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
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

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

- 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

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

⇒ Adaptation 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 = \{A, r, T, \{P_i\}\}
  - \(A\) = Attack Tree, \(r\) = top event,
  - \(G_1\) = secondary top, \(T\) = trigger,
  - \(P_i\) = “triggered” Markov processes
A first feel: a simple Remote Access Server attack

1. RAS ownership
2. Logged into the RAS
   - Wardialing
   - OR
      - RAS access granted
         - OR
            - Authentication by password
              - OR
                - Brute force
                - Social engineering
            - AND
               - Vulnerability found and exploited
               - Vulnerability exploitation
RAS attack BDMP – Step 0 (attack just started)

- RAS ownership
- Logged into the RAS
- Wardialing
- OR
  - Authentication by password
    - OR
      - Brute force
      - Social engineering
    - Vulnerability identification
  - Vulnerability found and exploited
    - Vulnerability exploitation
RAS attack BDMP – Step 1

RAS ownership

AND

Logged into the RAS

OR

Wardialing

Logged into the RAS

OR

Authentication by password

Brute force

Social engineering

AND

Vulnerability found and exploited

Vulnerability identification

Vulnerability exploitation
RAS attack BDMP – Step 1

- Social engineering
- Wardialing
- RAS ownership
- Vulnerability identification

Logged into the RAS
AND
OR
OR AND
Logged into the RAS

Wardialing

Authentication by password
Brute force
Social engineering
Vulnerability identification
Vulnerability exploitation
RAS attack BDMP – Step 1

- **RAS ownership**
- **Logged into the RAS**
- **Wardialing**
- **RAS access granted**
- **Authentication by password**
- **Vulnerability found and exploited**
- **Brute force**
- **Social engineering**
- **Vulnerability identification**
- **Vulnerability exploitation**
RAS attack BDMP – Step 2

RAS ownership

Logged into the RAS

Wardialing

RAS access granted

Authentication by password

Brute force

Social engineering

Vulnerability found and exploited

Vulnerability identification

Vulnerability exploitation
RAS attack BDMP – Step 2

RAS ownership

AND

Logged into the RAS

OR

Wardialing

OR

RAS access granted

AND

Authentication by password

Vulnerability found and exploited

Brute force

Social engineering

Vulnerability identification

Vulnerability exploitation
RAS attack BDMP – Step 3

RAS ownership

- AND

Logged into the RAS

- OR

Wardialing

RAS access granted

- OR

Authentication by password

- AND

Vulnerability found and exploited

- Brute force

- Social engineering

- Vulnerability identification

- Vulnerability exploitation
RAS attack BDMP – Attacker’s objective reached

- RAS ownership
  - AND
    - Logged into the RAS
      - OR
        - Wardialing
        - OR
          - RAS access granted
            - OR
              - Authentication by password
              - AND
                - Vulnerability found and exploited
                  - OR
                    - Brute force
                    - Social engineering
                    - Vulnerability identification
                    - Vulnerability exploitation
A zoom on the three basic security leaves

<table>
<thead>
<tr>
<th>Leaf type &amp; icon</th>
<th>Transfer between modes</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Target Icon" /></td>
<td>Attacker Action (AA)</td>
</tr>
<tr>
<td><img src="image" alt="Instantaneous Security Event Icon" /></td>
<td>Instantaneous Security Event</td>
</tr>
<tr>
<td><img src="image" alt="Timed Security Event Icon" /></td>
<td>Timed Security Event</td>
</tr>
</tbody>
</table>
A zoom on the three basic security leaves

<table>
<thead>
<tr>
<th>Leaf type &amp; icon</th>
<th>Idle Mode ($X_i=0$)</th>
<th>Active Mode ($X_i=1$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Target Icon]</td>
<td>![Potential] ![Success]</td>
<td>![On-going] ![Success]</td>
</tr>
<tr>
<td>![Instantaneous Security Event Icon]</td>
<td>![Potential] ![Realized]</td>
<td>![Not Realized] ![Realized]</td>
</tr>
</tbody>
</table>
A zoom on the three basic security leaves

