Attack and Defense Modeling with BDMP (Boolean logic Driven Markov Processes)

September 8th 2010

MMM-ACNS 2010, St Petersburg, Russia

Ludovic Piètre-Cambacédès

Marc Bouissou

EDF R&D

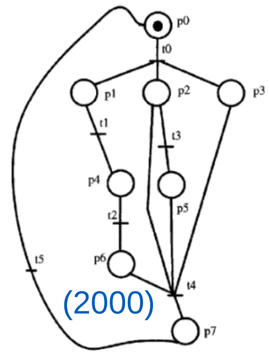
LEADING THE ENERGY CHANGE

Agenda

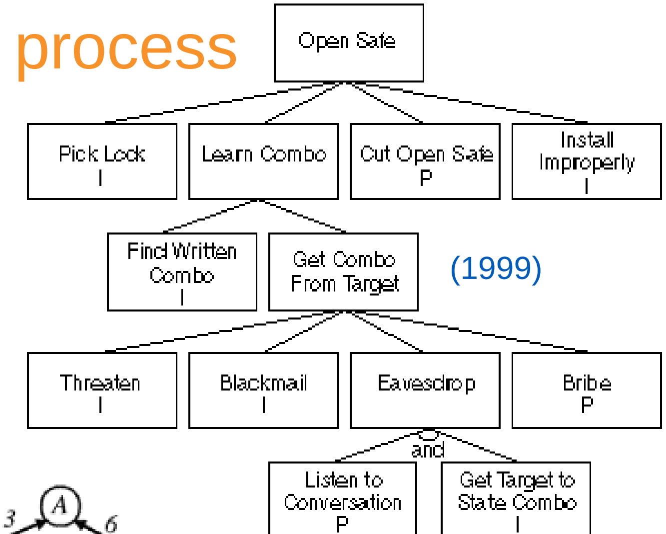
- **Introduction**
  - Graphical attack modeling
- **Attack modeling with BDMP**
  - Formalism description
  - Example & quantifications
- **Defensive aspects modeling**
  - Augmented theoretical framework
  - Use-case & quantifications
- **On-going work, perspectives**
  - Recent advance, future work
- **Conclusion and Q&A**

Graphical modeling of computer attacks

- Graphical representation of an attack process
  - Formalize reasoning
  - Share standpoints
  - Enhance coverage

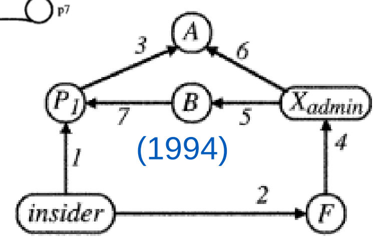


(2000)

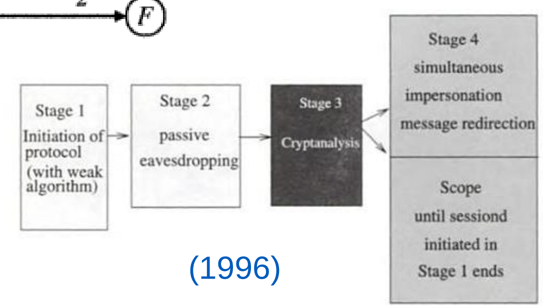


(1999)

- An active field of research
  - Static models (eg. attack tree)
  - Dynamic models (eg. Petri-net)



(1994)

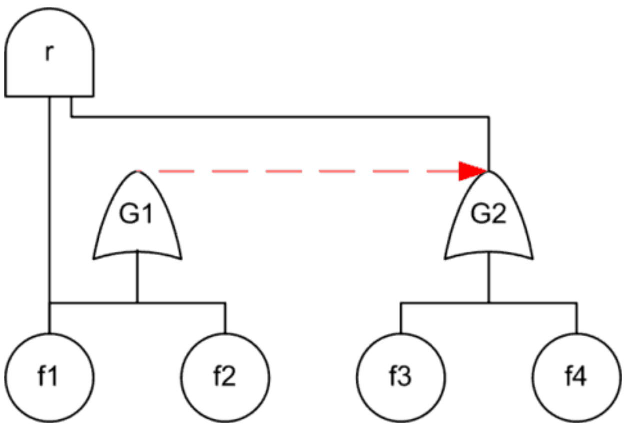


(1996)

- Different trade-offs
  - Readability, scalability, modeling and quantification capabilities

BDMP, the potential for an attractive trade-off

- Interest proven in reliability and safety engineering

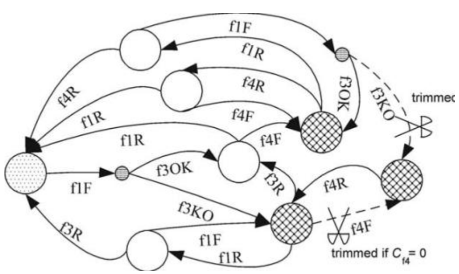


✓ Dynamic

✓ 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 attack modeling

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

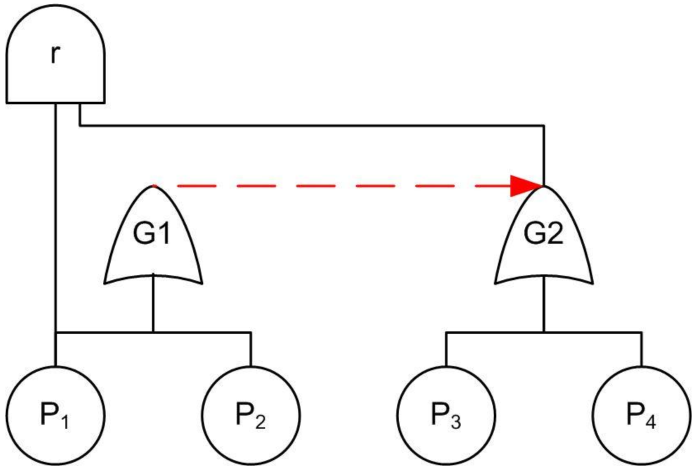
Graphical elements

- BDMP = $\{\mathcal{A}, r, T, \{P_i\}\}$

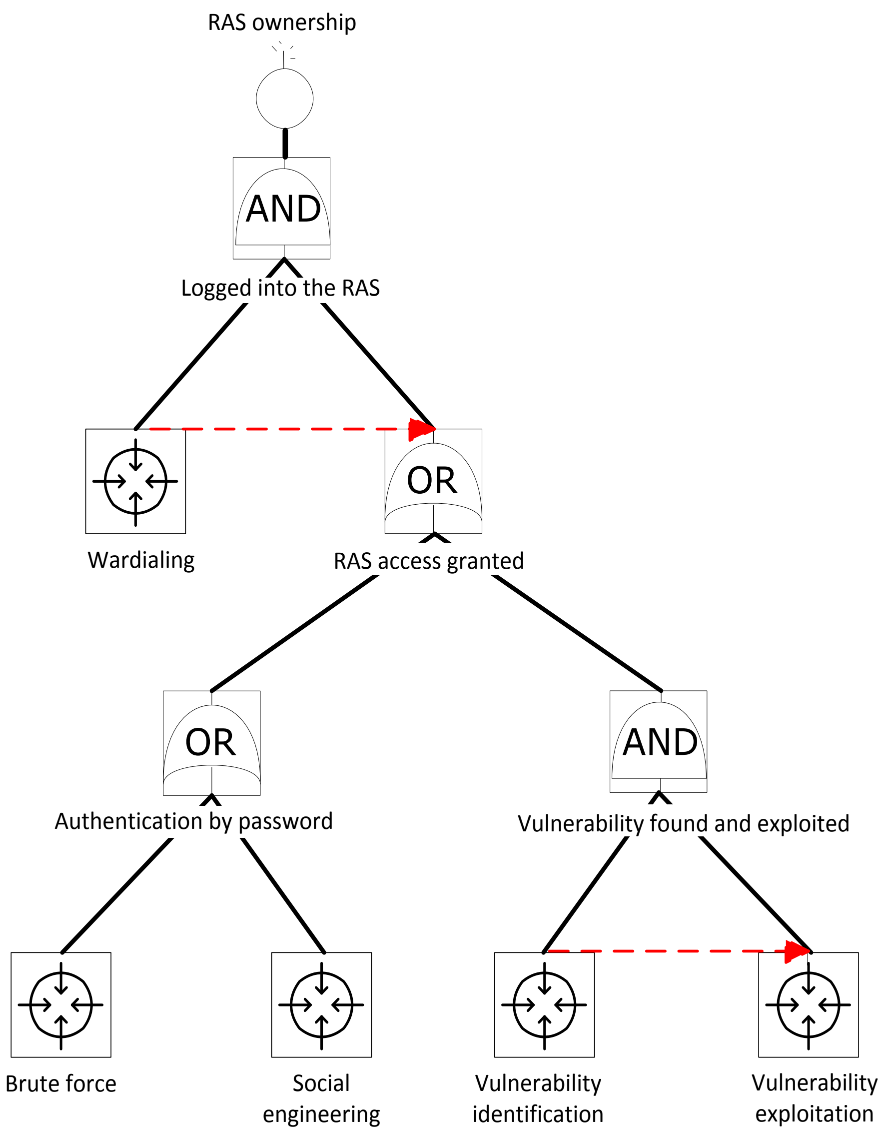
$\mathcal{A}$ = Attack Tree, r = top event,

