一个基于多策略的安全监视框架

温红子，卿斯汉，文伟平，李晓东
（中国科学院软件研究所 信息安全技术工程研究中心，北京 100080）

摘 要：当前的基于通用日志数据的安全监视手段存在日志数据冗余和异常检测时间延迟等问题。本文提出的基于多策略的安全监视框架(MP-SMF)，不但可以有效克服上述问题，而且还具有可配置的特性。并且通过把 Bell-LaPadula 机密性安全策略改写成为相应的关系模式，具体示例安全策略如何应用在 MP-SMF 中。

关键词：审计；安全监视；关系模式；Bell-LaPadula 机密性策略
中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2005)03-0086-06

Secure monitoring framework based on multi-policies

WEN Hong-zi, QING Si-han, WEN Wei-ping, LI Xiao-dong
(Engineering and Research Center for Information Security Technology, Institute of Software,
Chinese Academy of Sciences, Beijing 100080, China)

Abstract: The current secure monitoring facility using generic logging data has the problems of the redundancy of logging data and the delay of auditing. This essay proposes a formal secure monitor framework for multi-policies (MP-SMF), which can solve the above problems and is easy to be configurated. Additionally, the application of Bell-LaPadula secure policy in MP-SMF is introduced.

Key words: auditing; secure monitoring; relation pattern; Bell-LaPadula confidential policy

1 引言

审计的安全监视功能是安全信息系统的一个基本安全功能，其通过记录和检查系统安全相关事件，来检测由于外部渗透和内部误用所引起的各种系统异常[1]。但在多数现有的安全系统中，日志是自动的，而基于日志的审计活动则是以人工分析为主。为了利用审计活动达到相当程度的安全性，就要求尽可能多的日志系统活动数据。这样一方面给系统的性能和存储空间造成了较重的负担，另一方面也使得审计分析日志数据的时延增加，从而导致系统异常可能不被侦测到或者只能在它们发生后的很长时间才能被侦测到[2]。

显然，要有效解决上述问题，就应从日志数据项精确选择和系统异常机器自动检测两方面着手。文献[3]指出系统审计的目的在于为系统安全策略的有效实施提供一个附加级别的用户保障，这种保障主要通过基于审计的安全监视功能来提供，亦即安全监视功能通过对当前系统状态一致性的判定，给用户提供系统安全策略有效实施的情况。所以依据系统安全策略来精确确定日志数据项和自动检测系统异常是一条有效的途径。

本文依据上述思路提出了一种适合于多安全策略的安全监视框架(MP-SMF)，如图 1 所示。具

收稿日期：2003-11-18；修回日期：2004-06-29
基金项目：国家自然科学基金资助项目（60083007）；国家“973”重点研究发展规划基金资助项目（G1999035810）

体是首先参照各种安全策略的规则表达方式生成各种安全监视目标和日志项目集，然后系统主要参照日志项目集来生成日志数据，最后依据安全监视目标和策略来对日志数据进行合法性分析，从而达到对系统的状态进行及时地一致性检测的目的。该安全监视框架可以有效克服当前审计系统所具有的日志数据冗余和异常检测时间延迟等问题，而且具有可配置的特性。

2　基于多策略的安全监视框架（MP-SMF）

基于多策略的安全监视框架（MP- SMM）可用图 1 来表示，具体来讲可以分为 4 个功能模块：确定安全监视目标、确定日志项目、系统日志和安全监视等。这里 PolicyItem 为安全策略条目，AuditTarget 为安全监视目标，LogItem 为日志项目，SysData 为系统数据，LogData 为日志数据，SysSRP 为系统状态相关部分，所谓系统状态相关部分是指策略的系统相关部分，也就是为某一策略所约束的系统组件所构成的集合。Result 为裁判结果。相应地，POLICYITEMs 为安全策略条目集，AUDITTARGETs 为安全监视目标集，LOGITEMs 为日志项目集，SYSDATAs 为系统数据集，LOGDATAs 为日志数据集，SYSSRPs 为系统状态相关部分集，RESULTs 为裁判结果集。各主要功能的定义和规范如下。

