Parametric Attack Graph Construction and Analysis[*]

Leanid Krautsevich [**]

Department of Computer Science, University of Pisa
Largo Bruno Pontecorvo 3, Pisa 56127, Italy
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche
Via G. Moruzzi 1, 56124 Pisa, Italy
krautsev@di.unipi.it

Abstract. We present the first steps towards an implementation of attack graph construction and analysis technique based on inference rules. In our model, XML credentials describe basic attacks to the system, then inference rules allow composition of new attacks. We aim at modifying previously developed algorithm for the analysis of transitive trust models to the analysis of attack graphs. Important peculiarity of our model is exploitation of c-semirings for evaluation of system security level. C-semirings allow an application of the same algorithms for an analysis of attack graphs regardless of what metric is selected for the evaluation.

1 Introduction

Analysis and improvement of security of modern computer systems is a challenging task because the systems are extremely complex and heterogeneous. Often the analysis of security is based on attack graphs. Frequently, methods of the analysis are system and context specific and require manual adjustments. Moreover, most of the methods provide their own basic metric as the result of the analysis. We aim at creating a method that allows automated analysis of system security and works with wide range of security metrics without changing the core algorithm. Using different metrics for the evaluation helps to provide different views on system security and allows a security administrator to judge better on improvements to security of a system.

The essential elements of our method are basic attacks described as XML credentials similar to RTML [10]. Basic attacks form an attack graph with the nodes representing sets of resources and the edges representing the attacks. All the edges are labelled with costs of attacks. We introduce three inference rules, that allows us to make conclusions on the system security. The rules are compliant with rules presented for reasoning on transitive trust models. Thus, we can adopt an earlier developed algorithm [11,5] for the analysis of the attack graphs.

[*] This paper was partly supported by EU-FP7-ICT NESSoS project.

[**] Supervisor: Fabio Martinelli, Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy, e-mail: fabio.martinelli@iit.cnr.it.

We assume, that costs of attacks stand for security metrics, used for the evaluation of the system security. We associate each security metric with c-semiring which is algebraic structure used for the analysis of weighted graphs, e.g., for searching a shortest path in a graph. C-semirings allow to create an algorithm for the analysis of attack graphs that does not depend on the security metric selected for the analysis of the system.

1.1 Contributions

Main contributions of the paper are the following:

- the method for the analysis of attack graphs is based on inference rules similar to ones used for the analysis of transitive trust models, thus, the method may reuse the slightly changed algorithm developed for the analysis of transitive trust models;
- the method works regardless of the security metric selected for the evaluation due to the use of c-semiring algebraic structure.

The rest of the paper is structured as follows. Section 2 describes an application scenario and introduces inference rules. Section 3 discusses the exploitation of XML for representing basic attacks and introduces XML based rules for the processing of attacks. Section 4 observes the related work and Sect. 5 provides the conclusion and the future work.

2 Application Scenario

We consider a scenario where a security administrator performs the evaluation of security on the basis of resources available to an attacker. The features and the notation of the model: $ATT = \{a_1, \ldots, a_m\}$ is a set of attacks to a system, $RES = \{r_1, \ldots, r_n\}$ is a set of resources in the system, $S = \{a_1 \ldots a_k \mid a \in ATT\}$ is an attack sequence, R is a set of resources available to the attacker, G is a set of resources gained as the result of an attack, w is a cost of the attack, W is a cost of the attack sequence.

There is a set of basic attacks that can be applied when the attacker has an initial set of resources. The attacker obtains new resources by applying an attack. In our model, the resources are not consumed and the resources that can not be reached are not taken into account. We also consider the sequential composition of attacks, i.e., the attacker can perform attacks one by one. Moreover, all the attacks have costs, thus, all the potential resources are reachable with the corresponding costs. The attacker selects the attack with the best cost, e.g., the highest probability of success.

