How Good are Attack Trees for Modelling Advanced Cyber Threats?

Ola Flåten Mass Soldal Lund*
Norwegian Defence Cyber Academy, Lillehammer, Norway

Abstract

In this paper we present a study of the usefulness of attack trees for the modelling of advanced cyber threats. The study consisted of a case study where three cyber threats were modelled using attack trees and a judgement study where two cyber security experts were exposed to the attack tree models. We conclude that attack trees are not necessarily the best choice for modelling of advanced cyber threats.

1 Introduction

Attack trees [8] is a much used technique for analysing and describing attacks toward computer systems, and has become one of the more cited techniques for conducting security analysis. However, in recent years we have seen a development from simple malware with the ability to spread through self-replication to more advanced threats that cannot easily be stopped by anti-virus and similar technology. These threats often seek valuable data to gain an economic or military advantage, and they have the capability to persist over long periods of time; often they are referred to as *Advanced Persistent Threats (APTs)* [3]. The question we deal with in this paper is how well attack trees handles the emerging advanced cyber threats. More specifically, we present a small study into the use of attack trees as a technique to describe advanced cyber threats. The design of the study is presented in Section 2, the results are presented in Sections 3 and 4, and in Section 5 we provide conclusions. The full study is found in [2].

2 Study Design

For the study we formulated two research questions: *(1) To what degree are attack trees suited for modelling advanced cyber threats? (2) To what degree can attack trees help security experts increase their understanding of the threats modelled?* These questions were investigated by means of a small case study and a small judgement study. In the case study, three cyber threats – *Stuxnet* [1, 5], *GhostNet* [6, 9] and *NetTraveler* [4] – were modelled using attack trees based on publicly available literature. When the modelling was completed, the attack trees were subjected to a judgement study. The judgement study had two respondents; both cyber security experts working with monitoring and analysis of cyber threats for the Norwegian Armed Forces; both holding Master's degrees in information security; neither with prior experience with attack trees.

*Corresponding author: maslund@mil.no
Presented at the Norwegian Information Security Conference 2014 (NISK-2014).

After receiving a brief introduction to attack trees, they were then given the attack tree models, accompanied by textual descriptions, and had to answer a number of questions about the trees and the threats they modelled.

3 Modelling

Three cyber threats were modelled using attack trees. *Stuxnet* and *GhostNet* must be considered advanced cyber threats because they utilized targeted attacks with a variety of attack vectors, reconnoitred their targets, and showed persistence. *NetTraveler* is in itself not an advanced threat, but is assumed to be used by an advanced cyber threat.

Stuxnet

Stuxnet was a computer worm targeting Iranian nuclear enrichment facilities, allegedly developed by USA and Israel [7]; its ultimate goal was to damage the centrifuges used in the enrichment process. The attack tree modelling the threat is shown in Figure 1. The worm attacks industrial control systems by modifying the code on *programmable logic controllers (PLCs)*. PLCs are computers made specifically for automation of industrial systems; Step 7 is a software for programming PLCs.

The attack tree model gives a high-level view of Stuxnet. An alternative would be to model the threat at a technical level, e.g. make a model of how the worm installs itself on the infected computer. However, attack trees seem inappropriate for making such a model. The reason for this is that the installation follows a fixed procedure (with a few but not a lot of alternative paths) which are better illustrated in a flowchart (see e.g. the flowchart in [1, p. 16]).

