Accepted Manuscript

Title: Intelligent agents defending for an IoT world: a review

Author: Rory Coulter, Lei Pan

PII: S0167-4048(17)30251-1
DOI: https://doi.org/10.1016/j.cose.2017.11.014
Reference: COSE 1241

To appear in: *Computers & Security*

Received date: 17-1-2017
Revised date: 4-9-2017
Accepted date: 20-11-2017

Please cite this article as: Rory Coulter, Lei Pan, Intelligent agents defending for an IoT world: a review, *Computers & Security* (2017), https://doi.org/10.1016/j.cose.2017.11.014.

This is a PDF file of an unedited manuscript that has been accepted for publication. As a service to our customers we are providing this early version of the manuscript. The manuscript will undergo copyediting, typesetting, and review of the resulting proof before it is published in its final form. Please note that during the production process errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

ACCEPTED MANUSCRIPT

Intelligent Agents Defending for an IoT World: A Review

Rory Coulter[a,]*, Lei Pan[a,]*

[a]*School of Information Technology, Faculty of Science, Engineering and Built Environment, Geelong, VIC 3220, Australia*

Abstract

Transition to the Internet of Things (IoT) is progressing without realization. In light of this securing traditional systems is still a challenging role requiring a mixture of solutions which may negatively impact, or simply, not scale to a desired operational level. Rule and signature based intruder detection remains prominent in commercial deployments, while the use of machine learning for anomaly detection has been an active research area. Behavior detection means have also benefited from the widespread use of mobile and wireless applications. For the use of smart defense systems we propose that we must widen our perspective from not only security, but also to the domains of artificial intelligence and the IoT in better understanding the challenges that lie ahead in hope of achieving autonomous defense. We investigate how intruder detection fits within these domains, particularly as intelligent agents. How current approaches of intruder detection fulfill their role as intelligent agents, the needs of autonomous action regarding compromised nodes that are intelligent, distributed and data driven. The requirements of detection agents among IoT security vulnerabilities, challenges and their applicable methodologies. In answering aforementioned questions, a survey of recent research work is presented in avoiding refitting old solutions into new roles. This survey is aimed towards security researchers or academics, IoT developers and information officers concerned with the covered areas. Contributions made within this review are the review of literature of traditional and distributed approaches to intruder detection, modeled as intelligent agents for an IoT perspective; defining a common reference of key terms between fields of intruder detection, artificial intelligence and the IoT, identification of key defense cycle requirements for defensive agents, relevant manufacturing and security challenges; and considerations to future development. As the turn of the decade draws nearer we anticipate 2020 as the turning point

*Corresponding author

Email addresses: rcoult@deakin.edu.au (Rory Coulter), l.pan@deakin.edu.au (Lei Pan)

Accepted Manuscript

Download English Version:

https://daneshyari.com/en/article/6884092

Download Persian Version:

https://daneshyari.com/article/6884092

Daneshyari.com