网络安全联动模型的设计与应用*)

潘 炜 李伟华
(西北工业大学计算机学院 西安 710072)

摘 要 本文设计了满足通用性要求、符合标准化方向、具有很强可扩展性的安全联动模型。同时对该模型中的安全联动协议进行了具体分析,提出了安全联动信息描述模型及其格式,推证了相互独立的安全协议的组合理论,验证了安全联动模型的安全性。最后给出了模型的具体应用,可以与其他安全系统协调联动,实现网络的动态防御。

关键词 安全联动,防火墙,安全协议,入侵检测

Research and Application of Network Security Interaction Model

PAN Wei LI Wei-Hua
(School of Computer, Northwestern Polytechnical University, Xi'an 710072)

Abstract A self-contained security interaction model (SIM) is presented in this paper. This model is accordanted with the standard trend and fully scalable. Meanwhile, security interaction protocol family(SIPF) is discussed. Security interaction message description model (SIMDM) is defined to describe and format the security interaction messages. Then the security of SIM is verified according to combinatorial theory of security protocols which are independent each other. Based on the fact above, a firewall system, which has security interaction ability to manage other security systems, is designed and implemented to realize coordinated interaction and dynamic defence against illegal intrusion.

Keywords Security interaction, Firewall, Security protocol, Intrusion detection

1 引言

随着网络的迅速普及,网络所面临的安全威胁日渐加剧,传统防火墙的静态防御已不足以抵御日趋复杂多样的入侵行为。一个深层次、全方位的可信网络安全防御体系已经出现,它要求防火墙与入侵检测、安全审计、电子取证、灾难恢复等多种安全系统进行有机整合、协调联动。在这样的安全体系中,防火墙依然作为最可信赖的可靠的防护手段,负责集中控制管理网络的信息流动和安全策略制定,通过与入侵检测、漏洞扫描等检测系统间的安全联动,了解整个网络的安全状况,并根据适当的安全响应实现网络安全状态的动态调整,从不同层面上对网络实施安全保护。安全联动是实现防火墙系统与其他安全部件之间进行组合、协同工作的方式。

实现防火墙与其他安全系统间的联动不仅可以提升其自身的机动性和实时反应能力,同时增强了其他安全系统的功能,诸如可以提高入侵检测系统的阻断反应能力和安全审计系统的日志审计能力等。然而,目前业界缺乏相应的安全系统间联动的标准和技术规范。为了能更好地解决安全系统间的协调联动性问题,我们设计了安全联动模型 SIM,对该模型中的安全联动协议进行了具体分析,提出了安全联动信息描述模型及其格式。同时推证了相互独立的安全协议的组合理论,验证了安全联动模型的安全性,并给出了模型的具体应用。

2 安全联动模型

安全联动模型 SIM(Security Interaction Model)以防火墙为中心,为其他安全系统提供通用的、可扩展的联动框架,遵循 SIM 的安全系统之间可以实现协同工作、安全联动,从整体上构建一个安全联动系统。SIM 的核心是安全联动协议 SIPF(Security Interaction Protocol Family)和安全联动信息交换格式 SIMEF(Security Interaction Message Exchange Format)。

安全联动协议 SIPF 包含了一系列已经标准化的协议,满足通用性的要求,可以用于保证防火墙与其他安全系统间的安全互操作,实现安全联动信息的交换。它包括以下协议:

(1)块可扩展交换协议 BEEP[1,2](Block Extensible Exchange Protocol):是一个面向消息的异步交互的应用层协议,可作为构建安全联动协议的框架,加载于传输层协议之上。整个协议包括两个部分:BEEP 核心和 TUNNEL 配置文件。BEEP 核心定义了 BEEP 实体之间进行会话时数据通信的基本规程。由 BEEP 实体创建的会话包含多个通道,安全联动信息可以按优先级分类在不同的通道中进行传输。TUNNEL 配置文件可以保证各个通道中信息传输的可靠性。安全联动信息的安全性是通过创建 TLS 配置文件和 SASL 配置文件来保证的,它们可用于协商并取得 TLS 和 SASL 协议的支持,增强联动实体间对话的安全可靠性。TUNNEL 配置文件由 XML DTD 定义,在 BEEP 实体通道创建时使用。BEEP 协议对通道能够携带的数据类型没有限制,它使用 MIME 标准来支持任意类型。

