COMPUTERS & SECURITY 58 (2016) 106–124

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Proactively applied encryption in multipath networks

James Obert [a,*], Inna Pivkina [b], Hong Huang [b], Huiping Cao [b]

[a] Cyber R&D Solutions, Sandia National Labs, Albuquerque, NM, USA

[b] Computer Science & Electrical Engineering Departments, New Mexico State University, Las Cruces, NM, USA

ARTICLE INFO

Article history:
Received 30 January 2015
Received in revised form 12 November 2015
Accepted 24 December 2015
Available online 6 January 2016

Keywords:
Multipath security
Information assurance
Anomaly detection
Intrusion detection
Data encryption

ABSTRACT

In providing data privacy on multipath networks, it is important to conserve bandwidth by ensuring that only the necessary level of encryption is applied to each path. This is achieved by dispersing data along multiple secure paths in such a way that the highest encryption level is applied to those paths where threats are most likely to be present. Conversely, for those paths where the likelihood of attack is least, the encryption levels should be commensurately lower. In order to maintain data privacy, path encryption level adjustments should be proactive. In so doing, the multipath network should have the ability to calculate the probability of an attack and proactively adjust the encryption strength long before the final steps of an attack sequence occur. The unique methods described in this research, are able to sense when an attack sequence is initiated on a path. This is achieved by calculating the probability of the presence of specific attack sequence signatures along each network path using statistical learning techniques, and by deriving path information assurance levels using these probabilities. As an attack sequence progresses, the likelihood of the presence of specific attacks grows until a threshold level is met and an encryption adjustment for a path is warranted.

1. Introduction

Using multiple paths impedes an adversary's ability to focus the attack on a single path. A secure multipath network requires a sender to transmit data over multiple paths with a level of security enabled along each path commensurate with the relative threats and be proactively adjusted according to the foreseen attack environment. Even though the importance of proactively adjusting security measures is crucial, existing multipath routing protocols such as Multipath TCP lack the ability to sense threats or adjust the level of security along a path (Wei-wei and Hai-feng, 2010).

In this paper, we present a novel approach that utilizes machine learning techniques to determine the current and future information assurance levels of network paths in multipath networks. Through the use of mutual information theory, entropy analysis and Bayesian inference (Gelman, 2004), predicted future information assurance levels are calculated. With the ability to predict future attacks, a multipath network is able to proactively enforce appropriate security measures on the most vulnerable paths.

Compared to other types of multipath network security methods, which are based on heuristically derived trust models, the proposed approach is based on actual cloud infrastructure and service provider directed attack sequences.

* *Corresponding author.* Tel.: +0015056045519.
E-mail address: jobert@sandia.gov (J. Obert).

http://dx.doi.org/10.1016/j.cose.2015.12.003
0167-4048/

Additionally, our approach finds the likelihood of the presence of cloud directed attack patterns in data event windows and *proactively* assigns information assurance levels and applies appropriate encryption strength to paths. Although, the exact security measures applied to vulnerable paths depends on the type of attack sequence signature identified, in this paper, we only address attacks on data privacy where an increase in path encryption strength will preserve privacy.

In addition, the field of intrusion detection is quite expansive, and includes complex topics such as polymorphic and zero-day attacks, which we will not attempt to address in this paper directly. We refer the reader to Bilge and Dumitras (2012) and Polychronakis et al. (2009) for an extensive review of these topics. Although we recognize that polymorphic and zero-day attacks pose a real threat to multipath networks, we restricted our research to *slow attacks* where known static attack signature sequences are transmitted over multipath networks within an extended time period (see Section 3.1). Specifically, we explored scenarios where an attacker attempts to stagger the transmission of known attack signature elements over a *targeted network path* using a *slow attack* strategy in order to evade detection. Our methods calculate the probability of an attack occurring prior to the transmission of final attack signature elements. Once the probability of a slow attack on a path is calculated, the encryption level on the targeted path is proactively adjusted.