<table>
<thead>
<tr>
<th>Leaf type &amp; icon</th>
<th>Idle Mode ($X_i=0$)</th>
<th>Transfer between modes</th>
<th>Active Mode ($X_i=1$)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attacker Action (AA)</strong></td>
<td><img src="Potential" alt="Potential" /> <img src="Success" alt="Success" /></td>
<td>P⇔O (with $Pr = 1$) S⇔S (with $Pr = 1$)</td>
<td><img src="On-going" alt="On-going" /> $\lambda$ <img src="Success" alt="Success" /></td>
</tr>
<tr>
<td><strong>Instantaneous Security Event (ISE)</strong></td>
<td><img src="Potential" alt="Potential" /> <img src="Realized" alt="Realized" /></td>
<td>P⇔NR (with $Pr=1-\gamma$) P⇔R (with $Pr = \gamma$) R⇔R (with $Pr = 1$) P⇔NR (with $Pr = 1$)</td>
<td>![Not Realized](Not Realized) $\lambda$ <img src="Realized" alt="Realized" /></td>
</tr>
<tr>
<td><strong>Timed Security Event (TSE)</strong></td>
<td><img src="Potential" alt="Potential" /> <img src="Realized" alt="Realized" /> $\lambda'$ ![Not Realized](Not Realized) <img src="Realized" alt="Realized" /></td>
<td>P⇔NR (with $Pr = 1$) NR⇔NR (with $Pr=1$) R⇔R (with $Pr = 1$)</td>
<td>![Not Realized](Not Realized) $\lambda$ <img src="Realized" alt="Realized" /></td>
</tr>
</tbody>
</table>
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 \((g: G \rightarrow N^*, \text{with } g(i) \text{ the gate parameter } k)\)

- **A main top objective** \(r\)
- **Set of triggers** \(T\) is a subset of \((E - \{r\}) \times (E - \{r\})\) 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 \( \{Z^i_0(t), Z^i_1(t), f^i_{0\rightarrow 1}, f^i_{1\rightarrow 0}\} \)

- \( Z^i_0(t) \) and \( Z^i_1(t) \) two homogeneous Markov process

- \( f^i_{0\rightarrow 1}(x) \) and \( f^i_{1\rightarrow 0}(x) \) two “probability transfer functions”
  - For \( k \) in \( \{0, 1\} \) (modes), \( A^i_k \) state-space of \( Z^i_k(t) \)
  - \( S^i_k \subset A^i_k \), subset that generally corresponds to attacker action successes states (or event realization states)
  - For any \( x \in A^i_0 \), \( f^i_{0\rightarrow 1}(x) \) is a probability distribution on \( A^i_1 \) such that if \( x \in S^i_0 \), then \( \sum_{j\in S^i_1} (f^i_{0\rightarrow 1}(x))(j) = 1 \)
  - For any \( x \in A^i_1 \), \( f^i_{1\rightarrow 0}(x) \) is a probability distribution on \( A^i_0 \) such that if \( x \in S^i_1 \), then \( \sum_{j\in S^i_0} (f^i_{1\rightarrow 0}(x))(j) = 1 \)
Three families of Boolean functions of the time

- **Structure functions** \((S_i)_{i \in E}\)
  \[ \forall i \in G, \quad S_i = \sum_{j \in \text{sons}(i)} S_j \geq g(i) \]
  \[ \forall j \in B, \quad S_j = Z^j_{X_j} \in S^j_{X_j} \], 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 \(A\), then \(X_i = 1\) else
  \[ X_i \equiv \neg \left[ (\forall x \in E, (x, i) \in L \Rightarrow X_x = 0) \lor (\exists x \in E / (x, i) \in T \land S_x = 0) \right] \]