G1 = secondary top, T = trigger,

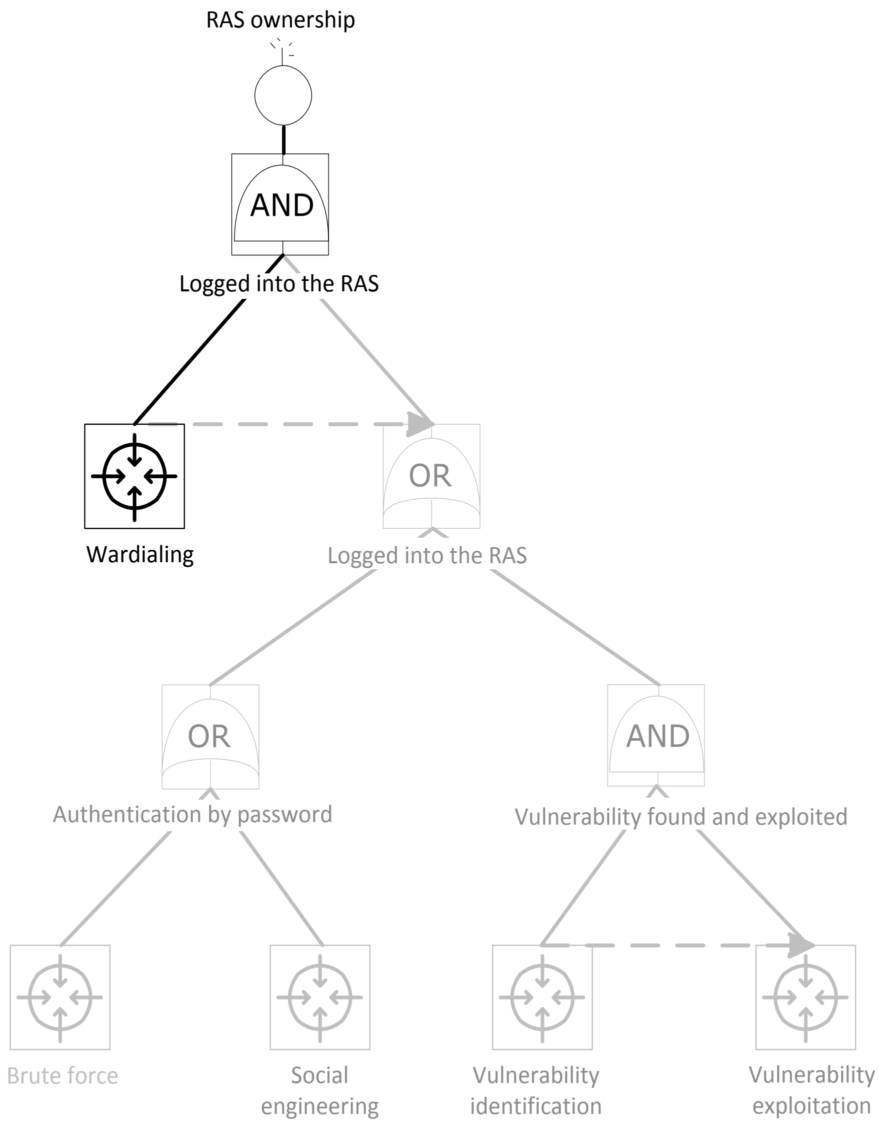
P_i =“triggered” Markov processes



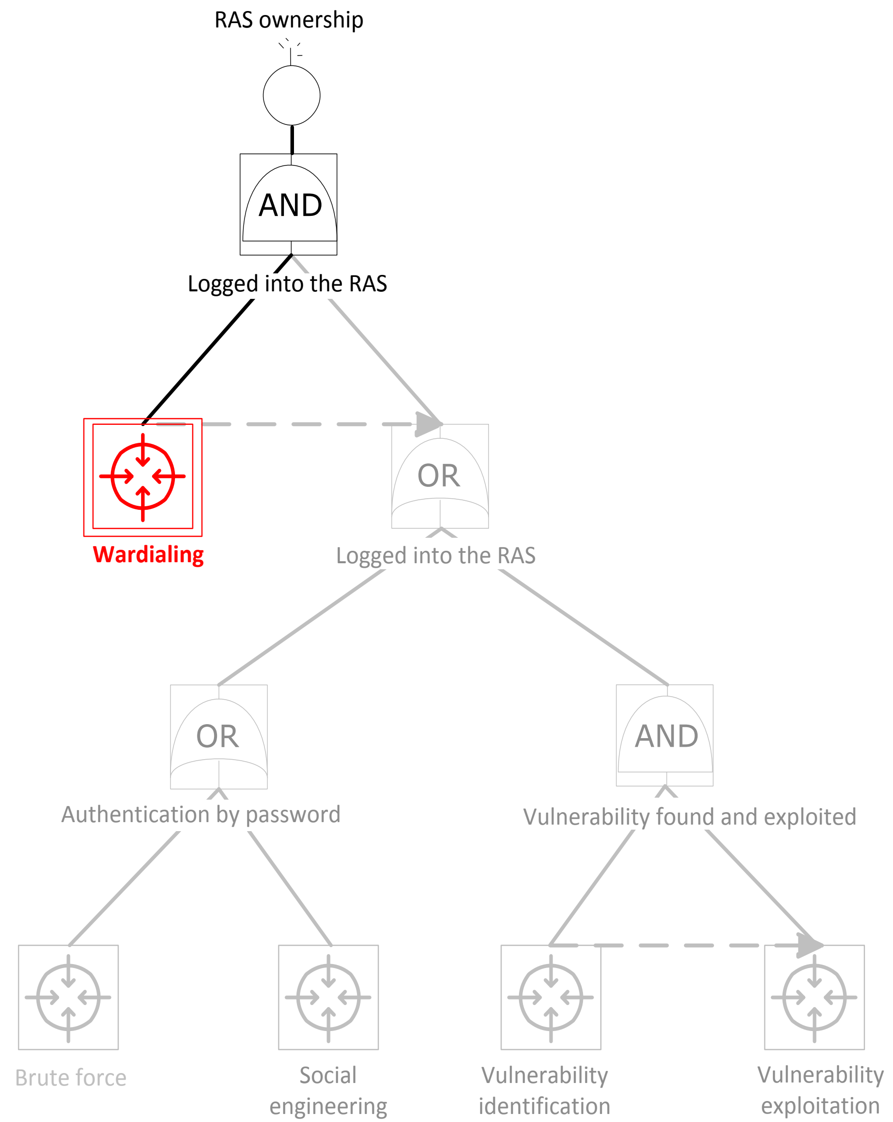
A first feel: a simple Remote Access Server attack



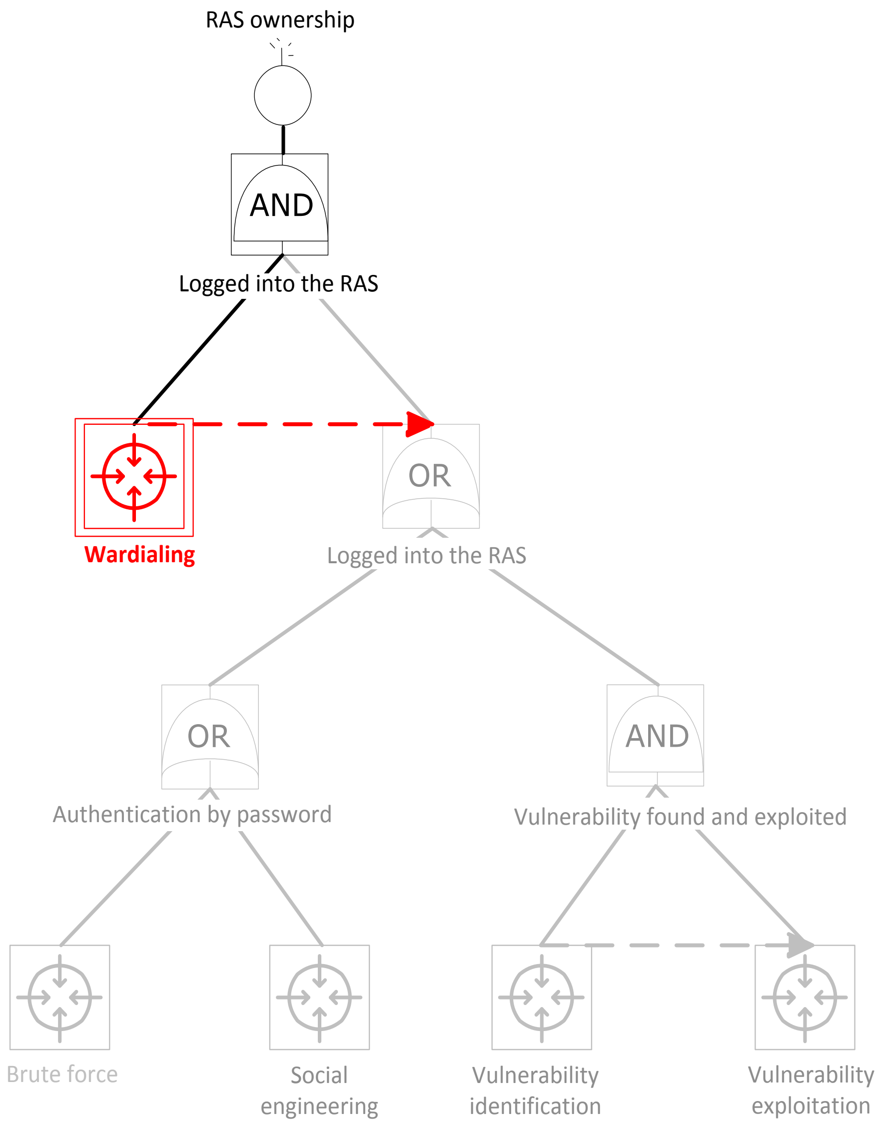
RAS attack BDMP – Step 0 (attack just started)



