ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/277870953

A Cyber Security Situational Awareness Framework to Track and Project Multistage Cyber Attacks

Conference Paper · March 2014

CITATIONS
5

READS
1,764

4 authors, including:

Parth Bhatt
CPQD
5 PUBLICATIONS **107** CITATIONS
SEE PROFILE

Edgar Toshiro Yano
Instituto Tecnologico de Aeronautica
35 PUBLICATIONS **227** CITATIONS
SEE PROFILE

Per M. Gustavsson
George Mason University
78 PUBLICATIONS **531** CITATIONS
SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Project Command &Control View project

Project Command and Control - theory, operations and technology View project

All content following this page was uploaded by Per M. Gustavsson on 08 June 2015.

The user has requested enhancement of the downloaded file.

A Cyber Security Situational Awareness Framework to Track and Project Multistage Cyber Attacks

Parth Bhatt[1], Dr. Edgar Toshiro Yano[1], Dr. Joni Amorim[2], Dr. Per Gustavsson[3]

[1]Department of Computer Science, Instituto Tecnológico de Aeronáutica ,São José dos Campos, Brasil
[2]University of Skövde, Skövde, Sweden
[3]Combitech Sweden, Swedish National Defence College / George Mason University, USA

parthbhatt09@gmail.com[1],
yano@ita.br[1],
joni.amorim@his.se[2]
per.m.gustavsson@combitech.se[3]

Abstract: In Security Operations Center there is a need to perceive, comprehend and project cyber activities. Therefore it requires developing Cyber Situational Awareness (CSA) capability that involves perception of different security events, comprehension of the meaning of the current cyber security situation in the organization, and the projection of future status in order to select better positioning of security mechanisms. Current techniques of CSA are limited by the high speed of events generation, large volume of information from multiple sensors, and the complexity of interactions of highly automated services that shape the Cyberspace. This study presents a framework to track and project multistage cyber-attacks supporting CSA activities and enables a faster correlation of event logs using Big Data Technologies.

Keywords: Hadoop, Security log analysis, multistage cyber-attacks detection, Intrusion Kill-Chain, Cyber Situational Awareness

1 Introduction / Background

A Security Operations Center (SOC) (Kowtha et.al 2012) has its outmost goal to timely detect, respond to, protect from, restore and mitigate effects of Cyber-attacks In order to enable cyber defenders to react to events more efficiently, a SOC needs to be able to project the opponent's next moves and intentions. Therefore there is a need for a Cyber Situational Awareness (CSA) (Tadda 2010) capability within a SOC.

1.1 Situational Awareness

Situational Awareness (SA) is formally defined as "the perception of the elements in the environment within a amount of time and space, the comprehension of their meaning and the projection of their status in the near future" (Endsley 1995) SA involves *Perception* of critical factors in the environment, *Comprehending* what those factors mean, and *Projection* of what will happen with the system in the near future. Extending Endsley SA definition, Cyber Situational Awareness (CSA) (Tadda 2010) involves the perception of attacks and attack tracks, comprehension of the attack patterns and correlations, and the projection of what will happen in the near future in terms of impact and threat levels towards the information and network assets.

1.2 Cyber Security

Generally, the intent of Cyber-attacks are categorized into Stealing, Altering, and Deleting of information or disrupt, deny, destroy, divert the business or sub functions within the attacked organisation/system. The attacks are often assumed as single and direct attacks to gain access; they are conducted inside or outside the targeted organization (Forward 2009, IMG-S 2012). However, the landscape is changing and attackers are avoiding attacking directly the systems and services that are normally well protected. Instead they attack specific users or infrastructure. These Targeted attacks (Sood 2013) are formed around the activities of selection of targets and then launching attacks on

such selected aims. On a highly sponsored level, they take the shape of multi-year intrusion campaigns with well-resourced and managed operations, such threat actors were recently named as Advanced Persistent Threats (APT) (Hutchins 2011). These attacks are advanced as they may leverage one or many zero day vulnerabilities (Falliere 2011) of the target system, which helps to bypass conventional security mechanisms. APTs usually perform multistage attacks (Vries et al. 2012) in which at each stage, the attackers get a certain level of privileges to start a new stage, they proceed similarly to attain the final goal. Persistence is maintained inside target environment using multiple intrusions and once inside they remain undetected.

Large scale data collection and analysis capability is not just sufficient to deal with such challenges, there is also a need of a conceptual model to support the data fusion process (Yang et al. 2009) inorder to clarify the cyber-attacks. The approach taken in this study combines the use of Attack Trees, Goal Oriented Action Planning (Bjarnolf etal.2008) and the Intrusion Kill Chain Method (Hutchins 2011) to model a multistage attack. The purpose is to model the behavior of advanced multistage attacks against security architectures.

