网格计算环境中的安全信任协商系统

张荣清 李建欣 怀进鹏

(北京航空航天大学 计算机学院, 北京 100083)

摘 要: 网格技术促进了广域网络环境下的资源共享和协同工作. 然而,在网格环境中,服务的提供方和请求方往往位于不同的安全域,如何为位于不同安全区域的陌生主体间动态地建立信任关系成为一项应用难题. 基于信任管理基础设施,通过协作主体间信任证、访问控制策略的交互披露逐渐为各方建立信任关系,设计并实现了一个保护协商方隐私信息的安全信任协商系统. 该系统采用一种基于属性的委托授权信任证、访问控制策略及一致性验证算法,实现策略的动态调整,从而生成满足访问控制策略的所有最小可满足信任证集,能够使理论上存在的信任关系得以自动建立. 通过在 CROWN 平台中的应用,显示该系统能够满足网格应用中信任自动建立和敏感信息保护的需求.

关 键 词: 网络; 信任管理; 信任协商; 一致性验证器; 协商策略

中图分类号: TP 393.08

文献标识码: A **文 章 编 号**: 1001-5965(2006)03-0347-05

Secure trust negotiation system for grid computing

Zhang Rongqing Li Jianxin Huai Jinpeng

(School of Computer Science and Technology, Beijing University of Aeronautics and Astronautics, Beijing 100083, China)

Abstract: Grid technology promotes resource sharing and collaboration over wide area network. However, service providers and requestors are always located in different secure domains in grid environment. How to establish trust between strangers without prior relationship has become a pressing problem. A system named secure trust negotiation system was designed and implemented, which depends on the trust management infrastructure, establishes trust between strangers with iterative disclosure of credentials and access control policies and can protect participants' private information. A sort of attributed-based authorization credential and access control policy was adopted. A novel algorithm for compliance checker of credentials and access policies was carefully designed, which can be used to generate all the minimal satisfied sets of credentials, so that the trust relationship exsited in theory can be established automatically. During the process of trust negotiation using this system, secure transmission of credentials disclosed was ensured by other subsystems of CROWN. Through the application in CROWN grid, it shows contributions to the automated trust establishment and privacy protection.

Key words: network; trust management; trust negotiation; compliance checker; negotiation strategy

网格计算促进了广域网络环境下的资源共享和协同工作. 传统的集中式安全管理域属于一个具有集中管理权威和安全策略的封闭域,活动中的每个实体都可以映射为域内控制的一种或多种主体身份[1]. 然而,在网格环境中,服务的请求方和提供方可能来源于各独立安全域,它们间信任关系是动态频繁变化的,很难依赖一套集中权威中心进行管理,"如何在这种动态无中心的开放网络中,采取一种有效的机制为数目庞大、动态分散的服务部署方和容器建立信任关系"成为面临

收稿日期: 2005-06-24

基金项目: 国家自然科学基金资助项目(90412011)

作者简介: 张荣清(1978-),女,吉林辽源人,硕士生,zrq88888@sina.com.

的一个挑战性问题. 1996年,M. Blaze等人首次提出了“信任管理(trust management)”的概念[2]. 在信任管理系统中,所依赖的资源访问请求方和服务提供方提供的信任证和访问控制策略都可能存在敏感信息,所以在建立信任的同时,需要有效保障各方信息的隐私需求和披露自治性. 针对上述问题,Winsborough等提出了自动信任协商ATN(Automated Trust Negotiation)的概念,ATN的定义是“通过信任证、访问控制策略的交互披露,资源的请求方和提供方自动地建立信任关系”[3~5].

ATN已经得到国际学术界的广泛关注. BYU(Brigham Young University)ISRL实验室的Kent Seamons和UIUC(University of Illinois at Urbana-Champaign)的Marianne Winslett等人联合承担了TrustBuilder项目[6];此外,斯坦福大学的“动态协作的快捷管理”AMDC项目和NAI实验室的“基于属性访问控制”ABAC项目也在开展有关ATN的理论和应用研究.