We introduce two operators $\otimes, \oplus$ over some domain D of values of costs, where the former operator serves for aggregation of costs of attacks in a sequence and the latter operator for the selection of the attack with the better cost. For example, the operator $\otimes$ equals $\times$ (multiplication), $\oplus$ equals max that stands for the selection of the attack sequence with the maximal probability of success, and the domain is $D = [0, 1]$. We can extend this basic set of operators to couples $(sequence, cost)$. Suppose, there are sequences of attacks a_1, a_2 with costs w_1, w_2:

$$(a_1, w_1) \otimes' (a_2, w_2) = (a_1 a_2, w_1 \otimes w_2)$$

$$(a_1, w_1) \oplus' (a_2, w_2) = \begin{cases} (a_1, w_1) & \text{if } (w_1 \oplus w_2) = w_1 \\ (a_2, w_2) & \text{if } (w_1 \oplus w_2) = w_2 \end{cases}$$

where $a_1 a_2$ is an order preserving concatenation of attacks.

Now we are ready to present three inference rules that allow us to analyse the above model.

First, we consider a set of resources available, say R_X. By starting from this set of resources, an intruder can perform a basic attack that simply needs a subset R_i of these resources and then acquires new resources G_j. This is modelled by the ***basic attack*** rule

$$\frac{R_i \overset{(a_q, w_q)}{\longrightarrow} R_j \quad R_i \subseteq R_X}{R_X \overset{(a_q, w_q)}{\longrightarrow} R_t} \tag{1}$$

where $R_j = R_i \cup G_j$ and $R_t = R_X \cup G_j$.

Then it is possible to compose several different basic attacks in a sequence and this is done by the ***composite attack*** rule. It states that starting from a set of resources by applying an attack the intruder gets new resources that serve as a basic set for another attack. Thus, a sequence of attacks is built.

$$\frac{R_i \overset{(a_q, w_q)}{\longrightarrow} R_j \quad R_j \overset{(a_p, w_p)}{\longrightarrow} R_k}{R_i \overset{(a_q, w_q) \otimes' (a_p, w_p)}{\longrightarrow} R_k} \tag{2}$$

Finally, the ***attack selection*** rule selects the attack with the better cost.

$$\frac{R_i \overset{(a_q, w_q)}{\longrightarrow} R_j \quad R_i \overset{(a_p, w_p)}{\longrightarrow} R_j}{R_i \overset{(a_q, w_q) \oplus' (a_p, w_p)}{\longrightarrow} R_j} \tag{3}$$

Rules 2 and 3 may be generalized for an application to attack sequences by using S and W instead of a and w.

The analysis of a system works as follows. Starting from the initial set of basic attacks, we build a graph whose nodes are sets of resources R and which arcs are labelled with attack costs. We need to apply the rules and to consider all the sequences exiting from the initial set R_i to the state $R_i \cup G_k$ and which cost is better than a total cost W. The overall protection goal can be to avoid the attacker to control the set of resources $R_i \cup G_k$ with the total cost better than the total cost W.

We propose to present costs as a special mathematical structure *c-semiring* (constraint semiring) [4]:

Definition 1. C-semiring T *is a tuple* $\langle D, \oplus, \otimes, \mathbf{0}, \mathbf{1} \rangle$*:*

- *D is a set of elements and $\mathbf{0}, \mathbf{1} \in D$;*
- *$\oplus$, is an additive operator defined over (possibly infinite) set of elements D, for $d_1, d_2, d_3 \in T$, it is commutative ($d_1 \oplus d_2 = d_2 \oplus d_1$) and associative ($d_1 \oplus (d_2 \oplus d_3) = (d_1 \oplus d_2) \oplus d_3$), and $\mathbf{0}$ is a* unit *element of the additive operator ($d_1 \oplus \mathbf{0} = d_1 = \mathbf{0} \oplus d_1$).*
- *$\otimes$ is a binary multiplicative operator, it is associative and commutative, $\mathbf{1}$ is its* unit *element ($d_1 \otimes \mathbf{1} = d_1 = \mathbf{1} \otimes d_1$), and $\mathbf{0}$ is its* absorbing *element ($d_1 \otimes \mathbf{0} = \mathbf{0} = \mathbf{0} \otimes d_1$);*
- *$\otimes$ is distributive over additive operator ($d_1 \otimes (d_2 \oplus d_3) = (d_1 \otimes d_2) \oplus (d_1 \otimes d_3)$);*
- *$\leq_T$ is a partial order over the set D, which enables comparing different elements of the semiring, the partial order is defined using the additive operator $d_1 \leq_T d_2$ (d_2 is better than d_1) iff $d_1 \oplus d_2 = d_2$ (idempotence).*

