The promising potential of the BDMP formalism for security modeling

Ludovic Piètre-Cambacédès[1,2], Marc Bouissou[1]
[1]*Electricité de France,* [2]*Telecom ParisTech*
{ludovic.pietre-cambacedes, marc.bouissou}@edf.fr

Abstract

After an overview of the existing cybersecurity graph-based models and their limitations, the paper introduces a new approach that may help overcoming them. It is based on BDMP (Boolean logic driven Markov processes), a powerful formalism initially used in reliability and safety engineering.

1. Introduction

Cybersecurity graph-based models constitute an active domain of research. This can be explained by their ability to formalize reasoning, help quantifying risk reduction and support security decision. Section 2 provides an overview of the main existing models, where logical trees play an important role, and recalls some limitations still to overcome. Section 3 introduces the idea and the interest of adapting the BDMP formalism [1], a powerful model in the reliability and system safety area, to cybersecurity. Perspectives and future work conclude the paper.

2. State of the art

Graphical attack representations have been manually used by security analysts at least since the 80's [2]. In the 90's, while AT&T then Sandia proposed to structure and automate the approach [3], Dacier *et al* developed privilege graphs [4], a mathematically-formalized model allowing security quantification. End of 90's, attack trees largely inspired by the fault-trees found in the safety arena, gained a wide popularity with Schneier [5]. Numerous academic and industrial works are still grounded based on them, e.g. [6,7]. In 2002, Sheyner *et al* published research taking advantage of model-checking [8], opening another very fertile field (e.g. [9]). Petri-nets entered the scene in the same period [10]. Compromise graphs with time-to-compromise metric constitute a recent framework developed by McQueen *et al* [11].

Classical attack tree models are clear and usable, but do not capture properly the dynamic essence of attacks. This aspect is better modeled by Markov chains or Petri-net based approaches. Unfortunately, those last families do not scale well and rapidly suffer from state-space explosion. Automatically generated graphs are even more susceptible to such limitations, which can be softened in some optimized variants downgrading their accuracy and representativeness.

3. Towards a new formalism for security

In the same way as fault-trees have been adapted from safety engineering, opening new perspectives in security [5], a more recent formalism seems to have promising applications for security modeling.

3.1. BDMP in a nutshell

The general idea of BDMP, as suggested by their name, is to associate a Markov process (which represents the behavior of a component or a subsystem) to each leaf of a fault-tree. This fault-tree is the structure function of the system. The basic Markov processes have two "modes", corresponding to the fact that the associated components/subsystems are required or are in standby. At any time, the choice of the mode of one of the Markov processes depends on the value of a Boolean function of other processes.

A BDMP (F, r, T, (P_i)) is made of a multi-top coherent fault-tree F, a main top event r of F, a set of triggers, a set of "triggered Markov processes" P_i associated to the basic events (i.e. the leaves) of F, the definition of two categories of states for the processes P_i (corresponding to working and failure states).

A trigger is represented graphically with a dotted line. It causes a mode change in the triggered Markov processes associated to all (or part of, if there are other triggers) the leaves of the subtree the trigger points at, when the event at the origin of the trigger becomes true.

For example in Fig. 1, f3 and f4 are events that can take place only after the occurrence of f1 or f2.

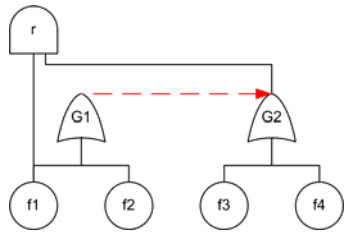

Figure 1. The BDMP formalism

The formal definition of BDMP, their mathematical properties and several examples can be found in [1].

3.2. Main interests for security modeling

A first obvious interest lies in their global appearance, close to traditional attack trees, ensuring easy appropriation and readability. But the underlying mechanics of BDMP and associated representation allow a full integration of the dynamic dimension of an attack process, mainly through the use of triggers. If needed, Petri-net leaves can be used when more appropriate to model subparts. The overall formalism allows modularity and reusability, respecting the hierarchical structure of traditional attack trees.

