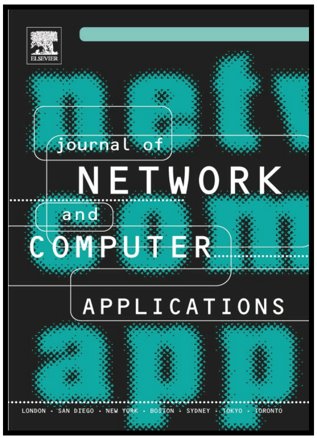
journal of
NETWORK
and
COMPUTER
APPLICATIONS
LONDON • SAN DIEGO • NEW YORK • BOSTON • SYDNEY • TOKYO • TORONTO

www.elsevier.com/locate/jnca

A Bayesian Inference-based Detection Mechanism to Defend Medical Smartphone Networks Against Insider Attacks

Weizhi Meng, Wenjuan Li, Yang Xiang, Kim-Kwang Raymond Choo

PII: S1084-8045(16)30281-8
DOI: http://dx.doi.org/10.1016/j.jnca.2016.11.012
Reference: YJNCA1763

To appear in: *Journal of Network and Computer Applications*

Received date: 8 August 2016
Revised date: 10 November 2016
Accepted date: 15 November 2016

Cite this article as: Weizhi Meng, Wenjuan Li, Yang Xiang and Kim-Kwang Raymond Choo, A Bayesian Inference-based Detection Mechanism to Defenc Medical Smartphone Networks Against Insider Attacks, *Journal of Network an Computer Applications,* http://dx.doi.org/10.1016/j.jnca.2016.11.012

A Bayesian Inference-based Detection Mechanism to Defend Medical Smartphone Networks Against Insider Attacks

Weizhi Meng[1,a], Wenjuan Li[b], Yang Xiang[c], Kim-Kwang Raymond Choo[d,e]

[a]Department of Applied Mathematics and Computer Science, Technical University of Denmark, Denmark
[b]Department of Computer Science, City University of Hong Kong, Hong Kong SAR, China
[c]School of Information Technology, Deakin University, Australia
[d]Department of Information Systems and Cyber Security, University of Texas at San Antonio, San Antonio, USA
[e]School of Information Technology and Mathematical Sciences, University of South Australia, Australia
[f]E-mail address: {weme@dtu.dk, wenjuan.li@my.cityu.edu.hk, yang.xiang@deakin.edu.au, raymond.choo@fulbrightmail.org }

Abstract

With the increasing digitization of the healthcare industry, a wide range of devices (including traditionally non-networked medical devices) are Internet- and inter-connected. Mobile devices (e.g. smartphones) are one common device used in the healthcare industry to improve the quality of service and experience for both patients and healthcare workers, and the underlying network architecture to support such devices is also referred to as medical smartphone networks (MSNs). MSNs, similar to other networks, are subject to a wide range of attacks (e.g. leakage of sensitive patient information by a malicious insider). In this work, we focus on MSNs and present a compact but efficient trust-based approach using Bayesian inference to identify malicious nodes in such an environment. We then demonstrate the effectiveness of our approach in detecting malicious nodes by evaluating the deployment of our proposed approach in a real-world environment with two healthcare organizations.

Keywords:
Emerging Architecture, Emerging Smartphone Networks, Intrusion Detection, Bayesian Inference, Insider Attacks.

1. Introduction

With the rapid advancements and interconnectivity of information and communications technologies (ICT), it is no surprise that ICT form the backbone of many aspects of the healthcare and medical industry. For example, it has been estimated that ICT could save 63 billion dollars in healthcare costs over the next fifteen years, with a 15-30 percent reduction in hospital equipment costs [11].

However, healthcare or medical networks are subject to more stringent scrutiny, in comparison to traditional networks [34], due to the sensitivity of information (e.g. patient data and medical history) and the number and diversity of devices that could potentially be exploited to target the system [31]. According to a survey by [16], for example, the number of information security breaches reported by healthcare providers soared 60 percent from 2013 to 2014, which is almost double the increase in other industries. A more recent McAfee report explained that vulnerabilities affecting networked medical devices are not different from other operational technologies (e.g. medical devices), consumer technologies (e.g. smartphones) and other forms of ICT (e.g. hospital networks) [17]. The networked medical devices may be vulnerable to accidental failures, privacy violations, intentional disruption, and widespread disruption.

It is no surprise that medical and mobile devices are targeted by cybercriminals due to the use of such devices to store and/or access sensitive information such as patient's personally identifiable information (PII) and medical history. In addition, with the widespread adoption of mobile technologies and the descreasing costs of mobile devices (e.g. Android and iOS devices), mobile devices are increasingly integrated in MSNs (e.g. recording patient's medical conditions and accessing patient's records in real-time during ward visits). These devices are generally connected to the organization's wireless network; thus, each device can be considered a node. Although such networks are private, they can

[1] Corresponding author and was known as Yuxin Meng.