(2)传输层安全协议 TLS[3](Transport Layer Security):可以保护传输层的安全,并在传输层协议 TCP 基础上提供对安全联动信息的加密、认证和完整性保证。

(3)简单认证和安全层协议 SASL[4](Simple Authentication and Security Layer):可以在 BEEP 创建过程中实现对应用实体的身份认证。

安全联动信息交换格式 SIMEF 是按照安全联动信息描

*)国家 863 发展计划项目资助(No. 2003AA142060)、西北工业大学青年科技创新基金项目资助。潘 炜 博士研究生,主要研究方向:计算机网络安全;李伟华 教授,博士生导师,主要研究方向:计算机网络安全、多媒体通信技术、智能决策支持系统。

述模型 SIMDM(Security Interaction Message Description Model)定义的,采用可扩展标记语言 XML 统一描述安全联动信息的数据格式,并实现文档类型定义 DTD(Document Type Definition)。定义的安全联动信息主要包括联动实体信息、环境因子信息、事件关联信息等,同时可以利用 XML 语言的特性对联动信息做进一步的扩展。

SIM 的整体结构如图 1 所示。

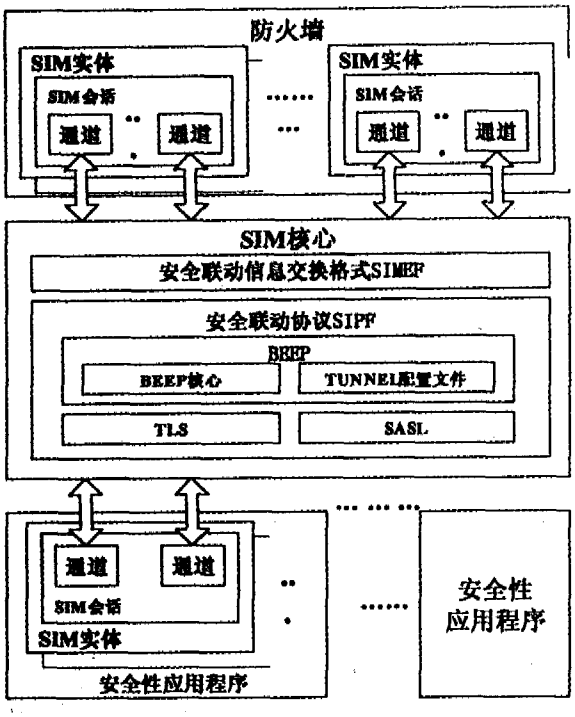

图 1 安全联动框架 SIM 的整体结构

1)SIM 实体:指由 SIPF 协议支持生成的用来传输安全联动信息的安全实体,可以是安全联动进程或线程。在防火墙中的 SIM 实体称为安全联动管理实体,是 SIM Server;安全性应用程序是指除防火墙以外的安全系统,在安全性应用程序中的 SIM 实体称为安全联动客户实体,是 SIM Client。

2)SIM 会话:指安全联动管理实体与安全联动客户实体间的会话,可以实现它们之间的安全通信。

3)SIM 通道:SIM 会话中可以创建多个通道,除了包含用于传输安全配置文件来保证安全性的特定通道外,其他通道则可以分别传输不同类型的联动信息。数据格式都是用统一语言 XML 表示的。

4)SIM 信息:SIM 实体间的信息按 SIMEF 规定的格式进行传输。

5)SIM 核心:包括安全联动信息交换格式 SIMEF 和安全联动协议 SIPF。

3 安全联动协议

SIPF 协议充分利用 BEEP 中的多通道特性,为安全联动信息提供了多级分类的可靠传输。通过创建 SIPF 配置文件和 SIPF 通道完成数据传输。通过创建 TLS 配置文件和 SASL 配置文件获得 TLS 和 SASL 协议支持,确保数据传输的安全。在进行数据交换时,可分 3 个阶段:连接建立、数据传输和连接关闭。在协议中所用到的一些基本术语如下:

A,B,P,Q,R,…:表示参与协议的合法实体。

Initialize Session(i):为实体 i 初始化一个会话;

Quit Session(i):为实体 i 关闭会话;

Setup Tunnel(i:n):为实体 i 建立通道 n;

