COMPUTERS & SECURITY 48 (2015) 35–57

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Combating advanced persistent threats: From network event correlation to incident detection

Ivo Friedberg, Florian Skopik, Giuseppe Settanni, Roman Fiedler*

Austrian Institute of Technology, Safety and Security Department, Donau-City-Straße 1, 1220, Vienna, Austria

ARTICLE INFO

Article history:
Received 11 June 2014
Received in revised form
3 September 2014
Accepted 28 September 2014
Available online 13 October 2014

Keywords:
Advanced persistent threat
Anomaly detection
Log file analysis
Intrusion detection
Event correlation
Self-learning system model

ABSTRACT

An advanced persistent threat (also known as APT) is a deliberately slow-moving cyber-attack that is applied to quietly compromise interconnected information systems without revealing itself. APTs often use a variety of attack methods to get unauthorized system access initially and then gradually spread throughout the network. In contrast to traditional attacks, they are not used to interrupt services but primarily to steal intellectual property, sensitive internal business and legal documents and other data. If an attack on a system is successful, timely detection is of paramount importance to mitigate its impact and prohibit APTs from further spreading. However, recent security incidents, such as Operation Shady Rat, Operation Red October or the discovery of MiniDuke – just to name a few – have impressively demonstrated that current security mechanisms are mostly insufficient to prohibit targeted and customized attacks. This paper therefore proposes a novel anomaly detection approach which is a promising basis for modern intrusion detection systems. In contrast to other common approaches, which apply a kind of black-list approach and consider only actions and behaviour that match to well-known attack patterns and signatures of malware traces, our system works with a white-list approach. Our anomaly detection technique keeps track of system events, their dependencies and occurrences, and thus learns the normal system behaviour over time and reports all actions that differ from the created system model. In this work, we describe this system in theory and show evaluation results from a pilot study under real-world conditions.

© 2014 Elsevier Ltd. All rights reserved.

1. Introduction

Global connectivity is the core principle of our information age (O'Neill, 2014) and the vital backbone for our economy. From an information provisioning point of view, distances seem to shrink since information can be immediately accessed from all over the world. We are used to, and highly dependent on, information and communication services. This dependency, however, is a considerable vulnerability too, and increasingly motivates a certain criminal exploitation (Barber, 2001). As ICT networks and their complexity have evolved in recent years, so did the goals and technical progress of attacks (Steer, 2014; Sood and Enbody, 2013). Further, the motivation for attacks has changed from causing immediate damage on abroad basis to more sophisticated and targeted forms of attacks, where stealing proprietary information or personal data is just one step in a multi-stage attack (Kraemer-Mbula et al., 2013; Tankard, 2011; Kjaerland, 2006; Caldwell, 2013).

* *Corresponding author.*
E-mail addresses: florian.skopik@ait.ac.at, florian.skopik@gmx.at (F. Skopik).
http://dx.doi.org/10.1016/j.cose.2014.09.006
0167-4048/© 2014 Elsevier Ltd. All rights reserved.

Since the emergence of the first ICT networks significant effort went into securing critical assets. Most companies have numerous guidelines and processes in place to decrease the chance of human failure. Additionally, one can choose from a variety of security solutions that deal with different attack schemes at different levels in the network: Firewalls that filter traffic at network borders between sub-networks, malware scanners that investigate binaries and executables for suspicious behaviour or intrusion detection systems (IDSs) that monitor events all over a network and verify them against predefined rules for anomalies. While IDSs are a widely accepted de-facto standard today, their common signature based approach brings two major drawbacks (Garca-Teodoro et al., 2009):

i Pre-defined rules are often insufficient to detect unique or tailored attacks. Those rules are often commonly known and, given enough effort is invested, can be circumvented. However, producing custom rule sets is mostly not feasible for most organizations.
ii For applications with low market share no sufficient parsers and rule sets are available (e.g., for specific industrial control components). As a consequence, the lack of sufficient rule sets that verify application specific operation sequences make common solutions inapplicable.

