一种计算机取证中需求定义的方法

孙 波[1], 刘欣然[1], 孙玉芳[2]

(1. 国家计算机网络应急技术处理协调中心, 北京 100029; 2. 中国科学院软件研究所, 北京 100080)

摘 要: 如何描述和规范计算机取证需求是计算机取证基本理论及基本方法研究中较为突出的一个问题. 本文结合软件工程及安全工程的思想提出了场景需求定义法, 它对计算机取证需求的制定给出了一套定义方法. 基于以上定义方法, 需求的制定可以面向所有计算机取证环境, 即它不限定哪类取证环境应该提供哪些取证需求, 而是在实际应用中根据实际需要来确定, 这为描述不断变化的复杂现实应用环境中的安全需求提供了灵活性.

关键词: 电子数据取证; 有效性; 真实性

中图分类号: TP309 文献标识码: A 文章编号: 0372-2112 (2006) 05-0921-03

Research on a Definition Method of Digital Forensic Requirement

SUN Bo[1], LIU Xin-ran[1], SUN Yu-fang[2]

(1. National Computer Network Emergency Response Technical Team /Coordination Center of China, Beijing 100029, China; 2. Institute of Software, Chinese Academy of Sciences, Beijing 100080, China)

Abstract How to describe and standardize the digital forensic requirement is an important part in digital forensic methodology. The paper propose the definition method of digital forensic requirement and an abstract model, named Environment Request Description (ERD). ERD definite three methods to describe digital forensic environment and requirement Components, Environment Profile and Environment Target. ERD don't depend on a special digital forensic environment. Customer, developer and others depending on active usage could decide requirement. It will be useful to definite a forensic requirement in different and complex digital forensic environment.

Key words digital forensics; validity; fidelity

1 引言

计算机犯罪不易被发现、追踪, 而且更不容易被诉诸法律[1], 因此各国的司法机关都在加速发展有效的数字证据收集及分析工具, 以应对快速发展的计算机犯罪. 但在不断研发数字取证工具的同时, 却忽视了计算机取证基本方法的研究, 使得取证工具的可靠性和有效性无法得到保证[2].

近年来计算机取证领域对计算机取证基本方法进行了较为深入的研究[3], 许多计算机犯罪调查研究机构对计算机取证的基本问题展开了较为热烈的讨论并进行了大量的实践工作, 其间产生的较为典型的四类计算机取证方法是: 基本过程模型 (Basic process model)[4]、事件响应过程模型 (Incident response process model)[5]、法律执行过程模型 (Law enforcement process model)[6] 和过程抽象模型 (An abstract process model)[7], 以上这些计算机取证方法均是针对特定的取证环境而提出的特定的取证需求, 这些需求几乎无法应用于新的取证环境中, 这使得取证需求无法形成统一的定义和评价标准, 大大地阻碍了这一研究领域的发展[2,4,6,8]. 因此, 如何统一、规范地制定各种计算机取证现场的取证需求是一个值得讨论的问题.

本文结合软件工程及安全工程的思想提出了一种计算机取证需求* 的制定方法——场景需求定义法 (Environment request description, ERD), 力图对制定统一、规范的计算机取证需求做进一步的探索.

2 一种计算机取证中需求的定义方法——场景需求定义法 (Environment request description, ERD)

本节将给出一种能够清晰、合理地制定不同计算机取证现场中计算机取证需求的方法——场景需求定义法 (ERD).

2.1 ERD定义

ERD是对取证需求进行定义的一套方法, 即取证需求以场景、组件的形式进行定义, 从而对取证需求进行分组归类. 首先, 把取证需求的全集, 根据不同的侧重点, 划分成若干大组, 每个大组就称为一个场景. 每个场景的取证需求, 根据不同的安全目标, 又划分成若干小组, 每个小组

收稿日期: 2004-04-05; 修回日期: 2006-02-14

基金项目: 国家自然科学基金 (No. 60073022); 国家 863高技术研究发展计划 (No. 306-ZD12-14-2); 中国科学院知识创新工程基金 (No. KGCX 1-09)

* 软件开发的工程过程是从需求分析开始的, 计算机取证方法的制定也不例外, 必须从计算机取证环境的需求分析开始, 本文中所指的取证需求是在取证之初, 基于取证环境制定的取证方法、取证对象以及保护措施等取证实施过程中应满足的要求.

