Beyond attack trees: Attack and defense modeling with BDMP

(Boolean logic Driven Markov Processes)

September 13th 2011

SaToSS Seminar, Luxembourg

Ludovic Piètre-Cambacédès[1]

Marc Bouissou[1,2]

[1]EDF R&D, *[2]École Centrale Paris*

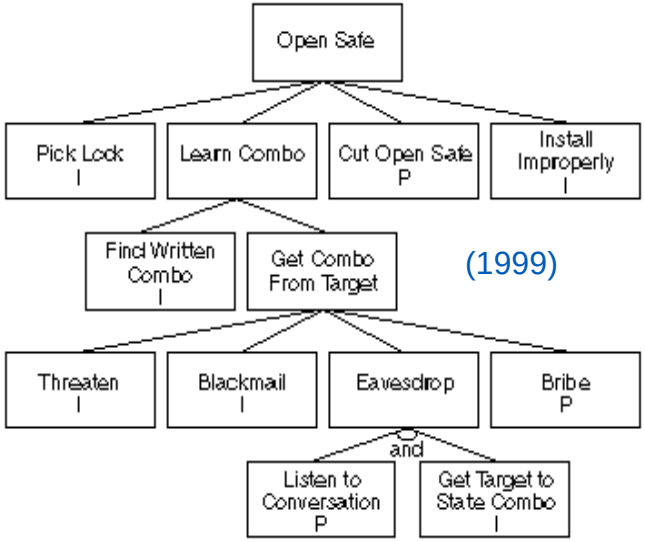
CHANGER L'ÉNERGIE ENSEMBLE

Agenda

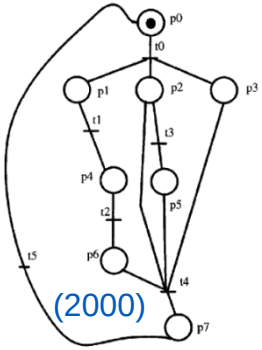
- Introduction
  - Graphical attack modeling and relevance of BDMP
- Attack and defense modeling with BDMP
  - Formalism description
  - Theoretical basis and description
  - Examples & quantifications
- Recent advances
  - Enhancements and complementary tools
- Perspectives and on-going work
- Conclusion and Q&A

Graphical modeling of computer attacks

- Graphical representation of an attack process
  - Red-team, risk analysis
  - Formalize reasoning
  - Share standpoints
  - Enhance coverage

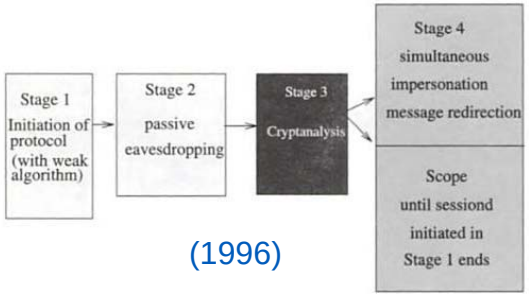


(1999)

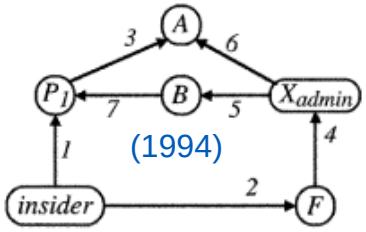


(2000)

- An active field of research
  - Different trade-offs
    - Ease of appropriation
    - Readability
    - Modeling power
    - Quantification capabilities
    - Scalability



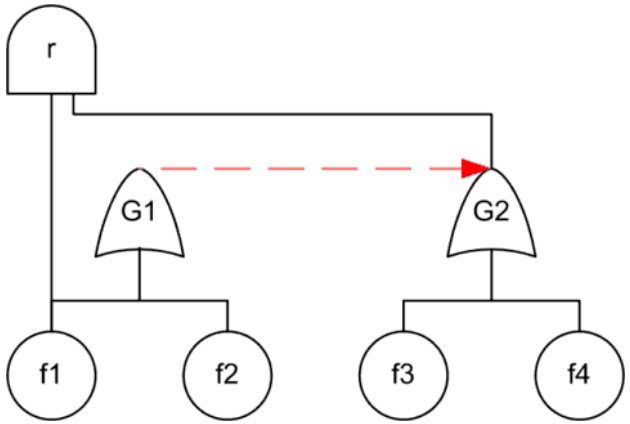
(1996)



(1994)

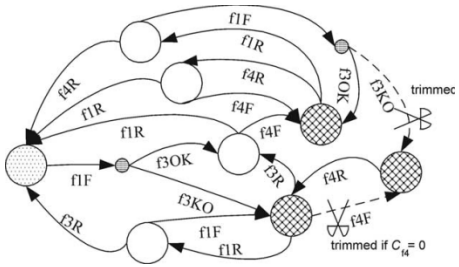
BDMP, the potential for an attractive trade-off

- 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

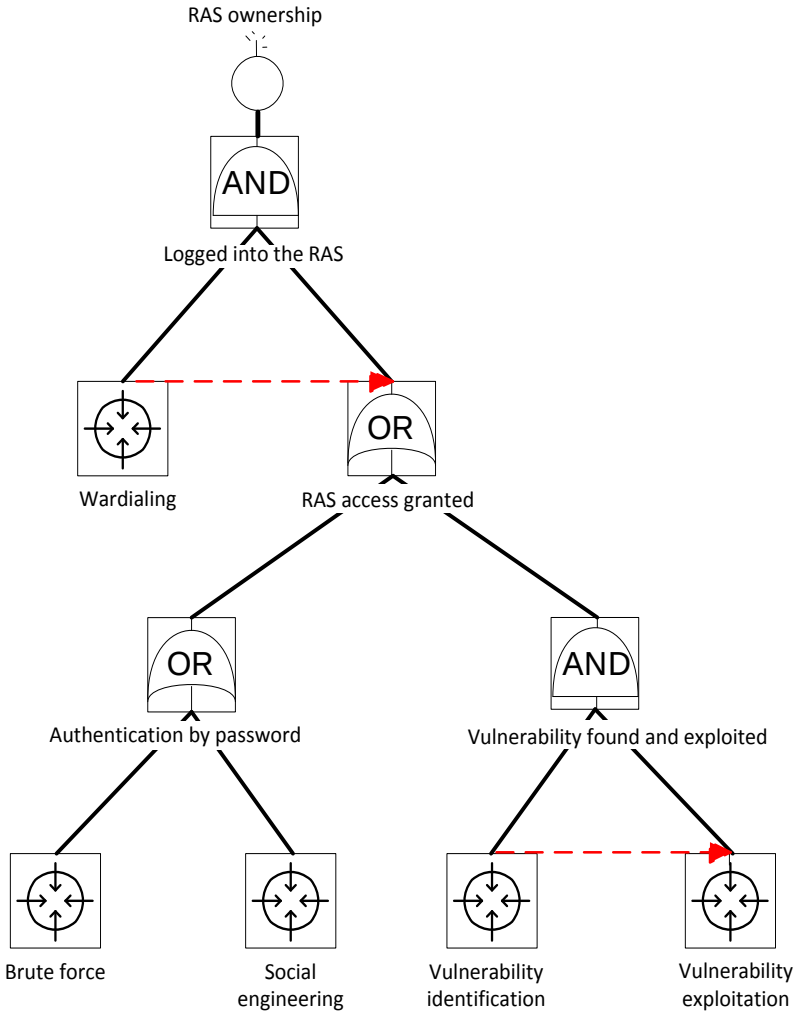


- Invented and used at EDF (NPP safety, substations, data centers reliability,…)
- Complete theory and software framework