Close Tunnel(i:n):为实体 i 关闭通道 n;

K_{ij}:实体 i,j 的共享会话密钥;

[m1|m2]:表示消息的级联;

T_i:实体 i 生成的时间戳;

Text1,Text2,…:消息常量;

E(K:m):表示用密钥 K 对消息 m 加密。

3.1 连接建立

用 SIPF 来传输安全联动信息的安全实体为 SIM 实体。SIM 实体之间通过 BEEP 协议建立一个 BEEP 会话来通信,BEEP 会话又可以建立一个或多个 BEEP 通道。SIM 实体可以是防火墙或者其他安全系统(入侵检测、审计系统等),它们之间是一对多或多对多的关系。例如,一个防火墙实体可以接受来自多个入侵检测(IDS)实体的联动报警信息。同样,一个 IDS 实体也可将联动报警信息发给多个防火墙实体。

一个 SIM 实体 A 同另一个 SIM 实体 B 之间建立 SIPF 通信,它应该先初始化一个 BEEP 会话,然后打开一个 BEEP 通道 0。BEEP 会话建立后,提供必需的安全身份认证特性的 SASL 配置文件和 TLS 配置文件应该最初协商。成功地完成 BEEP 配置文件 SASL profile 和 TLS profile 的协商后,取得 SASL 协议和 TLS 协议的支持,交换 SIPF 的"Greeting"信息,启动 SIPF 通道,连接完成。

具体过程如下:

1)A,B:Initialize Session(A,B);

2)A,B:Setup Tunnel(A,B:0);

3)A->B:Greeting,E(Kab:[Ta|Na],B,Text1);

4)B->A:Greeting,E(Kab:[Tb|Nb],A,Text2)。

3.2 数据传输

SIM 实体之间通过 BEEP 会话通信时,可以打开一个或是多个使用 SIPF 配置文件的 SIPF 通道,进行数据传输。如果需要,可以建立多个 BEEP 会话,提供额外的 BEEP 通道。然而,大多数情况下,使用 SIPF 配置文件的额外通道应该在一个已经存在的 BEEP 会话里面打开,而反对再创建新的 BEEP 会话来包含使用 SIPF 配置文件的额外通道。

在 SIPF 数据传输的时候,采用 C/S 结构,一边是客户端,一边是服务器。客户端发送数据,服务器接收数据。SIM 实体的客户端和服务器角色与在 BEEP 会话建立时的发起者和监听者的角色不相干,这是由 BEEP 的特性所决定的。

采用单个 BEEP 会话、多个 SIPF 通道的形式,对联动信息进行分类和优先级排队,方便了 SIPF 实体之间数据的传输。例如,IDS 实体向防火墙实体发送联动报警信息时,可以在不同的通道中发送不同的联动信息。IDS 实体在每一个通道上都作为客户端,防火墙将按照不同的分类来处理接收的联动信息。

具体过程如下:

1)A,B:Setup Tunnel(A,B:n);

2)A->B:Prior1,E(Kab:[Ta|Na],B,Text1);

3)B->A:Prior1,E(Kab:[Tb|Nb],A,Text2);

……

4)A,B:Setup Tunnel(A,B:n+1);

5)A->B:Prior2,E(Kab:[Ta′|Na′],B,Text3);

6)B->A:Prior2,E(Kab:[Tb′|Nb′],A,Text4);

……

3.3 连接关闭

SIM 实体在很多不同的情况下(比如处理中出现错误)可能会选择关闭 BEEP 通道。要关闭一个通道,实体在通道 0

上发送一个说明那个通道会被关闭的“close”元素。SIM 实体同样可以通过发送一个表示通道 0 会被关闭的“close”元素来选择关闭整个 BEEP 会话。由于创建一个应用层通道和 BEEP 安全配置文件存在开销问题，因此用于传输安全联动信息的 SIPF 通道的 BEEP 会话应该长期存活。另外，保持 SIPF 通道的连接也可以避免 SIPF 通道建立时的重复开销（例如 SIPF 的“Greeting”信息的交换），即使通道上没有进行数据的交换。因此，可以根据具体情况关闭及重新建立 BEEP 会话和 SIPF 通道。

