一种面向消息的安全传输中间件模型*)

汪林林　肖常俊　张学旺
(重庆邮电大学软件学院　重庆 400065)

摘　要　面向消息中间件(Message-Oriented Middleware,MOM)的安全消息服务的核心是基于安全协议的代理服务。MOM安全消息的路由和传送主要使用集中式消息服务器,导致消息服务可扩展性差和安全管理对象受限制等问题。针对MOM目前的问题,我们在普通MOM基础上提出一种加密传输中间件TSMQ(Transport Security Message Queue)模型。它采用将路由和传送功能分布在每台客户机上的方法,较普通MOM有更高的可扩展性和安全性,可有效保护敏感数据的传输安全。

关键词　面向消息,加密,安全传输中间件,安全路由

A New Message Oriented Model of Security Transportation Middleware

WANG Lin-Lin　XIAO Chang-Jun　ZHANG Xue-Wang
(College of Software, Chongqing University of Posts and Telecommunications, Chongqing 400065)

Abstract　The proxy service which is based on the security protocol is the core of security message service to the MOM (Message Oriented Middleware). The routing and delivering of the MOM security message mainly take charge of the centralized message server, causing problems of poor expansibility of message service and limitations of security management objects. In order to resolve these problem of the MOM, a new model called TSMQ(Transport Security Message Queue) based on the general MOM is put forward. Compared with the general MOM, TSMQ has better expansibility and security by distributing the functions of routing and delivering to each client host. By this way, the transportation security of sensitive data is achieved.

Keywords　Message-oriented, Encryption, Security transportation middleware, Routing

1　引言

面向消息中间件(Message Oriented Middleware,MOM)的消息路由和传送目前主要采用的是集中式消息服务器;消息服务位于TCP、SSL/TLS、HTTP或HTTPS协议的上一层,供应用程序客户端和管理客户端用来连接到代理服务器。采用SSL/TLS协议可以保证连接和传输的安全性,而位于HTTP上一层的服务使消息可以穿过防火墙。集中式消息服务器除上述优点外,还存在固有的一些缺点,例如:

(1)如果当某个群集代理服务器停机,那么在它的代理群集中,有关持久性实体(目标和长期订阅)的状态信息可能会失去同步。

(2)代理服务器在进行代理服务时,参与会话密钥协商;如果代理服务器被攻击者控制,则攻击者可以轻易地获取传入和传出的明文消息流。

(3)当需要进行扩展消息服务时,无论是"无状态水平扩展"还是"有状态水平扩展",这两种扩展方式都会使配置策略更为复杂,限制了网络上的客户端数量,增加了管理难度。

针对以上问题,我们提出加密传输中间件TSMQ(Transport Security Message Queue,以下同)通信模型。为实现安全传输,TSMQ在传统MOM中增加了签名认证、数据加密、证书管理、密钥协商等模块,它可以在已有MOM产品上进行扩展,初步解决了中间件安全、扩展性等方面存在的问题。

2　TSMQ中间件模型

2.1　相关技术

(1)中间件技术:中间件是一种介于客户端和服务器端的软件技术。它位于操作系统、网络和数据库之上,应用软件之下的一类软件,它的主要作用是用来屏蔽网络硬件平台的差异性和操作系统、网络协议的异构性。中间件可分为以下几类:基于远程过程调用(Remote Procedure Call,RPC)中间件;基于对象请求代理(Object Request Broker,ORB)中间件;基于面向消息的中间件(Message Oriented Middleware,MOM)。它们的区别在于基于RPC和ORB的中间件会创建紧密耦合组件系统,而基于MOM的系统允许组件进行更松散的耦合。目前有两种ORB的标准,分别是CORBA和DCOM,这两种标准是相互竞争的,而且两者之间有很大的区别,这在一定程度上阻碍了对象请求代理中间件的标准化进程。而MOM是作为专用产品实现的,为了给MOM制定一个标准的消息传送接口,1998年Sun推出了Java消息服务(Java Message Service,JMS)规范,使MOM产品的通用元素的标准得到进一步发展。

(2)密钥技术:密钥技术主要通过数据加密、签名数字摘要等技术实现保密性、鉴别性、完整性和不可否认性等机制,主要包括以下三种密钥技术:

对称密钥算法:是指加密和解密数据使用同一个密钥,即

*)资助项目:重庆市教委科研项目(项目编号KJ050508)。**汪林林**　教授,硕士生导师,副博导,主要研究方向:数据库及GIS、计算机网络等;**肖常俊**　硕士生,研究方向:计算机网络安全;**张学旺**　讲师,硕士,研究方向:网络信息安全、软件工程。

加密和解密密钥是对称的。典型的对称密码算法有 DES、AES 算法等。

非对称密钥算法：又称公钥密码算法，加密和解密分别使用两个不同的密钥。典型的公钥密码算法有 RSA、ECC 算法等。

单向散列函数：可以说是对明文的一种指纹或是数据摘要，对任意长度的明文 m，经由散列函数 h 可产生固定长度的散列值，却无法反向执行散列算法来恢复明文。典型的单向散列函数有 MD5、SHA-1 算法等。

(3)PKI 数字证书系统结构：采用 X．509 标准数字证书．系统主要由以下三个部分构成：

证书颁发机构 CA：出于安全考虑，CA 只和 RA 通信，处理来自 RA 的证书申请，并把生成的证书和证书废止列表放进公共查询数据库以供查询；

注册机构 RA：RA 位于 CA 和最终用户之间，受理用户的证书申请，并向 CA 提交证书申请；

公共查询数据库：用于存放 CA 签发的证书和证书废止列表，它是证书的集中存放地，是网上的一种公共信息库，用户可以从此处获得其他用户的证书和公钥。

(4)路由策略：采用面向连接服务的虚电路子网，主要的自适应路由算法分为距离矢量路由和链路状态路由协议。距离矢量路由协议定义距离为到目的网络所经过的路由器数，距离也称为跳数。每经过一个路由器，跳数就加 1。该类协议选择跳数最少的路由作为最佳路由。距离矢量路由协议有 RIP、IGRP 等。而链路状态路由协议中的路由器根据自己的路由表通过 SPF 算法计算到目的地的最短路径，选择最短路径作为路由。路由器常见的链路状态路由协议有 OSPF 和 I-SIS 等。

2.2 TSMQ 传输模型需求

(1)高效：TSMQ 的会话密钥协商、加/解密及身份认证等由会话双方完成，和路由服务器无关，路由服务器只负责传递消息。在消息传递过程中，每次路由服务器之间的连接无须进行代价高昂的会话密钥协商、加/解密、及身份认证等操作。

(2)安全：路由服务器只负责传递消息，并不参与密钥协商，消息体中的内容经过加密，密钥只有会话双方才知道，因此当第三方侦听到消息或者路由服务器已经被攻破也无法知道消息体中的内容。

(3)易扩展：基于普通中间件的功能基础之上，只需要在普通传输中间件中插入密钥协商、证书管理、加/解密及签名认证等模块即可实现功能的扩展，普通传输中间件路由服务器无须进行任何改动。TSMQ 传输模型如图 1 所示。