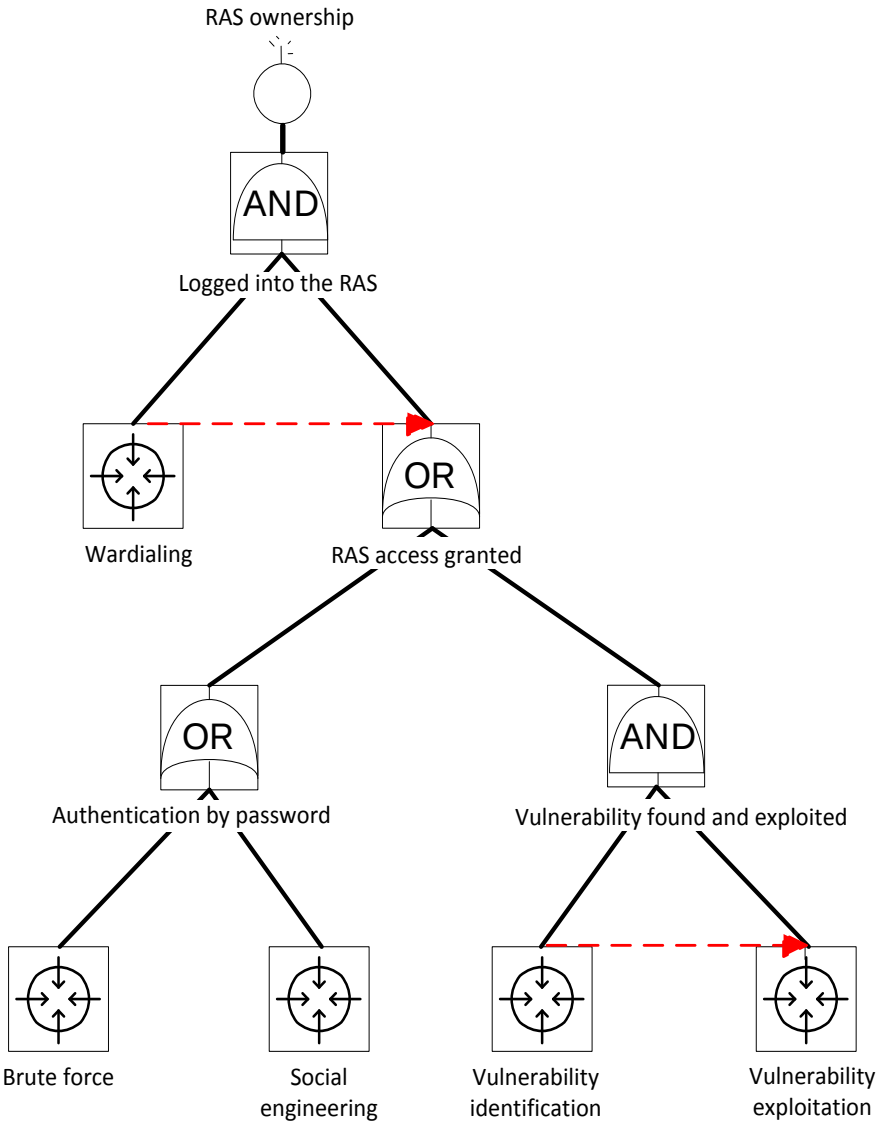
⇒ Adaptation to attack modeling

BDMP – Application to attack modeling

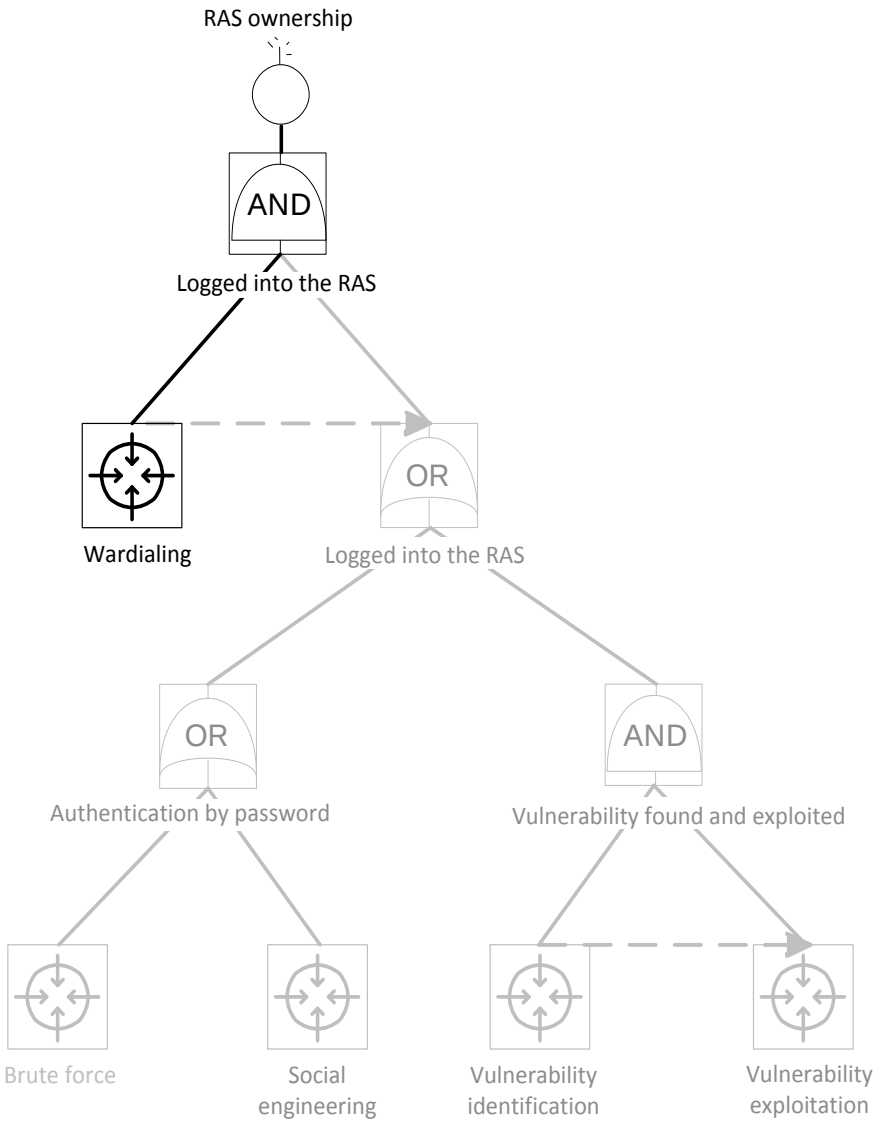
- In a nutshell…
  - The look of a classical attack tree
    - Objective = *top event*
    - Logical gates AND, OR, etc.
  - Triggers {T}
  - Leaves under two modes
    - « Idle » and « Active »
    - Triggered Markov processes
- Interest of BDMP in security
  - Dynamical (> attack trees)
  - Readable (close to attack trees)



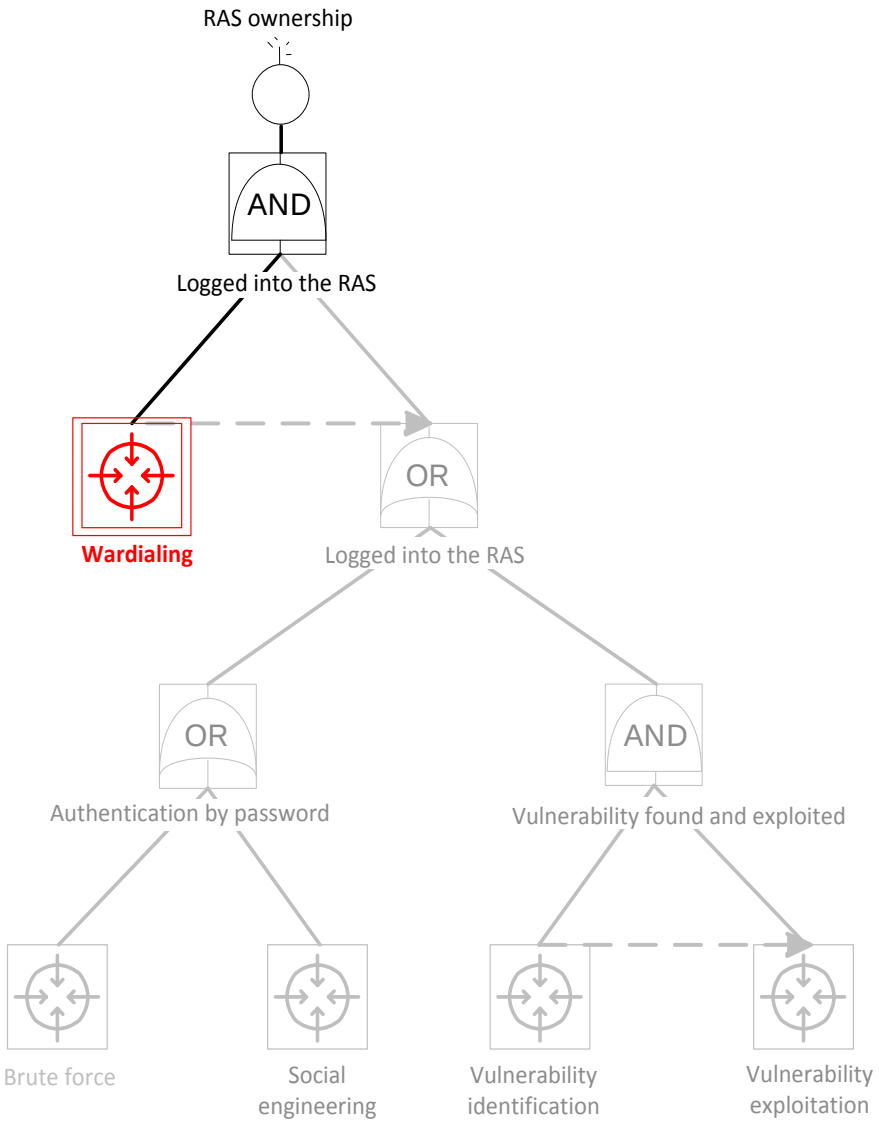
RAS attack BDMP – A simple use-case



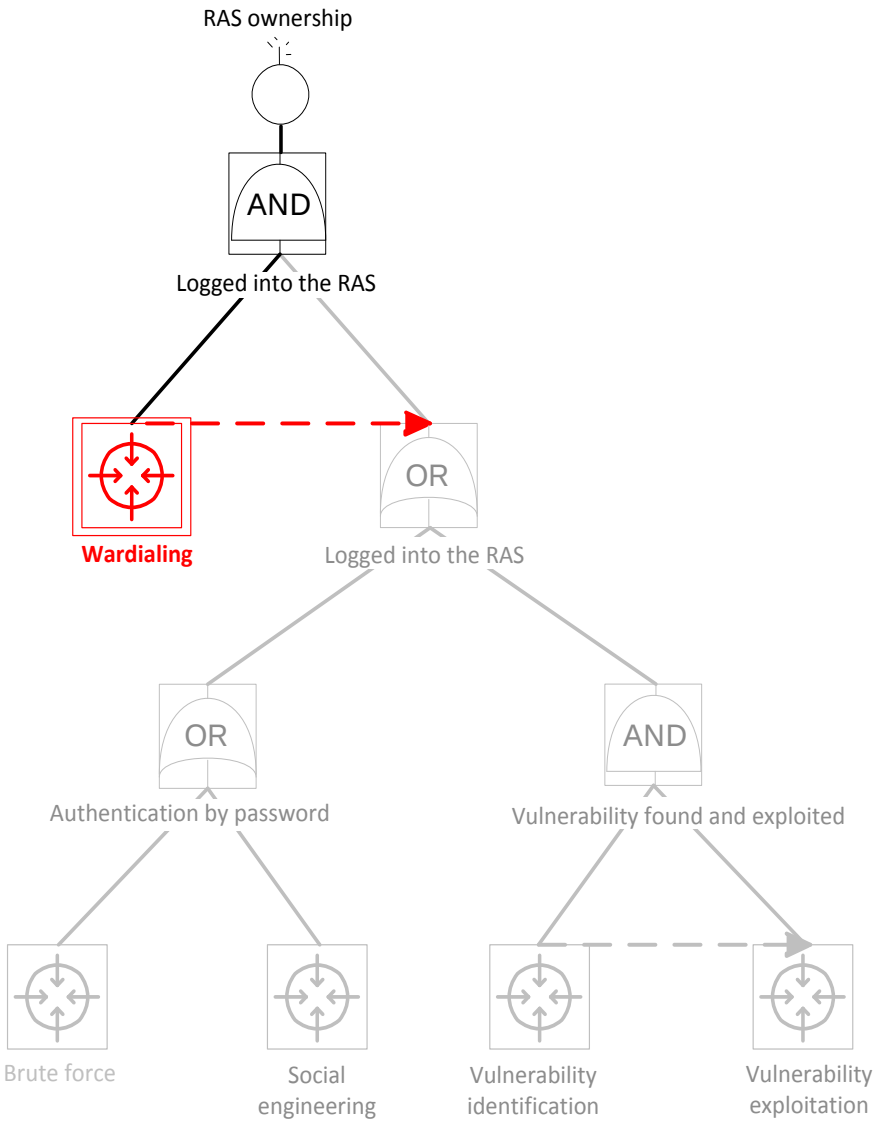
RAS attack BDMP – Step 0 (attack just started)