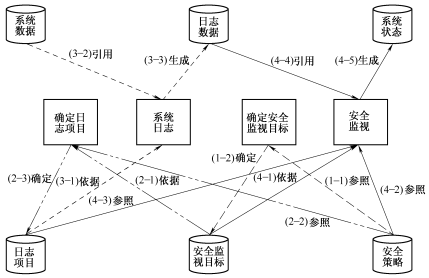

图 1　安全监视框架示意图

(1) 确定安全监视目标

$$CreatAuditTargets : 2^{POLICYITEMs} \rightarrow AUDITTARGETs$$

其功能是参照安全策略(1-1)来生成安全监视目标(1-2)。相应的安全监视目标到安全策略集上的投射为：

$$Map_{AuditTarget-POLICYITEMs} : AUDITTARGET \rightarrow 2^{POLICYITEMs}$$

这里 POLICYITEMs 是指系统所实现的安全策略条目集，所有的安全监视目标都由其中的元素决定。如在前言中所指出的，安全监视的根本目的在于使用户确信系统安全策略被正确实现和维持，确信系统处于安全一致性状态，在本文中这种需求是通过安全监视目标集来具体体现的，其中每个安全监视目标都反映了系统对部分（或全部）安全策略的满足状况。

每一个策略条目都存在一个与之对应的系统状态相关部分，该映射函数可定义为：

$$Map_{PolicyItem-SysSRP} : POLICYITEMs \rightarrow SYSSRPs$$

SYSSRPs 由各策略条目的系统状态相关部分构成，对策略条目 PolicyItem∈POLICYITEMs，其相应的系统状态相关部分在 SYSSRPs 中的索引表示形式为 $\sigma_{PolicyItem}$。

(2) 确定日志项目集

$$CreatLogItems : AUDITTARGETs \times 2^{POLICYITEMs} \rightarrow 2^{LOGITEMs}$$

该功能主要用以确定系统日志内容，其依据安全监视目标集(2-1)参照相关安全策略(2-2)来确定日志项目集合(2-3)，下边给出该功能的函数规范[注 1]：

$$\begin{aligned} &CreatLogItems(lis : 2^{LOGITEMs}) \lhd \\ &\quad at : AuditTarget; p : PolicyItem \\ &\quad lis = \bigcup_{at \in AUDITTARGETs} (\bigcup_{p \in Map_{AuditTarget-PolicyItems}(at)} Map_{PolicyItem-SysSRP}(P)) \rhd \end{aligned}$$

在上式中，先计算每一个安全监视目标中的相关策略的状态相关部分并集，然后据此得出系

注 1 在这里采用 Z 语言[4]来形式的描述 MP-SMF 中的几个关键功能函数的规范，惟一主要的变化是关于模式的表示：模式名(声明) ⊲ 命题;…;命题 ⊳

统中所有安全监视目标对应的策略的系统状态相关部分并集，其用 LOGITEMs 来表示。

(3) 系统日志

$$SysLog : 2^{SYSDATAs} \times LOGITEMs \to LOGDATAs$$

用于生成系统日志数据，系统日志功能依据日志项目集(3-1)和日志系统数据(3-2)，生成日志数据(3-3)。

为了处理日志项目到系统数据项上的映射（命名）问题，定义日志项目映射函数

$$Map_{LogItem-SysData} : LOGITEMs \to SYSDATAs$$

在多策略环境下，不同性质的安全策略对所约束的系统组件具有不同的命名体系和名字空间，通常情况下它们是不同的，这样就可能出现一个系统组件具有多个名字的情况，所以日志项目映射函数的一个主要功能就是处理这种各个策略的名字空间在系统组件上的投射问题，以期避免由于不同的名字空间所引起的对系统组件（系统数据）的重复日志问题。

为了处理单个系统数据项的日志问题，定义单项日志函数

$$SingleLog : SYSDATAs \to LOGDATAs$$

则系统日志函数规范为

$$\begin{aligned} &SysLog(lds : 2^{LOGDATAs}) \triangleleft \\ &\quad sd : SysData; li : LogItem \\ &\quad lds = \bigcup_{li \in LOGITEMs} (SingLog(Map_{LogItem-SysData}(li))) \triangleright \end{aligned}$$

在系统日志函数中，对于日志项目集中的所有日志项，首先完成从日志项目到系统数据项目的对应工作，然后再把其拷贝成为日志数据。

(4) 安全监视

$$AuditMointor : AUDITTARGETs \times 2^{LOGDATAs} \times 2^{POLICYITEMs} \to RESULTs$$