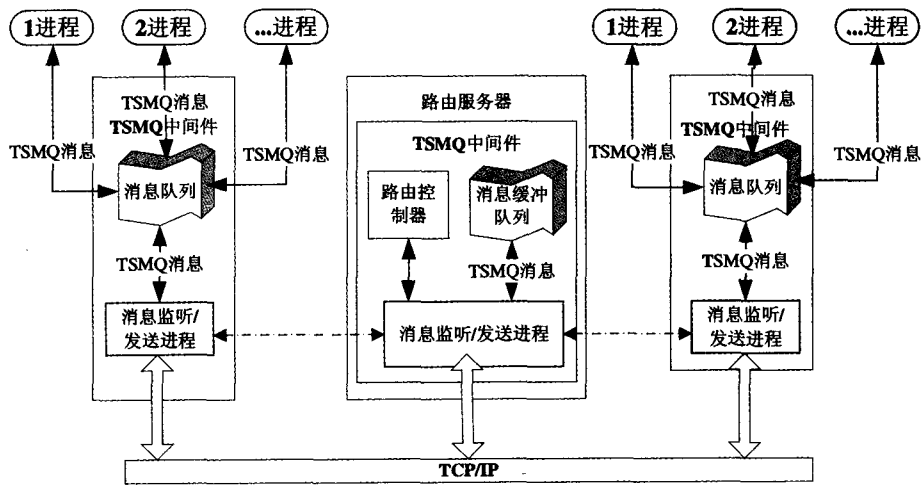

图 1　TSMQ 传输模型图

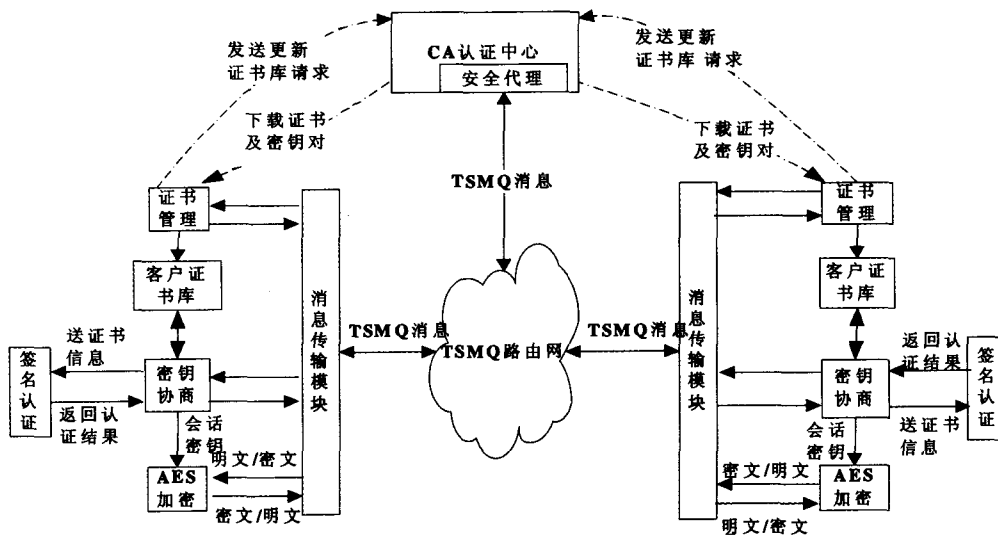

图 2　TSMQ 中间件体系结构

应用进程之间数据通信，由下一层的 TSMQ 中间件层完成。TSMQ 中间件层位于 TCP/IP 层之上并向应用程序提供传输服务，不同 TSMQ 中间件之间的数据传输通过 TSMQ 层协议实现。TSMQ 中间件向应用进程提供 TSMQ 消息读和写服务，其中中间件层的 TSMQ 路由器构成了 TSMQ 通信虚拟网，它负责将 TSMQ 消息从源消息队列路由至目的消息队列，然后目的方应用进程从目的方消息队列读取 TSMQ 消息并解析成初始明文。

2.3 TSMQ 结构设计

TSMQ 加密传输中间件运行于操作系统、网络和数据库之上，应用软件之下的一类软件，它的主要作用是用来屏蔽网络硬件平台的差异性和操作系统、网络协议的异构性，使应用软件能够比较平滑地运行于不同平台上。它为不同的应用程序之间提供一个安全的数据加密传输通道，应用程序只需要从通道里读取和写入所需要的数据流，而无须关心整个传输过程。TSMQ 体系结构如图 2 所示。

(1)证书管理：证书的下载和更新由证书管理模块实现，其中 CA 负责生成新证书和提供 ca. cert 证书等服务。

(2)密钥协商：由密钥协商模块完成，用于生成 AES 会话密钥。

(3)认证：由认证模块完成，采用 1024 位 RSA 非对称算法，实现通信双方之间的身份认证。

(4)TSMQ 消息协议：消息传输模块利用 TSMQ 消息协议实现 TSMQ 中间件层的数据传输。

2.4 TSMQ 的密钥协商流程

证书格式采用 X. 509 标准，证书安全散列函数采用 SHA-1，用 RSA(1024bits)进行签名。我们的协议假设用户 A 和用户 B 各有一对公/私密钥对和对应的数字证书，它们各自的证书可以从可信任的第 3 方机构(认证中心，即 CA)服务器上取得。密钥协商流程如图 3 所示。

