

Quantification (2/2) – Time-independent

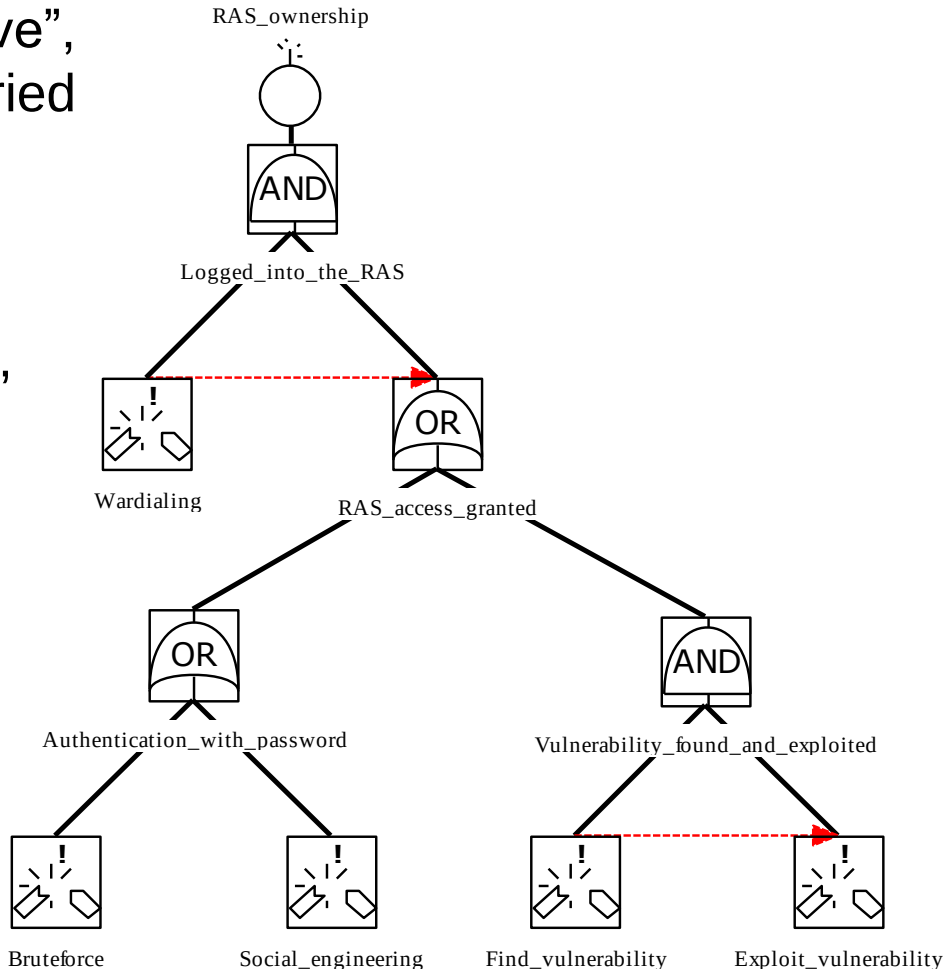
- Classical values attributed to attack tree leaves
  - Fixed probabilities → (dynamically) covered by stochastic processes
  - Monetary cost → scenario cost, average attack cost
  - Boolean indicators (specific requirements, properties)
    - Need of internal knowledge, internal support
    - Need of specific tool, piece of information

      → Characterization of selected scenarios
  - Minimum attacker skills
- (Generalization) Continuous, Boolean, Discrete attributes
  - Computable leveraging the logical tree structure / sequences