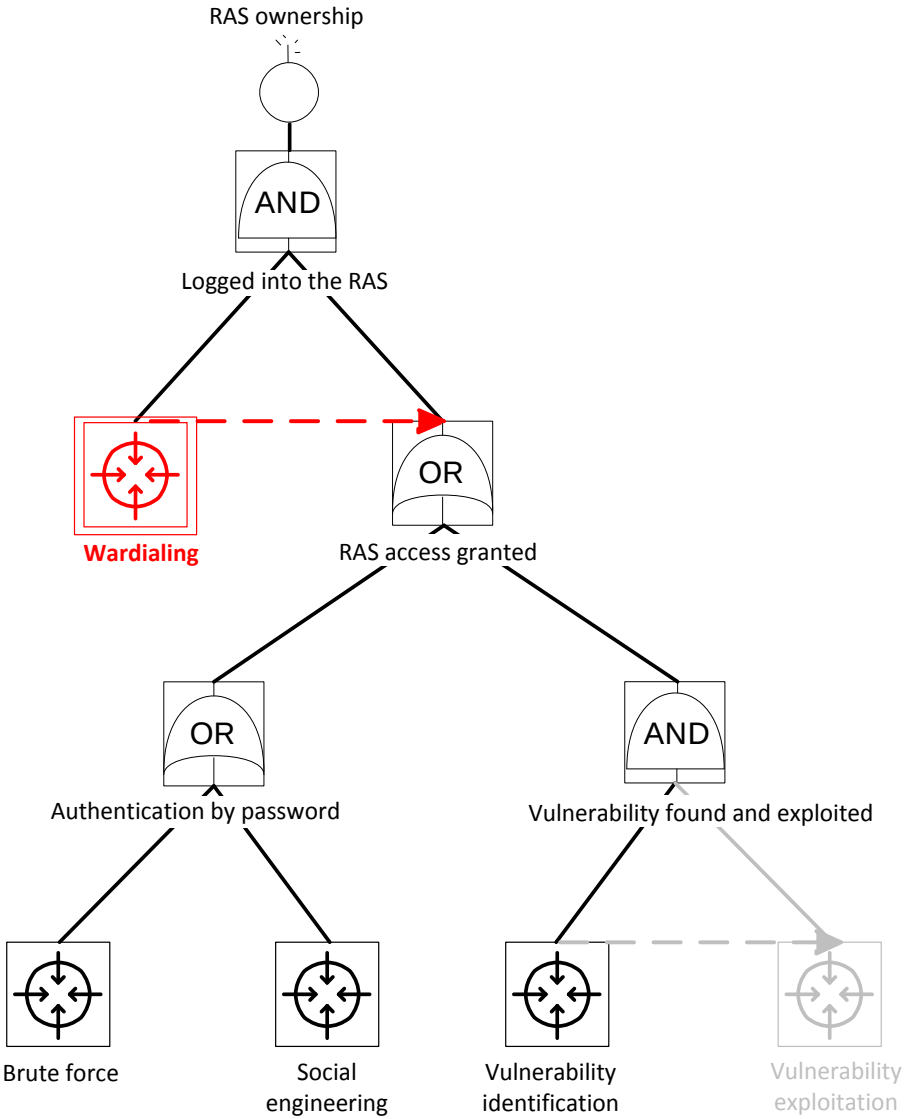
RAS attack BDMP – Step 1



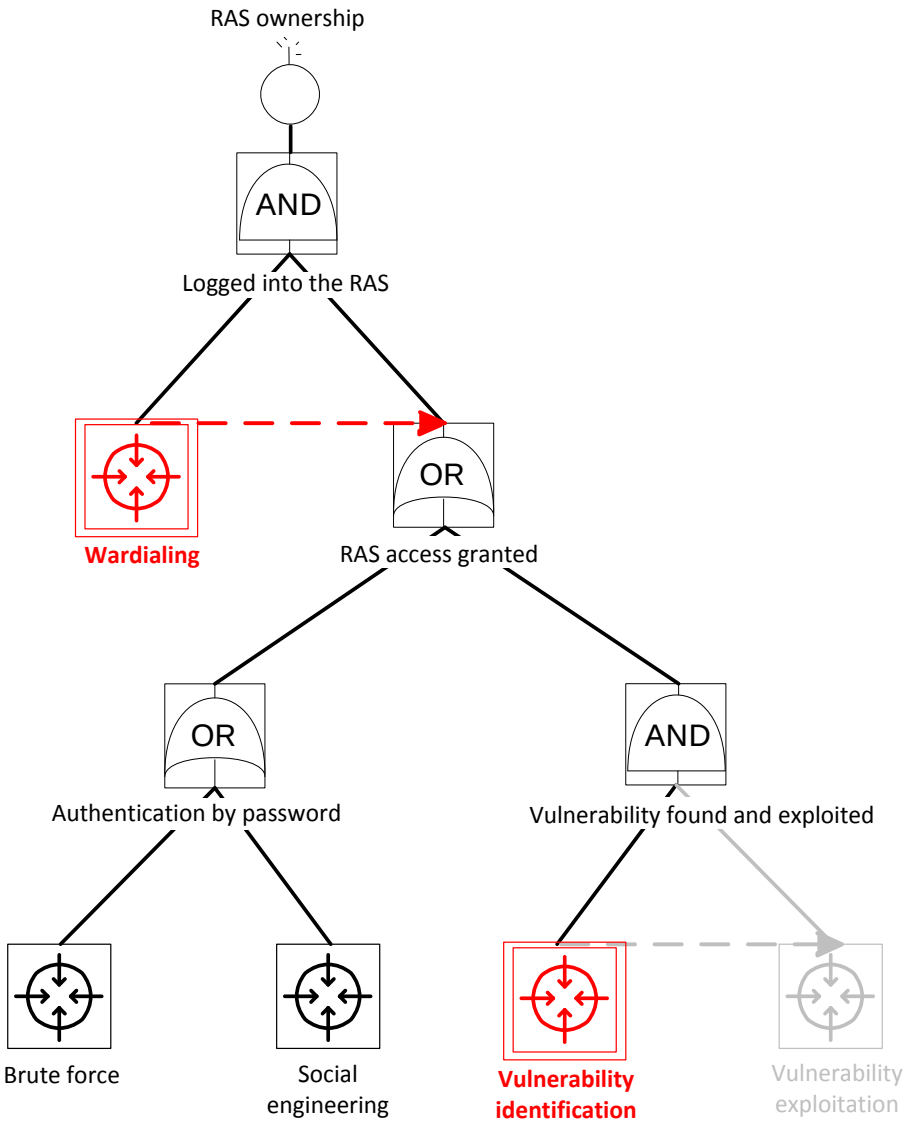
RAS attack BDMP – Step 1



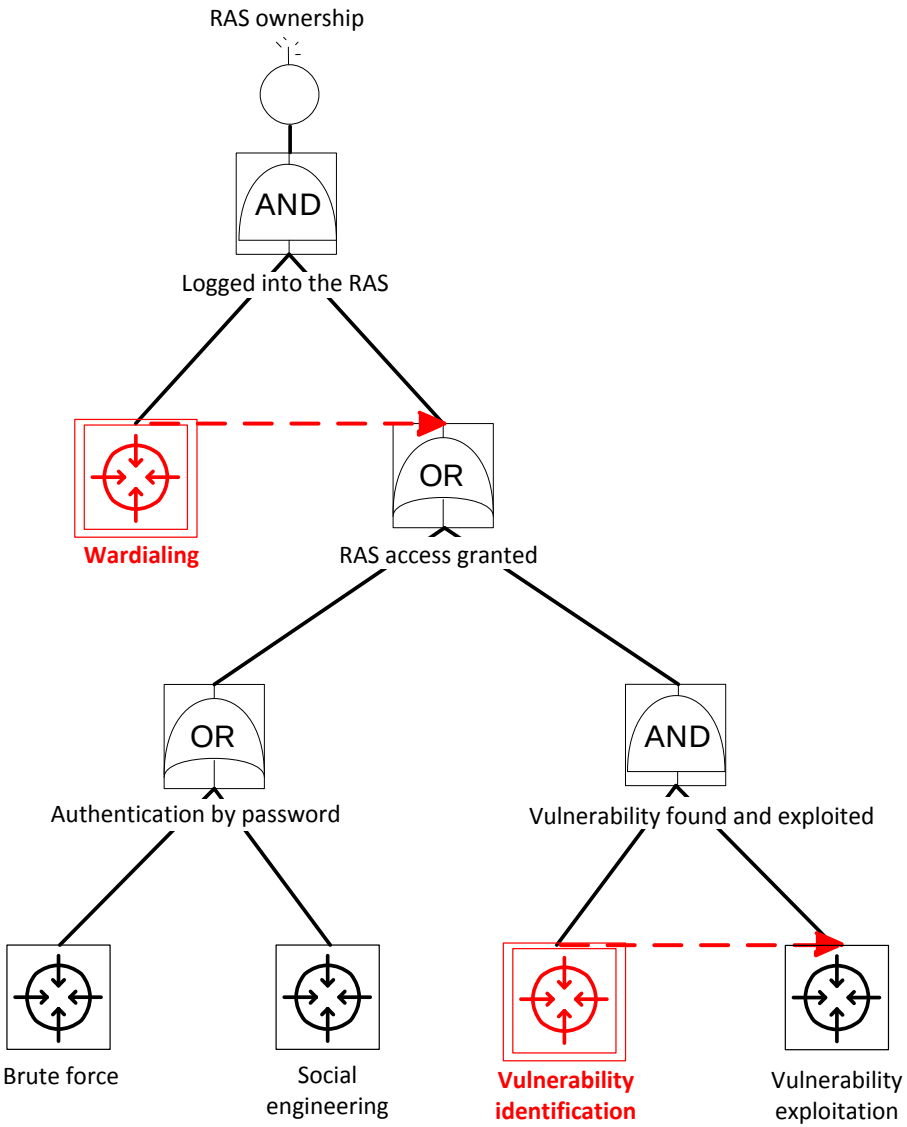
RAS attack BDMP – Step 1



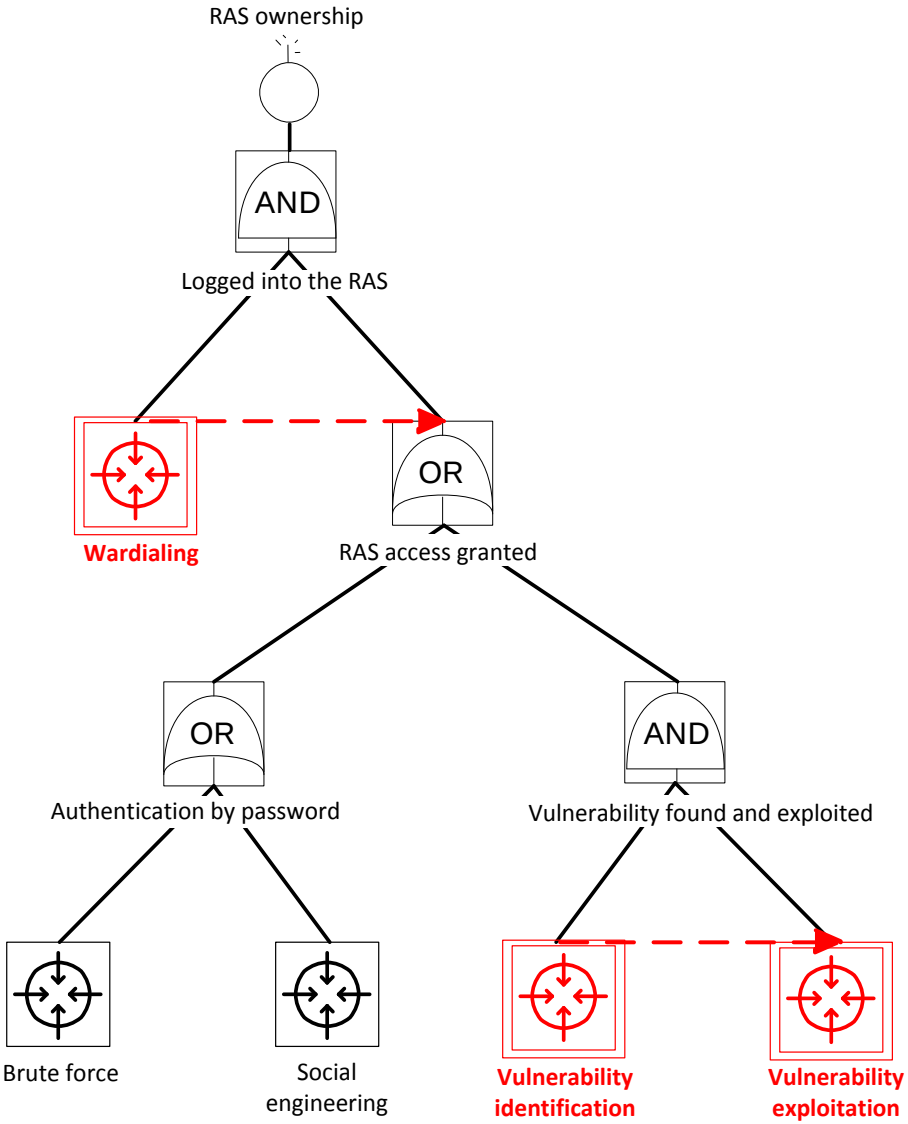
RAS attack BDMP – Step 2



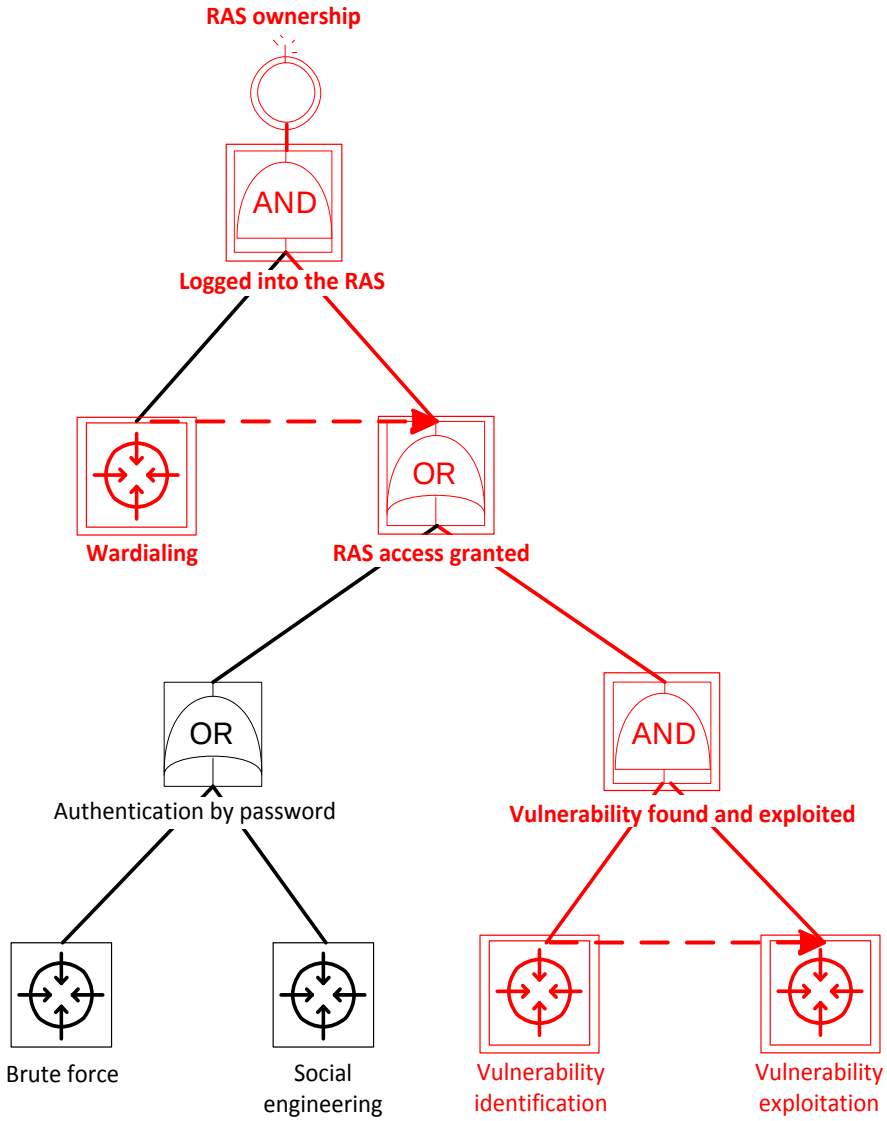
RAS attack BDMP – Step 2



RAS attack BDMP – Step 3

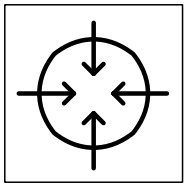


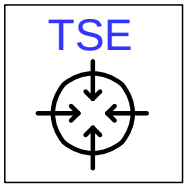