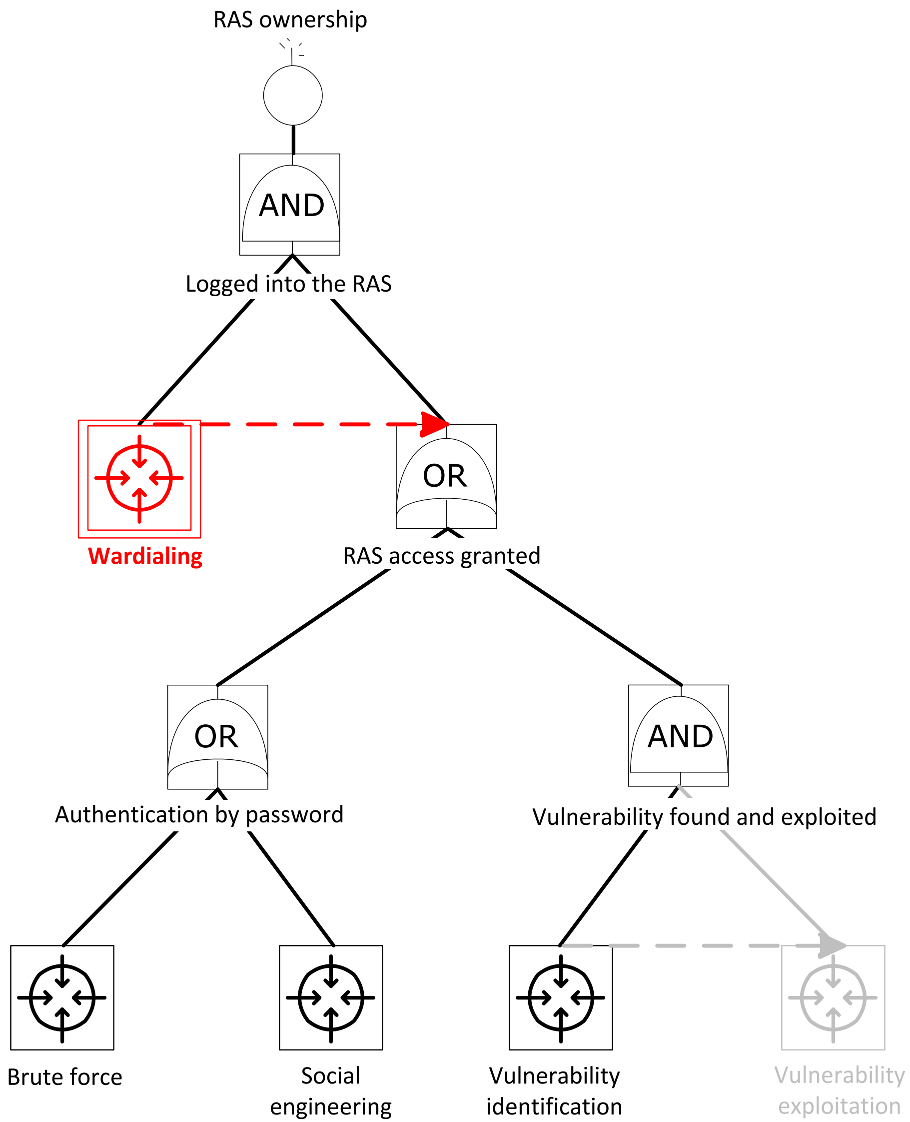
RAS attack BDMP – Step 1



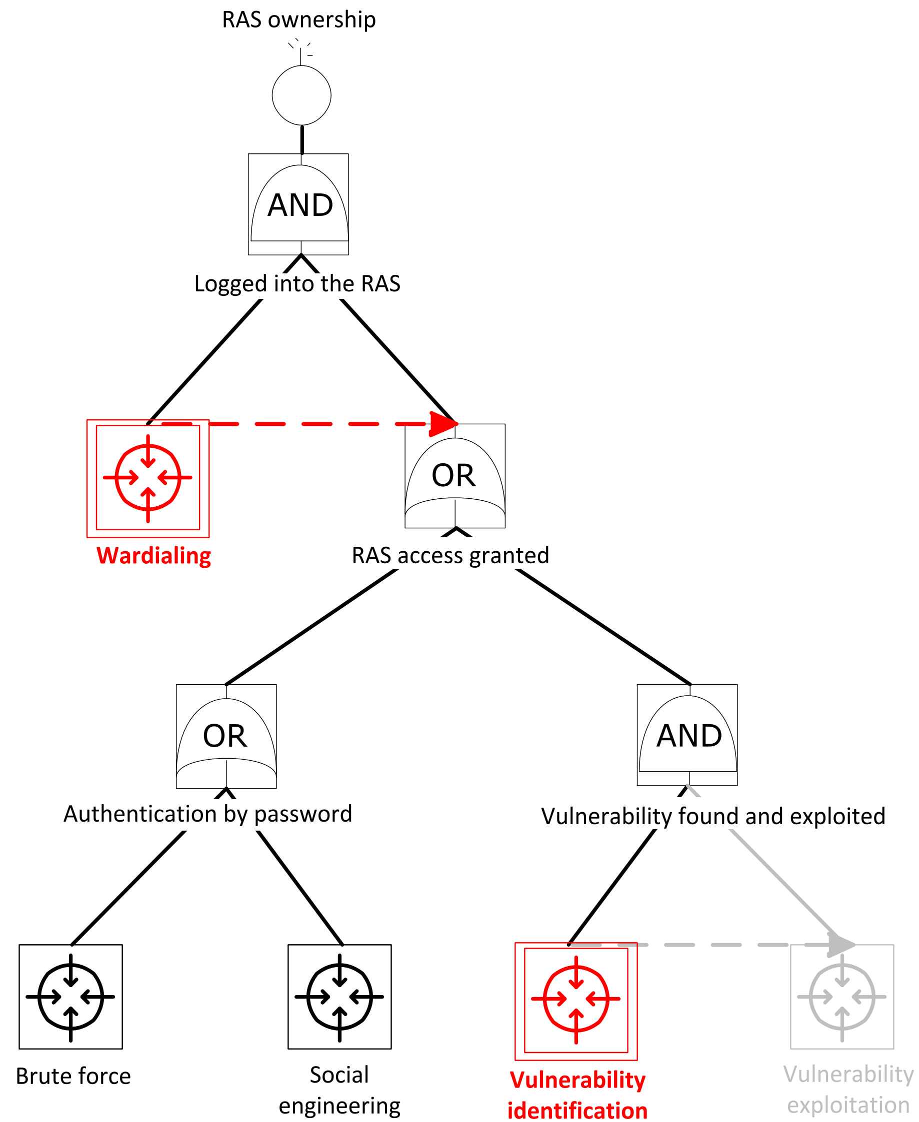
RAS attack BDMP – Step 1



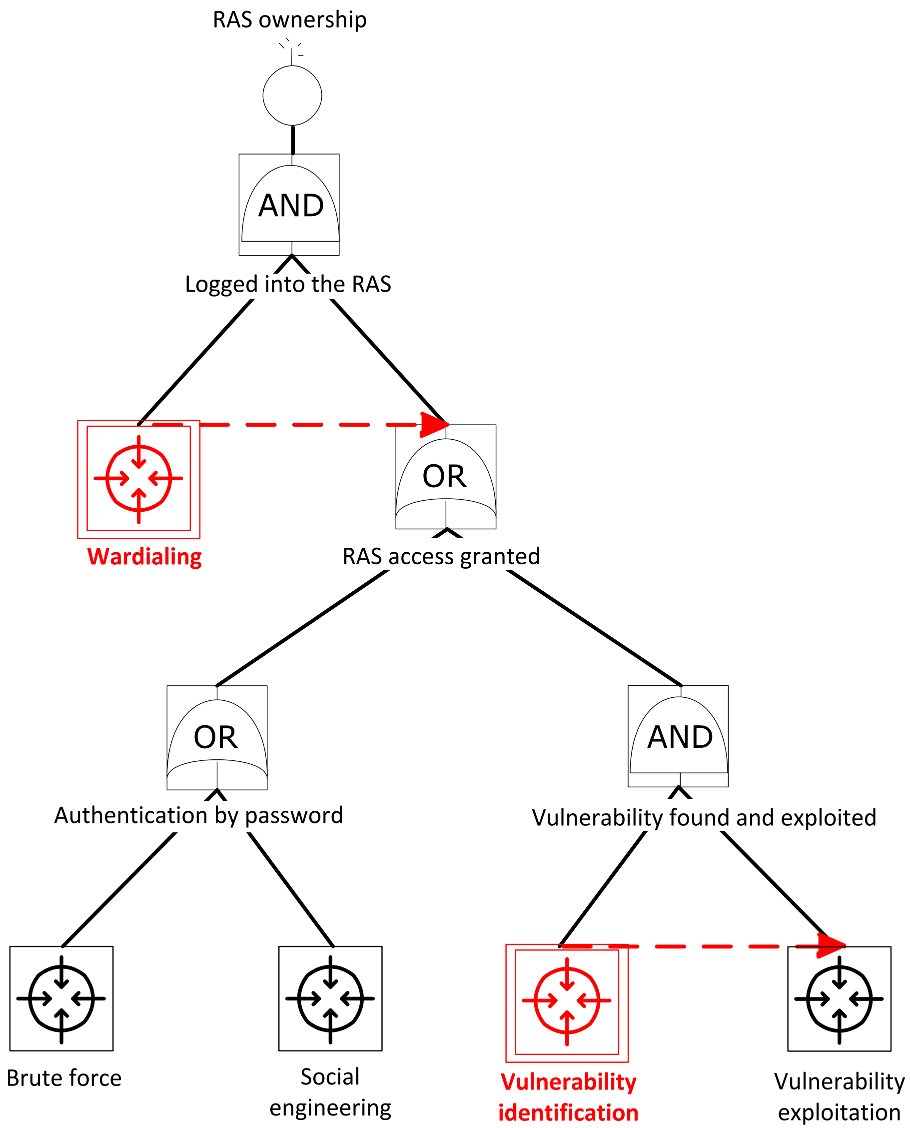
RAS attack BDMP – Step 1



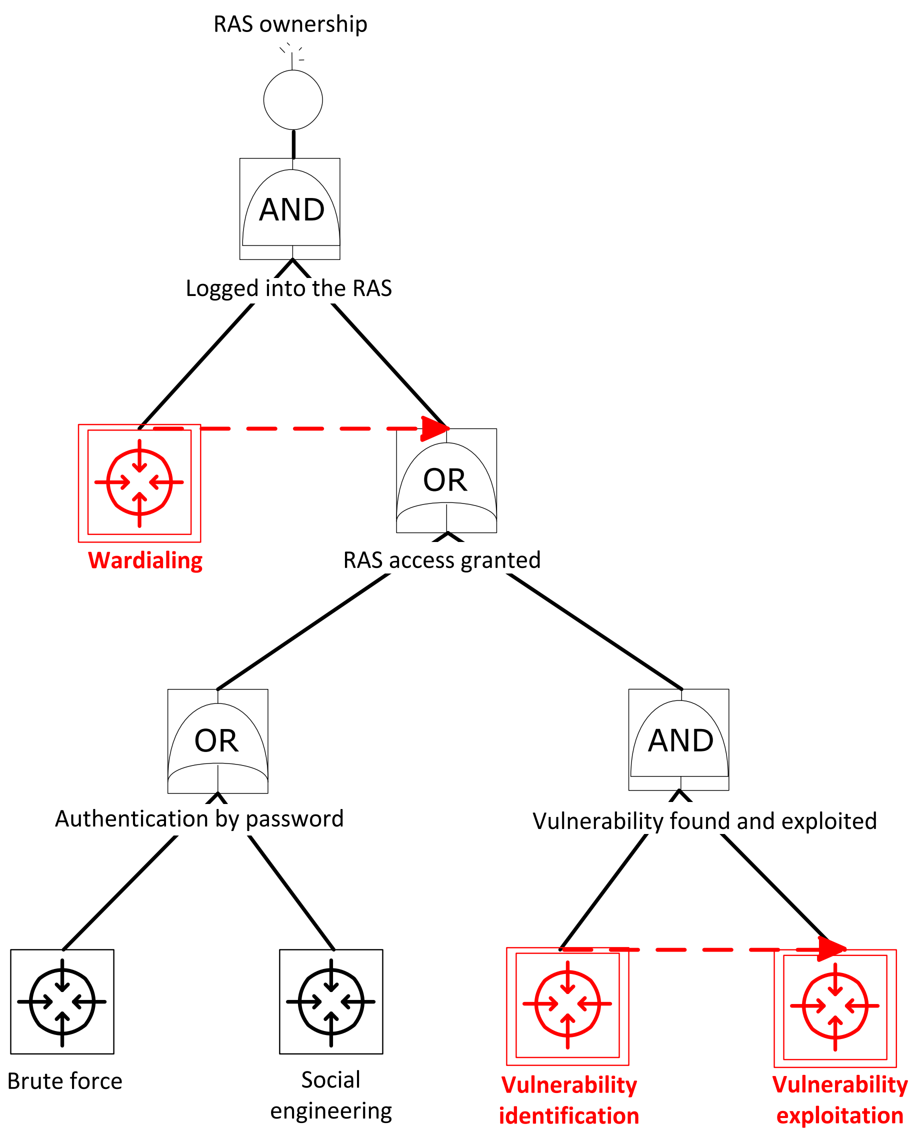