Advanced modeling - Phased attack steps

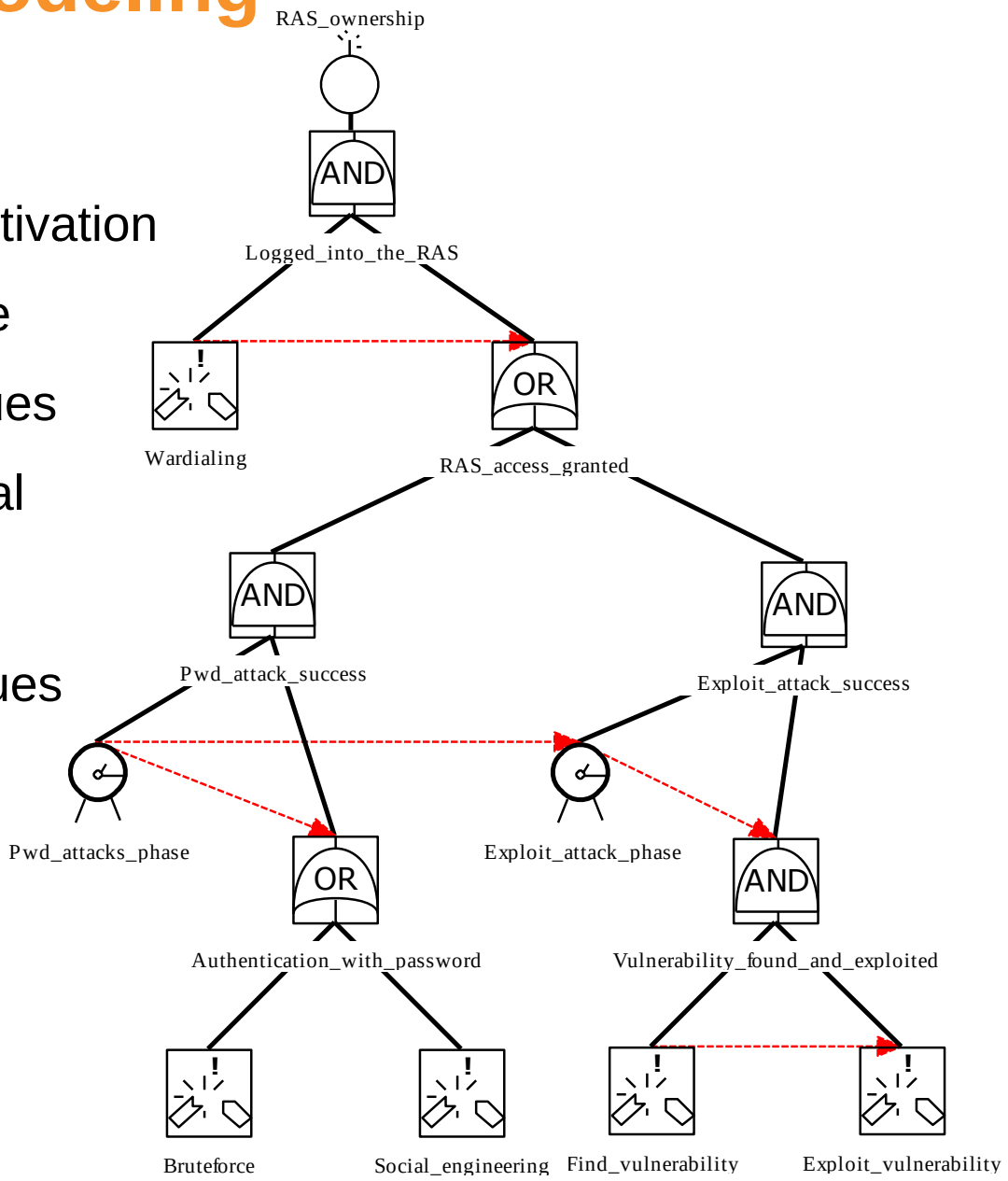
- Sequences are modeled by the triggers but….
  - for a given attack “sub-objective”, different techniques are tried simultaneously
- In our example
  - Once `Wardialing` succeeded,
    - `Bruteforce`,
    - `Social_engineering`,
    - `Find vulnerability`,

    are attempted in parallel.
  - This may be inappropriate



Phased behavior modeling

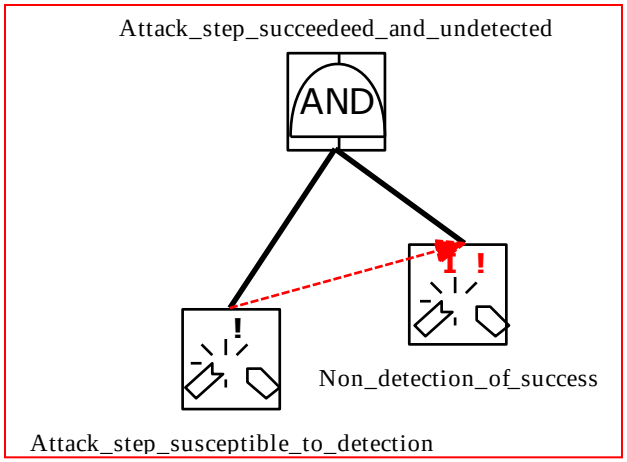
- Phase leaves
  - Success-independent activation
  - Fixed or exponential time
  - Order groups of techniques
  - Towards a given sub-goal
- In our example
  - Password-related techniques
    - `Bruteforce`
    - `Social-engineering`
  - Then, “exploit” process