就称为一个组件. 这样,取证需求由场景构成,场景由组件构成. 组件是取证过程中最小的可选取证需求集,是取证需求的具体表现形式.

2.2 ERD的结构

计算机取证环境具体的取证需求由组件体现,选择一个需求组件等同于选择一项取证需求. ERD建议尽可能选用已定义的取证需求组件,也允许自行定义其他必要的取证需求组件.

每个取证需求组件表示的是某项更有针对性的取证需求. 通常,一个取证调查环境总是融多项取证需求于一身,需要用多个需求组件以一定的组织方式组合起来进行表示. ERD定义了三种类型的用于描述产品取证需求的组织结构:组件包、环境轮廓定义(Environment profile, EP)和环境对象定义(Environment target, ET). 取证需求组件可以在这三种类型的组织结构中得到应用.

2.2.1 组件包

组件包是把多个取证需求组件组合在一起所得到的结果. 组件包可用于构造更大的组件包或用于构造 EP和 ET. 组件包可以表示一组对调查环境的取证需求,这些需求可以满足预定目标中的某个子目标的需要.

2.2.2 环境轮廓定义(EP)

环境轮廓定义(EP)是一份取证需求说明书. EP针对某一类安全环境确立相应的安全取证目标,进而定义为实现这些安全取证目标所需要的取证需求. EP给出的是一个与实现无关的取证需求定义,它所定义的这些需求没有针对具体的某一种取证调查环境,只针对比较明确的安全取证目标,通常,同一个 EP中所定义的取证需求可以在多种不同的具体的计算机取证过程中实现.

EP是抽象层次较高的取证需求说明书,可以由使用取证过程的用户或开发者或其他第三方来定义,它为用户陈述特定的取证需要提供了一种方法. 在 EP的定义中,通常都使用定义好的需求组件或由这些组件构成的组件包,同时,也可以使用自行定义的需求组件. 在具体环境的取证过程的制定过程中, EP通常在 ET的定义中被引用. EP的结构基本由以下几个部份组成: EP简述、取证环境、安全目标、取证需求、EP理论依据等. 其中,取证环境部份描述取证调查的使用环境中的有关安全因素;安全目标部份定义为达到所需级别的取证结果而要解决的取证环境中的各种安全问题所应确立的安全目标;取证需求部份定义取证过程为达到已确立的安全目标而应该满足的取证需求;理论依据部份为以下论点提供证明依据,(1)该 EP是一个完全的、一致的需求集合,(2)符合该 EP要求的取证过程能在其取证环境中提供合理有效的取证结果;这个部份包含两个方面的内容:取证目标理论依据和取证需求理论依据;取证目标理论依据需要保证 EP中的取证目标是从取证环境中导出的并能涵盖其中安全问题的各个方面;取证需求理论依据需要保证 EP中的取证需求是从取证目标中导出的并能满足取证目标各个方面的要求.

2.2.3 环境对象定义(ET)

ET的定义与 EP基本类似,不同的是 ET的取证需求是为某一特定的取证环境而定义的. ET的取证需求可通过引用某个(或多个)EP来定义,也可采用与定义 EP相同的方法从头定义. ET的结构由以下几个部份组成: ET简述、取证环境、安全目标、取证需求、概要说明、EP引用声明等. 其中, ET简述、取证环境、安全目标和取证需求等部份与 EP中的相应部份基本相似. 概要说明部份对取证需求给出例化定义,对具体的应用环境描述较为详细,把有关的实现情况表达清楚;如果 ET中有对 EP的引用,则 EP引用声明部份陈述有关援引 EP的情况,包括: ET与 EP间需求的一致性、ET中对 EP需求的进一步限定、ET中在 EP基础上的需求扩展等. 理论依据部份为以下论点提供证明依据:(1)该 ET是一个完全的、一致的需求集合;(2)符合该 ET要求的取证过程能在其应用环境中提供有效的取证步骤;(3)概要说明涵盖了所定义的所有取证需求;(4)EP一致性声明是有效的.