RAS attack BDMP – Attacker's objective reached

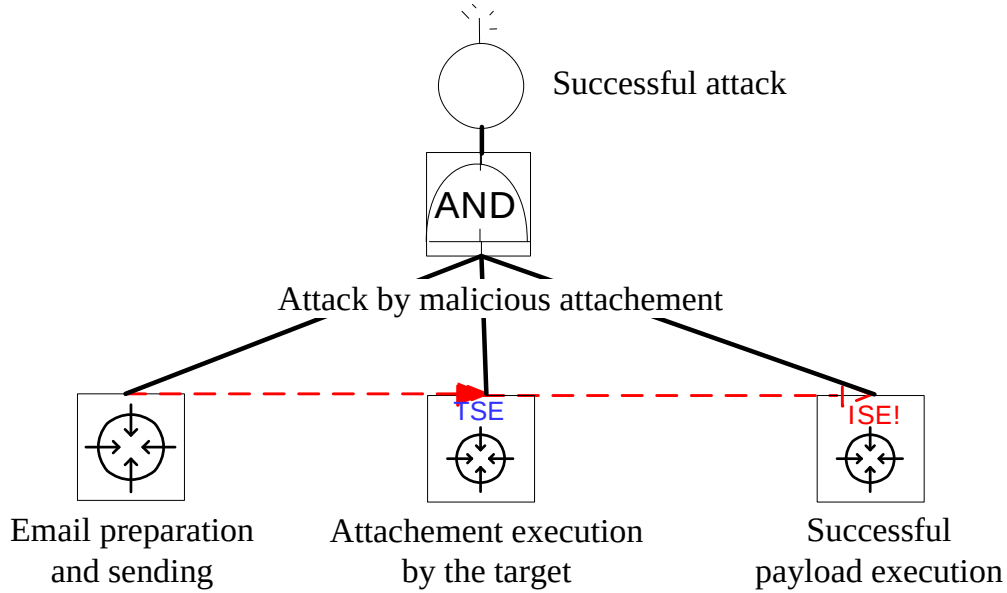


BDMP for attack modeling – Types of leaves

- Attack scenarios ⇒ 3 kinds of security leaves
  - Modeling of attacker's actions
    - AA (*Attacker Action*) leaves, timed leaves ($1/\lambda$ = MTTS)
  - Modeling of security events
    - TSE (*Timed Security Event*) leaves, timed as well
    - ISE (*Instantaneous Security Event*) leaves, instantaneous (γ)