System architects and administrators need to tackle these inadequacies in order to increase security. However, recent attacks like Operation Aurora (McClure et al., 2010) or Operation Shady RAT (Alperovitch et al., 2011) demonstrate that the current security mechanisms are insufficient to prevent unique sophisticated and tailored attacks, also known as Advanced Persistent Threats (APT). Furthermore, these advanced attacks raise the question if it is even possible to prevent intrusions with reasonable certainty (Alperovitch et al., 2011; Thomson, 2011). Some new approaches even deliberately accept successful first stages of attacks, and instead focus on the timely detection to limit negative effects on the longer run (Brewer, 2014).

Eventually, timely detection of intrusions is one major challenge when securing complex critical systems. As current security solutions are often not sufficient to deal with sophisticated and tailored attacks, novel approaches are required. One interesting core concept of these novel approaches is the mining of typically unnoticed relationships between different applications and components of a computer network. While many experts today argue that these disregarded relationships are the major weak spot abused by attackers to compromise systems (Patcha and Park, 2007) (e.g., users that utilize the same passwords on multiple services (Ives et al., 2004) or standard architectural patterns), we emphasize disregarded (and often much more subtle) relationship as one of the major strength for future intrusion detection systems.

This means, if we are able to detect these relations and harness them by correlating events on multiple machines across the entire network – and thus discovering unknown dependencies – we are able to automatically generate a system behaviour model that describes the common events and their relations. For example, in a hosting environment a quite obvious relation exists between incoming connections on a firewall, followed by an http request on a Web server and finally an issued SQL query on a database server. Consequently, a single direct SQL query without a preceding Web server request is an anomaly; moreover a firewall entry without a succeeding Web server request might be the sign of an intrusion too. The stronger these events coming from machines, network devices, and high level services, are connected, the harder it is for an attacker to exploit vulnerabilities without violating some of these implications and thus being detected. The actual art is to find these relations, model them, and enforce them with minimal human intervention – and with acceptable false positive rates.

The contributions of this article are as follows:

- *APT Detection Approach*. We explain why current security solutions are often insufficient to counter APT attacks and motivate the need for novel approaches.
- *Anomaly Detection Model*. We discuss the formal model definition of a novel anomaly detection approach based on log-line analysis (Skopik et al., 2014a; Skopik and Fiedler, 2013) that fulfils the motivated requirements.
- *Real-World Evaluation*. We perform a sophisticated evaluation of a prototype implementation of the presented approach, including an optimal configuration and the performance when challenged with real anomalies in a large-scale dataset.

The remainder of this paper is organized as follows: Section 2 gives an overview about recent research in the field of anomaly detection and intrusion detection systems. Sections 3 and 4 define the novel anomaly detection approach. Section 3 defines the general functionality; Section 4 describes how the system model is generated and continuously refined. Section 5 describes the test environments and the test data generation for the evaluation of the prototype implementation. Section 6 discusses the results of the different evaluation steps, and Section 7 concludes this article.

2. Related work

Nowadays various systems are in place in a corporate ICT network to ensure the three properties confidentiality, availability and integrity known as the security triangle (von Solms and van Niekerk, 2013). Any action attempting a violation of any of those properties can be seen as an intrusion (Yu, 2012). Intrusion Detection Systems (IDSs) (as originally proposed by Denning (1987)) aim at detecting those intrusions to take actions from triggering warnings to actively preventing the attacker from causing further harm. Literature as (Yu, 2012) or Sabahi and Movaghar (2008) classifies IDSs by different means. Differentiations can be made between host based, network based and hybrid approaches (Yu, 2012; Sabahi and Movaghar, 2008). While host based approaches focus on the events on one single host to detect suspicious behaviour, network based approaches look at parts of networks and analyse the traffic and protocol data to detect intrusions. Sabahi and Movaghar (2008)further classifies Hybrid approaches that use host and network data simultaneously as

Download English Version:

https://daneshyari.com/en/article/454439

Download Persian Version:

https://daneshyari.com/article/454439

Daneshyari.com