具体过程如下：

1) A->B:Close,E(Kab:[Ta|Na],B,Text1)；

2) B->A:Close,E(Kab:[Tb|Nb],A,Text2)；

3) A,B:Close Tunnel(A,B:0)；

4) A,B:Quit Session(A,B)。

4 安全联动信息的表示

4.1 安全联动信息描述模型

对于安全联动信息的描述，应该突出安全联动事件的共性，同时要能够清晰地表达根据联动事件或联动实体状态属性制定响应策略的整个过程。我们提出可以用一个 5 元组模型 SIMDM 来表示：

$\Psi(E,e_0,S,\Delta,f)$

其中，$E=\{e_i \mid i=1,2,\cdots,k\}$ 是安全联动事件序列，它的每一个元素都是与时间序列相关的联动事件。

e_0 是安全联动的初始事件，它的发生标识安全联动的开始。

$S=\{S_g,S_l\}$ 是系统的状态集，它的每一个元素形如状态属性定义。在 SIMDM 描述模型中有两种类型的系统属性：S_g 表示全局状态属性，它描述的内容是安全联动实体全局的状态，不局限于某一联动模式；S_l 表示局部状态属性，它描述的内容是特定联动模式的某一特征。

$\Delta=\{I,T\}$ 是安全联动的时间约束集，其中 I 是相对时间条件约束集，T 是实时条件约束集。

$f:I\to T$ 或 $f:\subseteq I\times I$。f 用来表示两种时间模型的映射集，它将两种模型的时间域值进行相互转换，从而实现时间域内联动事件或状态的关联。

因此，安全联动信息的描述包括联动实体描述、环境因子描述，事件关联描述以及响应方式描述。联动实体描述指描述安全联动过程中与时序相关的联动事件（如 IDS 的报警、防火墙的阻断、审计事件等）及联动实体状态属性的变化。环境因子描述指描述安全联动初始化时联动实体的相关状态属性以及需要满足的条件。事件关联描述指描述联动事件或状态属性关联分析的结论，对于复杂的关联描述，需要采用多级关联，即将部分联动事件相互关联构成多个关联描述分支，然后这些分支进行关联以构成更复杂的关联描述。响应方式描述指根据联动事件或状态属性的关联分析对相应的联动实体给出响应策略。

4.2 安全联动信息交换格式

依据 SIMDM 模型，我们定义了安全联动信息交换格式 SIMEF，并实现了文档类型定义，其格式框架如下：

```
〈entity〉
   〈event〉
      the context of event
   〈/event〉
   〈status〉
      the diversification of status
   〈/status〉
〈/entity〉
〈factor〉
   〈initialization〉
      initial status
   〈/initialization〉
   〈condition〉
      the requisite of condition
   〈/condition〉
〈/factor〉
〈association〉
    the association of event
    or
    the association of status
〈/association〉
〈response〉
    the format of response
〈/response〉
```

上面的框架分别给出了联动实体(entity)、环境因子(factor)、事件关联(association)和响应方式(response)的数据格式。SIMEF 采用可扩展标记语言 XML 作为统一描述安全联动信息的数据格式，从而方便了移植和可扩展。

5 模型的安全性

SIPF 协议的安全是在 BEEP 中建立安全配置文件 TLS profile 和 SASL profile 来保证的。只有完成安全配置文件的协商，取得 SASL 协议和 TLS 协议的支持，SIM 实体才是安全可信的。为了验证安全联动模型 SIM 的安全性，我们给出下面的定义。

定义 1(协议) 一个协议为 (P,υ)，其中 P 是协议中的所有实体，υ 是一个函数 $(\upsilon_A,A\in P)$ 的集合，其中 A 为协议的实体。每个函数 υ_A 将任意一个包含接收事件、发送事件和实体状态的集合映射为 A 的下一个行为的集合。

定义 2(模型) 协议 (P,υ) 的模型为 (M,s)，其中 M 是一个由有向顺序的所有事件集合构成的子集，s 是一个 M 的状态函数。而且，对于每个实体 A 和每个事件 $e\in M_A$，如果 $A\in P$，那么 $e\in\upsilon_A(s(e))$。

定义 3(安全协议) 协议 (P,υ) 如果是秘密安全的，也是时间安全的，那么协议就是安全的。

定义 4(安全模型) 模型 (M,s) 如果对于协议 (P,υ) 的实体 A 和所有事件 $e\in M_A$，$s(e)$ 的每个元素在 M 中的每个事件上是有效的，且协议是安全的，那么模型是安全的。

