ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.7—2003/ISO/IEC 10181-7:1996

信息技术　开放系统互连
开放系统安全框架
第7部分:安全审计和报警框架

Information technology—Open Systems Interconnection—
Security frameworks for open systems—
Part 7:Security audit and alarms framework

(ISO/IEC 10181-7:1996,Information technology—Open Systems Interconnection—Security frameworks for open systems:Security audit and alarms framework,IDT)

2003-11-24 发布　　2004-08-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

GB/T 18794.7—2003/ISO/IEC 10181-7:1996

中华人民共和国
国家标准
信息技术　开放系统互连
开放系统安全框架
第7部分:安全审计和报警框架
GB/T 18794.7—2003/ISO/IEC 10181-7:1996
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 1.5　字数 38 千字
2004年4月第一版　2004年4月第一次印刷
*
书号:155066·1-20587　定价 14.00 元

GB/T 18794.7-2003

附 录 D
（资料性附录）
审计事件的时间注册

不同的事件发生器或事件记录器之间在实际上不可能完全同步。在这种情况下，需要一种关联安全审计跟踪内时间的方法。安全审计记录由安全审计消息产生，该消息可以包含、也可以不包含时间戳。如果包含时间戳，则可以利用该安全审计消息里提供的时间指示来产生安全审计记录。后一种情况下，根据接收到的安全相关事件而产生的安全记录，则包含有可利用审计记录器的时间参考的时间戳。在这两种情况下，都必须产生具有事件发生器和审计记录器之间时间关系的审计记录。

在前一种情况，必须估计事件发生器时间参考与审计记录器时间参考之间的差值。审计记录必须包括事件发生器的身份标识，事件发生器的时间参考，审计记录器的时间参考，这些时间参考之间的延迟以及该延迟的容许度。在后一种情况，审计记录器必须指示事件发生器的身份标识，审计记录器的时间参考，事件发生器和审计记录器之间延迟的估值，以及该延迟的容许度。

要对每一个事件都产生这样的记录显然并不实际。只有依赖于时间参考之间的联系或偏移性质，才能产生这样的记录。如果经过一段观察时期后发现延迟是可以忽略的，则可以省去这些记录。如果没有延迟测量，则可以使用线性插值。

同一类型的问题也会在审计记录器时间参考与定位在另一端系统上的审计调度器时间参考之间发生。然而，在这种情况下，两个系统都将有时间参考。时间差值测量可以在两个通信者之间的任何时间进行，或在发生安全审计跟踪传送的时间进行。记录应包含事件发生器的身份标识，审计调度器的身份标识，审计记录器的时间参考，审计记录器和审计调度器之间延迟的估计值，以及该延迟的容许度。

确定两个事件中哪一个先发生，可以通过加上或减去一系列时间参考之间的延迟，并加上全部的容许度来实现。如果得到的延迟比容许度小，则无法区别先后次序。

同样的理由也适用于需要产生安全审计报告的时候。利用审计跟踪中提供的信息，可以按照不同的时间参考把事件分类。然而，只有在延迟容许度比该时间差加上下一事件的容许度小时，才能保证事件的次序正确。为此，必须能够计算每一个事件的累计容许度。