CROWN[7](China Research Environment Over Wide-area Network)是在国家自然科学基金“以网络为基础的科学活动环境综合实验平台”这一重大项目的支持下,由北航等多家单位共同承担的项目. 其目标是面向各个领域的科学家建立一个综合网络科研环境,连接国内重要的科学研究资源. STNS(Secure Trust Negotiation System)为CROWN的组件. 其主要贡献包括如下几点:①研究信任协商的关键算法和技术,主要包括一致性验证算法等;②基于IBM TPL设计信任协商引擎系统;③基于CROWN的安全组件,设计信任协商的可配置处理链节点及协商服务.

1 安全信任协商系统(STNS)

STNS被设计为一个独立的系统,为属性信任证和访问控制策略包含的敏感信息提供保护.

1.1 基本概念

参考文献[3]给出如下定义:

定义1 基础资源主要包括协商主体拥有的数据文件、进程或者服务等,记作 r.

定义2 信任证是由权威机构颁发的特权属性数字证书,包括颁发机构的签名,信任证持有方的公钥等,用于对主体授权,记作 C. 例如X.509 v3扩展证书、RT信任证等.

定义3 访问控制策略是网络安全防范和保护的主要策略,其任务是保证网络资源不被非法使用和非法访问. 信任协商中的访问控制策略规定了访问受保护资源所需提供的信任证集,记作 P'.

定义4 对于 r 的授权可以采用访问控制策略 P_0 保护,记作:$r \leftarrow P_0$;对于信任证也可能涉及到敏感信息.

在定义4中,假设Mary只允许拥有信任证 C_{tea} 或 C_{jw} 的主体才披露其信任证 C_{stu},则 C_{stu} 的访问控制策略 P_1 可以表示为:$C_{stu} \leftarrow C_{tea} \vee C_{jw}$. 访问控制策略本身也可能泄漏敏感信息,同样可以制定新的策略进行保护.

1.2 系统结构

STNS主要借鉴IBM TrustEstablish[8]的信任证和策略规范格式. 属性信任证采用X509 v3格式,对于属性对的扩展采用Profile文件定义字段名与OID之间的映射关系表示. 访问控制策略采用TPL语言描述,属于一种XML文档. 参考TrustBuilder的结构,设计了STNS的系统结构(如图1所示).

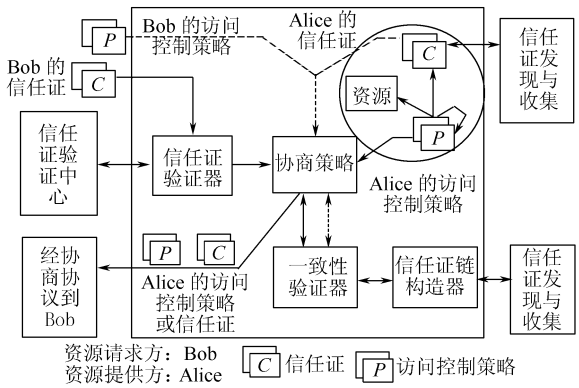


图1 STNS系统结构

STNS的主要功能模块包括:

1) 信任证验证器:用于验证收到的信任证. 验证内容包括:信任证有效性、协商对端是否确实拥有该信任证等.

2) 信任证链构造器:用于信任证链的构造. 当所需要的信任证不存在的时候,启动一个线程远程搜索所需要的信任证.

3) 一致性验证器:找到满足指定访问控制策略的信任证集合;判断所收到的信任证是否满足本地的访问控制策略.

4) 协商策略:指导信任关系的合理建立,控制协商披露的消息内容.

1.3 关键技术与算法

协商策略和一致性验证器属于STNS系统的核心功能模块,协商策略依赖于一致性验证器的执行结果.

1.3.1 一致性验证器

传统信任管理系统的一致性验证器特点为只根据提供的信任证集合判定其是否满足指定的访问控制策略,结果为 yes 或 no 的布尔类型值, 直接决定是否授权对受保护资源的访问;在信任协商应用中,这种功能显然不足,它要依赖双方信任证和访问控制策略的交换来逐渐提高信任级别,这就需要改进信任管理一致性验证器的算法. 针对这个问题,设计了一种增强型一致性验证算法 ECCA, 其功能不但判断所收到的信任证是否满足本地访问控制策略,而且能够根据指定访问控制策略搜索到所有可满足的信任证集合以及最小满足集.

定义 5　假设资源 R,保护的访问控制策略为 P,如果访问方披露的信任证集 $R=\{C_1,\cdots,C_n\}$,$n\in N$ 可满足 P,则记作 $R\Rightarrow P$,称 R 为策略可满足信任集.