For a security metric, we need to determine the domain of values D and two operators $\oplus$ and $\otimes$ that are further used for the analysis of an attack graph. An example may be *shortest attacks path* metric and c-semiring with $\oplus$ equals min, $\otimes$ equals summation, and the domain D is the set of natural numbers $\mathbb{N}$. Other c-semirings may be defined for other metrics.

3 Using XML Credential to Represent and Reason on Attacks

We use XML credentials to store the information about basic attacks. Basic attacks are used to compute composite attacks sequences. Composite attacks are also represented by XML credentials and are used when necessary. XML credentials allow us to use slightly modified algorithm for dealing with trust relationships for access control systems [11,5] to deal with attack graph. Thus, we use two kinds of credential: one for modelling a basic attack b, and another one for modelling a composed attack c, where an attacker is A.

In case of a ***basic attack***, a is a sequence which contains only a single attack, R is the minimal resources necessary to perform the attack, G is the set of gained resources and w is the cost of the attack:

$$A.b(a, R, G, w) \tag{4}$$

In case of a ***composite attack***, S is a sequence of attacks, R represents the initial set of resources, F is the final set of resources and W the cost of the attack sequence S.

$$A.c(S, R, F, W) \tag{5}$$

Instantiations of Equations 1, 2, 3 for XML credentials are the following.

$$\frac{A.b(a, R, G, w) \quad R \subseteq X}{A.c(a, X, X \cup G, w)} \tag{6}$$

$$\frac{A.c(S_1, R_1, F_1, W_1) \quad A.c(S_2, R_2, F_2, W_2) \quad R_2 \subseteq F_1}{A.c(S_1 S_2, R_1, F_2, W_1 \otimes W_2)} \tag{7}$$

$$\frac{A.c(S_1, R, F, W_1) \quad A.c(S_2, R, F, W_2)}{A.c(S_1 \odot S_2, R, F, W_1 \oplus W_2)} \tag{8}$$

where $S_1 S_2$ is a concatenation of attack sequences, $\odot$ corresponds to the selection of sequence with the better cost. Now we can adopt algorithm [5] to the analysis of attack graphs since the rules are similar to rules [5,11] for reasoning on trust.

4 Related Work

The attacker model we use in the paper could be seen as an attack graph [1,13,12,6]. E.g., in [1] a (constrained) graph model based on resource acquisition by the attacker has been developed, the model considers the local knowledge of the attacker stored in nodes during the attack-path analysis (also for the selection of countermeasures).

Different security metrics are used for analysis of attack graphs: probability of successful attack [15], minimal cost of attack [14], minimal cost of reduction [16], shortest path [13]. Some of these metrics could be seen as specific instance of semirings, thus also suitable for the analysis with out approach. On the other hand, our approach is parametric and can also use other metrics for the analysis.

Krautsevich et al., [7] formally modelled and defined several security metrics which measure security system out of the context. The metrics were analysed in order to check if some of them provide the same evaluation. The next step in this study was establishing relations between these metrics and risk [8]. Every metric study was considered separately, when our current work is more generic.

To our knowledge, there are several attempts of applying semirings in security area [2,3]. The authors used semirings for the analysis of integrity policies, cryptographic protocols, and computation of trust levels through trust chains. Krautsevich et al., [9] applied semirings to analysis of security of process-like structures for describing web services. In this work, we provide a wider range of application of semirings for security analysis.

