Research Repository UCD

Title	E-government Alerts Correlation Model
Authors(s)	Al-Mahrouqi, Aadil, Abdalla, Sameh, Kechadi, Tahar
Publication date	2014-11-19
Publication information	Al-Mahrouqi, Aadil, Sameh Abdalla, and Tahar Kechadi. "E-Government Alerts Correlation Model," 2014.
Conference details	Qatar Foundation Annual Research Conference, 18-19 November 2014, Qatar
Item record/more information	http://hdl.handle.net/10197/6619

Downloaded 2023-04-07T10:52:29Z

The UCD community has made this article openly available. Please share how this access benefits you. Your story matters! (@ucd_oa)

© Some rights reserved. For more information

E-government Alerts Correlation Model

Aadil Al-Mahrouqi, Sameh Abdalla, Tahar Kechadi

University College Dublin (UCD), Ireland

aadil.al-mahrouqi@ucdconnect.ie

Background & Objectives

Qatar's IT infrastructure is rapidly growing to encompass the evolution of businesses and economical growth the country is increasingly witnessing throughout its industries. It is now evident that the country's e-government requirements and associated data management systems are becoming large in number, highly dynamic in nature, and exceptionally attractive for cybercrime activities. Protecting the sensitive data e-government portals are relying on for daily activities is not a trivial task. The techniques used to perform cybercrimes are becoming sophisticated relatively with the firewalls protecting them. Reaching high-level of data protection, in both wired and wireless networks, in order to face recent cybercrime approaches is a challenge that is continuously proven hard to achieve.

In a common IT infrastructure, the deployed network devices contain a number of event logs that reside locally within its memory. These logs are in large numbers, and therefore, analyzing them is a time consuming task for network administrators. In addition, a single network event often generates a redundancy of similar event logs that belong to the same class within short time intervals. The large amount of redundancy logs makes it difficult to manage them during forensics investigation. In most cybercrime cases, a single alert log does not contain sufficient information about malicious actions

background and invisible network attackers. The information for a particular malicious action or attacker is often distributed among multiple alert logs and among multiple network devices. Forensic investigators mission is to detect malicious activities and reconstruct incident scenarios is now very complex considering the number as well as the quality of these event logs.

Methods

My research will focus on involving mathematics and algorithm science for each proposed sub models in the Alerts correlation model to help us to validate the proposed framework. The alert correlation model will collect alert logs. These logs will be stored in the alert logs warehouse. The stored alert log contains redundancy data and irrelevant information. The alert correlation model used to filter out all redundancy data and irrelevant information from the alert logs. The alert correlation model contains two stages format standardization and redundancy management. The format standardization process aims unified different event logs format into one format, while the redundancy management process aims to reduce the duplication of the single event. Furthermore, this research will try to utilized criminology science to enhance security level of the proposed framework. Moreover, this research forensics experiments tools to validate the proposal approach.

Results

In response to attacks and potential of attacks against network infrastructure and assets, my research focuses on how to build an organized legislative e-government environment. We present a new approach for a network alert logs correlation mechanism. The idea of this approach is to forensically utilize the current network security output by collect, analysis and present evidence of network attack in an efficient manner. After data mining process we utilized our preprocessing results for e-government awareness purpose. This research considered as an initial step towards reconstructing the attack

scenario, data mining techniques and forensics expert knowledge to build a complete cybercrime management model.

Conclusions

This research proposed Qatar e-government alerts correlation model. The proposed model used to process and normalize the captured network event logs. The main point of designing the model is to find a way to forensically visualize the evidence and attack scenario in e-government infrastructure.

e-Government Network Forensics Correlation Model

Aadil Al-Mahrouqi, Sameh Abdalla, Tahar Kechadi

Introduction

Qatar's IT infrastructure is rapidly growing to encompass the evolution of businesses and economical growth. The country is increasingly witnessing this throughout its industries. The country's e-government requirements and associated data management systems are becoming large in number, highly dynamic in nature, and exceptionally attractive for cybercrime activities. Protecting the sensitive e-government data, which are relied on for daily activities is not a trivial task. The techniques used by cybercrimes are becoming sophisticated relatively with the firewalls protecting them. Reaching high-level of data protection, in both wired and wireless networks, in order to face recent cybercrime approaches is a challenge that is continuously proven hard to achieve.

The Challenge

Analyzing network events logs is a time consuming task for network administrators. One network event often generates a redundancy of similar event logs that belong to the same class within short time intervals. The large amount of redundancy logs makes it difficult to manage them during forensics investigation. In most cybercrime cases, a single alert log does not contain sufficient information about malicious actions background and invisible network attackers. The information for a particular malicious action or attacker is often distributed among multiple alert logs and among multiple network devices. The forensics investigation mission now very complex considering the number as well as the quality of these event logs.

Our Approach

In response to attacks and potential of attacks against network infrastructure and assets, our research focuses on how to build an organized legislative e-government environment. We present a new approach for a network alert Logs correlation mechanism. The idea of this approach is to forensically utilize the current network security output by collect, analysis and present evidence of network attack in an efficient manner. After data mining process we utilized our preprocessing results for e-government awareness purpose. This research considered as an initial step towards reconstructing the attack scenario, data mining techniques and forensics expert knowledge to build a complete cybercrime management model.

Our Model

The Network Forensics Correlation Model will helps collect alert logs and network configuration files. The collected files will store in the central repository. The stored alert log contains redundancy data and irrelevant information. The Network Forensics Correlation Model used to filter out all redundancy data and irrelevant information from the alert logs. The format standardization process aims unified different event logs format into one format, while the redundancy management process aims to reduce the duplication of the single event. Furthermore, this research will try to utilized criminology science to enhance security level of the proposed framework.

CONCLUSIONS

Our e-Government Network Forensics Correlation model addresses the problem of processing and normalizing the captured network event logs and network configuration files. The main challenge our model resolves is to visualize the evidence and attack scenario in e-Government infrastructure which in return facilitates the forensics investigation mission.