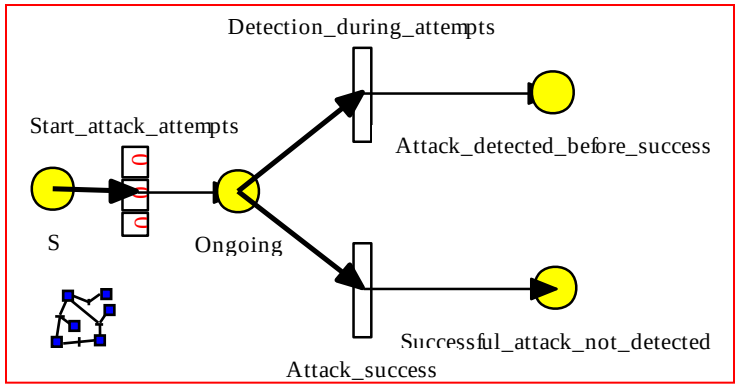


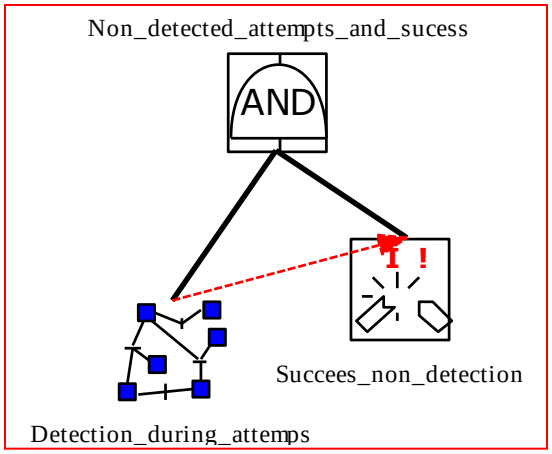
Defensive aspects: detection and reaction modeling

Detection Modeling

- The IOFA distinction
  - **I**nitial / **O**n-going / **F**inal / **A** posteriori
- In the EDCC paper (Oct. 2009)
  - Type I & F detection → Straightforward
  - Type O detection → Petri-net packaged as a new leaf
  - Type A detection → Easily modeled as Petri-nets as well but…
- Globally, an awkward approach







Reactions modeling

- In the former theoretical framework (EDCC paper)
  - Attack is stopped when detected
  - More complex to model change of parameter
  - Theory adapted for offensive aspects, insufficient for defensive ones
- Recent work
  - IOFA detection and reactions without Petri leaves
  - Complete integration in the theoretical framework
    - "Detection status indicator" D_i ; new Markov models
  - Changes in the parameters and/or in the BDMP structure
- Content of a new paper
  - Check the authors' webpage for update (cf. last slide)

Elements of comparison

BDMP and Attack Trees,
BDMP and Petri-net based approaches

Attack Trees

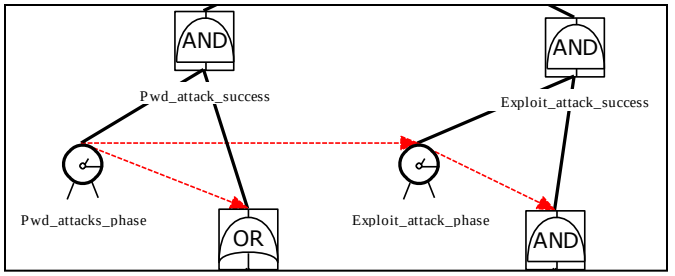
- Well-known and wide-spread model
  - Numerous citations of Schneier's paper (1999)
  - Control systems, protocols, online banking, ad-hoc net, smartcards,…
  - Part of several Risk Analysis methods (CMU Square, DoD MORDA…)
- Main limitations related to their static nature
  - No way to decompose attacks into chronological sequences
  - No time-domain analysis
  - Probabilistic quantifications ⇨ leaves independence
  - No way to take into account dynamic dimension (detection, reaction)
- BDMP provide solutions regarding these limits
  - The formalism stays graphically close (new semantics)