RAS attack BDMP – Step 2



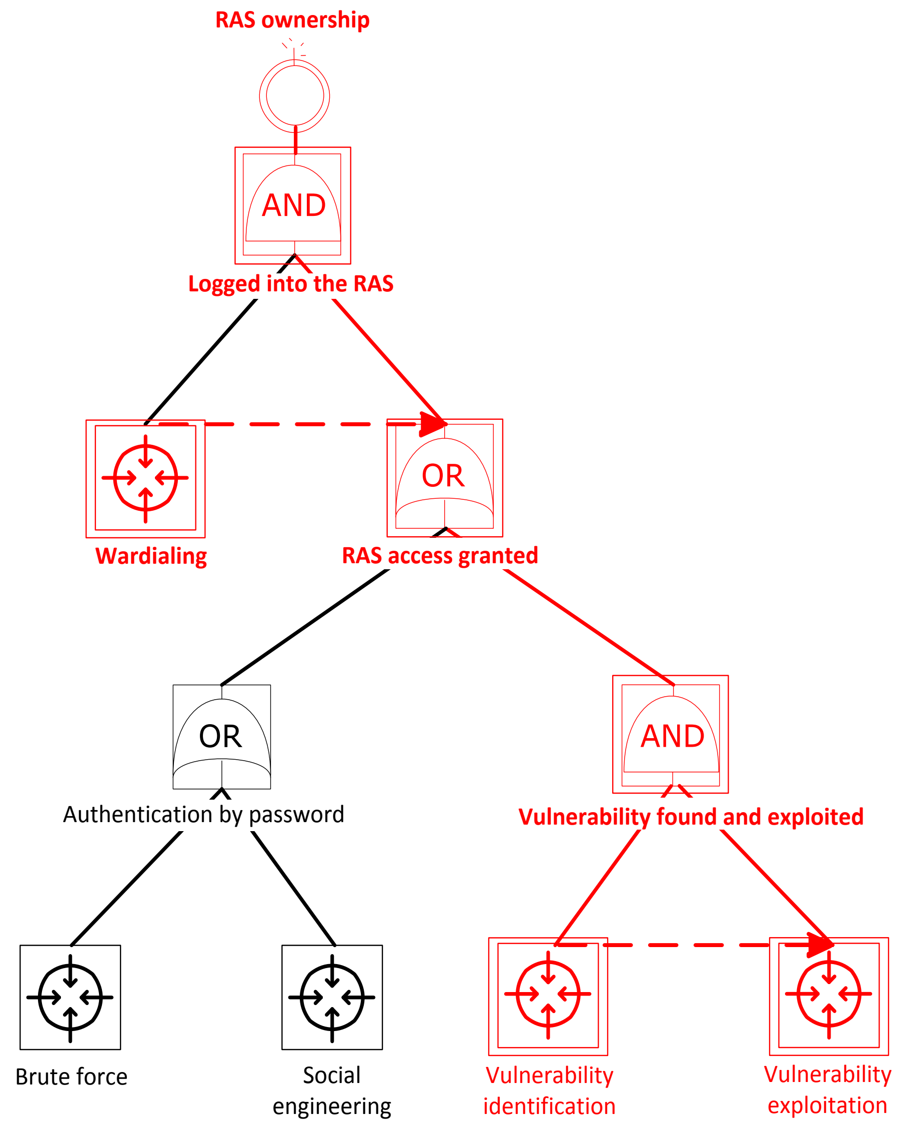
RAS attack BDMP – Step 2



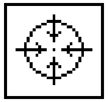
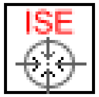
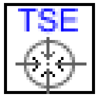
RAS attack BDMP – Step 3