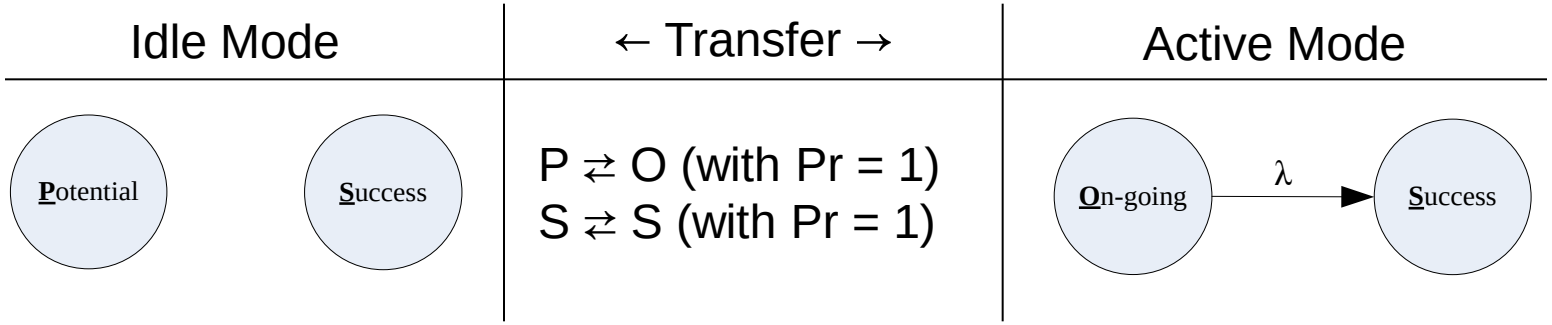






BDMP for attack modeling – Going deeper

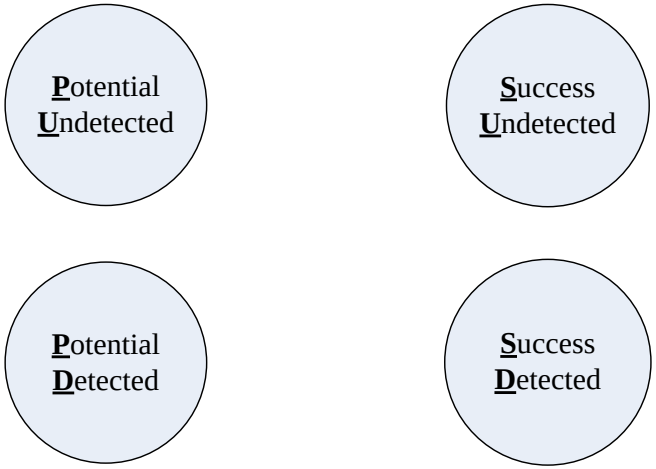
- Triggered Markov processes (e.g., AA leaf without detection)



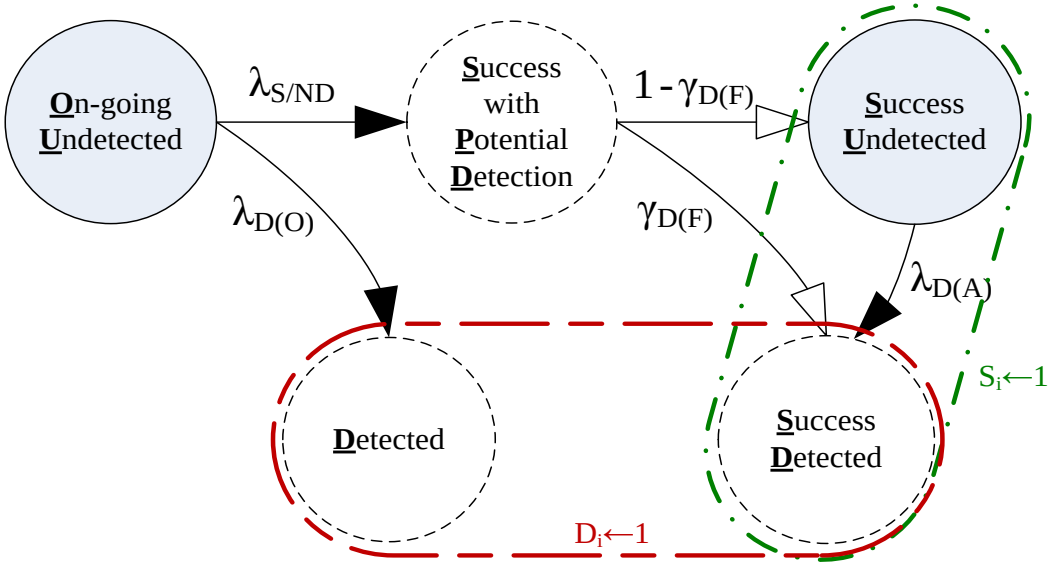
- Leaf specifications for AA, ISE and TSE
- Detection and reaction modeling
  - Four types (IOFA): Initial, On-going, Final, A posteriori
  - Three modes instead of two
    - Idle, Active Detected, and Active Undetected

Detections/reactions for AA leaves

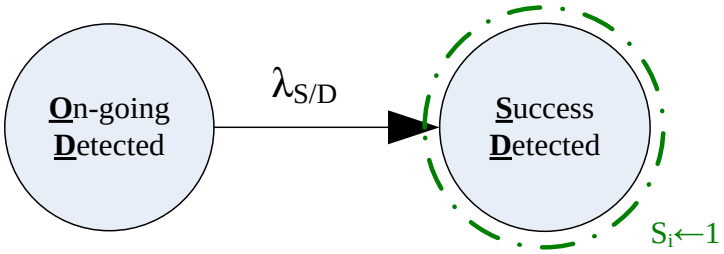
Idle Mode



Active Undetected Mode



Active Detected Mode



Transfer functions

$f^{i}_{0\to 1\,0}(PU)=\{Pr(OU)=1-\gamma_{D(I)},\ Pr(D)=\gamma_{D(I)},\ Pr(SD)=0,\ Pr(SU)=0\}$

$(PD)=\{Pr(OU)=0,\ Pr(D)=1,\ Pr(SD)=0,\ Pr(SU)=0\}$

$(SU)=\{Pr(OU)=0,\ Pr(D)=0,\ Pr(SD)=0,Pr(SU)=1\}$

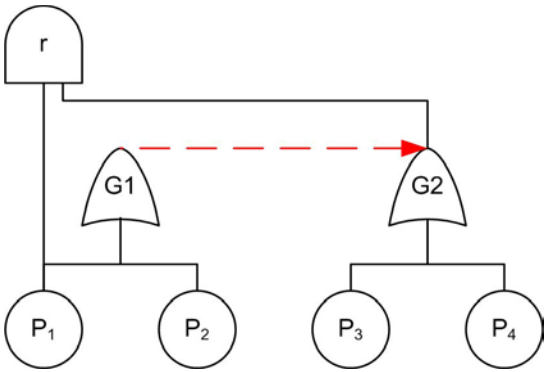
$(SD)=\{Pr(OU)=0,\ Pr(D)=0,\ Pr(SD)=1,Pr(SU)=0\}$

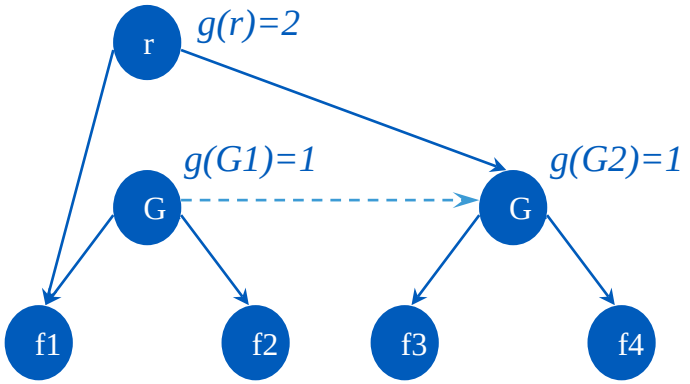
[…]

Formal foundations – snapshot 1/3

A (security-oriented) BDMP $(\mathcal{A}, r, T, P)$ 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 2/3

- $P=\{P_i\}_{i\in E}$, triggered Markov Processes

$$P_i=\left\{Z_0^i(t), Z_{10}^i(t), Z_{11}^i(t), f_{0\to 10}^i, f_{0\to 11}^i, f_{10\to 11}^i, f_{10\to 0}^i, f_{11\to 0}^i\right\}$$

  - $Z_0^i(t)$, $Z_{10}^i(t)$ and $Z_{11}^i(t)$ three homogeneous Markov process
    - For k in $\{0, 1\}$ (modes), A_k^i state-space of $Z_k^i(t)$
    - $S_k^i \subset A_k^i$, subset of successes/security event realizations
    - $D_k^i \subset A_k^i$, subset of detected states
  - $f_{0\to 10}^i(x)$ […] $f_{11\to 0}^i(x)$ "probability transfer functions" with
    - $\forall x \in A_0^i$, $f_{0\to 10}^i(x)$ is a probability distribution on A_{10}^i such that $x \in S_{10}^i \Rightarrow \sum_{j\in S_1^i}(f_{0\to 10}^i(x))(j)=1$ and $x \in D_{10}^i \Rightarrow \sum_{j\in D_1^i}(f_{0\to 10}^i(x))(j)=1$
    - […] x 5 $\left\{f_{0\to 11}^i, f_{10\to 11}^i, f_{10\to 0}^i, f_{11\to 0}^i\right\}$

Formal foundations – snapshot 3/3

- Four families of Boolean functions of the time
  - Structure functions $(S_i)_{i \in E}$

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

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

  - Process selectors $(X_i)_{i \in E}$

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

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

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

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

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

  - Detection status indicators $(D_i)_{i \in E}$

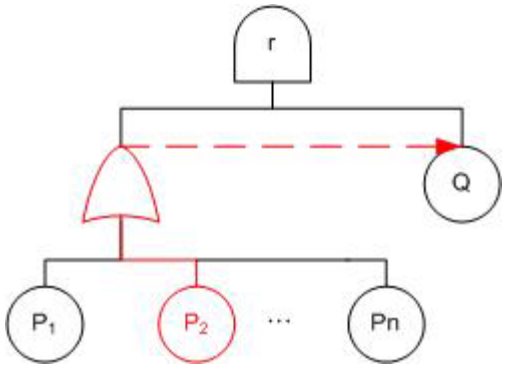
$$\forall i \in B, \quad D_i \equiv \left(Z^i_{X_i} \in D^i_{X_i}\right) \vee \left(\exists j \in B \,/\, j \neq i \wedge D_j = 1\right) \quad \forall j \in G, \; D_j \equiv \left(\exists i \in B \,/\, D_i = 1\right)$$

Mathematical properties

Robustness

- Theorem 1: $(S_i)(X_i)(Y_i)\ )(D_i)_{i\in E}$ 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 $(\{P_1,Q\},\{P_1,P_2,Q\},\{P_1,P_3,Q\},\ldots)$