Fig. 2 gives a simple example where the attack objective is to log into a Remote Access Server connected to a dial-up modem. The red triggers model the sequence in which the tree has to be read and the leaves are activated. Some of them should naturally be developed with more details than in this example.

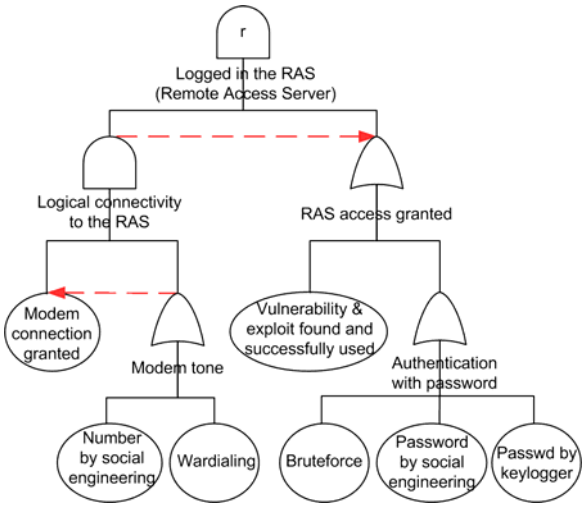

Figure 2. A security-oriented BDMP example

4. Perspectives and future work

This fast abstract has only introduced the potential of BDMP in security modeling. We are currently investigating the implications on the mathematical foundations of such use, and the appropriate adaptations to use security-oriented parameters. This will allow running meaningful simulations and quantifications over a sound graphical model. The integration with the time-to-compromise metric is considered [4,11]. Complete cases and scenarii are also being developed, mainly in the field of industrial control systems cybersecurity. Nevertheless, physical security and systemic view of critical infrastructure protection can also be addressed. Finally, when mature enough, the model will be integrated within the KB3 platform [12], the natural software tool for BDMP.

5. References

[1] M. Bouissou & J.L. Bon, “A new formalism that combines advantages of fault-trees and Markov models: Boolean logic-driven Markov processes,” *Reliability Engineering & System Safety*, vol. 82, Nov. 2003, pp. 149-163.

[2] US DoD, “System security engineering program management requirements", *MIL-STD-1785*, 20 June 1988.

[3] C. Phillips & L. Swiler, “A graph-based system for network-vulnerability analysis,” *Proc. NSPW'98*, pp. 71-79.

[4] M. Dacier & Y. Deswarte, “Privilege graph: an extension to the typed access matrix model,” *Proc. ESORICS'94*, Springer-Verlag, pp. 319-334.

[5] B. Schneier, “Attack trees,” *Dr. Dobb’s journal*, vol. 24, 1999, pp. 21-29.

[6] S.C. Patel, J.H. Graham, & P.A. Ralston, “Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements,” *Int. J. of Information Management*, vol. 28, Dec. 2008, pp. 483-491.

[7] I.N. Fovino & M. Masera, “Through the description of attacks: a multidimensional view,” *Proc. SAFECOMP 2006*, Springer-Verlag, pp. 15-28.

[8] O. Sheyner, J. Haines, S. Jha, R. Lippmann, & J.M. Wing, “Automated generation and analysis of attack graphs,” *Proc. IEEE Symp. on Security & Privacy 2002*, pp. 273-284.

[9] S. Jajodia, S. Noel, & B. O’Berry, “Topological analysis of network attack vulnerability,” *Managing Cyber Threats*, Springer US, 2005, pp. 247-266.

[10] J.P. McDermott, “Attack net penetration testing,” *Proc. NSPW'2000*, ACM, pp. 15-21.

[11] M.A. McQueen, W.F. Boyer, M.A. Flynn, & G.A. Beitel, “Time-to-compromise model for cyber risk reduction estimation,” *Quality of Protection, Advances in Information Security*, vol. 23, Springer US, 2006, pp. 49-64.

[12] EDF R&D software webpage, http://rdsoft.edf.fr