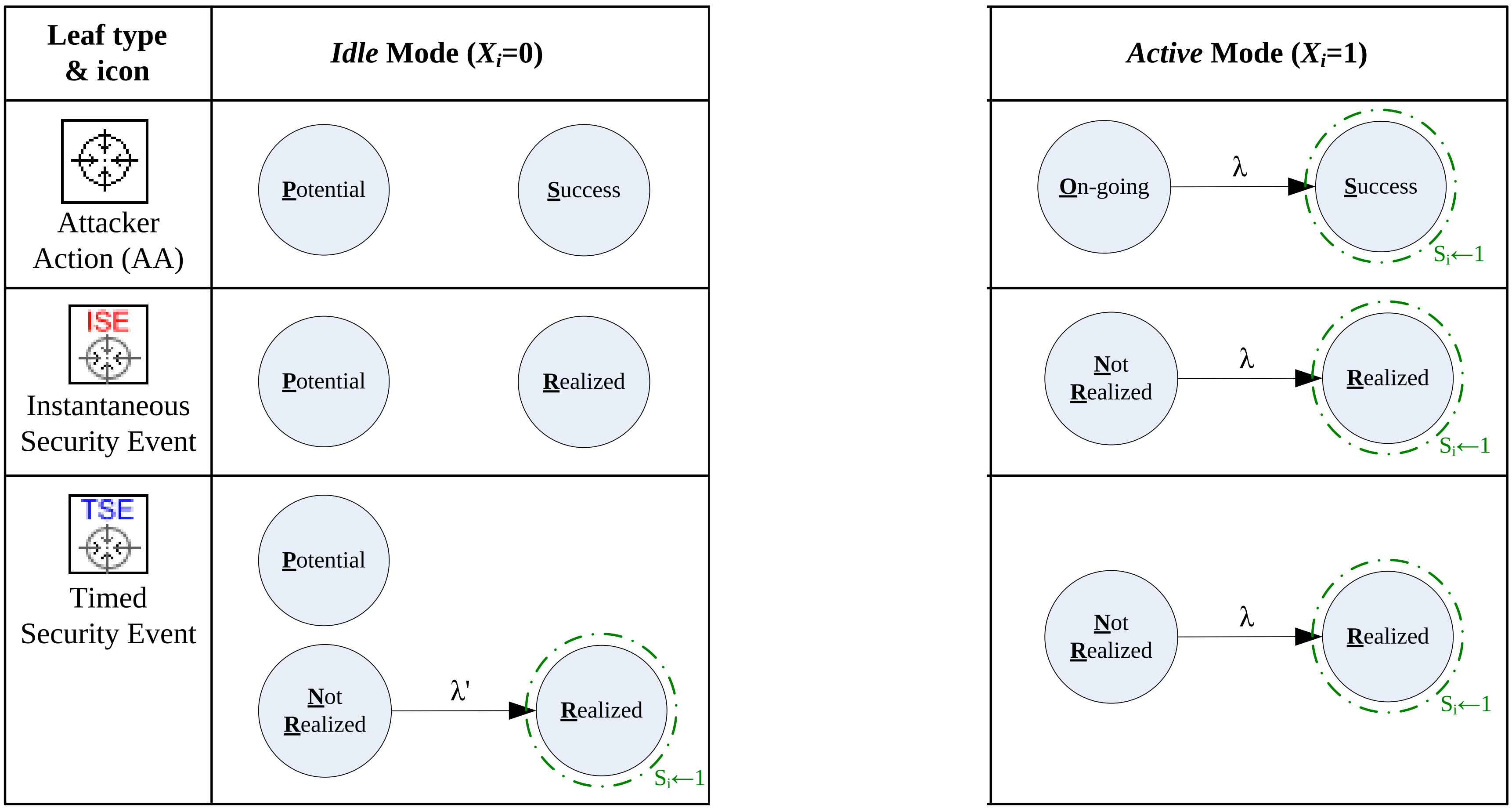
RAS attack BDMP – Attacker’s objective reached



A zoom on the three basic security leaves

Leaf type & icon
 Attacker Action (AA)
 Instantaneous Security Event
 Timed Security Event

A zoom on the three basic security leaves



A zoom on the three basic security leaves

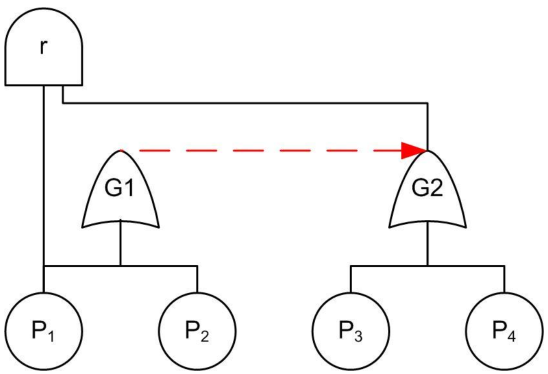
Leaf type & icon	*Idle* Mode (X_i=0)	Transfer between modes	*Active* Mode (X_i=1)
Attacker Action (AA)	**P**otential; **S**uccess	P⇔O (with $Pr = 1$) S⇔S (with $Pr = 1$)	**O**n-going →λ→ **S**uccess ($S_i \leftarrow 1$)
ISE Instantaneous Security Event	**P**otential; **R**ealized	P⇨NR (with $Pr=1-\gamma$) P⇨R (with $Pr = \gamma$) R⇔R (with $Pr = 1$) P⇦NR (with $Pr = 1$)	**N**ot **R**ealized →λ→ **R**ealized ($S_i \leftarrow 1$)
TSE Timed Security Event	**P**otential; **N**ot **R**ealized →λ'→ **R**ealized ($S_i \leftarrow 1$)	P⇨NR (with $Pr = 1$) NR⇔NR (with $Pr=1$) R⇔R (with $Pr = 1$)	**N**ot **R**ealized →λ→ **R**ealized ($S_i \leftarrow 1$)

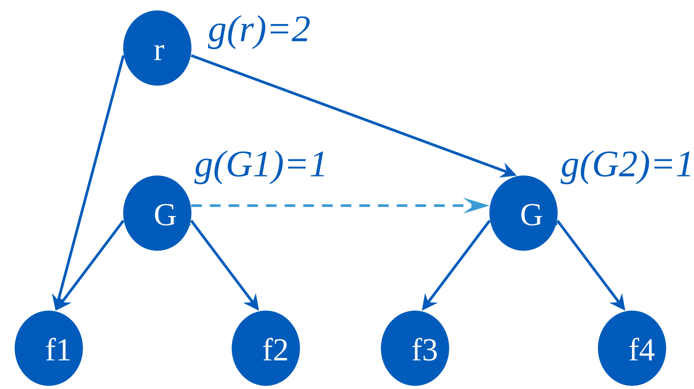
EDF

Formal foundations – snapshot 1/3

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

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

Formal foundations – snapshot 2/3

- $P = \{P_i\}_{i \in E}$, triggered Markov Processes $\{Z_0^i(t), Z_1^i(t), f_{0\to1}^i, f_{1\to0}^i\}$
  - $Z_0^i(t)$ 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 3/3

- Three families of Boolean functions of the time
  - 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

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

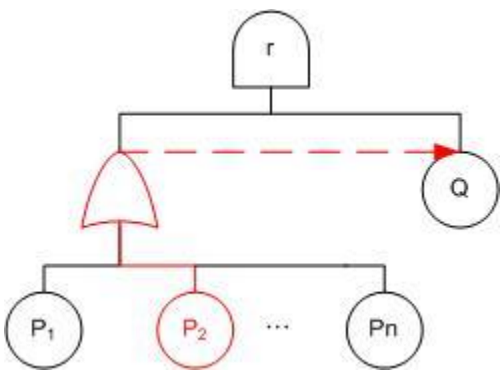
$$Y_i \equiv \left(\exists x \in E / (x,i) \in L \wedge Y_x \wedge S_x = 0\right) \vee \left(\exists y \in E / (i,y) \in T \wedge S_y = 0\right)$$

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 $(\{P_1,Q\},\{P_1,P_2,Q\}, \{P_1,P_3,Q\},\ldots)$