3 ERD定义计算机取证需求

计算机取证需求的制定过程可依次分为以下阶段:现实取证环境分析、确立取证环境、确立取证目标和确立取证需求等. 从 ERD职能的表现形式的角度,取证需求的制定过程可依次分为以下阶段:需求组件定义、组件包定义、EP定义、ET定义等,可以认为:组件用于构造组件包,组件包用于构造 EP, EP用于构造 ET, ET用于构造特定环境的取证需求,作为取证方法制定的依据. 但也不绝对,比如, EP和 ET都可以直接由组件来构造. 本模型可使用 ERD预定义的组件,也允许自行定义组件;或者,把该包中的某组件替换成相应的强度更高的组件.

如上文所述, ERD将取证需求以场景、组件的形式进行定义. ERD对计算机取证需求的定义就是把取证需求的全集划分成若干大组,每个大组就称为一个场景. 每个场景的取证需求根据不同的安全目标,又划分成若干小组,每个小组就称为一个组件. 这样,取证需求由场景构成,场景由组件构成. 可见, ERD是通过场景和组件来定义计算机取证需求的,为了对 ERD有一个直观的认识,以下将对 ERD的一些场景和组件进行简要介绍:

(1)攻击预防场景(Pre-incident preparation scene)

文[1]曾提到过攻击预防的概念,它的提出成为专业取证方法区别于非专业的关键步骤,使得取证过程研究又向前迈进了一步. ERD设立攻击预防场景的主要思想是在在攻击发生之前建立电子证据收集机制,在攻击发生的同时对系统环境进行记录,尤其对易丢失数据进行同步记录. 预备调查场景主要包含以下组件:设备准备组件(PPS-DEV)、人员准备组件(PPS-PEO)、收集机制准备组件(PPS-COL)[9]、侦测和告知组件(PPS-DET)、取证过程策略制定

组件(PPS-STRA)、法律许可组件(PPS-LAW)、授权组件(PPS-AUT)等.

以上组件均应设置于攻击发生之前,在此阶段合理的进行配置,使得系统的取证方法由事件发生之后的被动调查转为在事件发生之前的主动防御,避免了办案人员在案发后不得不在海量数据中无目的地查找零散证据,使得有目的地、最大限度地提取电子数据证据成为可能.

(2)被攻击现场调查场景(Crime scene investigation scene)

数字取证调查的目标之一就是查获犯罪嫌疑人,因而在被攻击现场的物理及数字证据的收集是必须的.此场景的主要任务就是收集、分析物理现场证据,基本包括如下组件:物理现场保护组件(CSIS-PHYPRE)、数字现场保护组件(CSIS-DIGPRE)、物理证据调查组件(CSIS-PHY-INVE)、"零散证据(Fragile evidence)①"保存组件(CSIS-FEPRE.0)、"零散证据"保存组件(CSIS-FEPRE.1)、取证过程策略制定组件(CSIS-STRA)、物理现场记录组件(CSIS-REC)、搜查和提取组件(CSIS-COL)等.

被攻击现场调查场景中所收集的证据将被送往取证实验室作进一步的分析,并将结果以文本的方式进行记录.

