COMPUTERS & SECURITY 45 (2014) 293–304

Available online at www.sciencedirect.com

ScienceDirect

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

Computers & Security

Time and space interval record schedule consistency analysis for atomic items without interactions in open spaces with stationary locations☆

*Fred Cohen**, *Don Cohen*

Fred Cohen & Associates, PO Box 811, Pebble Beach, CA 93953, USA

ARTICLE INFO

Article history:
Received 4 January 2014
Received in revised form
25 January 2014
Accepted 2 March 2014
Available online 1 April 2014

Keywords:
Consistency analysis
Record schedule analysis
Digital forensics
Travel time analysis
Subversion detection

ABSTRACT

Attacks on systems often produce records that are distinguishable from normal records because, by the nature of the subversions they undertake, they produce records that the system could not produce under normal operation. This paper outlines a basis for understanding and determining one class of such discernible subversion inconsistencies associated with time and space interval record schedule consistency analysis for atomic items in open spaces without interactions as a method of questioned digital record examination. It starts with a brief introduction to the issues and description of the specific problem at hand, develops an approach to solving the problem, and identifies an algorithm for near-linear time detection of inconsistency or demonstration of a feasible schedule for special cases likely to occur in real-world record-keeping.

1. Objectives, methodology, background, and overview

1.1. Objectives

The objective of this paper is to describe an algorithm and method by which inconsistency analysis may be applied to detect attempts to subvert systems. The particular algorithm is suitable for time and space interval record schedule consistency analysis for atomic items without interactions in open spaces with stationary locations.

1.2. Methodology

The methodology applied was to (1) identify the nature of the problem, (2) partition the problem by identifying characteristics of relevance, (3) identify an approach to addressing the inconsistency analysis problem for the particular cases, (4) identify candidate algorithms based on knowledge, skills, training, education, and experience, (5) analyze these algorithms to determine their utility and complexity, (6) implement versions of these algorithms, (7) test these algorithms on sample data both generated and real, (8) write up the results, and (9) submit them to a peer reviewed journal for consideration.

1.3. Background

Attacks on systems often produce records that are distinguishable from normal records because, by the nature of the subversions they undertake, they produce records that the system could not produce under normal operation. One of a potentially unlimited number of examples of this is when a

☆ The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. Approved for Public Release, Distribution Unlimited.

* *Corresponding author*. Fred Cohen & Associates, PO Box 811, Pebble Beach, CA 93953, USA. Tel.: +1 925 454 0171.

http://dx.doi.org/10.1016/j.cose.2014.03.002
0167-4048/

user uses another user's identity through privilege escalation. Other examples include, without limit, deletion or alteration of logs, use of another user's account, altering ownership of files or directories, removal of a disk to duplicate it during system downtime, altering the names of files to avoid firewall rules, and use of another user's facility access badge. Some of these might be done by altering records, theft of devices, breaking and entering, exploiting backup and recover mechanisms, and any number of other mechanisms.

Rather than seeking to identify the mechanisms of privilege escalation, facility entry, disk removal, facility break-ins, backup interception and substitution, and every other mechanism that might produce these sorts of records and then identifying all of the conditions of those records indicative of each such mechanism, along with the extensive time and effort associated with doing such, we seek generic solutions that leverage computational advantage to the defender. One notion for such a defensive mechanism is consistency analysis.

Consistency analysis, as a broad concept, has an enormous range of possibilities, and if done rapidly enough, can be used as a detection mechanism with real-time response that allows it to form a preventive mechanism. But even if we cannot do detection and response in real-time, whether because of the lack of real-time access to records or the computational complexity of analysis, a consistency analysis approach that drives the computational complexity of undetected attack high enough to make it infeasible is an advantage to the defender, if it can be done with reasonable resources.