这里 RESULT={TURE, FALSE}，TRUE 表示一致状态，FALSE 则为异常状态，TRUE 和 FALSE 是布尔值，要求作用于其上的运算符合布尔运算法则。系统安全监视功能根据某一安全监视目标(4-1)参照相关安全策略(4-2)和与策略系统状态相关部分对应的日志项(4-3)，读取该系统状态相关部分所规定项目日志数据(4-4)，再根据上述信息决定系统所处的状态(4-5)。

定义策略评估函数：

$$Evaluate : POLICYITEMs \times 2^{LOGDATAs} \to RESULTS$$

日志项目－日志数据映射函数用于处理日志项目到日志数据项上的映射问题：

$$Map_{LogItem-LogData} : LOGITEMs \to LOGDATAs$$

其出现背景和日志项目映射函数相同，可以参照理解。安全监视功能规范为：

$$\begin{aligned} &AuditMo\,\mathrm{int}\,or(decision : RESULTs) \triangleleft \\ &\quad at : AuditTarget; p : PolicyItem; ss : SysSRP; lds : LOGDATAs \\ &\quad ss = Map_{PolicyItem-SysSRP}(p) \\ &\quad lds = \bigcup_{li \in ss} \{Map_{LogItem-LogData}(li)\} \\ &\quad decision = \bigwedge_{p \in Map_{AuditTarget-POLICYITEMs}(at)} Evaluate(p, lds) \triangleright \end{aligned}$$

在安全监视功能的规范中，针对一个安全监视目标，利用策略评估函数分别评估对这个安全监视目标所涉及的每一个策略的满足情况，然后得出该安全监视目标的满足情况。如果评估值为 TRUE，则称系统相对于当前安全监视目标处于一致状态；如果值为 FALSE，则表明相对于当前安全监视目标系统处于非法状态，于是就报警或调用预定义的响应程序。

3 Bell-LaPadula 机密性在 MP-SMF 中的应用

Bell-LaPadula 机密性安全模型[5]是应用于政府安全策略的最早数学模型，是军界标准安全策略，也是美国国家计算机安全中心评估可信计算机系统的基石[6]，所以以其为例来具体说明安全策略在 MP-SMF 中的应用方式。

为了验证系统所处的安全状态，必须把安全

策略应用于由日志数据所提供的状态信息，评估当前状态信息对安全策略的满足情况，从而达到安全监视的目的。但是 Bell-LaPadula 安全策略的现有陈述形式很难直接应用于 MP-SMF 这种以机器为主的自动判定操作之中，因此必须先把这些安全策略条目改写为适当的易于应用的形式，本文采用关系模式这种形式化的表示方式。

3.1　关系和模式

各种完整性安全策略的实质是用于定义维持系统安全一致性状态的各种约束，这些约束常用一致性断言的形式表达。但是关系是状态相关的，而策略是状态无关的，显然关系是不能直接用来描述策略，因此本文采用关系模式来描述策略。这种策略的关系模式只有与其相关的系统状态信息（称为系统状态相关部分）结合后才可以形成用以判定当前状态合法性（安全性）的具体关系。

3.2　Bell-LaPadula 机密性安全策略关系模式

令 Subject 为主体、Object 为客体、Op 为操作，则 Capability 为一个形如(Subject, Object, Op)的元组，称为存取权能，用以表示主体 Subject 具有使用操作 Op 来存取客体 Object 的权限，相应地，SUBJECTs、OBJECTs、OPs、CAPABILITYs 分别为主体集、客体集、操作集和存取权能集；SecureLabel 是安全标签，其为形如(SecureLevel, SecureCategory)的元组，SecureLevel 为安全标签中的安全级、SecureCategory 为安全标签中的安全类，安全级之间为线性支配关系，而安全类之间则为集合包含支配关系，SECURELABLEs、SECURELEVELs、SECURECATEGORYs 为安全标签集、安全级集和安全类集；SubjectSL 是和系统主体相关的安全标签，称为主体标签，表示为(Subject, SecureLabel)元组的形式，ObjectSL 是和系统客体相关的安全标签，表示为(Object, SecureLabel)元组的形式，相应的主、客体安全级标签集为 SUBJECTSLs 和 OBJECTSLs。

为了鉴别系统中具体操作的类型，定义操作分类函数

$$OpClass : OPs \rightarrow OPCLASSs$$

这里 OPCLASSs＝{Read, Write}，为操作类别集。上述函数是说一个操作要不属于 Read 类（读，操作的结果并不改变操作对象的值），要不属于 Write 类（写，操作的结果改变操作对象的值）。