The remainder of this paper is organized as follows. We provide in Section 2 a review of related work. Section 3 presents derived network path information assurance level and proactive encryption methods. In Section 4, evaluation results and conclusion are presented.

2. Background

Early forms of multipath routing entailed using no encryption and data were split among different routes in order to minimize the effects of malicious nodes. In the case of fixed bandwidth networks, the approach in Lee et al. (2005) uses existing multiple paths such that an intruder needs to spread resources across several paths to seriously degrade data confidentiality. Later approaches presented in Monnet and Mokdad (2013) and Younis et al. (2009) statically apply fixed encryption strengths to data on each path according to heuristically predetermined data sensitiveness on a path. The approach in Younis et al. (2009) randomly alternates the encryption strengths along paths as a means to confuse an adversary. The primary limitation of Younis et al. (2009) is accurately forecasting the data sensitivity of data transmitted along a path. None of the approaches suggests an adequate or explicit means for combining dispersive data security methods with intelligent, dynamically differentiating path data security measures. Additionally, little progress has been made in providing resilience to protocol attacks, slow attacks or evasive attacks in multipath networks.

The differentiating approach proposed in this paper is to *proactively* sense initiated attack sequences present along each network path and correspondingly increase the encryption strength on more vulnerable paths while decreasing it on the less vulnerable ones. In order to manage throughput loss, the transmission rates on more vulnerable paths will drop, while it will increase on the less vulnerable ones.

3. Network path security determination

Given a network, let I be the information assurance factor, C be the path cost factor (i.e., Open Shortest Path First Cost (Li and Kwok, 2005)), and E be the encryption scaling factor. The information assurance factor I is a measure of how secure a network path is. If I is determined to be low on a network path P, the probability of a network threat being present on that path is high and that path is considered to be vulnerable. The encryption scaling factor E is a factor representing how much encryption is to be applied to a network path in order that the path can be effectively protected from an attack. The path cost factor C represents the impedance presented by a network path. When C is high, network traffic is less likely to travel down a specific path.

For distinct paths in a multipath network, the values of these factors are different. I_i, E_i and C_i are the information assurance, encryption scaling, and cost factors, respectively, for a path P_i. Given a message L transmitted through a multipath network from source node v_s to a destination node v_e, the data of L are divided among the network paths using multipath routing. If the network attack threat levels are sensed on each path, then the information assurance factor I_i for each path can be determined based on these threats. Data security is enforced by decreasing C_i and E_i on less vulnerable paths while increasing these factors on more vulnerable ones.

For example, assume that the network routing algorithm decides to use two paths P_i = path (v_1, v_6, v_3, v_4, v_2) and P_j = path (v_1, v_6, v_5, v_7, v_2) to send a message L from v_1 to v_2 as shown in Fig. 1. Then, the loss of throughput through the multipath network is lowered by increasing or decreasing C and E on each path according to the value of I derived for each path. The values of C and E are varied inversely to the path value of I over n paths. The data are transmitted to destination vertex v_2 and protected by dynamically adjusting encryption E scaling factors according to the values of the information assurance factor I over each path.

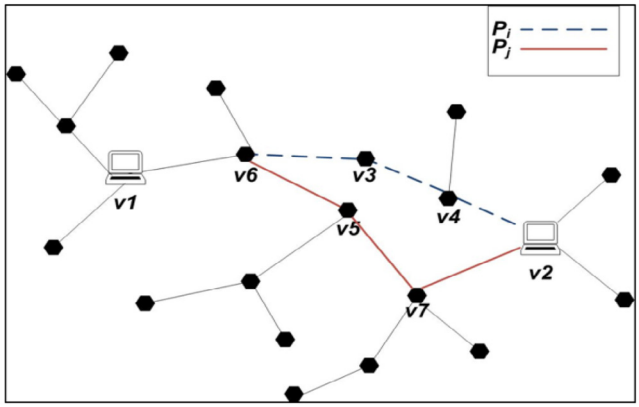

Fig. 1 – Multipath graph.