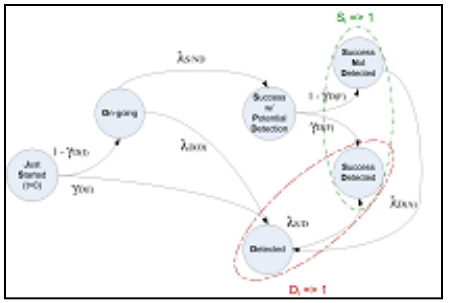
Petri-net based approach

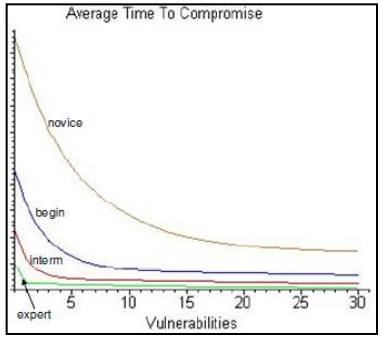
- Some facts
  - Powerful and versatile modeling capabilities
  - Attack patterns for IDS (94), Graphical attack modeling (2000), …
  - Numerous formalisms flavors, reflected in the security adaptations
- Main limits
  - Readability (in our case)
    - Less known by security experts
    - Formalism diversity
    - Structure functions
  - Validation (closely linked to the former point)
  - State-space explosion (cf. relevant events mechanisms in BDMP)

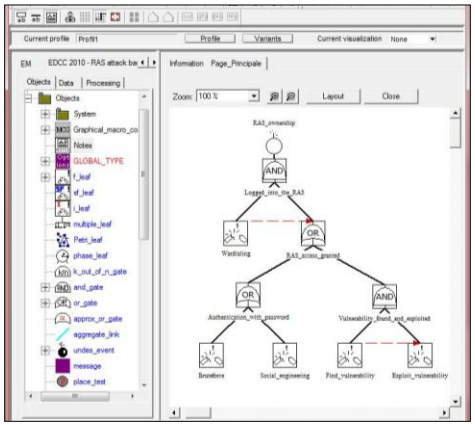
On-going work and perspectives

Perspectives 1/2









- Modeling capabilities extension
  - E.g. “Probabilized” phases and choice gates
- Leverage the extended theory (with D_i)
  - Detection triggers, new values of interest
- Experiment different probability distributions
  - Quantification with Monte-Carlo simulation
- Assist the analyst in security decisions
  - Sensitivity analysis, sequence discrimination
- Extending the KB3 software suite
  - Security-oriented “knowledge basis” (Figaro)

Perspective 2/2 - Scope extension

- (Straightforward) Other security domains
  - Physical security
  - Everywhere the AT and PN formalisms have been considered!
- Integrating safety and security studies
  - Historically, two separated communities and methodologies
  - Recent cross-fertilization (Attack Trees, and most recently… BDMP)
  - Safety and security issues converging on the same systems
    - Industrial Control Systems, SCADA systems, Safety-Instrumented Systems
  - Their strong interdependencies are still to be characterized
  - BDMP could contribute through a common formalism

Conclusion

Conclusion

- Graphical security modeling
  - Different balances between readability, scalability, modeling power and quantification capabilities
- A adaptation of BDMP to security modeling
  - An original and attractive trade-off
  - With a sound mathematical framework
  - Already an operational formalism, but evolutions to come
- Inherent limits
  - Attacker behavior stochastic modeling
  - Security and quantitative assessments
  - Complementary tool for the security analyst

Some references

On BDMP & KB3

- M. Bouissou, J.L. Bon, A new formalism that combines advantages of fault-trees and Markov models: Boolean logic Driven Markov Processes, Reliability Engineering and System Safety, Vol. 82, Issue 2, Nov. 2003, pp. 149-163
- M. Bouissou, Automated Dependability Analysis of Complex Systems with the KB3 Workbench: the Experience of EDF R&D, Proc. CIEM 2005, Bucharest, Romania, Oct. 2005
- M. Bouissou, Gestion de la complexité dans les études quantitatives de sûreté de fonctionnement de systèmes, Lavoisier, éditions TEC&DOC, Oct.2008.
- Homepage of Marc Bouissou http://perso-math.univ-mlv.fr/users/bouissou.marc/

On BDMP & Security

- L. Piètre-Cambacédès, M. Bouissou, The promising potential of the BDMP formalism for security modeling, Proc. DSN 2009 (FA, Supplemental Volume), Estoril, Portugal, 2009.
- L. Piètre-Cambacédès et M. Bouissou, Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP), Eighth European Dependable Computing Conference (EDCC-2010), Valencia, Spain, April 28-30, 2010
- Homepage of Ludovic Pietre-Cambacedes http://perso.telecom-paristech.fr/~pietreca/

Thank you for your time