定义 6　对于 P,有 2 个信任证集合 R' 和 R,如果满足:

$$\forall R'\subset R, R'\not\Rightarrow P$$

即 R 的任何真子集都不能满足 P,则称 R 为最小可满足信任证集,记作 $R\Rightarrow\min(P)$

定义 7　一致性验证器可以定义为一个映射关系:

$$f:\{\sum C_i, P\}\rightarrow P$$

式中, $\sum C_i$ 是一个信任证集合;P 是一条访问控制策略;R 是 $\sum C_i$ 的子集,即 $R\Rightarrow\min(P)$ 关系. 当 $\sum C_i=\varnothing$ 或不存在可满足集,$R=\varnothing$.

ECCA 算法主要是在 IBM TE 一致性验证器的基础上提出的. 该算法通过递归调用一致性验证器来生成所有满足策略的最小信任证集合. 算法的输入参数为本地的 $\sum C_i$ 和 P. 核心思想是逐渐优化生成的可满足信任证集合,最终求解出 $R\Rightarrow\min(P)$. 具体方法是根据 P 策略结构进行解析,得到所有相关信任证集合:

$$\sum C_{\text{rel}}=T(P)$$

然后对 $\sum C_{\text{rel}}$ 中信任证进行逐渐减少,交给一致性验证算法 Compliancecheck 进行验证. 算法的输入参数 $\sum C_{\text{loc}}$ 代表本地信任证集合,则 ECCA 算法的伪代码描述:

```
ECCA(∑C_loc, P){
∑C_rel = T(P)
// 初始化临时存储变量
S = ∑C_rel = {C_1, C_2, ⋯, C_k};
//存放每个可满足集不可缺少 Credential
S_sol = ∅;
for(∀C_k ∈ S){
if(C_k ∈ S_sol){
      continue;
}else{
//检验去除的信任证是否能够满足策略
   if(compliancecheck(S-{C_k}, P)){
      S = S-{C_k};
   }else{
      S_sol = S_sol ∪ {C_k}
      }
}
}
// 返回一组最小可满足信任证集合
Return R = S_sol
      }
```

1.3.2　协商策略

协商策略用来指导信任关系的合理建立,决定披露消息的内容,主要包含 5 个功能模块:

1) 策略收集器:获取服务的访问控制策略.

2) 策略处理器:对于每一个新收到的策略,调用一致性验证器找到满足策略的一个最小可满足信任证集合.

3) 信任证处理器:对于每一个新收到的经验证通过的信任证,调用一致性验证器得到该信任证对协商对端已认证角色的影响结果.

4) 消息披露器:根据协商策略确定协商消息的披露内容. 如果协商对端已经满足某个本地信任证的策略要求,则披露该信任证,否则披露保护该信任证的访问控制策略.

5) ECCA 算法执行器:在协商对端没有披露任何新策略和新信任证的情况下,执行 ECCA 算法,找到满足策略的所有最小信任证集合.

在实际应用系统中,可以通过 STNS 系统的策略配置设置协商轮数、协商时间等约束条件. 当约束条件被破坏时,将终止协商,并拒绝对服务的访问.

2　CROWN 中的应用

在 CROWN 中采用的安全基础设施(CROWN-ST)独立于 GT4 原始安全设施. CROWN-ST 通过配置底层 Apache Axis 的消息处理链,将截获消息转交给相应的安全配置引擎处

理,引擎调用各个安全处理链节点对 SOAP 消息进行相应的签字/加密、验签/解密等处理.

2.1 STNS 系统的应用

对于 STNS 的应用,需要在服务请求方和提供方的请求链上分别配上 ATNClientHandler 和 ATNHandler,并在服务提供方部署 ATNService 服务. ATNService 相当于一个信任协商代理,代表目标服务与服务请求方进行信任协商.

STNS 系统需要安全通信机制,以保护披露的信任证. 在双方的消息请求链和消息应答链配置相应的 Sec Message Handlers 根据所配置的位置对消息进行加密、签字以及验证、解密处理, 提供 SOAP 级别的安全传输,保证了披露的信任证的安全性. 图 2 为 STNS 应用于 CROWN-ST 的体系结构图. 以 CROWN 中的一个计算服务 CounterService 实例说明 STNS 系统在 CROWN 中的应用.