One class of such inconsistency detection methods deals with the movement of people, things, programs, data, or anything else for which there are records, and the record-keeping systems associated with such movements. This is the issue of time and space. Because all digital records must be of finite accuracy and precision in theory, and in practice all such records are so, rather than dealing with exact times and locations, we need to deal with less precise information, and thus we deal with intervals. The notion of things moving over time can be considered in light of the notions of scheduling, an area that has been studied for a long time as part of the field of operations research, and a field for which there are many known algorithms. Record schedule consistency analysis is then the set of analytical methods associated with detecting consistency (confirmation) or inconsistency (refutation) of the validity of a schedule of times and spaces reflected in records. A subfield of this area of study is cases where the things whose times and locations are associated with the schedules are not multi-part or separable, and thus cannot appear in two disjoint intervals of space simultaneously (i.e., they cannot be in two places at once). For example, people and other physically unique items can be considered atomic items for intervals large enough to envelope the items. Interactions between people and other atomic items can be considered in light of all interactions between them, but the present effort focuses on how to perform analysis without taking such interactions into account, and thus the current study is without interactions. The movement of items through space and time can be, and often is, restricted, for example by one way streets or impediments such as walls, which are stationary, and by things like ships, airplanes, and other moving things that may contain mechanisms capable of producing records. The present study examines only open spaces with stationary locations, a subset of the more complex overall problem. Thus, this paper is about identifying inconsistencies between records and realistic possibilities to detect subversions of systems resulting from attacks on those systems.

Like any mechanism producing traces, some knowledge of the nature of the mechanisms is required in order to understand the nature of what is being examined and meaningfully examine it. Many digital records self-indicate[1] the presence of an item at a location at a time. For example, a record may indicate that a particular credit card was present at a particular card reader at a particular time.[2] Multiple records associated with this credit card may be used to partially trace its movement over time. With a few assumptions, we can then trace the movement of the person using the credit card over time. But suppose the records are inconsistent in that they show the same credit card was used in Los Angeles, California, USA and London, England within a 15 min time span.[3] This would indicate a problem in terms of the use of these records for forensic purposes, and show the tracking of the card and/or the individual using it to be unreliable.[4]

Consistency analysis for digital records in limited contexts has been considered in the literature.[5] Papers on audit trail consistency,[6] semantic integrity checking,[7] and formalized event reconstruction[8] focussed largely on the theoretical basis for such analysis. As the field progressed, additional efforts were undertaken for more specific problems, such as rigorous checking for consistency in systems modeled with finite granularity,[9] hypothesis analysis for alternative hypotheses about time stamps,[10] and hypotheses based on investigative approaches.[11]

More recent papers associated with automated reconstruction tend to focus more on translating multiple traces into

[1] Self-indicating records, on their own, indicate the specified condition.

[2] When we indicate a "time" we mean it to include date, time, zone, and other relevant details.

[3] We will assume times indicated are reconciled to a common time base for the purposes of this paper.

[4] Per L. Duranti, "Diplomatics", Encyclopedia of Library and Information Sciences, Third Edition DOI: 10.1081/E-ELIS3-120043454, 2010, Taylor & Francis. Reliability: the record as a true statement of fact relates to the extent to which the record reflects the reality it purports.

[5] Summarized in F. Cohen, "Digital Forensic Evidence Examination – 4th Ed.", ASP Press, 2009–2012. ISBN # 1-878109-47-2.

[6] F. Cohen, "A Note on Detecting Tampering with Audit Trails", 1995, available at http://all.net/books/audit/audmod.html.

[7] T. Stallard and K. Levitt, "Automated Analysis for Digital Forensic Science: Semantic Integrity Checking", ACSAC-2003.

[8] P. Gladyshev, "Formalising event reconstruction in digital investigations." PhD Dissertation; University College Dublin; 2004-08.

[9] P. Gladyshev and A. Enbacka, "Rigorous Development of Automated Inconsistency Checks for Digital Evidence Using the B Method ", International Journal of Digital Evidence, Fall 2007, Volume 6, Issue 2.

[10] Svein Yngvar Willassen, "Hypothesis-based investigation of digital timestamps", chapter in Advances in Digital Forensics IV, Ray and Shenoi ed., Springer, ISBN# 978-0-387-84926-3, 2008.

[11] B. Carrier, "A Hypothesis Based Approach to Digital Forensic Investigation." PhD Dissertation; Purdue University; May, 2006.