Computers and Electrical Engineering 37 (2011) 624–628

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

Technical Communication

Attribution of attack trees ☆

John N. Whitley, Raphael C.-W. Phan *, Jie Wang, David J. Parish

High Speed Networks Research Group, Department of Electronic and Electrical Engineering, Faculty of Engineering, Loughborough University, Leicestershire LE11 3TU, United Kingdom

ARTICLE INFO

Article history:
Received 1 October 2010
Received in revised form 11 April 2011
Accepted 15 April 2011
Available online 19 May 2011

ABSTRACT

An attack tree is a useful analytical technique to model security threats and/or risks, and hence model attacks as actual realizations of the former. Research on attack trees have focused either on applying such trees to model various ranges of security systems, or on advancements to this technique in itself. In this paper, we revisit the notion of attack tree attribution, i.e. how explicit attribute values of child nodes are aggregated to form the attribute of the parent node, and propose a novel attribution approach. We then show using this approach within the context of analyzing the weakest links of security systems, how the weakest link may not necessarily always be so, but instead it depends on the existence of other stronger links within the system.

1. Introduction

The notion of attack trees was popularized by the seminal work of [1]. An attack tree is a useful analytical technique to model security threats, and hence attacks as actual realizations of the former. Attack trees have been applied to model diverse security systems in different settings, e.g. the work of [2–7]. In a parallel direction, work has also been dedicated to enriching the attack tree technique itself. Some notable works consider: different node combinators; node attribution; multi-attribute (or parameter) nodes; and augmented edges. See [8,9,2,10,4,11–14].

Taking a step in this direction, we revisit the notion of attack tree attribution, i.e. how explicit attribute values of child nodes are aggregated to form the attribute of the parent node, and present a novel attribution approach. We use this attribution within the context of analyzing the weakest links of security systems; and thereby demonstrate how the weakest link may not necessarily always be so, instead it depends on the existence of other stronger links.

1.1. Background and related work

This subsection discusses relevant research on the theory behind attack trees, these include: node attributes; combinator functions; edge augmentation; and formalisation of the tree.

Nodes have had a number of different attributes proposed, including (multi-) attributes of probability of achievement, or time to live and completion confidence within the enhanced attack trees (eATs) by [2]. Defense trees extend attack trees with leaf node attributes representing countermeasures, see [15]; while the notion of attack–defense tree by [16] considers both attack nodes and defense nodes co-existing within the same tree, with attributes defined generally as a useful property of the node e.g. minimal attack cost, expected impact. Fovino et al. [17] considered integrating attack trees with fault trees,

☆ Reviews processed and approved for publication by Editor-in-Chief Dr. Manu Malek.

* Corresponding author.

E-mail addresses: J.N.Whitley@lboro.ac.uk (J.N. Whitley), R.Phan@lboro.ac.uk (R.C.-W. Phan), J.Wang3@lboro.ac.uk (J. Wang), D.J.Parish@lboro.ac.uk (D.J. Parish).

0045-7906/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2011.04.010

essentially by viewing fault events as potentially caused by an attack with a corresponding attack tree having the attack as its root (goal); and where to each node is assigned a probability of its achievement. The addition of precondition and postcondition assertions to nodes of an attack tree has been described by [13], and similarly for the case of multi-attribute nodes by [8,10,4,18]. As our contribution in this paper is in terms of an attribution approach, thus it is not directly affected by which particular type of attribute a node is defined to have, e.g. whether it is probability of achievement, time to live, or completion confidence. Our discussion in later sections considers the attribute type as resistance to attack; without loss of generality, it is worth noting here that it is possible for the other common types of node attributes e.g. probability of achievement, time to live, completion confidence, attack cost, to be translated to the notion of resistance. Essentially, they're all measures of how easy or difficult it is for an adversary to get from one node to another (modelling subgoals that an adversary has to get through en route to the ultimate goal).

Researchers have proposed different combinator functions to combine children nodes which are connected via edges to their parent node, including ordered-AND by [2], inhibit-AND and exclusive-OR by [9], ordered weighted averaging (OWA) combinators by [14], and more formal generic combinators as by [11,16]. Our attribution approach bases on the popular combinator functions OR and AND; other combinator functions e.g. as described above, are more restrictive special cases or combinations of OR and AND, thus our attribution definitions can be adjusted accordingly to include the restrictions or combinations. For instance, ordered-AND is a sequential version of the AND combinator where all child nodes need to be achieved in some prescribed order; inhibit-AND is the AND combinator with an extra gate input to control whether the output can be finally released; exclusive-OR is a special case of the OR combinator which only considers a subset of the latter's combination of child node achievements; while OWA is a variant of nested AND-OR combinators.

Augmented attack trees (aATs) have been proposed by [12], where edges are additionally defined to contain details of particular sequences of events that cause the transition along the edge between its two endpoint nodes. As attribution is performed irrespective of whether the edge is augmented or not, this is not directly related to our focus in this paper but we included here this kind of attack tree theory research, i.e. edge augmentation, for completeness.

There has been a study initiated by [11] and later by [16] of the use of attack (–defense) trees into a more rigorous setting by defining formal semantics and notions for operating on attack (–defense) trees, including generic forms of attribution and projection. [11] and [16] gave generic abstract definitions of the conjunctive combinator and disjunctive combinator, and suggested some example instantiations such as +, min or max functions. In contrast, the attribution approaches we propose in this paper provide a novel insight notably into OR-based attribution and its relation with the weakest link analysis; whereas existing OR-based attributions in literature cannot sufficiently capture this.

2. Definitions

We use notations similar to those used in the proposal of aATs by [12] in order to define the basic attack tree.

Definition 1 (*Attack tree*). An attack tree is a rooted tree denoted by $\mathsf{AT} = \langle \mathcal{V}, \mathcal{E}, \theta \rangle$ where

- $\mathcal{V}$ is the set of nodes in the tree representing the different states of partial compromise or sub-goals that an adversary needs to move through in order to fully compromise a system, such that for the two subsets $\mathsf{leafNodes} \subset \mathcal{V}$ and $\mathsf{internalNodes} \subset \mathcal{V}$, we have
  - ○$\mathsf{leafNodes} \cup \mathsf{internalNodes} = \mathcal{V}$
  - ○$\mathsf{leafNodes} \cap \mathsf{internalNodes} = \emptyset$ and
  - ○$v_0 \in \mathcal{V}$ is the root and represents the ultimate goal of the adversary, i.e. system compromise.
- $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$ is the set of edges in the attack tree. An edge $\langle u, v \rangle \in \mathcal{E}$ represents the state transition (emergent) from a child node v (and incident) to a parent node u, where $u, v \in \mathcal{V}$.
- θ is a set of tuples of the form $\langle u, \mathsf{combiningOperator} \rangle$ where
  - ○$u \in \mathsf{internalNodes}$ and
  - ○$\mathsf{combiningOperator} \in \{\mathsf{AND}, \mathsf{OR}\}$.

Definition 2 (*AND Combinator node*). A node $u \in \mathsf{internalNodes}$ is an AND combinator if all edges v_i incident to the node are connected by the AND combining operation, or there is exactly one edge incident to the node.

Definition 3 (*OR Combinator node*). A node $u \in \mathsf{internalNodes}$ is an OR combinator if all edges v_i incident to the node are connected by the OR combining operation.

3. Attribution

To the best of our knowledge, notable work on attribution of attack tree nodes is by [2,11], in addition to informal mention of associating attribute values to nodes by [1]. Most other definitions of attack trees do not involve node attributes.

To cast node attributes into a more formal setting, we propose an advanced attack tree definition as below.