则 Bell-LaPadula 机密性安全策略中的简单安全特性(简称为 BS 策略)可以用下列 Bell-LaPadula 简单特性关系模式来描述

$$\begin{aligned} R_{BS} : \forall capability \in CAPABILITYs \bullet [\exists subject \in SUBJECTs, object \in OBJECTs,\\ subjectSC \in SUBJECTs, objectSC \in OBJECTSCs, op \in OPs] \wedge\\ capability = (subject, object, op) \wedge subjectSC.1 = subject \wedge objectSC.1 = object \wedge\\ OpClass(op) = Read \wedge subjectSC.2.1 \geqslant objectSC.2.1 \wedge objectSC.2.1 \supseteq objectSC.2.1 \end{aligned}$$

上式是说对于任何一个存取权能，都有一个存取权能元组与之对应（该权能元组形如主体，客体，操作），元组中的主体和客体被分别赋予了主体安全级标签和客体安全级标签，当操作的类别为读操作时，主、客体安全标签之间存在这样的关系：主体安全级标签中的安全级支配（高于）客体安全级标签中的安全级，而且主体的类别支配（包含）客体的类别。

从 BS 策略关系模式表达式中所引用的系统组件容易得出它的系统状态相关部分为

$$\sigma_{BS} = \{SUBJECTs, OBJECTs, OPs, SECURELEVELs, SECURECATFORYs\}$$

*-特性(简称为 B*策略)分别可以用下列 Bell-LaPadula*-特性关系模式来描述

$$\begin{aligned} R_{B*} : \forall capability \in CAPABILITYs \bullet [\exists subject \in SUBJECTs, object \in OBJECTs,\\ subjectSC \in SUBJECTs, objectSC \in OBJECTSCs, op \in OPs] \wedge\\ capability = (subject, object, op) \wedge subjectSC.1 = subject \wedge objectSC.1 = object \wedge\\ OpClass(op) = Write \wedge subjectSC.2.1 \leqslant objectSC.2.1 \wedge objectSC.2.1 \subseteq objectSC.2.1 \end{aligned}$$

上式和 R_{BS} 的语义基本相同，不同之处在于要求操作类型为写操作，要求主体的安全级和类型分

别为客体的安全级和类型所支配。B*策略的系统状态相关部分为

$$\sigma_{B^*} = \{SUBJECTs, OBJECTs, OPs, SECURELEVELs, SECURECATFORYs\}$$

3.3 Bell-LaPadual关系模式在MP-SMF中的应用

当系统实现了 Bell-LaPadual 机密性策略后，此时在 MP-SMF 中有 POLICYITEMs={BS, B* }，是由 Bell-LaPadual 机密性策略关系模式条目构成，所有的安全监视目标都由其中的元素决定。SYSSRPs＝{σ_{BS}, σ_{B^*}}，是由 Bell-LaPadual 机密性策略的各关系模式条目的系统状态相关部分构成，对于策略关系模式条目 PolicyItem ∈POLICYITEMs，其相应的系统状态相关部分在 SYSSRPs 中的索引形式为 $\sigma_{PolicyItem}$，例如策略关系模式条目 BS 的系统状态相关部分就为 σ_{BS}。

4 MP-SMF 分析

4.1 MP-SMF 安全性分析

MP-SMF 安全性问题是指根据当前安全监视目标集对系统进行监视是否能够决定当前整个系统状态一致性的问题。其可归结为命题 1。

命题 1 MP-SMF 判定系统处于一致性状态的充要条件是

$$(1)\bigcup_{at\in AUDITTARGETs} Map_{AuditTarget-POLICYITEMs}(at) = POLICYITEMs$$

$$(2)\forall at \in AUDITTARGETs \bullet \bigwedge_{p\in Map_{AuditTarget-POLICYITEMs}(at)} Evaluate(p,(\bigcup_{li\in Map_{PolicyItem-SysSRP}(p)}\{Map_{LogItem-LogData}(li)\})) = TRUE$$

证明 MP-SMF 对于系统安全状态的监视主要是由安全监视目标决定的。由于每个安全监视目标仅仅只涉及部分（或全部）系统安全状态，致使依据一个安全监视目标只能确定一个系统的部分状态，所以就有：