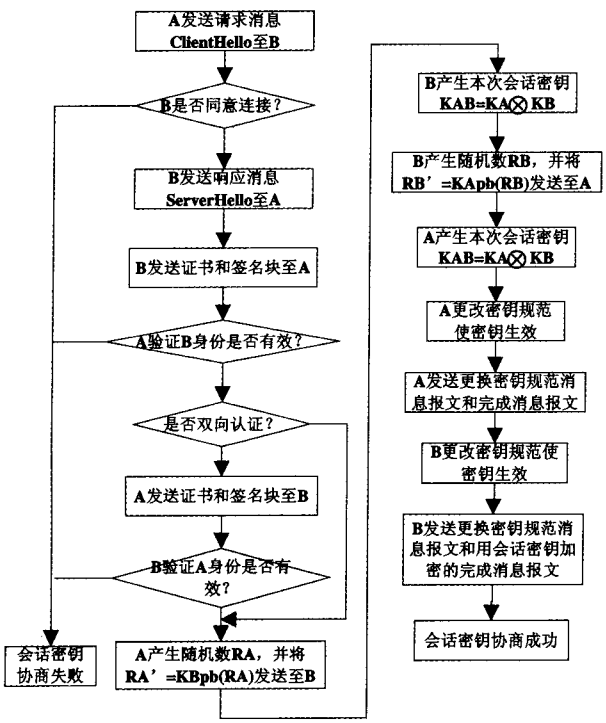

图 3 密钥协商流程图

(1) 每个用户在安装时都安装有一个 CA 证书和密钥对，一个与自己的公钥和身份信息绑定的经过 CA 签过名的数字证书；为了保证密钥的安全性，PKI 可以定期更新用户端的公/私密钥对和数字证书，用户就可以定期从 CA 服务器上定期下载更新自己的公/私密钥对和数字证书。有时候用户端的证书需要定期更新，用户定期向 CA 服务器发送证书更新请求，当 CA 服务器收到客户端的请求后，CA 先生成新的证书和密钥对，然后将其加密后发送给用户，整个通信过程和客户端之间的通信过程相同。当通信过程结束后，CA 和用户端立即更新此用户的证书信息和密钥对，此时该用户新的证书和密钥对生效。

(2) 用户 A 首先向用户 B 发送连接请求 ClientHello，B 收到连接请求后响应一个 ServerHello 消息，以及 B 的数字证书和签名块，用户 A 收到 B 的数字证书和签名块后，用 CA 公钥对签名块进行解密(该签名块是 CA 用自己的私钥对 B 数字证书 SHA-1 散列值的签名)，同样用户 A 用 SHA-1 计算 B 的数字证书散列值，如果两者的值相等，则 A 可以验证 B 的效性，确认其身份。

(3) TSMQ 的所有用户必须是 TSMQ 的授权用户，系统中用户程序之间的通信都必须是双向认证的。用户 A 收到 B 的证书后将自己的证书和签名块一起发送给用户 B，用户 B 收到 A 发送至 B 的信息，当验证了 A 的身份后，则决定是否要和 A 通信，否则退出协商过程。

(4) 用户 A 产生一个随机数 RA，并用 B 证书中的公钥加密该随机数 RA′=KBpb(RA)并发送给用户 B 以协商共享密钥。

(5) 对于收到的 RA′，只有用户 B 才能用自己的私钥解密。用户 B 先用自己的私钥解密 RA′，得到 RA = KBpv (RA′)。

(6) 用户 B 也挑选一个随机数 RB，并计算出本次会话密钥 KAB=RA ⊕ RB，接着用用户 A 的公钥加密 RB，得到 RB′ = KApb(RB)，然后将 RB′发送给用户 A。

(7) 因为只有用户 A 知道自己的私钥，只有用户 A 才能解密。用户 A 先用自己的私钥 KApv 解密 RB′，RB= KApv (RB′)；用户 A 根据解密出的 RB 计算出本次会话密钥 KAB =RA ⊕ RB。

(8) 用户 A 和 B 都得到了会话密钥 KAB，会话密钥用于 AES 加密，这样就可以采用 AES 对称加密算法加密数据用于传输。

2.5 TSMQ 协议

2.5.1 TSMQ 消息定义

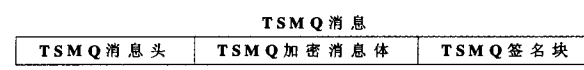

图 4 TSMQ 消息结构

(1) TSMQ 消息头：指明了消息目的主机以及目的 QUEUE 名；

(2)TSMQ 加密消息体：存放用户程序用对称算法 AES 加密过的消息内容；

(3)TSMQ 签名块：用 SHA-1 散列函数对 TSMQ 消息头和 TSMQ 消息体进行散列，再用用户端私钥进行签名，确保消息没有被攻击者篡改。

2.5.2 协议流程

用户进程 A 在 TSMQ 消息头中指定消息的目的 Queue (在一个 TSMQ 系统环境中的每一个 Queue 由字符串名指定

并且唯一)。

将需要发送的数据插入 TSMQ 消息体之前，此时 TSMQ 的 API 需要先完成用 AES 算法对要发送的数据进行加密(加密的密钥是密钥协商过程产生的会话密钥)，然后在将加密过的密文插入 TSMQ 消息体。