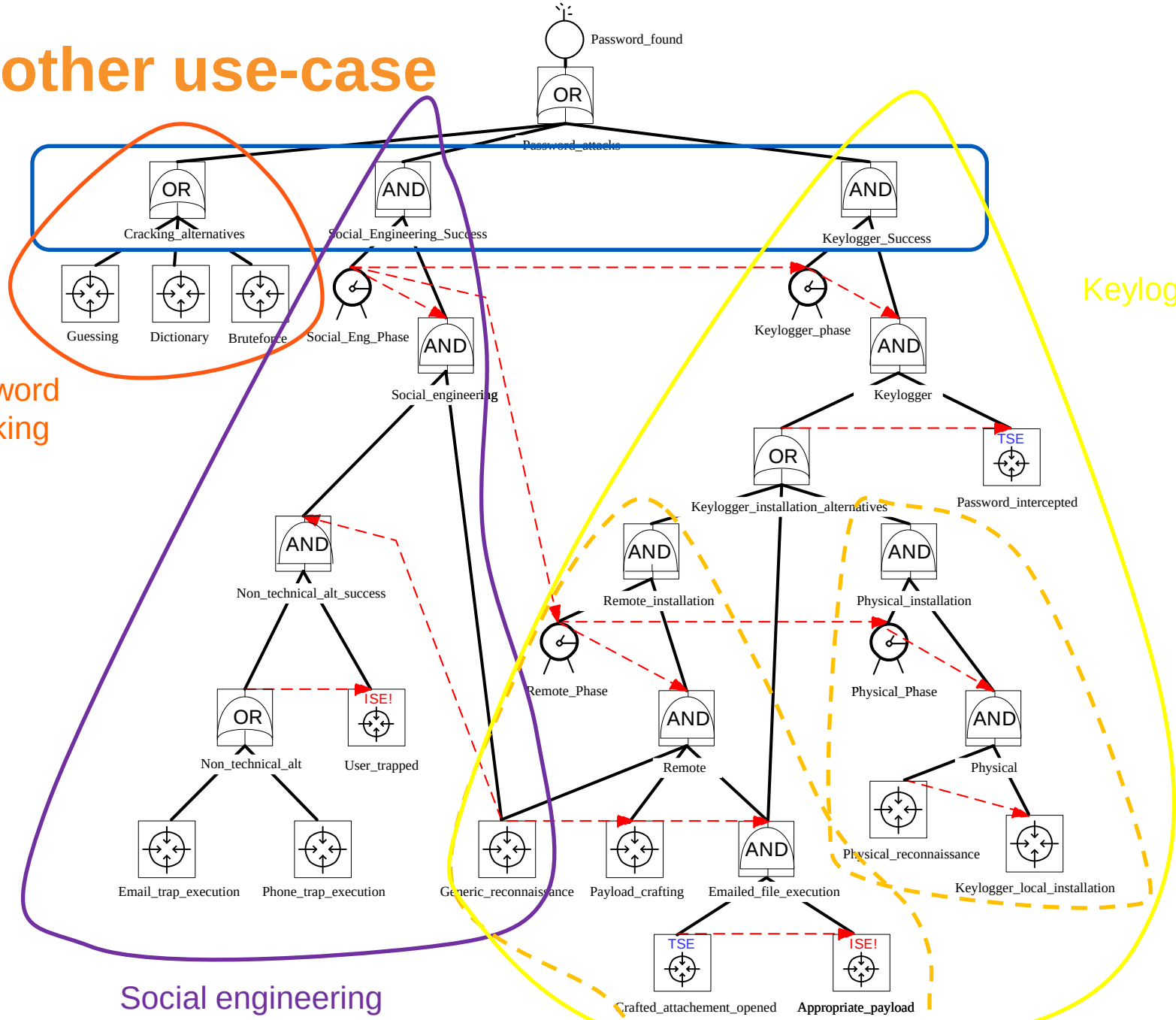
- Theorem 3: if the P_i are such that $\forall i \in B, \forall t, \forall t' \geq t, S_i(t)=1 \Rightarrow S_i(t')=1$* and detection aspects are not considered, $Pr(S_r(t)=1)$ is unchanged whether irrelevant event ($Y_i=0$) are trimmed or not.

* This is always the case in our framework

Quantifications

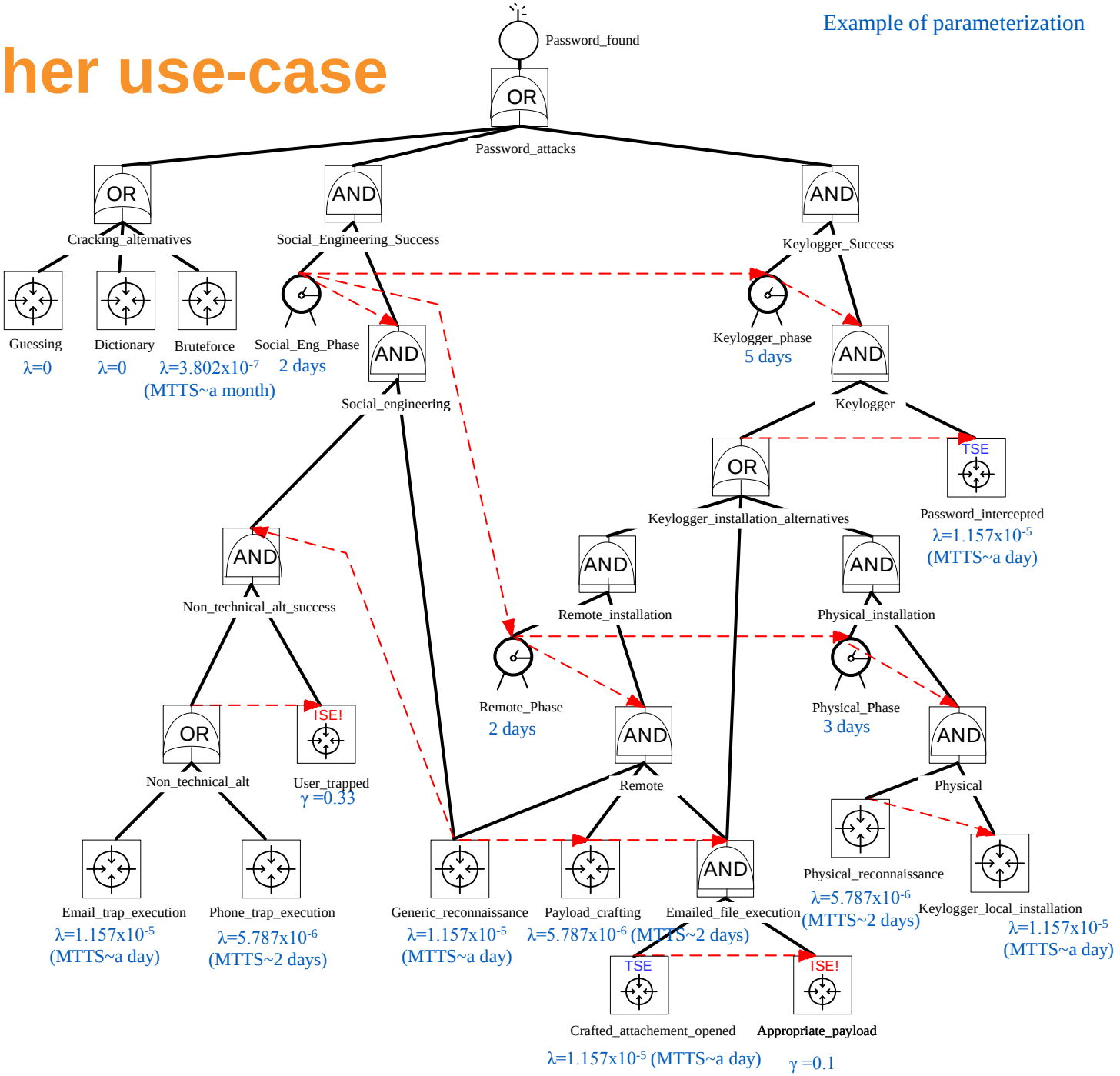
- Time-independent (static) - Classical attack tree parameters
  - Monetary cost → scenario cost, average attack cost
  - Boolean indicators (specific requirements, properties)
  - Minimum attacker skills
- Time-domain analysis – Leveraging the BDMP framework
  - Quantification tools, algorithms and 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

Another use-case



Another use-case

Example of parameterization



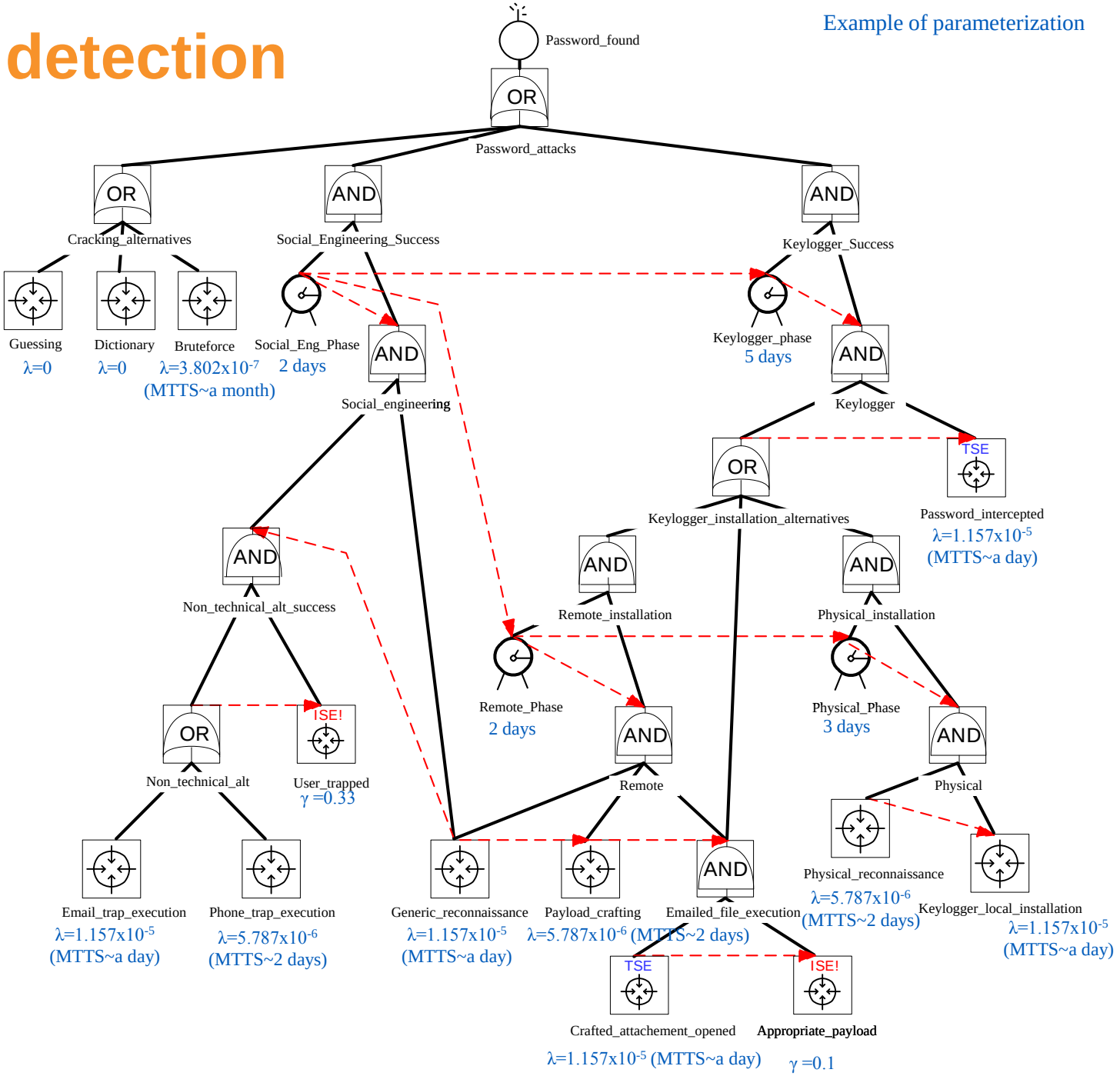
Results

- Overall probability in a week = 0.422 (MTTS = 22 days)
- Ordered list of attack sequences (654 sequences)