（充分条件）只有(1)当所有的安全监视目标所涉及到的安全策略集的并等于系统安全策略条目集合时，才能确保当前的安全监视功能可以反映所有的系统安全策略的维持状况，才可以说当前安全监视目标集反映了整个系统的安全状态；(2)当所有安全监视目标中的安全策略约束都被满足时，可以保证被安全监视目标集中的目标所强调的部分系统处于一致状态。结合(1)和(2)可以保证整个系统处于一致状态。

（必要条件）当系统处于一致状态时，根据系统安全状态一致性的定义，要求系统当前的状态信息可以满足系统中所有的安全策略约束，其包含了两个方面的意思：(1)必须要求所有的安全策略都可以在至少一个安全监视目标中涉及，也就是要求所有安全监视目标在安全策略集上的投射并必须全面覆盖系统安全策略；(2)从系统安全状态的定义可知，系统处于一致状态表明对所有安全监视目标中的所有安全策略都可以满足。

推论 1 在 MP-SMF 中，如果有一个安全监视目标不能满足时，此时整个系统都处于非法状态；但当所有安全监视目标都被满足时，并不能确定此时整个系统处于一致状态，除非安全监视目标另外满足命题 1 中的条件(1)。

4.2 性能分析

在多数现有的安全系统中，日志是自动的，而基于日志的审计活动则是以人工分析为主。为了利用审计活动达到相当程度的安全性，就要求尽可能多的日志系统活动数据。这样一方面给系统的性能和存储空间造成了较重的负担，而另一方面使得审计分析日志数据时延增加，从而系统异常可能不被侦测到或者只能在它们发生后的很长时间才能被侦测到[2]。

MP-SMF 从提高日志数据的利用效率和审计分析的自动化两方面着手有效解决了上述问题。在 MP-SMF 中，通过确定日志项目集从而得到了最小日志项目集，从根本上提高了日志数据的利用效率，这里最小日志项目集是指系统所选择的日志项目足以供一定目的的审计分析（安全监视）之需，但同时要求除此之外没有其它的项目被冗余日志；通过把安全策略条目改写为策略关系模式，从而可以把安全策略直接应用于对日志数据的自动审计分析中，解决了系统异常侦测时延过大的问题。

可配置特性是 MP-SMF 的另一个优势，当不考虑整个系统的一致性问题时，如果仅仅对特定的部分系统状态进行安全监视，则只需根据特定的安全监视项目集来确定日志项目，对相关策略集的满足情况进行评估即可。这样会使得安全监视系统更为高效和灵活。

5　实验及其结果分析

本文以中科院信息安全技术工程研究中心自行研制开发的安胜结构化保护级（B2 级）安全操作系统为基础，设计了一个测试环境。该操作系统是一个多策略安全操作系统，其中实现了 Bell-LaPadula、RBAC、DTE 等安全策略，具有很强的安全控制功能。这里的安全监视目标是监视 Bell-LaPadula 多级安全策略的有效性，所以依据 Bell-LaPadula 策略选取了最小日志项目集，为了对比起见，还测试了不对安全策略进行审计和对所有安全策略进行审计的情况。这里以 1000 次系统调用为基本测试单位，分别评估审计活动对于系统调用响应时间的影响以及对于存储空间的消耗情况，结果如表 1～表 3 所示，其中表 1 列举了没有日志审计时安全操作系统的性能参数；表 2 列举了对最小日志项目集进行审计时安全操作系统的性能参数；表 3 列举了对所有日志项目集进行审计时安全操作系统的性能参数。

表 1　　关闭日志审计时的性能参数

执行序列	运行时间/μs	占用磁盘空间/kB
1	24341	0
2	33563	0
3	24781	0
4	24745	0
5	24718	0

表 2　对最小日志项目集进行审计时的性能参数

执行序列	运行时间/μs	占用磁盘空间/kB
1	41810	99.4
2	61204	120.4
3	42210	99.8
4	50353	103.7
5	42150	87.1

表 3　对所有日志项目集进行审计时的性能参数

执行序列	运行时间/μs	占用磁盘空间/kB
1	219494	201252
2	236375	216332
3	291772	253235
4	224468	202154
5	273609	257192

从表 1～表 3 的数据可以看出，MP-SMF 通过确定日志项目集从而得到了最小日志项目集，提高了日志数据的利用效率，显著降低了审计系统对操作系统的性能消耗，整体上提高了安全操作系统的性能。

