Automating the Analysis of Honeypot Data (Extended Abstract)

Olivier Thonnard[1], Jouni Viinikka[2], Corrado Leita[1], and Marc Dacier[3]

[1] Institut Eurecom
[2] France Telecom R&D
[3] Symantec Research Labs, France

Abstract. We describe the on-going work towards further automating the analysis of data generated by a large honeynet architecture called Leurre.com and SGNET. The underlying motivation is helping us to integrate the use of honeypot data into daily network security monitoring. We propose a system based on two automated steps: *i)* the detection of relevant attack events within a large honeynet traffic data set, and *ii)* the extraction of highly similar events based on temporal correlation.

Key words: honeypots, Internet threats analysis, malicious behavior characterization

1 Introduction

We look to identify and characterize certain large-scale phenomena that are active on the Internet by detecting similarities across network attack traces in an automated manner. The analyzed data is extracted from datasets collected through Leurre.com [4] and SGNET honeypot deployments [5]. By automating our analysis, it should help us to integrate the use of honeypot data into daily network security monitoring. To achieve this we need to identify relevant periods of activity on the sensors shortly after they occurred. These periods of activity are analyzed to detect temporal and spatial similarities within the observed attack processes.

In [2] the authors highlighted the usefulness of analyzing temporal correlations between different attacks collected through a honeynet, e.g. to highlight synchronized attack patterns which are part of a very same phenomenon, or to discover stealthier attack phenomena related to botnet propagation schemes or "multi-headed" attack tools [3].

Once groups of similar attack events are revealed, we can perform a more in-depth analysis of those specific groups so as to characterize them with respect to other relevant attack features, e.g. by analyzing the spatial and temporal characteristics of the attackers, or by looking at other meta-information obtained from the SGNET sensors, such as shellcode or malware characteristics when the attacks have led to a successful upload of shellcode commands and malicious binaries.

Thanks to the extensive characterization of those similar attack events, we seek to discover other types of similarities across attack events, even when they occurred at different periods of time. As a result, this process should facilitate the identification of possible root causes for new attack phenomena. The characterization and correlation steps may currently require some manual or semi-automated work.

2 Analysis process

The main idea of our ongoing effort consists to automatically i) detect relevant attack events within a large honeynet traffic data set shortly after it has been collected, and ii) group highly similar temporal events by relying on *clique* algorithms and appropriate similarity metrics.

We propose to use in step i) an approach based on non-stationary autoregressive (NAR) modeling using Kalman fixed-lag smoothers [1] and in step ii) we use clique algorithms described in [2,6].

The strengths of the detection algorithm are its capability to flag the beginnings of activity periods and isolated activity peaks. Our initial results show that the algorithm is effective when applied to the three different types of time series identified in [2], i.e. ephemeral spikes, sustained bursts and continous patterns. The shortcomings are related to detection of the end of an activity period, the association of the end to the beginning, and the risk of an activity peak begin masked by closely preceding peak. We look to improve these aspects of the detection algorithm.

Then, to correlate the identified attack events, we use an approach based on *maximal cliques* [6], which are able to group all events having important similarities in an unsupervised manner. The main advantage of this approach is that the number of groups (or cliques) does not need to be specified before executing the clustering, and many different feature vectors and similarity distances can be used transparently. We currently use two different techniques: *i)* the dominant sets approach developed by Pavan and Pelillo[7], and *ii)* the quality-based clustering developed in [2]. While the first approach provides a real approximation of the maximum clique problem (known to be NP-hard), the second approach is more pragmatic and is mainly focused on finding cliques having a high quality garantee with a low computational overhead. The choice of one or another clique algorithm depends on the intrinsic characteristics of the data set, as well as the *feature vectors* used in the data mining process.

References

1. Viinikka, J., Debar, H., Mé, L., Lehikoinen, A., Tarvainen, M.: Processing intrusion detection alert aggregates with time series modeling. Information Fusion Journal (2008) Special Issue on Computer Security, to appear.
2. Olivier Thonnard and Marc Dacier. A Framework for Attack Patterns Discovery in Honeynet Data. *Digital Forensic Research Workshop (DFRWS)*, 2008.
3. F. Pouget, G. Urvoy-Keller and M. Dacier. Time signatures to detect multi-headed stealthy attack tools. *18th Annual FIRST Conference*, Baltimore (USA), 2006.
4. The Leurre.com Project. http://www.leurrecom.org
5. Corrado Leita and Marc Dacier. SGNET: a worldwide deployable framework to support the analysis of malware threat models. In *Proceedings of EDCC 2008, 7th European Dependable Computing Conference*, May 7-9, 2008, Kaunas, Lithuania.
6. F.Pouget, M.Dacier, J.Zimmerman, A.Clark and G.Mohay. Internet attack knowledge discovery via clusters and cliques of attack traces. *Journal of Information Assurance and Security*, Volume 1, Issue 1, March 2006.
7. M. Pavan and M. Pelillo. A new graph-theoretic approach to clustering and segmentation. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*, 2003.