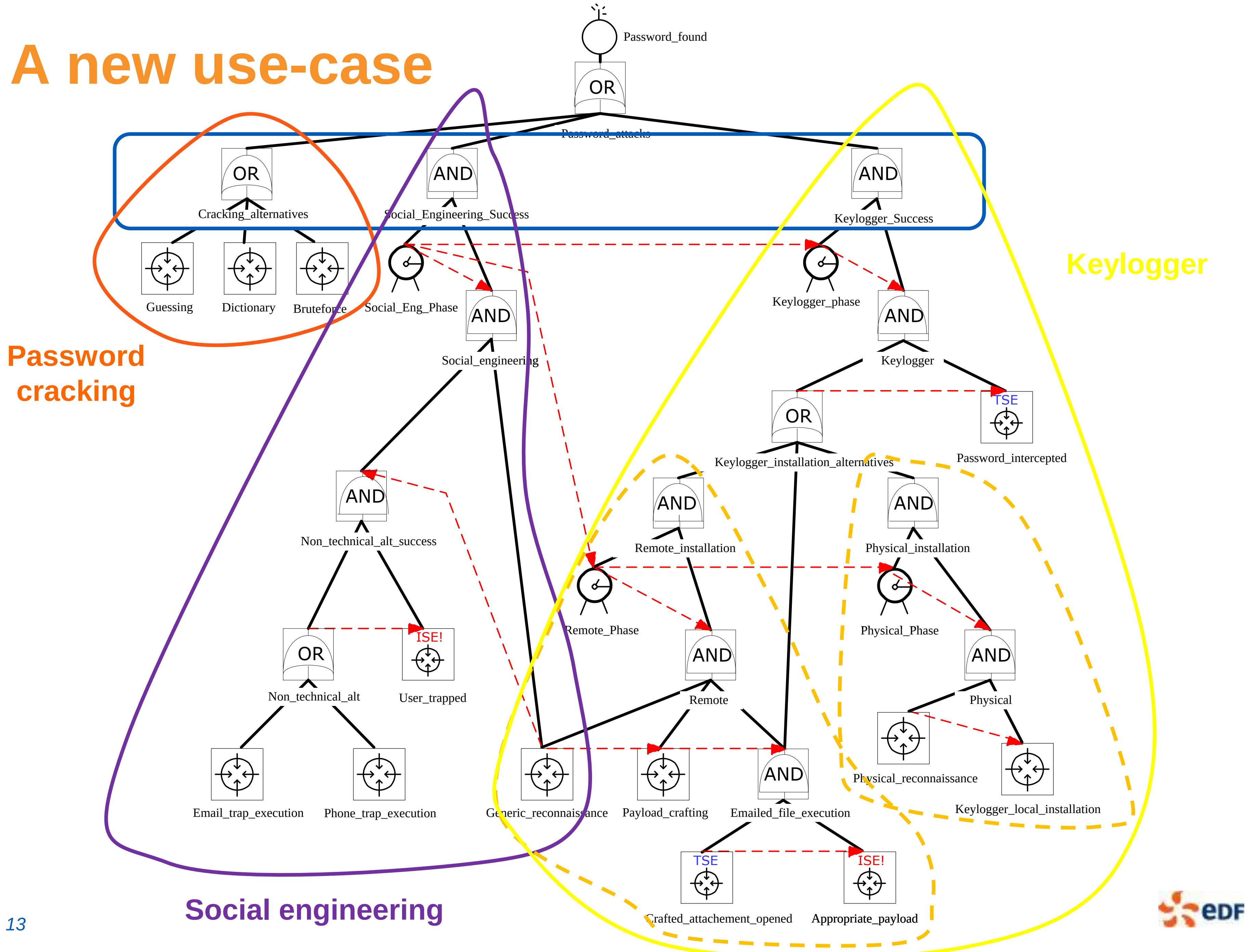
- Theorem 3: if the P_i are such that $\forall i \in B, \forall t, \forall t' \geq t, S_i(t) = 1 \Rightarrow S_i(t') = 1$ *
$Pr(S_r(t)=1)$ is unchanged whether irrelevant event ($Y_i=0$) are trimmed or not

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

Quantifications

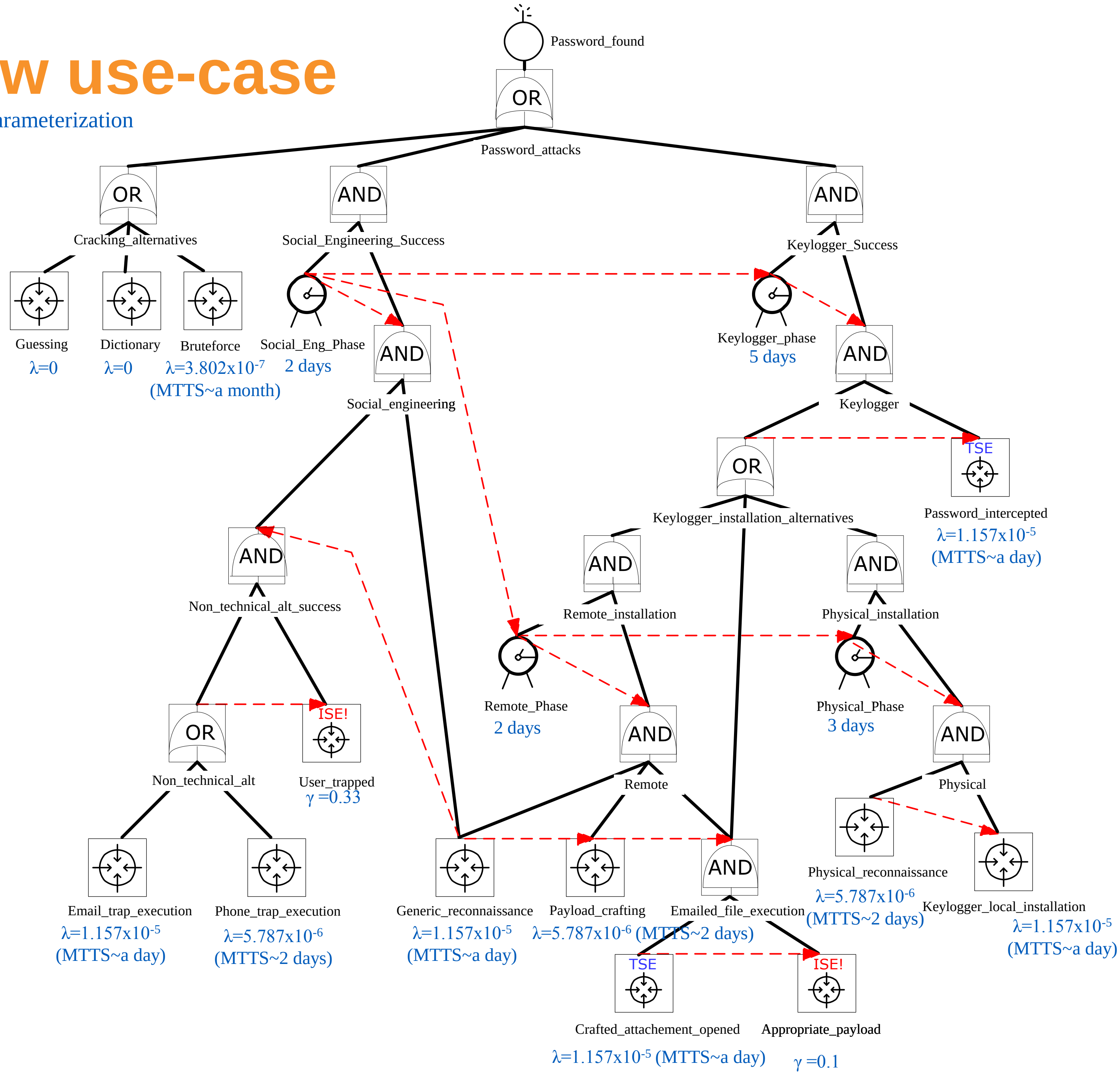
- Time-domain analysis – Leveraging the BDMP framework
  - Quantification tools, algorithms and optimizations
  - Efficient sequence exploration with trimming
    - Probability to reach the objective in a given time
    - Overall mean time to the attack success
    - Probability of each explored sequence
    - Ordered list of sequences
- Time-independent (static) - Classical attack tree parameters
  - Monetary cost → scenario cost, average attack cost
  - Boolean indicators (specific requirements, properties)
  - Minimum attacker skills

A new use-case



A new use-case

Example of parameterization



Results

- Overall probability in a week = 0.422
- Overall 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%

Detection Modeling

Main points

- The IOFA distinction: **I**nitial / **O**n-going / **F**inal / **A** posteriori
- Changes in the parameters and/or in the BDMP structure
- Introduction of a “Detection status indicator” D_i

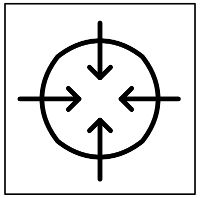
Changes in the modes

- “Active” is divided in “Active Undetected” and “Active Detected”
- Allows for parameter change, and even leaf cancellation
- The mode is selected based on $X_i D_i$

$X_i D_i$	00	01	10	11
Mode	Idle (I)		Active Undetected (AU)	Active Detected (AD)

New Markov models and probability transfer functions

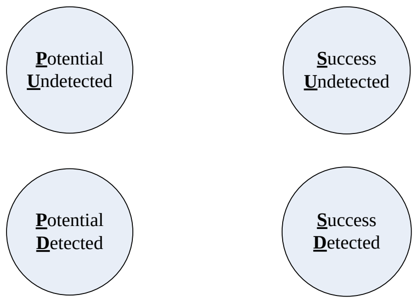
New definitions – e.g. the Attacker Action leaf