实例:服务提供方(SP) 提供计算服务 CounterService,与服务请求者(SR)位于 2 个独立安全域,各自维护自己的信任证和访问控制策略. SR 要访问 SP 提供的 CounterService 服务,双方无预先的信任关系.

为实现对服务的访问,首先需要进行自动信任协商. 假设 SR 和 SP 均对各自消息请求链做了正确的配置,同时 SP 的主机上已经成功部署了 ATNService 服务. 表 1 给出了协商双方信任证和访问控制策略配置情况.

表 1 协商双方的信任证和访问控制策略

类别	SR	SP
信任证	C_1:ACT. member←SR C_2:SR. school←BUAA C_3:SR. owner←ACT	C_4:BUAA. lab←SP C_5:SP. shool←BUAA C_6:SP. owner←ACT
策略	保护 C_1 的策略 P_C: C_1←SR. school. lab. 含义是只有角色 SR. school 的成员定义的 lab 角色的成员才有权获取该信任证.	CounterService 的策略 P_S: Service←SP. owner. member. 含义是只有角色 SP. owner 的成员定义的 member 角色的成员才授权访问.

在以上配置情况下,双方能够依赖本地信任证和访问控制策略建立信任关系. 当 SR 收到 P_S 后,找到满足 P_S 的 C_1,但是 C_1 受 P_C 保护,P_C 要求 SP 披露 C_4,对于 SP,C_4 可以无条件披露,所以 SP 披露 C_4. SR 收到 C_4,P_C 被满足,并披露 C_1 最终使得 SP 的 P_S 得到满足,最后 SP 返回协商成功的状态消息,并授权 SR 对 CounterServcie 进行访问.

2.2 实验及结果分析

在 CROWN 平台中,设计相应的实验,对 STNS 系统的性能进行测试和分析.

2.2.1 实验设计

按照 2.1 节中实例所述,将客户端和 CounterService 分布部署在实验室局域网的 2 个子网内的 2 台普通 PC 上. 设计 2 组实验来分析 STNS 系统的性能.

实验组 1 分析并比较协商时间 t 和协商轮数 n 的关系. 在上述网络拓扑中,启动实例对应的应用场景,分别在 3 轮交互过程结束点,记录每轮交互的消耗的时间值 t_i. 重复实验 10 次,取平均值作为每次交互消耗时间.

实验组 2 分析并比较在多次并发情况下配置协商服务和不配置协商服务的服务访问时间关系. 运行实例对应的应用场景,在 1 ~ 8 个客户端并发访问情况下,分别记录服务访问的消耗总时间值. 重复实验 3 次,取平均值.

2.2.2 结果与分析

图 3 为实验组 1 的实验结果. 从协商初始化配置后计时,第 1 轮交互时间为 438 ms,到第 2 轮交互结束耗时为 1 281 ms,最后一轮结束耗时为

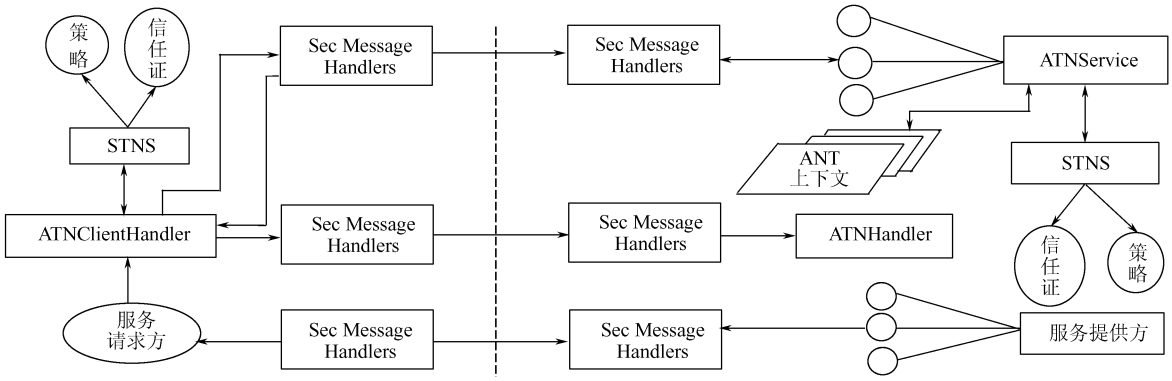


图 2 CROWN STNS 体系结构

1 953 ms. 该结果说明:协商过程的协商轮数基本与协商时间成线性关系,不会出现某轮协商消耗时间异常情形. 这样协商双方可以通过计算能容忍的最大耗时值,给出相应的协商轮数约束值,避免协商无休止地进行下去.