2 Framework

The proposed framework provides a SOC with capability of performing CSA activities by detecting and analyzing multistage cyber-attacks on layered security architectures.

This research framework has the following components:

- Layered Security architecture Model;
- Multistage attack model
- Intrusion Management System

2.1 Layered Security architecture

The security architecture structures the system to be protected in a series of layers of privilege levels. Each layer identifies a set of privileges required to access the assets of that level or an internal layer. The rationale is to position the most valued assets inside internal layers of the architecture thus, to access those assets a multistage attack (at least one stage to bypass each layer) should be expected from the intruder. Layered security architecture also identifies prevention devices that deny unauthorized access or use and detection devices that identify anomalies; policy rules breaks, and configuration tampering.

Privilege Level	Assets	Prevention Devices	Detection Devices
External Ring	External Host Files, Management team credentials	Firewall,External Host ACL	NIDS, HIDS at External Host
Internal Ring	Security Server Files, Firewall ACL, Internal Host files, Admin credential	Firewall. Internal Host ACL	NIDS, HIDS at Internal Host

Table 1 – Security Architecture Example.

2.2 Multistage attack model

In our proposal, multistage attacks are modeled using attack trees. The final goal of an attack is a privilege level required to access a desired asset. Figure 1 is an example of one such attack tree.

In the following example, to access the Security Files Server the attacker must execute a multistage attack with the following goals for each stage:

1. Obtain the access to the external ring host, then an internal host.
2. To steal a management team credential and get access to an internal ring host.
3. To steal the admin credential and get access to the security server.

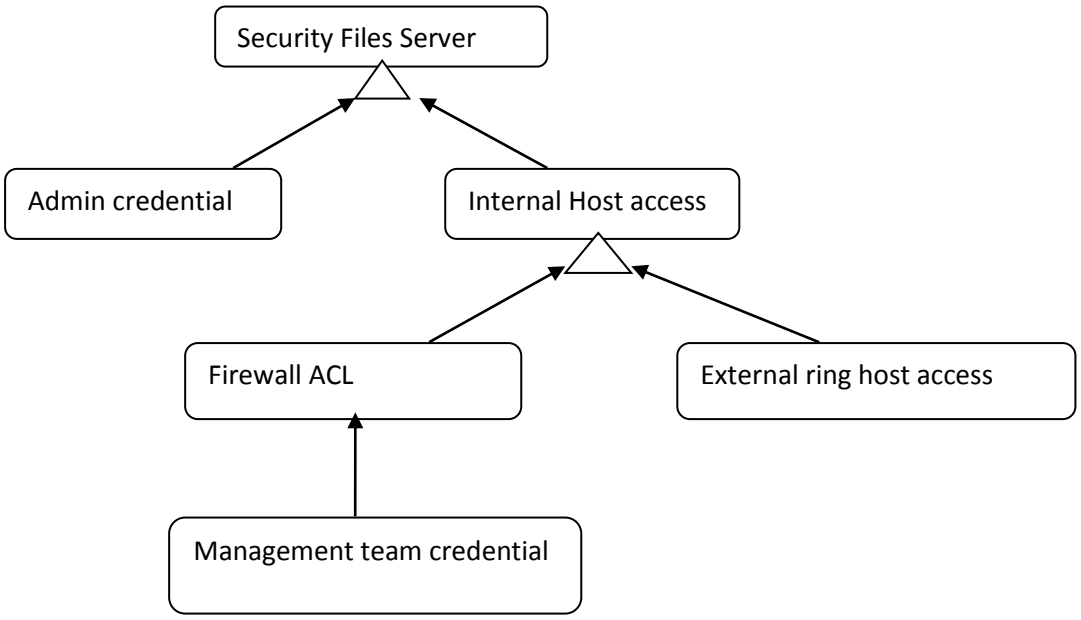

Figure 1 – Attack tree example

For modeling stages of each intrusion we adopted the Intrusion Kill Chain Model. It consists of seven phases that an attacker must follow to carry out intrusions; figure 2 shows a intrusion kill chain. Kill chain phases are explained as follows:

Figure 2: Intrusion Kill Chain

- Reconnaissance– Adversaries collect information about the target for example email addresses, or network scans.
- Weaponization – A weapon is developed to exploit identified vulnerabilities of the target environment. It is usually a malicious file container with exploit and backdoor, a drive by download link, or a command injection.
- Delivery- The weapon is delivered into the target environment.
- Exploitation- Using a vulnerability of the target system the malicious code is executed.
- Installation - A backdoor is generally installed which allows the adversary to maintain their persistence and carry out operations.