- **Relevance indicators** \((Y_i)_{i \in E}\)
  If \(i = r\) (finale objective), then \(X_i = 1\) else
  \[ Y_i \equiv \left( \exists x \in E / (x, i) \in L \land Y_x \land S_x = 0 \right) \lor \left( \exists y \in E / (i, y) \in T \land S_y = 0 \right) \]
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 \((\{P_1,Q\},\{P_2,Q\},...\)
    - exponential otherwise \((\{P_1,Q\},\{P_1,P_2,Q\}, \{P_1,P_3,Q\},...\)

  - **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

Password cracking

Social engineering

Keylogger

Cracking_alternatives

Social_Engineering_Success

Keylogger_Success

Guessing

Dictionary

Bruteforce

Social_Eng_Phase

Password_found

Password_intercepted

Remote_Phase

Remote

Remote_installation

Physical

Physical_Phase

Physical_installation

Physical_reconnaissance

Keylogger_local_installation

TSE

ISE!

Non_technical_alt_success

User_trapped

Email_trap_execution

Phone_trap_execution

Generic_reconnaissance

Payload_crafting

Emailed_file_execution

Crafted_attachment_opened

Appropriate_payload

Password_cracking

Social engineering

Keylogger
A new use-case

Example of parameterization

- **Password_attacks**
  - OR
    - **Cracking_alternatives**
      - Guessing
        - 
      - Dictionary
        - 
      - Brute-force
        - 
      - Social_Engineering_Success
        - Social_engr
          - AND
            - **Non_technical_alt_success**
              - Email_trap_execution
                - 
              - Phone_trap_execution
                - 
            - User_trapped
              - 
            - 
          - 
  - AND
    - **Keylogger_Success**
      - Keylogger
        - 
      - Keylogger_phase
        - 
      - Keylogger_installation_alternatives
        - 
      - Password_intercepted
        - 
      - 
    - TSE
      - 
    - 
  - 
  - 
  - 

### Results

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

<table>
<thead>
<tr>
<th>Sequences</th>
<th>Probability in a week</th>
<th>Average duration</th>
<th>Contrib.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1  &lt;Social Eng&gt;Generic reconn., Email trap exec., User trapped</td>
<td>$1.059 \times 10^{-1}$</td>
<td>$9.889 \times 10^{4}$</td>
<td>25.1%</td>
</tr>
<tr>
<td>2  &lt;Social Eng&gt;Generic reconn., Phone trap exec., User trapped</td>
<td>$5.295 \times 10^{-2}$</td>
<td>$9.889 \times 10^{4}$</td>
<td>12.5%</td>
</tr>
<tr>
<td>3  Bruteforce</td>
<td>$2.144 \times 10^{-2}$</td>
<td>$5.638 \times 10^{4}$</td>
<td>5.1%</td>
</tr>
<tr>
<td>4  &lt;Social Eng&gt;&lt;Keylogger&gt;&lt;Remote&gt;&lt;Physical&gt; Physical reconn., Keylogger local installation, Password intercepted</td>
<td>$1.749 \times 10^{-2}$</td>
<td>$2.976 \times 10^{5}$</td>
<td>4.1%</td>
</tr>
<tr>
<td>5  &lt;Social Eng&gt;&lt;Keylogger&gt;&lt;Remote&gt;Generic reconnaissance, Keylogger local installation, Password intercepted</td>
<td>$1.350 \times 10^{-2}$</td>
<td>$3.677 \times 10^{6}$</td>
<td>3.2%</td>
</tr>
<tr>
<td>6  &lt;Social Eng&gt;Generic reconnaissance, Email trap execution, User trapped (failure), Bruteforce</td>
<td>$1.259 \times 10^{-2}$</td>
<td>$2.610 \times 10^{6}$</td>
<td>3.0%</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 &lt;Social Eng&gt;&lt;Keylogger&gt;&lt;Remote&gt;Generic reconnaissance, Payload crafting, Appropriate payload, Password intercepted</td>
<td>$2.500 \times 10^{-3}$</td>
<td>$2.761 \times 10^{5}$</td>
<td>0.6%</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>34 &lt;Social Eng&gt;&lt;Keylogger&gt;&lt;Remote&gt;Generic recon., Payload crafting, Crafted attachment opened, Appropriate payload, Physical reconn., Keylogger local installation, Password intercepted</td>
<td>$1.506 \times 10^{-3}$</td>
<td>$4.594 \times 10^{6}$</td>
<td>0.4%</td>
</tr>
</tbody>
</table>
Detection Modeling