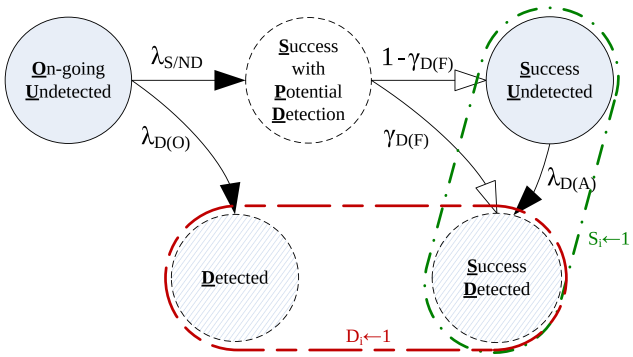
Attacker Action (AA)

Markov processes

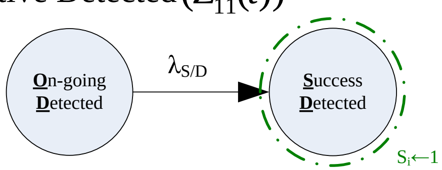
Idle $(Z_0^i(t))$



Active Undetected $(Z_{10}^i(t))$



Active Detected $(Z_{11}^i(t))$



Probability transfer functions

$f^i_{0\to 10}(PU)=\{Pr(OU)=1-\gamma_{D(I)}, Pr(D)=\gamma_{D(I)}, Pr(SD)=0, Pr(SU)=0\}$

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

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

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

$f^i_{0\to 11}(PU)=\{Pr(OD)=1, Pr(SD)=0\}^*$

$(PD)=\{Pr(OD)=1, Pr(SD)=0\}$

$(SU)=\{Pr(OD)=0, Pr(SD)=1\}^*$

$(SD)=\{Pr(OD)=0, Pr(SD)=1\}$

$f^i_{10\to 11}(OU)=\{Pr(OD)=1, Pr(SD)=0\}^*$

$(D)=\{Pr(OD)=1, Pr(SD)=0\}^{**}$

$(SD)=\{Pr(OD)=0, Pr(SD)=1\}^{**}$

$(SU)=\{Pr(OD)=0, Pr(SD)=1\}^*$

$f^i_{11\to 0}(OD)=\{Pr(PU)=0, Pr(PD)=1, Pr(SD)=0, Pr(SU)=0\}$

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

$f^i_{10\to 0}(OU)=\{Pr(PU)=1, Pr(PD)=0, Pr(SD)=0, Pr(SU)=0\}$

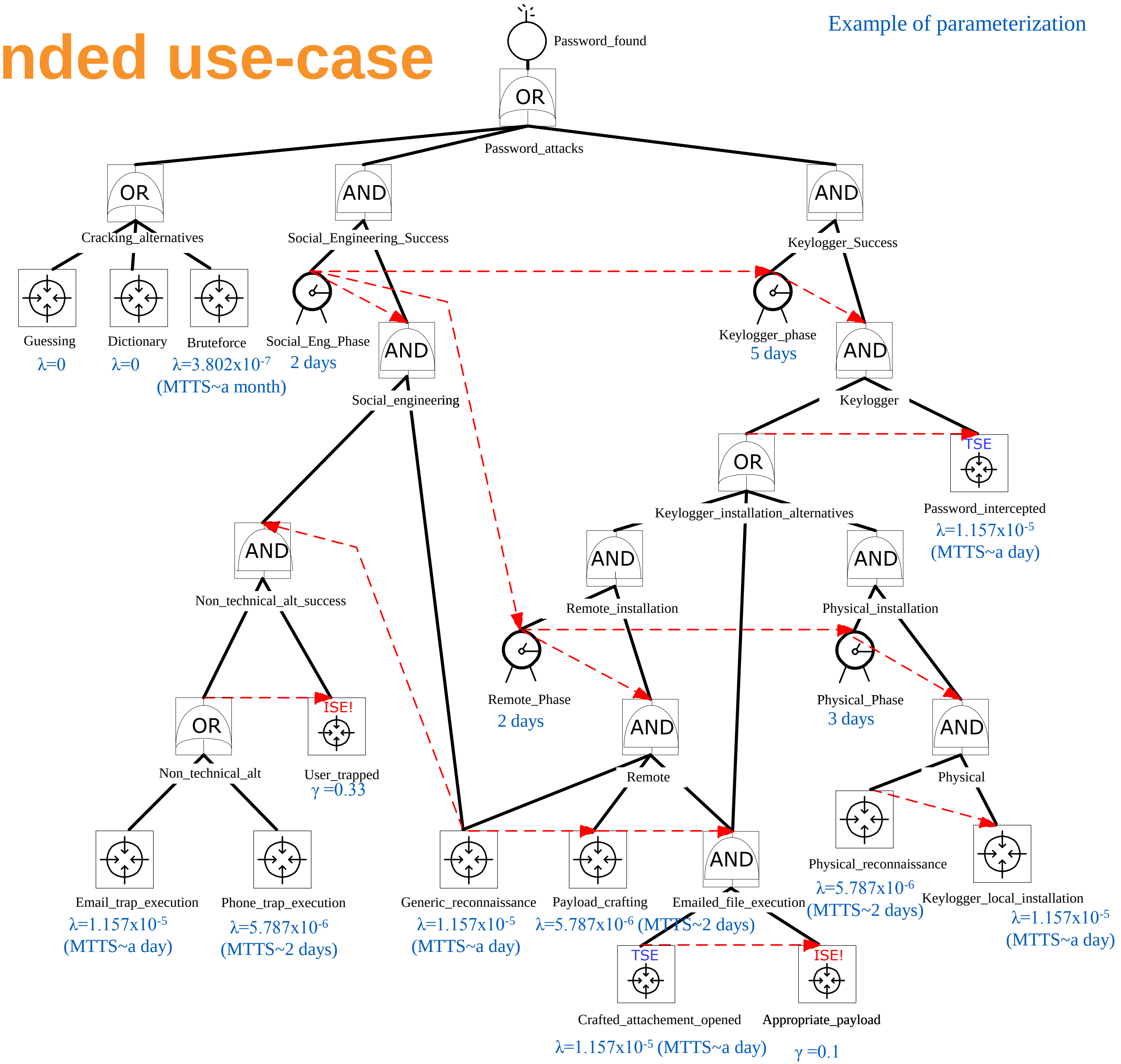
$(SU)=\{Pr(PU)=0, Pr(PD)=0, Pr(SD)=0, Pr(SU)=1\}$

** The detection has occured at a different leaf*

*** Despite D and SD having null durations, these lines are necessary to specify the transfer function, the transfer being potentially triggered by the leaf itself.*