GhostNet

GhostNet was a cyber espionage network uncovered in March 2009. The network consisted of 1295 infected computers in 103 different countries; up to 30 % of them

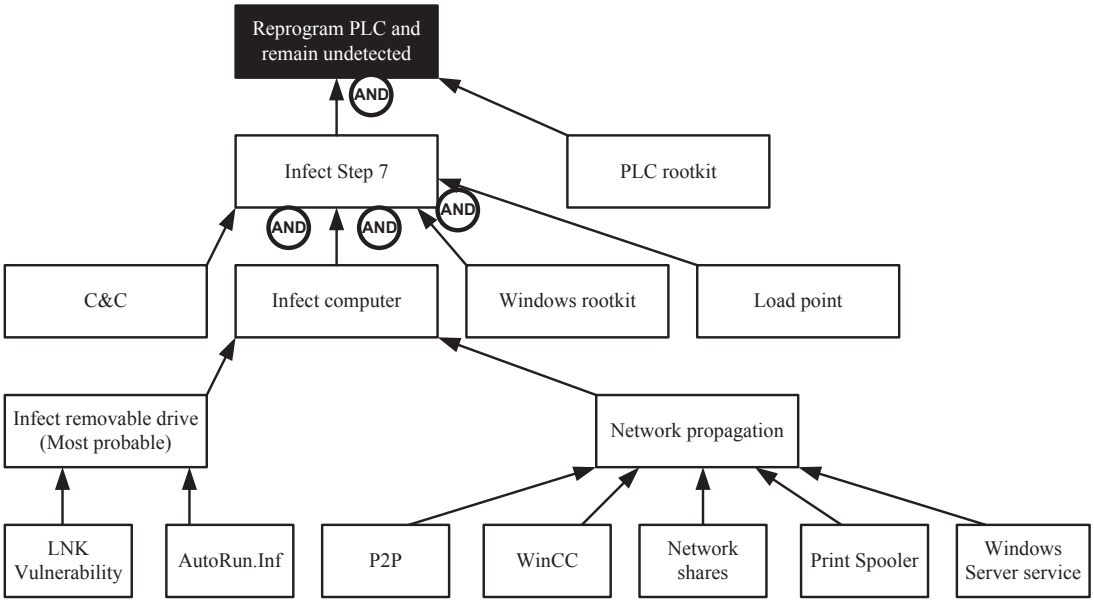

Figure 1: Attack tree modelling *Stuxnet*

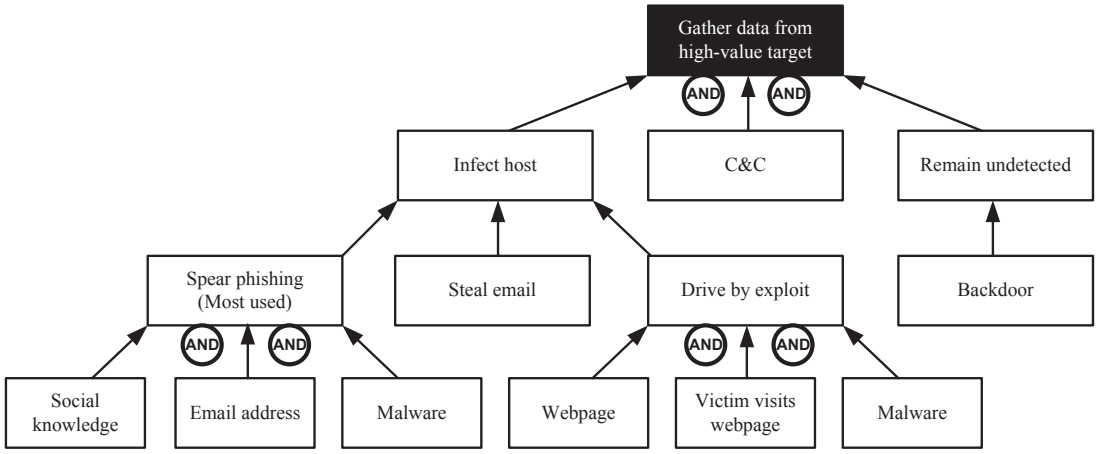

Figure 2: Attack tree modelling *GhostNet*

high-value targets. Who was behind has never been proven, but most of the control and command structure was traced to China.