Main points

- The IOFA distinction: Initial / On-going / Final / 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 $X_iD_i$

<table>
<thead>
<tr>
<th>$X_iD_i$</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Idle (I)</td>
<td>Active Undetected (AU)</td>
<td>Active Detected (AD)</td>
<td></td>
</tr>
</tbody>
</table>

New Markov models and probability transfer functions
### New definitions – e.g. the Attacker Action leaf

<table>
<thead>
<tr>
<th>Markov processes</th>
<th>Probability transfer functions</th>
</tr>
</thead>
</table>
| **Idle** $(Z_0^i(t))$ | \[ f_{0 \rightarrow 10}^{i}(PU) = \{ Pr(OU) = 1 - \gamma_{D(1)}, \; Pr(D) = \gamma_{D(1)}, \; Pr(SD) = 0, \; Pr(SU) = 0 \} \]
| Probability transfer functions | \[ (PD) = \{ Pr(OU) = 0, \; Pr(D) = 1, \; Pr(SD) = 0, \; Pr(SU) = 0 \} \] |
| Probability transfer functions | \[ (SU) = \{ Pr(OU) = 0, \; Pr(D) = 0, \; Pr(SD) = 0, \; Pr(SU) = 1 \} \] |
| Probability transfer functions | \[ (SD) = \{ Pr(OU) = 0, \; Pr(D) = 0, \; Pr(SD) = 1, \; Pr(SU) = 0 \} \] |
| **Active Undetected** $(Z_{10}^i(t))$ | \[ f_{0 \rightarrow 11}^{i}(PU) = \{ Pr(OD) = 1, \; Pr(SD) = 0 \} \] **
| Probability transfer functions | \[ (PD) = \{ Pr(OD) = 1, \; Pr(SD) = 0 \} \] **
| Probability transfer functions | \[ (SU) = \{ Pr(OD) = 0, \; Pr(SD) = 1 \} **
| Probability transfer functions | \[ (SD) = \{ Pr(OD) = 0, \; Pr(SD) = 1 \} **
| **Active Detected** $(Z_{11}^i(t))$ | \[ f_{10 \rightarrow 11}^{i}(OU) = \{ Pr(OD) = 1, \; Pr(SD) = 0 \} \] **
| Probability transfer functions | \[ (OD) = \{ Pr(OD) = 1, \; Pr(SD) = 0 \} **
| Probability transfer functions | \[ (SU) = \{ Pr(OD) = 0, \; Pr(SD) = 1 \} **
| Probability transfer functions | \[ f_{1 \rightarrow 10}^{i}(OD) = \{ Pr(PU) = 0, \; Pr(PD) = 1, \; Pr(SD) = 0, \; Pr(SU) = 0 \} \] 
| Probability transfer functions | \[ (SD) = \{ Pr(PU) = 0, \; Pr(PD) = 0, \; Pr(SD) = 1, \; Pr(SU) = 0 \} \] 
| Probability transfer functions | \[ f_{10 \rightarrow 1}^{i}(OU) = \{ Pr(PU) = 1, \; Pr(PD) = 0, \; Pr(SD) = 0, \; Pr(SU) = 0 \} \] 
| Probability transfer functions | \[ (SU) = \{ Pr(PU) = 0, \; Pr(PD) = 0, \; Pr(SD) = 0, \; Pr(SU) = 1 \} \] 

* The detection has occurred 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
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)

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

![Graph showing probability of success for the attacker within a week with different attack methods: Keylogger local installation, Brute force, Payload crafting, Generic reconnaissance.](image)
**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


On BDMP & Security

- MMM-ACNS paper!

Thank you for your attention!

Большое спасибо

Questions & Answers