用 SHA-1 散列函数对 TSMQ 消息头和 TSMQ 加密消息体进行散列计算得到散列值，然后用用户 A 自己的 RSA 私钥对散列值签名得到数字签名块，并将该签名块附加在 TSMQ 消息体尾。

用户 A 进程将 TSMQ 消息通过 API 调用写入路由服务器的 Queue 中，路由服务器 Queue 之间的通信通过 TCP/IP 协议传输。

路由服务器在传递 TSMQ 消息的时候，可以取得消息头中以明文存放的目的 Queue 名，通过标准的路由算法，将 TSMQ 消息路由至目的 Queue。在整个路由过程中 TSMQ 消息体中用户数据都以密文存放，采用 AES 算法加密，因此即使被第三方截获也可以保证其安全性。

当用户 B 取得 A 发送过来的 TSMQ 消息后，先用 SHA-1 用 SHA-1 散列函数对 TSMQ 消息头和 TSMQ 加密消息体进行散列计算得到散列值，然后用用户 A 的 RSA 公钥对 TSMQ 签名块进行解密，如果解密后的值和散列值相等可以确认该 TSMQ 消息的真实性，当确认 TSMQ 消息的真实性后，就可以用密钥协商阶段协商的会话密钥进行解密，否则丢弃该 TSMQ 消息并向用户 B 进程进行报警。

2.6 TSMQ 路由

路由服务器主要功能是将 TSMQ 消息从源 TSMQ 队列路由到目的 TSMQ 队列，其原理类似于 OSI 网络层的功能，而不同的是它在应用层实现，这样就可以屏蔽网络层之间的差异，即使在两个不同网段的 LAN 也可以容易地实现相互访问。多个路由服务器集合可以构成一个通信子网，子网的拓扑结构由系统设置来完成，而不是由实际情况决定，因为应用层程序很难知道网络层的实际情况。在较复杂的子网中，消息需要通过多跳(hop)中间路由服务器才能到达目的地。

路由策略采用 RIP(Routing Information Protocol)路由算法，RIP 是内部路由器协议使用最广泛的一种，它的最大优点是简单，但仅适用于小网络。它的特点是从相邻路由器看网络拓扑、每经过一个路由器就增加 HOP 数(跳数)、周期性的更新，收敛速度慢、每隔 30 s 给相邻路由器传送自己的路由表。路由表中最主要的信息是：到某某路由器的距离，以及应经过的下一站。路由表更新的原则是使到目的地的距离最短。RIP 协议让网络中的所有路由器与其相邻路由器不断交换距离信息，并不断更新路由表，最后将到每一个目的地的最佳路由算出。RIP 不能在两个网络之间同时使用多条路由，它选择一个具有最少路由器的路由，即使还存在另一条高速但路由器较多的路由。RIP 限制一个通路最多只能包含 15 个路由器，所以跳数的最大值为 16 时即认为不可达。

3 安全性分析

(1) 实现实体之间的双向认证，具有较强的防假冒攻击能力。如果有第 3 方冒充发送方发出了一个连接请求消息给接收方时，接收方要求证书和数字签名块，使用 CA 的公钥对签名块进行解密，并且对发送方的数字证书进行散列计算，由于第 3 方不知道 CA 的私有密钥，解密出来的签名块和数字证书的散列值必然是不相同的。这就提供了一个安全的确认发送方身份的方法。所以该协议中，CA 数字证书保证了密钥协商双方的相互认证，如果有一方不合法就不可能协商会话密钥。

(2) 防止第 3 方窃取和恶意更改会话密钥，对密钥交换提供较强的安全性。采用 RSA(1024 位) 非对称密码算法，即用接收方的公有密钥加密，以保证只有用接收方的私有密钥解密后，才能确保密钥交换的安全性。