我们认为安全协议之间是相互独立、不互相干扰的，那么当它们组合时，其安全性质是可以保证的，且它们组合构成的模型也是安全的。对安全协议之间的相互独立性，我们给出这样的定义：

定义 5(协议独立性) 两个协议 $P1=(P_1,\upsilon_1)$ 和 $P2=(P_2,\upsilon_2)$，如果对于所有的状态集合 s 和 $A\in P_1$，$\upsilon_A^1(s)=\upsilon_A^1(s-send(P_2))$，其中 $send(P_2)$ 是在协议 P2 中传递的所有消息的集合，那么 P1 和 P2 是相互独立的。

对于组合后的协议的安全性和模型的安全性可以用反证法进行证明：如果有两个相互独立的安全协议 $P1=(P_1,\upsilon_1)$ 和 $P2=(P_2,\upsilon_2)$，$P1\cup P2$ 为两者的组合。假设 $P1\cup P2$ 不是安全的，那么存在一个 $P1\cup P2$ 的模型 M 不是安全的。由于 P1 和 P2 是相互独立的，对 M 的每个事件 e 按照定义 2 和定义 5 进行逐一考虑，要么将之加入 M1，要么加入 M2。当 M 中的所有事件考虑完毕，最后得到的 M1 或 M2 是不安全的，则对应的 P1 或 P2 是不安全的。这是和已知矛盾的。

对于 TLS 和 SASL 协议来说，两者都是标准化的安全协议，分别能够完成对安全联动信息的加密传输以及对安全联动实体的身份认证，且相互独立。安全联动协议 SIPF 通过 BEEP 中带有 TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA 加密序列的 TLS 安全配置文件得到 TLS 协议的支持，从而保证了联动信息传输的机密性和完整性。通过使用

SASL 安全配置文件获得 SASL 协议的支持，提供联动实体间的认证。

因此，根据上面给出的定义和证明，在此基础上组合而成的 SIPF 的安全性质是可以保持的，且安全联动模型 SIM 的安全性得到保证。

6 模型的应用

根据上述的安全联动模型，我们在 Linux 环境下实现了 SIM 应用程序库 Libsim，它的核心是一个无限的循环，它等待联动事件的出现并处理它们。联动事件由 SIM 的通信模块 Beepcore 来处理，然后再调用用户定义的其他函数做进一步的处理。SIM 应用程序库 Libsim 的结构如图 2 所示。

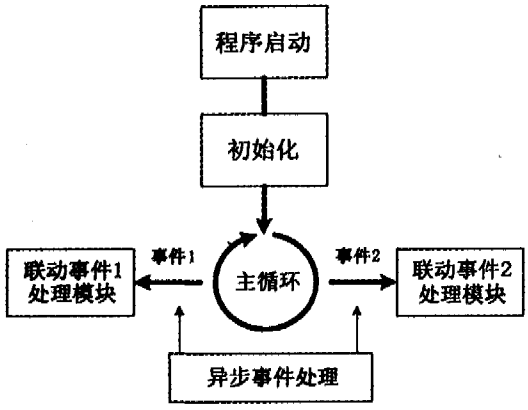

图 2 SIM 应用程序库的结构

以 SIM 为框架，可以实现防火墙和 IDS、Honeypot、安全审计系统等之间的联动，从整体上构建一个安全联动系统。在 Linux 环境下，我们使用 Netfilter/Iptables、Snort 和 Libsim 构建了一个由防火墙与 IDS 组成的安全联动系统，结构如图 3 所示。

在这里，入侵检测系统中集成了一个安全联动 Client，即前面所说的 SIM Client；而防火墙系统中集成了一个安全联动管理 Console，即 SIM Server。入侵检测系统中的传感器/分析器和管理器，对网络数据流进行监视，一旦发现入侵行为发生，立即生成报警、阻断信息。安全联动 Client 将事件信息发送给安全联动管理 Console，实现它们之间的通信。其中的联动事件转换模块主要完成对联动事件信息格式的转换和加密。在 SIM 模型中，联动信息都采用 SIMEF 格式描述，XML 负责数据的表示。安全联动管理 Console 通过事件引擎完成对联动事件信息的收集和分类，再由事件分析模块结合联动策略库，分析匹配接收的联动事件，对分类的联动事件采取不同的响应策略，达到阻断攻击、主动防御的目的。