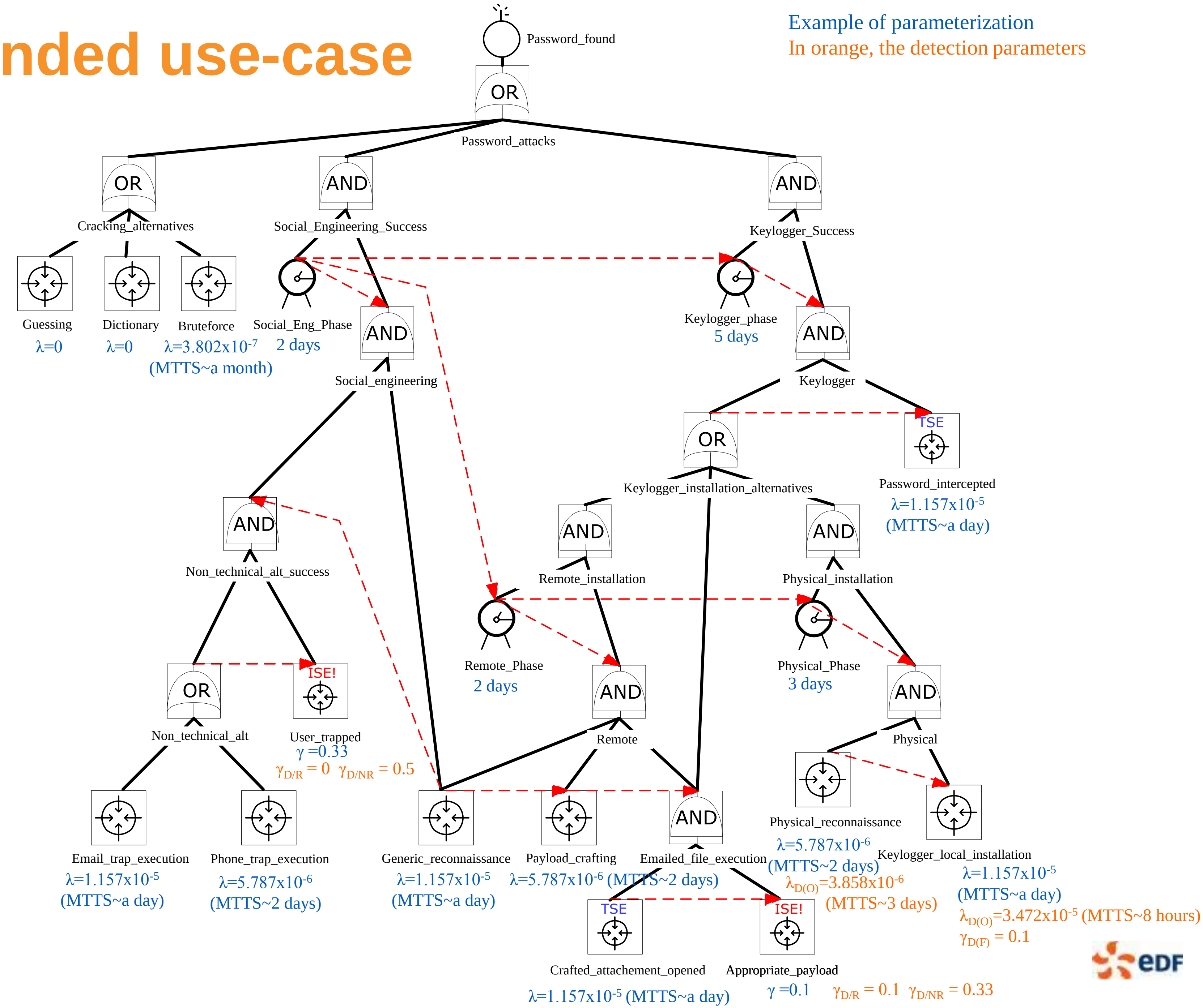
Extended use-case

Example of parameterization



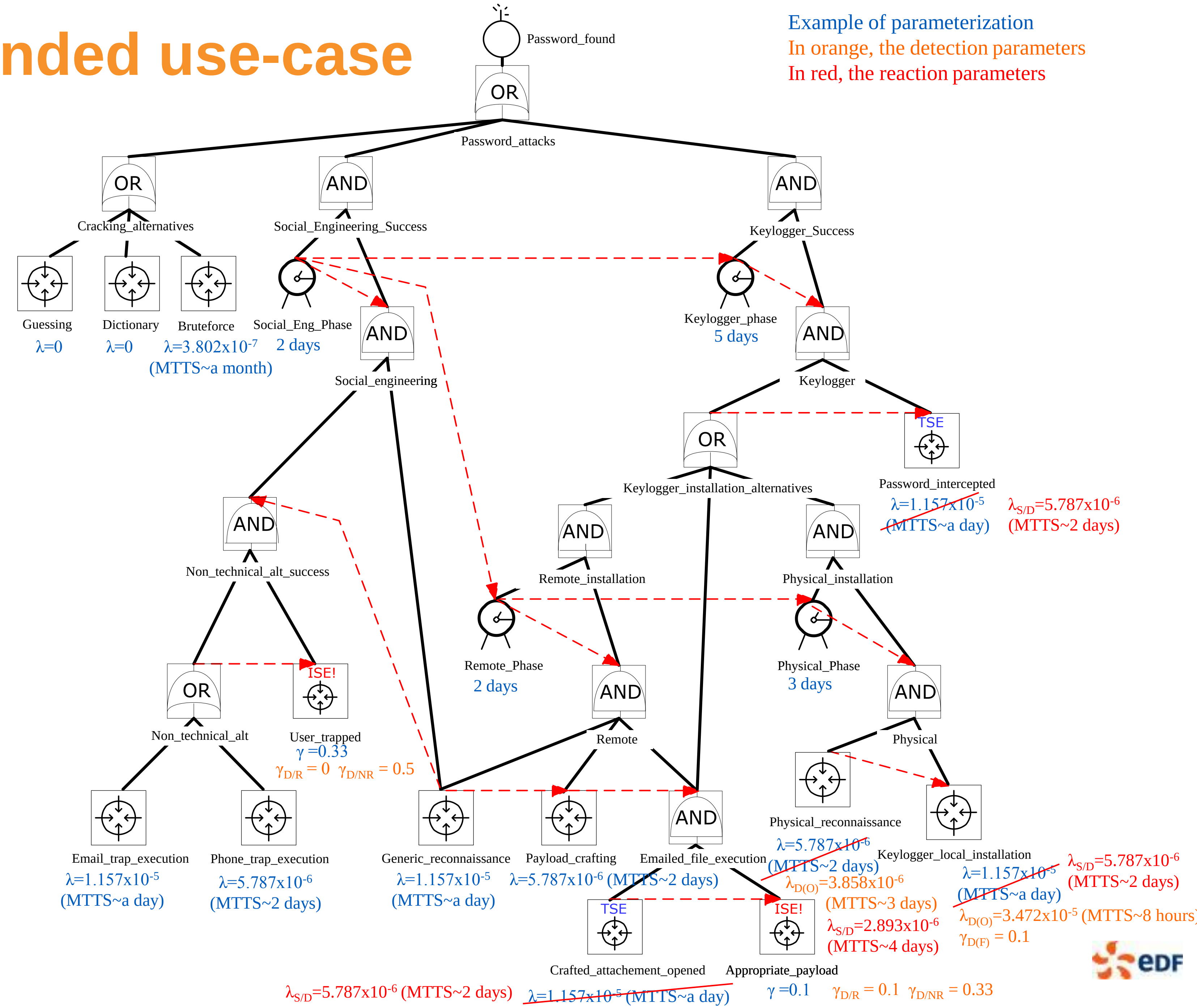
Extended use-case

Example of parameterization
In orange, the detection parameters



Extended use-case

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



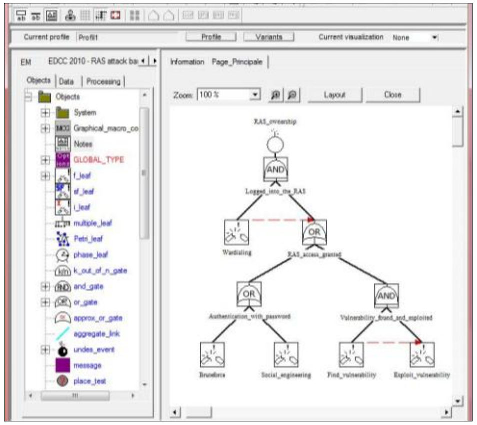
Typical results

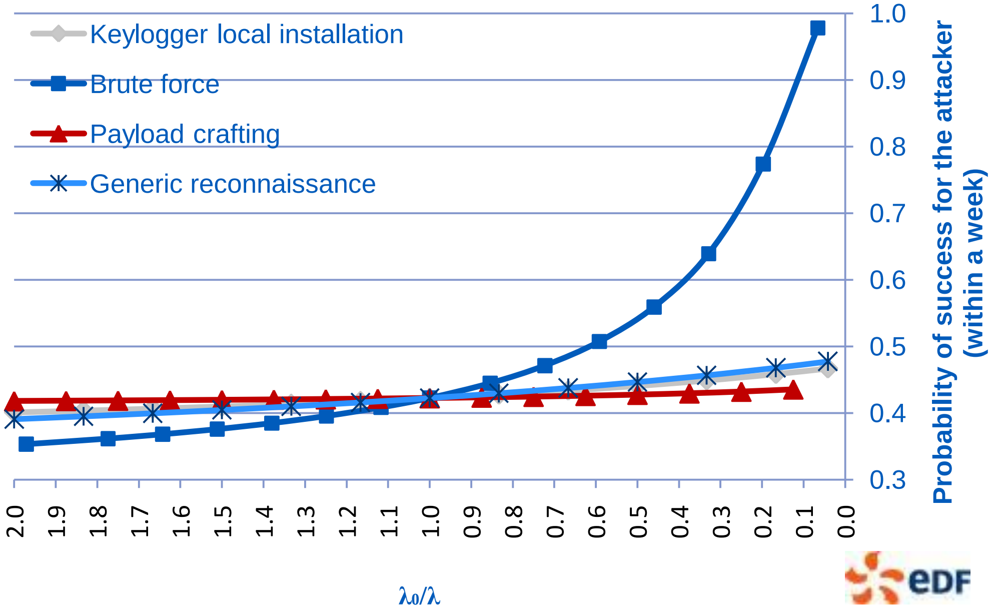
- Probability of success within a week: 0.364 (-14 %)
- Representative sequences (4231 vs 656)

	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 advances and on-going work

- Extension of the KB3 software suite
  - Security-oriented "knowledge basis" (Figaro)
  - Directly usable by analysts
- Assist the analyst in security decisions
  - Sequences discrimination on attacker profile
  - Sequences presentation
  - Sensitivity analysis
- Safety and Security
  - Integrated models
  - Interdependenncies





Perspectives

- Enhance usability
  - (Internal) users feedback
  - Develop the side-tools (sensitivity script HMI, etc.)
  - Attack patterns 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.

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
- Inherent limits
  - 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, Proc. CIEM 2005, Bucharest, Romania, Oct. 2005

Marc Bouissou's homepage: http://perso-math.univ-mlv.fr/users/bouissou.marc/

On BDMP & Security

- L. Piètre-Cambacédès and M. Bouissou, "Beyond attack trees: dynamic security modeling with Boolean logic Driven Markov Processes (BDMP)," 8th European Dependable Computing Conference (EDCC-2010), Valencia, Spain, April 28-30, 2010
- MMM-ACNS paper !
- L. Piètre-Cambacédès and M. Bouissou, "Modeling safety and security interdepedencies with BDMP (Boolean logic Driven Markov Processes)," IEEE International Conference on Systems, Man, and Cybernetics (SMC 2010), Istanbul, Turkey, oct. 2010. Accepted.

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

Thank you for your attention!

Большое спасибо

Questions & Answers