目 次

前言 …… Ⅲ
引言 …… Ⅳ
1 范围 …… 1
2 规范性引用文件 …… 1
3 术语和定义 …… 2
4 缩略语 …… 4
5 注释 …… 4
6 安全审计和报警的一般性论述 …… 4
6.1 模型和功能 …… 4
6.1.1 安全审计和报警功能 …… 4
6.1.2 安全审计和报警模型 …… 4
6.1.3 安全审计和报警功能编组 …… 5
6.2 安全审计和报警过程的几个阶段 …… 6
6.2.1 检测阶段 …… 6
6.2.2 辨别阶段 …… 6
6.2.3 报警处理阶段 …… 6
6.2.4 分析阶段 …… 6
6.2.5 聚集阶段 …… 6
6.2.6 报告生成阶段 …… 6
6.2.7 归档阶段 …… 7
6.3 审计信息的相关性 …… 7
7 安全审计和报警的策略及其他方面 …… 7
7.1 策略 …… 7
7.2 法律问题 …… 7
7.3 保护需求 …… 7
7.3.1 审计信息保护 …… 7
7.3.2 审计和报警服务的保护 …… 8
8 安全审计和报警信息及设施 …… 8
8.1 审计和报警信息 …… 8
8.1.1 安全审计消息 …… 8
8.1.2 安全审计记录 …… 8
8.1.3 安全报警 …… 8
8.1.4 安全报告 …… 8
8.1.5 构成审计和报警信息的示例 …… 8
8.2 安全审计和报警设施 …… 8
8.2.1 确定和分析安全事件——审计和报警功能准则 …… 9
9 安全审计和报警机制 …… 10
10 与其他安全服务和机制的交互 …… 10

10.1 实体鉴别 …… 10
10.2 数据源鉴别 …… 10
10.3 访问控制 …… 10
10.4 机密性 …… 10
10.5 完整性 …… 10
10.6 抗抵赖 …… 10
附录 A（资料性附录） 开放系统互连的安全审计和报警通则 …… 11
附录 B（资料性附录） 安全审计和报警模型的实现 …… 13
附录 C（资料性附录） 安全审计和报警设施概览 …… 15
附录 D（资料性附录） 审计事件的时间注册 …… 16

附 录 C
（资料性附录）
安全审计和报警设施概览

<table>
<tr><td colspan="2" rowspan="3">安全设施概览</td><td rowspan="3">元素</td><td colspan="3">实体：审计机构、报警管理者、安全审计者。</td></tr>
<tr><td colspan="3">功能：事件辨别器、审计记录器、报警处理器、审计分析器、审计跟踪检验器、审计提供器、审计调度器、审计跟踪收集器。</td></tr>
<tr><td colspan="3">信息对象：安全审计消息、安全审计记录、安全报告。</td></tr>
<tr><td colspan="5">服务目标：保证信息开放式系统的安全相关信息被记录在案，并且在适当的时候，做出报告。</td></tr>
<tr><td rowspan="6">设施</td><td>实体</td><td colspan="4">审计机构</td></tr>
<tr><td>功能</td><td colspan="4">确定和分析安全相关事件</td></tr>
<tr><td>管理相关的活动</td><td colspan="4">准则 1：事件辨别
准则 2：审计跟踪检验
准则 3：审计跟踪分析</td></tr>
<tr><td>实体</td><td>报警管理器</td><td>安全审计者</td><td colspan="2">发起者/目标
主体/客体</td></tr>
<tr><td>功能</td><td>事件辨别器
报警处理器
审计分析器</td><td>事件
辨别器
审计分析器
审计记录器
审计跟踪
检验器
审计提供器
审计归档器</td><td colspan="2"></td></tr>
<tr><td>操作相关的设施</td><td>产生报警
收集报警</td><td>产生审计消息
收集审计消息
分析审计消息</td><td colspan="2"></td></tr>
<tr><td rowspan="3">信息</td><td rowspan="2">审计机构管理的数据元素</td><td>准则 1
——事件类型
——时间
——实体</td><td>准则 2
——记录类型
——事件类型</td><td colspan="2">准则 3
——时间类型
——发生数量
——时间周期</td></tr>
<tr><td>——待采取的动作
——待产生的安全信息</td><td>——记录清单</td><td colspan="2">——待采取的动作</td></tr>
<tr><td>操作中使用的信息类型</td><td colspan="4">——消息/信息类型
——元素的可区分标识符
——消息原因
——事件辨别器、审计提供器和/或审计记录器的可区分标识符</td></tr>
<tr><td colspan="2">控制信息</td><td colspan="4">——时间，发生率</td></tr>
</table>