(3) 实体之间通过协商确定共同的会话密钥，防止由于通信一方指定会话密钥产生的安全隐患。由协议可知，用于计算会话密钥的随机数每次都分别由 A 和 B 随机选取，A 和 B 无法单独控制密钥的生成，从而保证了密钥协商的公平性。攻击者要获取协议中生成的会话密钥必须付出比获取通信一方指定会话密钥更多的代价。

(4) 实现了抗重传攻击。协议中每次会话使用的随机数都不相同，即使攻击者获知本次通话的会话密钥，也不可能由此计算出下一次通话的会话密钥，因此可以防止重传攻击。

(5) 整个 TSMQ 消息路由过程中，路由服务器只知道 TSMQ 消息头，即消息的目的主机及目的 Queue 名，而不知道 TSMQ 的用户消息内容，加密的消息内容只有会话的双方用户才能用会话密钥进行解密，因此当 TSMQ 路由器被第三方攻击者攻破也无法得到会话双方之间通信的具体消息，即实现了 TSMQ 的消息的安全路由。

4 实现流程

(1)创建 CA 服务器

为 CA 产生 RSA(1024bits)密钥对，然后生成 ca. cert 证书(采用 X. 509 标准)，ca. cert 这个证书成为整个 TSMQ 系统信任的 CA。然后为每个客户端生成自己的证书。通信双方可以定时或者通过接收指令，定期从 CA 服务器下载和更新自己证书。

(2)建立安全路由网

为 TSMQ 系统需要彼此连接的网络节点上建立路由服务器，由于是应用层路由，需要给每个路由服务器上配置邻近的路由服务器地址，这样路由服务器可以定期向邻近的路由服务器发送矢量表以实时更新系统路由表。

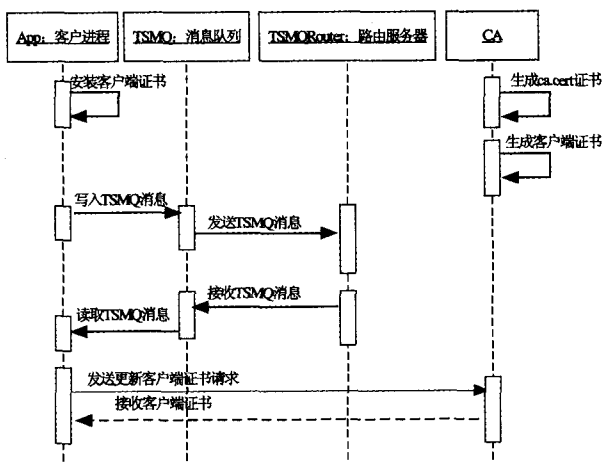

图 5 TSMQ 通信实现流程图

(3)建立安全通信

首先将客户端的证书装入通信双方应用程序，为双方应用程序配置一个或多个 Queue 名，但是每个 Queue 名在整个 TSMQ 系统中必须是唯一的。应用程序运行后，中间件会负责 Queue 的创建和回收。当应用程序开始将 TSMQ 消息写

入 TSMQ 队列时，路由服务器会自动地从 TSMQ 队列中将消息转发出去，直至目的地。通信实现流程如图 5 所示。

结束语 与用 SSL 协议开发的面向消息传输中间件不同的是，TSMQ 只是在普通 MOM 上增加模块实现功能的扩展，并不是在中间件与传输层之间增加一个新的安全套接层，即可以简化系统的复杂度，提高系统运行效率，也可以避免增加安全套接层后带来应用层数据安全路由的问题。因为增加安全套接层以后密钥的协商和数据通信的加密工作就放在安全套接层了，无论是客户端与路由服务器，还是路由服务器与路由服务器之间的连接，路由服务器都要参与会话密钥的协商，也就是说路由服务器的安全直接决定整个通信的安全性，这就带来了巨大的安全隐患，路由服务器一旦被攻击者控制，攻击者就可以轻易地取得消息明文。而在整个 TSMQ 通信过程中，路由服务器只知道消息的目的地而不知道传输的具体明文，这只有知道会话密钥的会话双方客户端才知道，从而消除了安全隐患。

参 考 文 献

1 Blahut R，Clancy T，Hua X，et al. Secure Middleware for Infrastructure Systems [R]. University of Illinois，Urbana-Champaign，January 2004. http://www.ifp.uiuc.edu/～kiyavash/papers/secureMW_04_TR.pdf