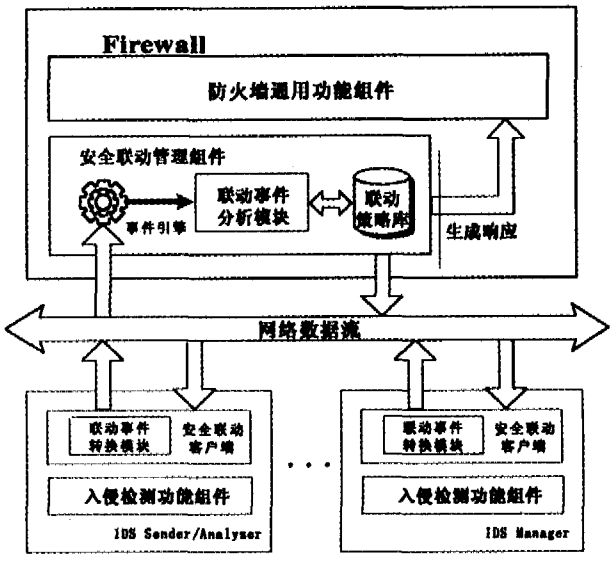

图 3 防火墙与 IDS 联动的实现过程

结束语 本文构建的安全联动模型 SIM 采用标准化协议，保证了各个安全系统间联动信息的安全通信，并对数据格式进行统一描述，具有通用性、可扩展性好的特点，方便实现。采用 SIM 模型实现的防火墙系统可以具备安全联动管理的能力，能够实现对其他安全系统的联动管理、协同控制，及时遏制网络不安全事态的发展。

参 考 文 献

1 Rose M T. The Blocks Extensible Exchange Protocol Core [S]. RFC3080, 2001
2 Rose M T. BEEP: The Definitive Guide[M]. O'Reilly Press, 2002
3 Dierks T. The TLS protocol version 1.0[S]. RFC2246, 1999
4 Myers J. Simple Authentication and Security Layer (SASL)[S]. RFC2222, 1997
5 Curry D. Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language Document Type Definition [EB/OL]. http://www.ietf.org/proceedings/03nov/I-D/draft-ietf-idwg-idmef-xml-10.txt, 2003
6 Menga J. CCSA NG: Check Point Certified Security Administrator Study Guide[M]. Sybex Press, 2003

(上接第 87 页)

人们进行协同工作的模式，突破了服务器的瓶颈，使系统更加高效和具有良好的鲁棒性。同时，由于 JXTA 是一个开源项目，我们可以根据自己的需要进行修改。在 FP2PCD 系统里，节点和点组之间双向认证的组成员资格服务和使用会话密钥对传输的内容加密的管道服务替换了 JXTA 默认的服务，使系统更加安全。但是，我们还需要进一步研究具体的 CAD 软件实体结构、API 命令，充实和完善中间协议，使 FP2PCD 更好地集成不同的 CAD 软件。

参 考 文 献

1 Pahng F, Senin N, Wallace D R. Distributed modeling and evaluation of product design[J]. Computer-Aided Design, 1998, 30(5): 411～423
2 陆薇，孙家广. CAD 支撑系统构件-软总线模型[J]. 计算机辅助设计与图形学学报，2001，13(1)：1～7
3 Gree K. Vehicle analysis using an agent based analysis tools frameworks[A]. In: Proc. of 2001 ASME Design Engineering Technical Conference[CD], Pittsburgh, Pennsylvania, 2001, DETC2001/CIE-21290
4 林守勋，林宗楷，郭玉钗，等. 多 Agent 系统工作环境 MACE [J]. 计算机学报，1998，21(2)：188～193
5 高曙明，何发智. 分布式协同设计技术综述[J]. 计算机辅助设计与图形学学报，2004. 849～855
6 Project JXTA. http://www.jxta.org/
7 Zhang Dehua, Zhang Yuqing. SAP2P: A P2P Network Security Architecture based on Trust Management System. In: The 2004 International Conference on Parallel and Distributed Processing Techniques and Applications, PDPTA'04, Las Vegas, Nevada, USA, 2004. 849～855