As with the *Stuxnet* tree, the attack tree of *GhostNet* (Figure 2) is also very high-level. The reason for this is that the tree is a model of the (cyber espionage) actor rather than the malware involved in the attack (among other reasons because the publicly available sources are sparse on the technical details). Still, three methods of infecting a host that *GhostNet* employs were difficult to fit into the tree: "Impersonate victim", "Victim forwards spear phishing email" and "Remote administration Trojan". The reason for this is that these attack methods require that a host is already infected, which means that these nodes should have the node "Infect host" as both parent and child. Attack trees do not seem to have a mechanism for expressing this kind of repeated attacks.

NetTravler

NetTraveler is a kind of malware used for cyber espionage; more than 350 high-profile targets in 40 countries have been affected. As in the case of *Stuxnet* we found attack trees not to be appropriate for modelling the threat at a technical level and instead made a high-level attack tree describing an actor applying *NetTraveler*. The attack tree then turned out to be very similar to the attack tree modelling *GhostNet* (and we therefore do not reproduce the model here). The reason we get similar attack trees in these two cases might be that we have identified a kind of general pattern of cyber espionage.

4 Judgement Study

Two cyber security experts were asked to answer a number of questions based on the attack tree models and accompanying text. The respondents saw some potential in the attack trees as a means to give high-level overviews of the threats, but expressed very clearly that the trees lacked the sufficient detail to be of any particular use in detection and analysis. They were also of the opinion that adding the necessary details would make the trees very complex at the expense of readability, and thus did not regard this a good solution. They commented that the models of *GhostNet* and *NetTraveler* seem to fit cyber espionage in general, and thus have less use for the expert already familiar with the characteristics of cyber espionage. For these experts, just getting an overview of a threat

is not sufficient, and they were therefore of the opinion that for the purpose of detection and analysis there are probably other methods of describing cyber threats that are more suitable. One of respondents suggested the "Intrusion Kill Chains" of Hutchins *et al.* [3] as one such method.

5 Conclusions

The goal of this study was to investigate the usefulness of attack tree for the purpose of modelling advanced cyber threats. As an answer to the first of our research questions we conclude that high-level modelling may provide a good overview of a threat, but there may also be aspects of a threat that are difficult to fit into an attack tree. In the cases we investigated, the attack trees did not seem to be particularly suited for modelling at the technical level. With respect to the second research question we conclude that the attack tree models did not to any particular degree improve the experts' understanding of the threats. The reason for this is that they already had a good understanding of cyber threats in general and therefore did not have so much to learn from the high-level models. Finding the right balance between level of detail, complexity and readability of the attack trees is difficult, and maybe impossible. We therefore conclude that attack trees are not necessarily the best choice for modelling of advanced cyber threats.

Acknowledgements

We wish to thank the respondents in the judgement study for their valuable contribution.

References

[1] N. Falliere et al. *W32.Stuxnet Dossier. Version 1.4*. Symantec, 2011.

[2] O. Flåten. *Modellering av cybertrusler med attack trees*. Norwegian Defence Cyber Academy, 2013. In Norwegian.

[3] E. M. Hutchins et al. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. In *6th International Conference on Information Warfare and Security (ICIW 2011)*, 2011.

[4] Kaspersky Lab. *The NeTTraveler (aka 'TravNeT'). Part 1 (public)*, 2013.

[5] A. Matrosov et al. *Stuxnet Under the Microscope. Revision 1.31*. ESET, 2010.

[6] S. Nagaraja and R. Anderson. The snooping dragon: social-malware surveillance of the Tibetan movement. Technical Report UCAM-CL-TR-746, Computer Laboratory, University of Cambridge, Mar. 2009.

[7] D. E. Sanger. Obama order sped up wave of cyberattacks against Iran. New York Times, June 1, 2012.

[8] B. Schneier. Attack trees: Modeling security threats. *Dr. Dobb's Journal*, 24(12):21–29, 1999.

[9] The SecDev Group. *Trakcing GhostNet: Investigating a Cyber Espionage Network*, 2009. Information Warfare Monitor JR02-2009, Munk Center for International Studies, University of Toronto.