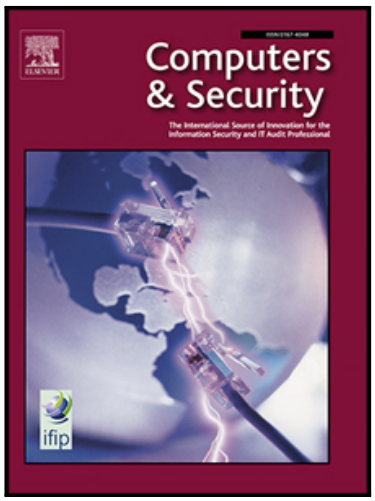

Evaluating Practitioner Cyber-Security Attack Graph Configuration Preferences

Harjinder Singh Lallie, Kurt Debattista, Jay Bal

PII: S0167-4048(18)30616-3
DOI: https://doi.org/10.1016/j.cose.2018.08.005
Reference: COSE 1383

To appear in: *Computers & Security*

Received date: 30 May 2018
Revised date: 25 July 2018
Accepted date: 15 August 2018

Please cite this article as: Harjinder Singh Lallie, Kurt Debattista, Jay Bal, Evaluating Practitioner Cyber-Security Attack Graph Configuration Preferences, *Computers & Security* (2018), doi: https://doi.org/10.1016/j.cose.2018.08.005

Evaluating Practitioner Cyber-Security Attack Graph Configuration Preferences

Harjinder Singh Lallie, Kurt Debattista, Jay Bal

University of Warwick, WMG, Gibbets Hill Road, Coventry, CV4 7AL

Abstract

Attack graphs and attack trees are a popular method of mathematically and visually representing the sequence of events that lead to a successful cyber-attack. Despite their popularity, there is no standardised attack graph or attack tree visual syntax configuration, and more than seventy self-nominated attack graph and twenty attack tree configurations have been described in the literature - each of which presents attributes such as preconditions and exploits in a different way. This research proposes a practitioner-preferred attack graph visual syntax configuration which can be used to effectively present cyber-attacks.

Comprehensive data on participant (*n=212*) preferences was obtained through a choice based conjoint design in which participants scored attack graph configuration based on their visual syntax preferences. Data was obtained from multiple participant groups which included lecturers, students and industry practitioners with cyber-security specific or general computer science backgrounds.

The overall analysis recommends a winning representation with the following attributes. The flow of events is represented top-down as in a flow diagram - as opposed to a fault tree or attack tree where it is presented bottom-up, *preconditions* - the conditions required for a successful exploit, are represented as ellipses and *exploits* are represented as rectangles. These results were consistent across the multiple groups and across scenarios which differed according to their attack complexity. The research tested a number of bottom-up approaches - similar to that used in attack trees. The bottom-up designs received the lowest practitioner preference score indicating that attack trees - which also utilise the bottom-up method, are not a preferred design amongst practitioners - when presented with an alternative top-down design. Practitioner preferences are important for any method or framework to become accepted, and this is the first time that an attack modelling technique has been developed and tested for practitioner preferences.

Keywords: attack modelling, threat modelling, cyber-security, security usability, security visualisation

Email address: HL, K.Debattista, Jay.Bal}@warwick.ac.uk (Harjinder Singh Lallie, Kurt Debattista, Jay Bal)