	Sequences	Probability in a week	Average duration	Contrib.
1	<Social Eng>Generic reconn., Email trap exec., User trapped	1.059×10^{-1}	9.889×10^{4}	25.1%
2	<Social Eng>Generic reconn., Phone trap exec., User trapped	5.295×10^{-2}	9.889×10^{4}	12.5%
3	Bruteforce	2.144×10^{-2}	5.638×10^{4}	5.1%
4	<Social Eng></Social Eng><Keylogger><Remote></Remote> <Physical> Physical reconn., Keylogger local installation, Password intercepted	1.749×10^{-2}	2.976×10^{5}	4.1%
5	<Social Eng></Social Eng><Keylogger> <Remote>*Generic reconnaissance* </Remote><Physical>Physical reconnaissance, Keylogger local installation, Password intercepted	1.350×10^{-2}	3.677×10^{5}	3.2%
6	<Social Eng>*Generic reconnaissance*, *Email trap execution*, *User trapped(failure)*, Bruteforce	1.259×10^{-2}	2.610×10^{5}	3.0%
...				
20	<Social Eng></Social Eng><Keylogger><Remote>Generic reconnaissance, Payload crafting, Appropriate payload, Password intercepted	2.500×10^{-3}	2.761×10^{5}	0.6%
...				
34	<Social Eng></Social Eng><Keylogger> <Remote>Generic reconn., *Payload crafting* </Remote> <Physical>*Crafted attachement opened*, *Appropriate payload*, Physical reconn., Keylogger local installation, Password intercepted	1.506×10^{-3}	4.594×10^{5}	0.4%

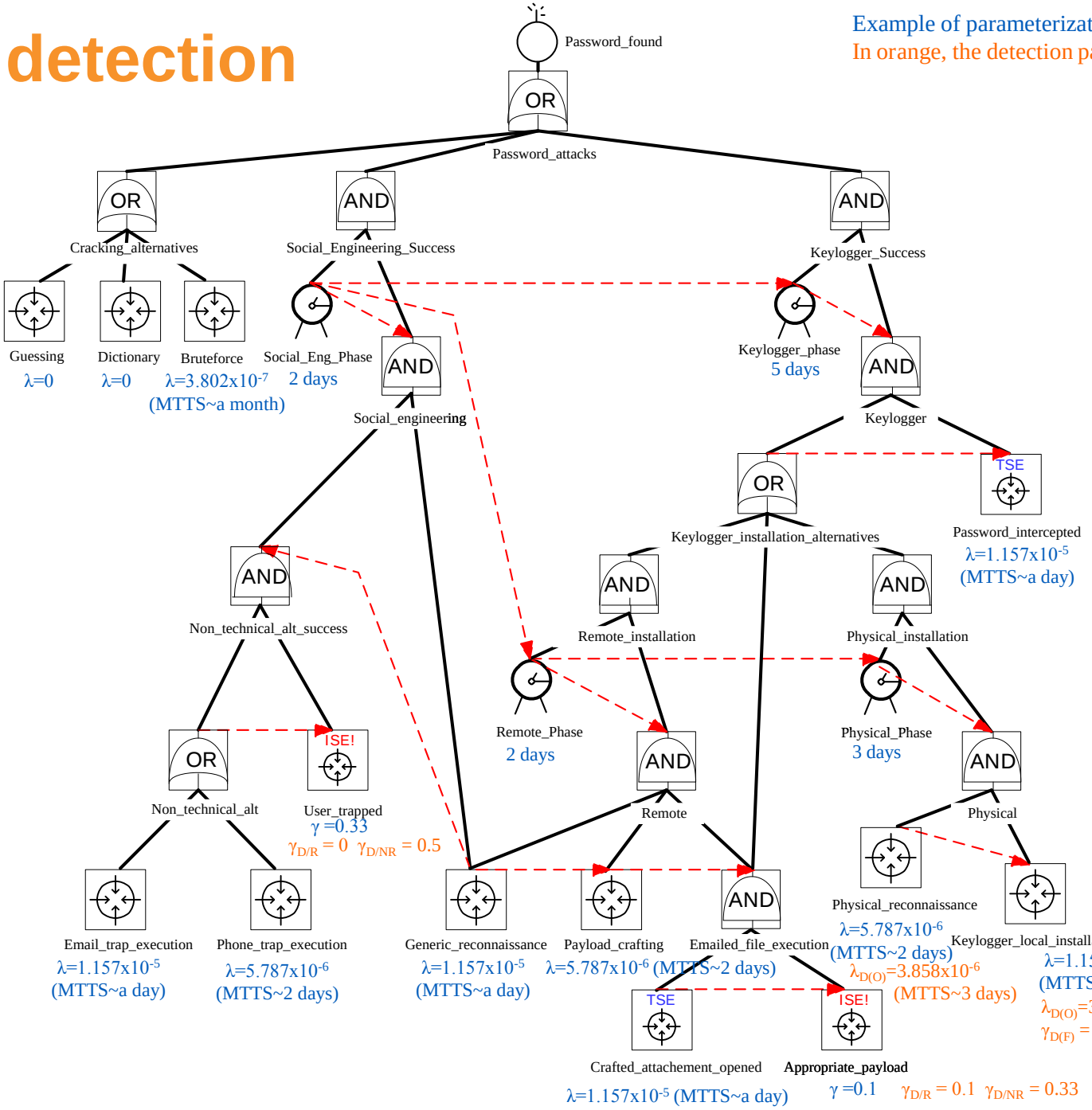
With detection

Example of parameterization



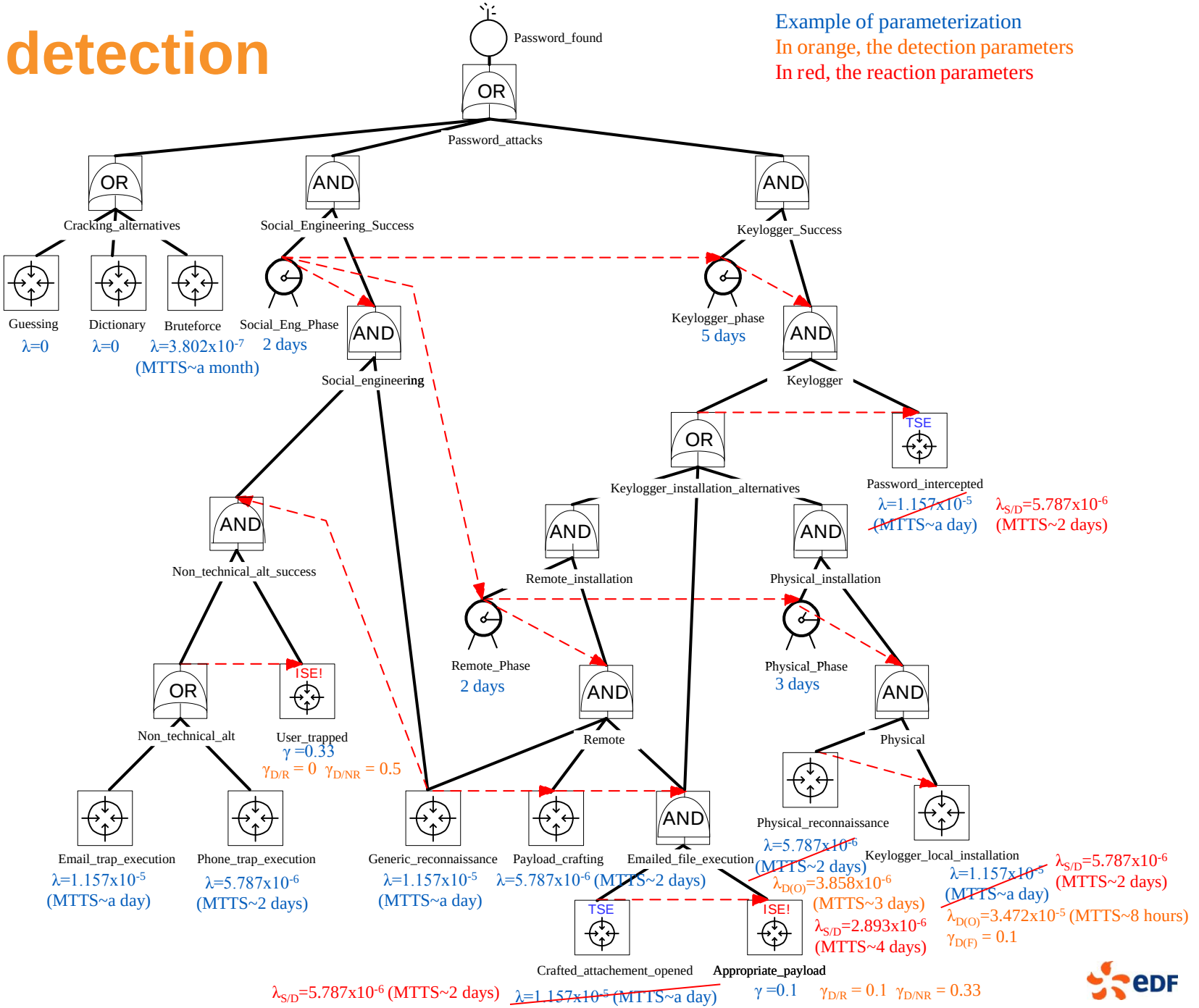
With detection

Example of parameterization
In orange, the detection parameters



With detection

Example of parameterization
In orange, the detection parameters
In red, the reaction parameters