2 ndersen A，Blair G，Myrvang P H，Stabell-Kulo T. Security and middleware [C]. In：Object-Oriented Real-Time Dependable Systems，2003. Proceedings of the Eighth International Workshop on，Jan. 2003. 186 ～ 190

3 Stallings W. Cryptography and Network Security Principles and Practice (ThirdEdition)[M]. PrenticeHall，2003

4 Nash A，Duane W 著. 张玉清，等译. 公钥基础设施(PKI)：实现和管理电子安全[M]. 北京：清华大学出版社，2003

5 Tanenbaum A S 著. 潘爱民译. 计算机网络(第 4 版)[M]. 北京：清华大学出版社，2004. 8

6 李婉婷. 基于 J2EE 的安全中间件的研究与实现[D]. 解放军信息工程大学，2005. 6

(上接第 283 页)

6 Ravindran B，Li Peng，et al. Proactive resource allocation for asynchronous real-time distributed systems in the presence of processor failures. Journal of Parallel and Distributed Computing，2003，63(12)：1219～1242

7 Sih G C，Lee E A. A Compile Time Scheduling Heuristic for interconnection Constrained Heterogeneous Processors Architectures. IEEE Trans. Parallel and Distributed Systems，1993，4(2)：175～187

8 王永炎，王强，等. 基于优先级别表的实时调度算法及其实现. 软件学报，2004，15(3)：360～370

9 Bajaj R，Agrawal D P. Improving Scheduling of Tasks in a Heterogeneous Environment. IEEE Transaction on Parallel and Distributed Systems，2004，15(2)：107～118

10 Paulin P G，Knight J P. Force Directed Scheduling for the Behavioral Synthesis of ASICs. IEEE Trans. Comuter-Aided Design of Integrated Circuits and Systems，1989，8(6)：661～679

11 Wang C Y，Parhi K K. Resource Constrained Loop List Scheduler for DSP Algorithms. J VLSI Signal Processing，1995，11：75～96

12 Ito K，Lucke L. ILP-Based Cost Optimal DSP Synthesis with Module Selection and Data Format Conversion. IEEE Trans. VLSI systems，1998，6：582～594

13 Shao Z，Zhuge Q F，et al. Efficient Assignment and Scheduling for Heterogeneous DSP Systems. IEEE Trans. Parallel and Distributed Systems，2005，16(6)：516～525

(上接第 287 页)

法利用两种方法分别对二进制代码进行反汇编，引入了相互验证的过程。这种二次反汇编算法能够报告出反汇编结果中的错误，从而限制错误的传播。错误的代码可以根据应用的需求进一步进行处理。在 SPECint-95 和 SPECint-2000 上的实验证明，这种方法可以有效地对二进制文件进行反汇编。

参 考 文 献

1 GNU Project - Free Software Foundation，objdump，GNU Manuals Online. http://www.gnu.org/manual/binutils-2.10.1/html chapter/binutils4.html.

2 Larus J R，Ball T. Rewriting Executable Files to Measure Program Behavior. Software-Practice and Experience，1994，24(2)：197～2181994.

3 Larus J R，Schnarr E. EEL：Machine-Independent Executable Editing. In：Proc. SIGPLAN '95 Conference on Program-ming Language Design and Implementation，June 1995. 291～300

4 Cifuentes C，Van Emmerik M，Ung D，et al. Preliminary Experiences with the UQBT Binary Translation Framework. In：Proc. Workshop on Binary Translation，Oct. 1999

5 Theiling H. Extracting Safe and Precise Control Flow from Binaries. In：Proceedings of the 7th Conference on Real-Time Computing Systems and Applications，Dec. 2000

6 Cifuentes C，Gough K J. Decompilation of Binary Programs. Software-Practice and Experience，1995，25(9)

7 Cifuentes C，Van Emmerik M. Recovery of Jump Table Case Statements from Binary Code. In：Proceedings of the Inter national Workshop on Program Comprehension，May 1999

8 De Sutter B，De Bus B，De Bosschere K，et al. On the Static Analysis of Indirect Control Transfers in Binaries. In：Proc. International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA)，2000

9 罗云彬. Windows 环境下 32 位汇编语言程序设计. 北京：电子工业出版社，2002