5 Conclusion

We used XML credentials to describe basic attacks and proposed inference rules for composition and selection of the attacks. C-semiring allows us to make the method independent of what security metric is selected for the evaluation. Finally, we worked towards an adoption of existed algorithm for reasoning on transitive trust to the analysis of parametric attacks graphs.

As a future work, we would like, first, to introduce modified algorithm for the analysis of attack graphs. Second, we would like to extend our approach for other models of attack graphs, e.g., privileges graph. Moreover, we would like to implement our method as a software prototype and perform an analysis the properties of the method, e.g, performance. For the implementation, we plan to minimally modify the code of algorithm for evaluation of RTML credentials with semirings developed in [5].

References

1. F. Baiardi, F. Martinelli, L. Ricci, and C. Telmon. Constrained automata: a formal tool for risk assessment and mitigation. *Journal of Information Assurance and Security*, 3:304–312, 2008.
2. G. Bella, S. Bistarelli, and S. N. Foley. Soft constraints for security. In *Proceedings of the First International Workshop on Views on Designing Complex Architectures (VODCA '04)*, volume 142 of *Electronic Notes in Theoretical Computer Science*, pages 11–29. Elsevier, 2006.
3. S. Bistarelli, F. Martinelli, and F. Santini. A semantic foundation for trust management languages with weights: An application to the rt family. In *Proceedings of the 5th international conference on Autonomic and Trusted Computing*, ATC '08, pages 481–495, Berlin, Heidelberg, 2008. Springer-Verlag.
4. S. Bistarelli, U. Montanari, and F. Rossi. Semiring-based constraint satisfaction and optimization. *J. ACM*, 44(2):201–236, March 1997.
5. D. Fais, M. Colombo, and A. Lazouski. An implementation of role-base trust management extended with weights on mobile devices. In *Proceedings of the 4th International Workshop on Security and Trust Management*, volume 244 of *Electronic Notes in Theoretical Computer Science*, pages 53–65. Elsevier, 2009.
6. S. Jha, O. Sheyner, and J. M. Wing. Minimization and reliability analyses of attack graphs. Technical Report CMU-CS-02-109, Carnegie Mellon University, 2002.
7. L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal approach to security metrics. what does "more secure" mean for you? In *Proceedings of the 1st International Workshop on Measurability of Security in Software Architectures*, 2010.
8. L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal analysis of security metrics and risk. In *Proceedings of the IFIP Workshop on Information Security Theory and Practice*, volume 6633, pages 304–319. 2011.
9. L. Krautsevich, F. Martinelli, and A. Yautsiukhin. A general method for assessment of security in complex services. In *Proceedings of 4th European Conference ServiceWave*. Springer, 2011.
10. N. Li, J. C. Mitchell, Y. Qiu, W. H. Winsborough, K. E. Seamons, M. Halcrow, and J. Jacobson. Rtml: A role-based trust-management markup language. Technical report, Purdue University, 2004.
11. F. Martinelli and M. Petrocchi. On relating and integrating two trust management frameworks. In *Proceedings of the Second International Workshop on Views on Designing Complex Architectures (VODCA '06)*, volume 168 of *Electronic Notes in Theoretical Computer Science*, pages 191–205. Elsevier, 2007.
12. S. Noel and S. Jajodia. Managing attack graph complexity through visual hierarchical aggregation. pages 109–118, New York, NY, USA, 2004. ACM Press.
13. R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. 25(5):633–650, 1999.
14. J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest-adversary security metric for network configuration security analysis. In *QoP '06: Proceedings of the 2nd ACM workshop on Quality of protection*, pages 31–38. ACM Press, 2006.
15. L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. An attack graph-based probabilistic security metric. In *Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security*, pages 283–296, Berlin, Heidelberg, 2008. Springer-Verlag.
16. L. Wang, S. Noel, and S. Jajodia. Minimum-cost network hardening using attack graphs. *Journal Computer Communications*, 29(18):3812–3824, 2006.