6　结论

作为系统审计的一个主要目标，安全监视功能通过记录和检查系统安全相关事件，来检测由于外部渗透和内部误用所引起的各种系统异常，达到对系统状态进行及时检测和响应的目的，但当前的基于通用日志数据的安全监视手段存在日志数据冗余和异常检测时间延迟等问题。本文所提出的基于多策略模式的安全监视框架(MP-SMF)，其不但可以有效克服当前基于通用日志数据的安全监视活动中的日志数据冗余和异常检测时间延迟问题，而且具有可配置的特性。此外本文还介绍了 Bell-LaPdula 机密性安全策略在 MP-SMF 中的具体应用，并且通过在一个安全操作系统的实况测试，具体表现了该框架对于系统安全监视性能的改善能力。

参考文献：

[1] SEIDEN K, MELANSON J. The auditing facility for a VMM security kernel[A]. IEEE Symposium on Security and Privacy[C]. Oakland CA, 1990. 2-19.

[2] SIMONE F H. IT-Security and Privacy[M]. Springer, 2001. 35-104.

[3] National Computer Security Center. A Guide to Understanding Audit in Trusted Systems[R]. Version 2, NCSC-TG-001, Fort George G. Meade, MD, 1988.

[4] WOODCOCK J, DAVIES J. Using Z[M]. New Jersey: Prentice Hall, 1996.

[5] BELL D E, LAPADULA L J. Secure Computer Systems: Mathematical Foundations and Model[R]. Technical Report M74-244, The MITRE Corporation, Bedford, MA 01730, 1974.

[6] U.S. Department of Defense. Trusted Computer System Evaluation Criteria[S]. DOD 5200.28- STD, National Computer Security Center, Fort Meade, MD, 1985.

（下转 129 页）

了可能。同时，时序结构图可作为视频流的一种有效的非线性索引方式用于视频内容检索等应用中。

参考文献：

[1] ZHANG H J, *et al*. An integrated system for content-based video retrieval and browsing[J]. Pattern Recognition, 1997, 30(4): 643-658.

[2] ZHONG D, ZHANG H J, Chang S F. Clustering methods for video browsing and annotation[A]. Proceedings of SPIE: Storage and Retrieval for Still Image and Video Databases IV[C]. 1996. 239-246.

[3] YEUNG M M, YEO B L, LIU B. Segmentation of video by clustering and graph analysis[J]. Computer Vision and Image Understanding, 1998, 71(1): 94-109.

[4] 王东辉, 朱淼良, 吴春明. 基于时序结构图的视频流描述方法[J]. 计算机学报, 2001, 24(9): 944-950.

[5] BORECZKY J S, ROWE L A. Comparison of video shot boundary detection techniques[A]. Proceedings of SPIE: Storage and Retrieval for Still Image and Video Databases IV[C]. 1996. 170-179.

[6] 朱淼良, 王东辉. 基于视频页的的视频流分割方法[J]. 计算机辅助设计与图形学学报(A 版), 2000, 12(8): 585-589.

[7] 王东辉, 朱淼良, 吴春明. 一种用于自动视频分段的 WIPE 转换检测和模式识别方法[J]. 计算机研究与发展, 2002, 39(2): 247-253.

作者简介：

王东辉（1970-），男，江苏高邮人，浙江大学人工智能研究所博士后，主要研究方向为网络媒体信息安全、视频内容分析。

钱徽（1974-），男，浙江金华人，博士，浙江大学计算机科学学院讲师，主要研究方向为智能机器人、图像处理。

朱淼良（1946-），男，浙江桐乡人，浙江大学教授、博士生导师，主要研究方向为智能机器人、多媒体信号处理、网络安全。

（上接 91 页）

作者简介：

温红子（1969-），男，甘肃静宁人，工程师，中科院软件所博士生，主要研究方向为信息系统安全理论和技术、信息系统集成。

文伟平（1976-），男，湖南桃江人，中科院软件所博士生，主要研究方向为信息安全对抗、恶意代码。

卿斯汉（1939-），男，湖南隆回人，中科院软件所研究员、博士生导师，主要研究方向为信息系统安全理论和技术。

李晓东（1970-），男，山东临朐人，工程师，主要研究方向为网络信息安全和分布式计算。