(3)实验室分析场景(Lab analysis scene)

实验室分析场景一般起始于被攻击现场调查场景之后,即已从现场将物理数字设备作为物理证据收集,且作为证据的网络通讯信息已被记录.在这个阶段,计算机被当作犯罪现场而被调查.目的是模仿物理犯罪现场调查过程,识别系统中发生的事件.在 ERD中,每个数字设备被当作一个犯罪现场,分析结果将被传送给"犯罪现场重构(Crime scene reconstruction)"组件.该场景基本包括如下组件:数字调查组件(LAS-DIGINVE)、数字现场记录组件(LAS-REC)、完整性保护组件(LAS-INTEPRO)、监督链(Chain of custody)组件(LAS-COC)、搜查和提取组件(LAS-COL.0)、搜查和提取组件(LAS-COL.1)、审核组件(LAS-AUD)、犯罪现场重构组件(LAS-RECON)等.

4　结束语

计算机取证需求的定义是计算机取证基本理论及基本方法研究中较为突出的一个问题[2].它在很大程度上决定了取证结果的合理性和有效性.本文结合软件工程及安全工程的思想提出了一种计算机取证需求的定义方法——场景需求定义法(Environment request description, ERD).ERD不但为计算机取证需求提供了一个较为清晰的定义方法,而且面向所有计算机取证环境,即它不限定哪类取证调查环境应该提供哪些取证过程,所有这些,由产品的用户、开发人员或其他第三方在实际应用中根据实际需要来确定,这为描述不断变化的复杂现实应用环境中的安全需求提供了灵活性.

ERD下一步研究的重点为:(1)ERD仅在计算机取证的功能需求的制定上进行了研究,然而,对于由需求组件组成的取证需求,还缺乏评价标准的衡量,因此,对于评价标准的研究是下一步工作的重点之一;(2)作为取证过程需求的最小组成单位——组件,刻画的还不够细致,也不够全面.因此,对于 ERD的细化也是下一步工作重点之一.

参考文献:

[1] Gary Palmer. A Road Map for Digital Forensics Research [R]. Rome Research Site: Air Force Research Laboratory, 2001.

[2] US Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders[DB/OL]. http://www.ncjrs.org/pdffiles1/nij/187736.pdf, 2001.

[3] Maher-Heather. Online and Out of Line: Why is Cybercrime on the Rise, and Who's Responsible[DB/OL]. http://abcnews.go.com/sections/us/DailyNews/cybercrime_000117.html, 2002.

[4] Brian Carrier, Eugene Spafford. Getting physical with the digital forensics investigation[J]. International Journal of Digital Evidence, 2003, 2(2): 29-49.

[5] Farmer D, Venema W. Computer Forensics Analysis Class Handouts[DB/OL]. http://www.fish.com/forensics/class.html, 1999.

[6] Mandia K, Prosise C. Incident Response[M]. Osborne: McGraw-Hill, 2001.

[7] 孙波,孙玉芳,等.电子数据取证研究概述[J].计算机科学, 2005, 32(2): 13-19.
Sun Bo, Sun Yufang. Research of requirement based computer forensics process[J]. Computer Science, 2005, 32(2): 13-19. (in Chinese)

[8] 孙波,孙玉芳,等.电子数据证据收集系统保护机制的研究与实现[J].电子学报, 2004, 32(8): 1374-1380.
Sun Bo, Sun Yufang. Research and implementation of the protection mechanism for digital evidence collecting system [J]. Acta Electranica Sinica, 2004, 32(8): 1374-1380. (in Chinese)

[9] Noblett M-G, Pollitt M-M, Presley L-A. Recovering and examining computer forensic evidence[J]. Forensic Science Communications, 2000, 2(4): 9-18.

作者简介:

孙　波　男,1975年3月生于辽宁,博士,主要研究方向为信息安全和系统软件.E-mail: Sunbo@mail.nisac.gov.cn

刘欣然　男,1971年出生于黑龙江鸡西,博士,国家计算机网络应急技术处理协调中心研究员,北京邮电大学兼职教授,主要研究方向为网络与信息安全、计算机网络等.

① 零散证据指可被远端计算机销毁的,正在运行并与网络连接的计算机中的数字证据.