- Command and control (C2) - Adversaries require a communication channel to control thier malware and continue their actions.
- Actions - At this phase the adversary performs actions towards to the final goal. Example: data search and exfiltration.

Defenders can be confident that the attacker achieves their goals using a model with these phases (Hutchins et al. 2011).

2.3 Intrusion Management System (IMS)

The IMS provides rapid processing of large amount of security log data (structured or unstructured logs in text files) from different sources and collected in big time frame (1-2 years or more). This system (Bhatt, Yano 2013) uses Apache Hadoop (White 2012) figure 3 provides overview of Hadoop based IMS. IMS modules are as follows:

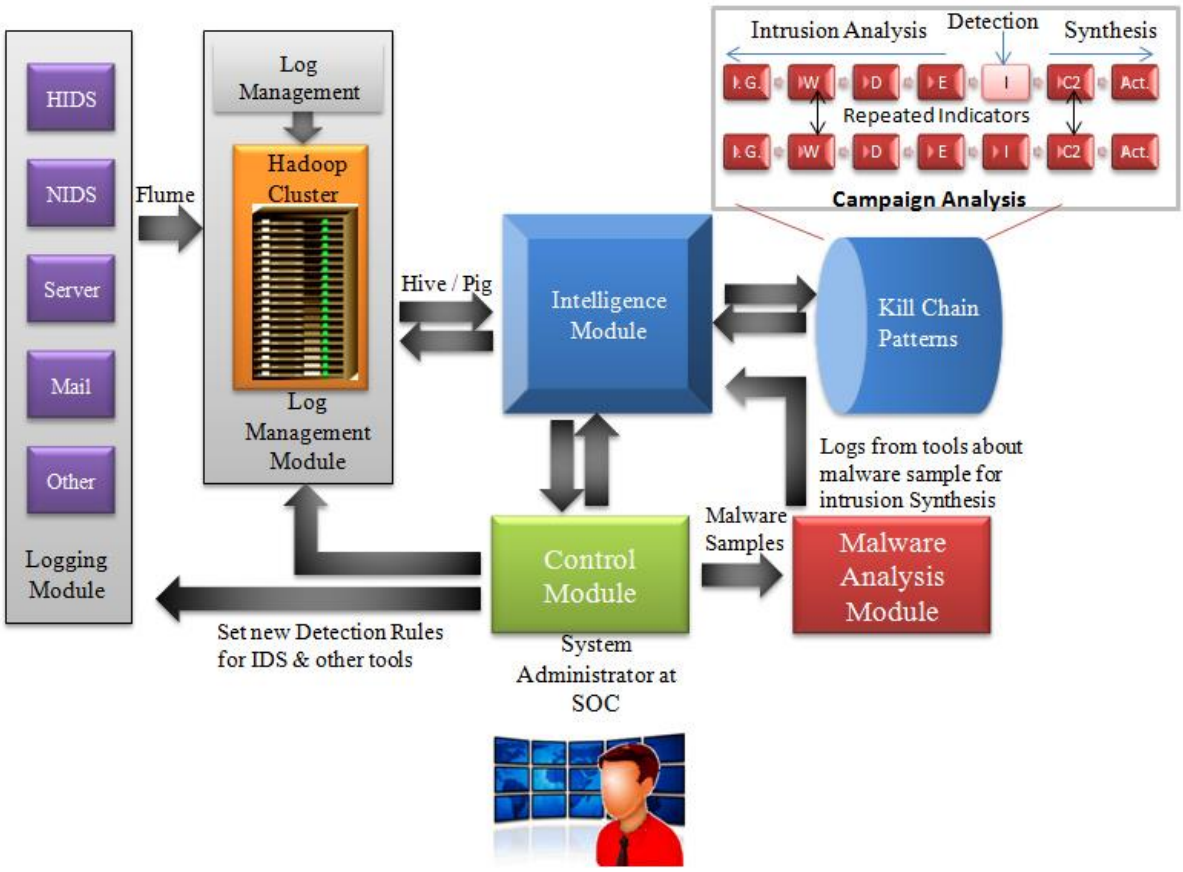

Figure 3: Hadoop Based Intrusion Management System

2.3.1 Logging Module

This module consists of collecting logs from different sources, such as HIDS (Host intrusion detection system) and NIDS (Network intrusion detection system) , Web Server and Mail server.