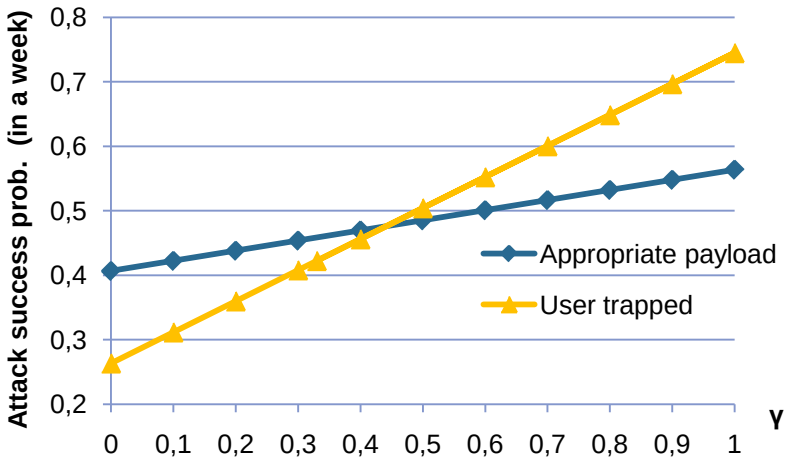
Results

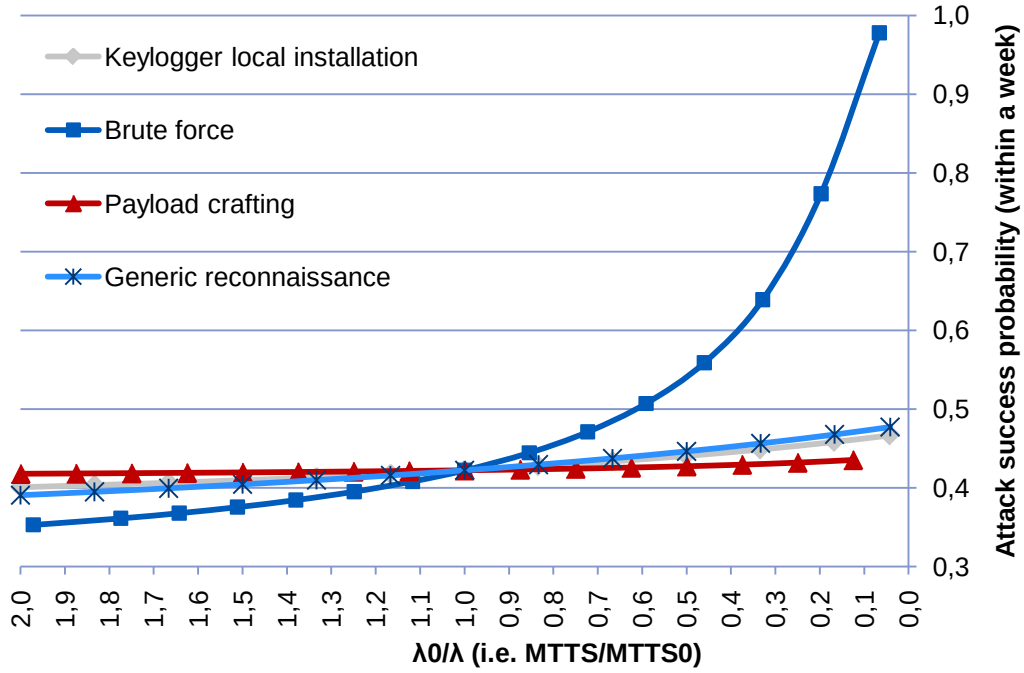
- Probability of success within a week = 0.364 (-14 %)
- Representative sequences (4231 vs 654)

	Sequences	Probability in a week	Average duration	Contrib.
1	<Social Eng>Generic reconn., Email trap exec., User trapped	1.091×10^{-1}	9.889×10^{4}	30.0%
2	<Social Eng>Generic reconn., Phone trap exec., User trapped	5.456×10^{-2}	9.889×10^{4}	15.0%
3	Bruteforce	2.144×10^{-2}	5.638×10^{4}	5.9%
4	<Social Eng>*Generic reconnaissance*, Bruteforce	1.055×10^{-2}	9.889×10^{4}	2.9%
...	([...], Bruteforce) × 9			
14	<Social Eng><Social Eng><Keylogger><Remote>Generic reconnaissance, Payload crafting(no detection), Appropriate payload(no detection), Password intercepted	2.250×10^{-3}	2.761×10^{5}	0.6%
...	([...], Bruteforce) × 2			
17	<Social Eng>Generic reconnaissance <Social Eng><Keylogger><Remote>Payload crafting(no detection), Appropriate payload(no detection), Password intercepted	1.923×10^{-3}	2.688×10^{5}	0.5%
...	([...], Bruteforce) × 2			
20	<Social Eng>*Generic reconnaissance, Email trap exec., User trapped(failure and detection)* <Social Eng><Keylogger><Remote><Remote><Physical>Physical reconn., Keylogger local installation, Password intercepted	1.549×10^{-3}	5.991×10^{5}	0.4%

Recent enhancements & complementary tools

- Sequence analysis
  - Filtering by static/time-independant parameters, i.e. attacker profile
  - Sequence presentation (visual conventions)
- Sensitivity analysis
  - Optimize security efforts
  - Most “significant” leaves
  - Iterated treatments

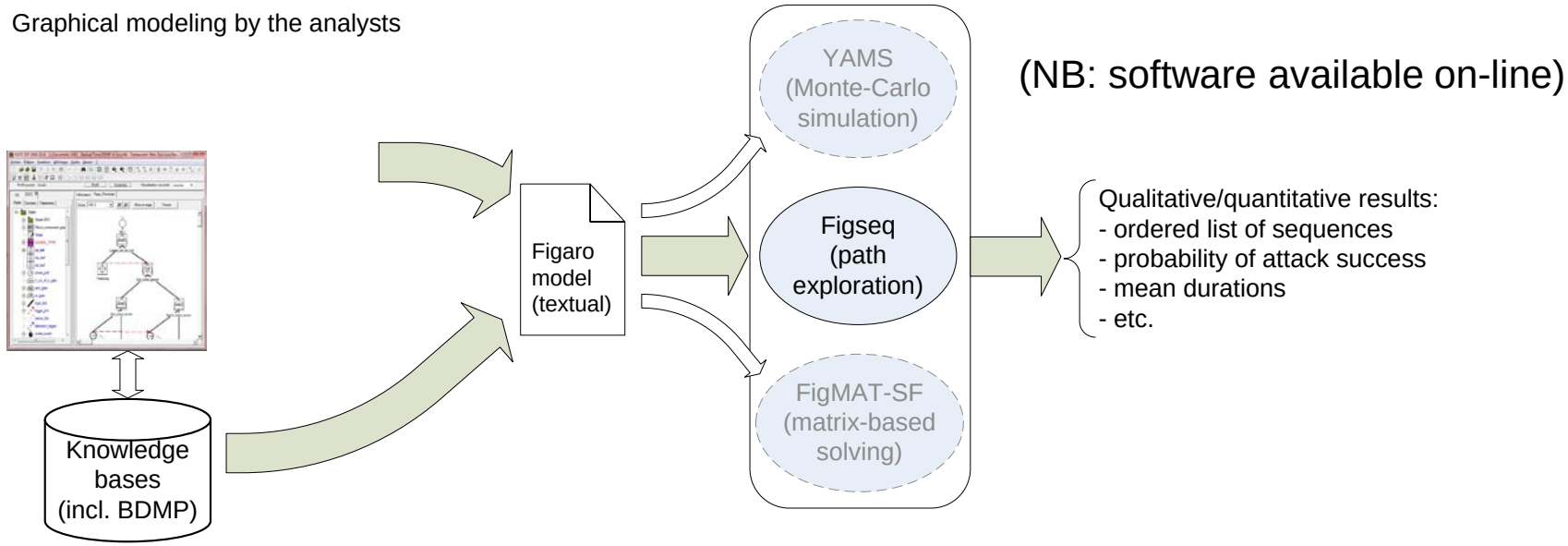




A few words about the implementation

Leveraging of the KB3 platform (EDF)

- Used at EDF for dependability studies for more than 15 years
- Modularity thanks to “Knowledge Bases”, written in Figaro



A dedicated security knowledge basis

- Implementation was easy and fast (available on-line)

Perspectives and on-going work

- Enhance usability
  - Users' feedback, case-studies, tutorials
  - Side-tools (sensitivity script HMI, etc.)
  - Attack pattern library
- Theoretical extensions
  - Experiment different probability distributions (e.g., McQueen *et al.*)
  - Integration with Bayesian networks
  - Many attack trees extensions could be adapted
    - Intervals, fuzzy sets, OWA gates, game theory, etc.
  - Uncertainty handling and propagation
- Internal and external dissemination! (thanks ☺)

Conclusion

- Graphical security modeling
  - Different balances between readability, scalability, modeling power and quantification capabilities
- BDMP, an original and attractive trade-off
  - With a sound theoretical framework
  - Already an operational formalism
- Limits
  - Inherent limits of BDMP (e.g., with cyclic behaviors/loops)
  - Attacker behavior stochastic modeling – subjective probabilities
  - More generally, 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,” *Proceedings of CIEM 2005*, Bucharest, Romania, oct. 2005

Marc Bouissou’s homepage: http://marc.bouissou.free.fr/

On BDMP & Security

- L. Piètre-Cambacédès et M. Bouissou, “Attack and defense dynamic modeling with BDMP,” in *Proc. 5th International Conference on Mathematical Methods, Models, and Architectures for Computer Networks Security (MMM-ACNS-2010)*, St Petersburg, Russia, sept. 2010
- L. Pietre-Cambacedes, Y. Deflesselle and M. Bouissou, "Security modeling with BDMP: from theory to implementation," in *Proc. 6th IEEE International Conference on Network and Information Systems Security (SAR-SSI 2011)*, La Rochelle, France, may 2011
- L. Piètre-Cambacédès and M. Bouissou, “Modeling safety and security interdepedencies with BDMP (Boolean logic Driven Markov Processes),” *Proc. IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010*), Istanbul, Turkey, oct. 2010.

Ludovic Pietre-Cambacedes’ homepage: http://perso.telecom-paristech.fr/~pietreca/

Try the tools:
Free download on Sourceforge/Visualfigaro
(or look for « KB3 EDF » in Google)

THANK YOU VERY MUCH!