图 4 为实验组 2 的实验结果. 该结果说明:

1) 配置信任协商服务和不配置信任协商服务的服务总访问时间消耗值基本是恒定的,表现在实验结果上就是 2 条线间距不会有大的起伏;

2) 对于多个并发客户端访问,信任协商服务的消耗时间会略有增加,但增加幅度不是很大.

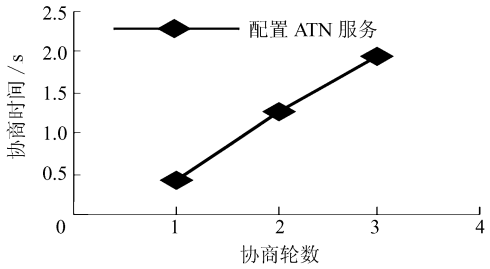


图 3　协商时间和协商轮数关系图

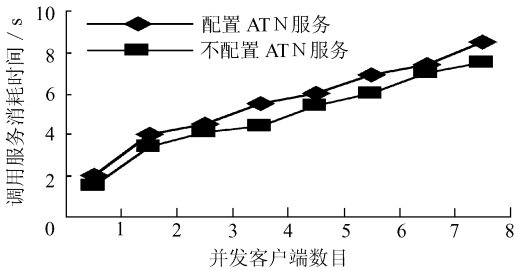


图 4　实验组 2 访问时间关系图

2 个实验组都一定程度说明信任协商虽然带来额外的通信和处理时间代价,但对整体的服务访问性能影响不是很显著,同时协商时间增长存在一定规律性,能够进行有效控制.

3　结 束 语

网格技术的发展对安全基础设施提出新的挑战. 通过设计一个用于网格环境的安全信任协商系统,针对用于信任管理的一致性验证器的特性提出并实现了 ECCA 算法,使之成为满足自动信任协商要求的一致性验证器. 通过 CROWN 中安全基础设施的集成,能够有效地保护具有特殊类型安全需求的服务.

STNS 系统也存在一些不足,例如,在信息保护中仅仅提供对属性信任证内容披露的保护方案,但在更多应用中,从协商主体的行为监控,能够判断一个主体是否拥有某种属性的信任证.

参考文献 (**References**)

[1] Yu T, Winslett M. A unified scheme for resource protection in automated trust negotiation[A]. IEEE Symposium on Security and Privacy[C]. Berkeley, California:IEEE, 2003. 110 ~ 122

[2] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [A]. Proceedings of 17th Symposium on Security and Privacy [C]. Oakland:IEEE, 1996. 164 ~ 173

[3] Winsborough W H, Seamons K E, Jones V E. Automated trust negotiation[A]. DARPA Information Survivability Conference and Exposition[C]. IEEE, 2000. 88 ~ 102

[4] Barlow T, Hess A, Seamons K E. Trust negotiation in electronic markets[A]. Eighth Research Symposium in Emerging Electronic Markets[C]. Maastricht, Netherlands, 2001

[5] Li Ninghui, Winsborough W H, Mitchell J C, *et al*. Distributed credential chain discovery in trust management[A]. Proceedings of the 8th ACM Conference on Computer and Communications Security[C]. ACM Press, 2001. 156 ~ 165

[6] Winslett M, Yu T, Seamons K E, *et al*. Negotiating trust on the web[A]. IEEE Internet Computing[C]. IEEE, 2002. 30 ~ 37

[7] Hu Chunming, Huai Jinpeng, Zhu Yanmin, *et al*. Efficient information service management using service club in CROWN grid [A]. Proceedings of the 2005 IEEE International Conference on Services Computing[C]. IEEE Computer Society Press, 2005. 5 ~ 12

[8] Amir H, Yosi M, Joris M, *et al*. Access control meets public key infrastructure[A]. Proceedings of the 2000 IEEE Symposium on Security and Privacy[C]. Oakland: IEEE Computer Society Press, 2000. 2 ~ 14