2.3.2 Log Management Module

All the logs generated in the Logging Module are moved, stored and pre-processed in the Hadoop Distributed File System (HDFS) (White 2012) where they are managed and accessed as required for search and correlation of security events.

2.3.3 Intelligence Module

Intelligence module contains the algorithms for event correlation and automatic intrusion kill chain search, based on the high alert malicious events detected by logging module. In order to enable the analysis of multi-year and multistage attacks, the intelligence module has a campaign analysis component. Using it, indicators from previous intrusions are collected and correlated in order to identify a potential continuation of those attacks. The layered security architecture model, attack tree model and data collected from the campaign analysis are used to infer the attacker's intention, attack likelihood and its impact on affected assets.

2.3.4 Malware Analysis Modules

Explaining malware analysis in detail is out of scope of this paper. It is adopted from (Li et al. 2011) method of malware analysis. Detailed malware analysis should be performed for understanding methods, vulnerabilities and targets of the attack and corresponding log information should be returned to the intelligence module to complete the kill chain reconstruction.

2.3.5 Control Module

Using this module the Administrator of the SOC sets new rules for IDSs, manages Hadoop Cluster, maintains CSA activities in the right direction and examines suspicious samples to guide the framework operations of tracking and projecting multistage attacks.

3 Conclusions and Future Works

In this paper, we discussed a framework based on Apache Hadoop and intrusion kill chain technique that provides a SOC with CSA capabilities for tracking and projecting multistage cyber-attacks.

Experiments from our previous research (Bhatt, Yano 2013) on intrusion kill chain reconstruction for single stage attacks provided promising results. Thus, a similar framework is adopted as a component (section 2.3) of the complete framework of this research. Ongoing experiments with this framework have the objective to reconstruct kill chains for each compromised layer of security architecture and their projection with attack trees, in order to understand the intent of the intruder and gain actionable intelligence for defending against next possible targets of a multistage attack.

The future work is to further test the framework for realistic multistage scenarios and use probabilistic models to project intrusion campaigns for reducing false positives.

Acknowledgements

The authors would like to thank the following organizations for their support: University of Skövde (HiS),Sweden, Swedish National Defence College (SNDC),Sweden, Combitech AB, Sweden, and National Council for Scientific and Technological Development, Brazil.

References

Bhatt P., Yano E.T.(2013), "Analyzing Targeted Attacks using Hadoop applied to Forensic Investigation" The Eight International Conference on Forensic Computer Science http://dx.doi.org/10.5769/C2013004

Bjarnolf P., Gustavsson Per M, Christoffer Brax, and Mikael Fredin. (2008), Threat Analysis Using Goal-Oriented Action Planning. In *Proceedings of the Fall Simulation Interoperability Workshop*,

Endsley M. R.,(1995) "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors: The Journal of the Human Factors and Ergonomics Society,* vol. 37, pp. 32-64, 1995.

Falliere N., Murchu L.O., and Chien E. (2011) Symantec “W32.Stuxnet Dossier” Version 1.4
Forward (2009) - EU FP-7, Managing Emerging Threats in ICT Infrastructures, Forward Consortium - EU FP7, 2009.
Li F, Atlasis A, (2011)“ A Detailed Analysis of an Advanced Persistent Threat Malware” SANS Institute InfoSec Reading Room
Hutchins Eric M., Cloppert Michael J., Amin Rohan M,(2011) “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains” ICIW2011
IMG-S Integrated Mission Group for Security (2012), “IMG-S Position paper for Horiztion 2020,” IMG-S, 2012.
Kowtha S., Nolan L. and Daley R.,(2012) ”Cyber security operations center characterization model and analysis,” i *2012 IEEE Conference on Technologies for Homeland Security (HST)*
Sood A.K., Enbody R.J. (2013) “ Targeted cyber attacks: A Superset of advanced persistent threats” Security & Privacy, IEEE Volume 11 , Issue 1 2013
Vries, J.D. and Hoogstraaten H. and Berg, J.V.D. and Daskapan S,. (2012) Systems for Detecting Advanced Persistent Threats CyberSecurity. 54-61, IEEE Computer Society
White, T.,(2012) Hadoop: The Definitive Guide, Third Edition,O’Reilly
Yang S. J., Stotz A., Holsopp J., Sudit M. and Kuhl M., (2009) “High level information fusion for tracking and projection of multistage cyber attacks,” *Information Fusion ,* vol. 10

View publication stats