一种有效的信任协商多方安全计算模型 *

平震宇[1,2], 李培峰[1], 朱巧明[1]
(1. 苏州大学 计算机科学与技术学院, 江苏 苏州 215006; 2. 江苏信息职业技术学院 计算机工程系, 江苏 无锡 214101)

摘 要: 以 DataLog 逻辑描述语言的 Herbrand 模型为基础定义策略语言,实现访问控制与授权控制逻辑,提出了积极协商策略,以解决信任协商中的多方协商问题。

关键词: 自动信任协商; 访问控制; 授权; 策略
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2012)01-0290-04
doi:10.3969/j.issn.1001-3695.2012.01.080

Efficient secure multi-party function computation scheme for trust negotiation

PING Zhen-yu[1,2], LI Pei-feng[1], ZHU Qiao-ming[1]
(1. *School of Computer Science & Technology, Soochow University, Suzhou Jiangsu* 215006, *China*; 2. *Dept. of Computer Engineering, Jiangsu College of Information Technology, Wuxi Jiangsu* 214101, *China*)

Abstract: This paper introduced the theory of Herbrand model for Datalog which could be applied to trust negotiation. It defined a Datalog-based policy language, authorization and released control logic and negotiation protocol.
Key words: automated trust negotiation; access control; authorization; strategy

随着网络和通信技术的快速发展,资源共享和协同工作越来越受到人们的青睐。在开放式环境中,资源的提供者和请求者往往隶属于不同的安全域,交互主体间的生疏性以及共享资源的敏感性成为跨安全域信任建立的屏障。如何在分布式计算环境中的通信和交易主体间建立信任关系成为一个重要的问题。为了解决这个问题,有学者提出了信任协商这个新理论来保护开放、分布式系统。

Winsborough 等人[1]提出了自动信任协商概念,指出了通过逐步向对方披露数字证书以在陌生者之间建立信任关系的一种访问控制方法,并定义了 ATN 的抽象模型,将双方实体间的信任建立抽象为构造一条信任证披露序列。Li 等人[2,3]提出了一种基于角色的信任管理框架(role-based trust-management framework)。Yu 等人[4,5]提出了披露树模型表述 ATN 的状态,并证明了信任协商的目标是构造一棵信任证书完全披露树。这些人的关键理论研究工作奠定了 ATN 应用基础。

自动信任协商定义了两个独立陌生主体间通过信任证书访问控制策略的交换披露建立信任关系。但现实授权系统中通常涉及两个以上参与方。Yu 在文献[6]中提出相应的问题:其信任协商模型是两方的计算问题,需将多方安全计算方法运用到信任协商中。本文将研究信任协商中的多方协商问题,首先定义策略语言和实现访问控制与授权控制逻辑,并提出了积极协商策略。

1 策略语言

策略语言是描述和实现访问控制策略的重要工具。提供一种良好的策略语言是信任协商成功实施的基础和保障。当前,已有许多种策略语言用来实现跨域的资源共享,如 PSPL、TPL、X-Sec、RT、Trust-X、KeyNote 等。本文策略语言基于 DataLog 逻辑描述语言[7],因此一阶逻辑的定理都适用。

1.1 语义

以 DataLog 逻辑描述语言的 Herbrand 模型为基础定义策略语言的语义。假设开放系统是一个有限节点集合 N,对于每个节点 A 有规则 P_A。系统当前状态由规则 $P=\{(A, P_A) \mid A\in N\}$ 确定,称为系统配置。$I=\{(A, I_A) \mid A\in N\}$ 为 P 上的一个解释,I_A 是基披露集合。定义语义如下:

a) 当且仅当 $d\in I_A$,在 I 中 A 的单基披露 $d=A\uparrow\delta\downarrow A$ 为真。

b) 当且仅当 $\{d, A\uparrow\delta\downarrow A\}\in I_A$ 且 A 等于 B 或者 C,在 I 中的 A 的远程基披露 $d=B\uparrow\delta\downarrow C$ 为真。

c) 当且仅当在 I 中节点 A 的 D_0 为真或者存在 $D_i(1\leqslant i\leqslant n)$ 为假,则基规则 $D_0\leftarrow D_1\wedge D_2\wedge\cdots\wedge D_n$ 为真。

对于 I 中节点 A 的非基规则或披露为真,必存在一个替换 θ 使其实例为真。如果基实例为真,则非基规则或披露为真。

1.2 策略语言定义

假设开放系统是一个有限的集合 N,每个节点 A 都有一个局部知识库 P_A,系统中所有节点的局部知识库的集合组成系统的全局知识库 P。各节点通过相互协商,交互提交证书和访问控制策略信息来建立完成交互所需要的信任关系。策略语言定义如下:

Rule::=discloseure←disclosure_sequcence

disclosure_sequcence::= disclosure_sequcence ∧ disclosure_sequcence | disclosure_sequcence ∨ disclosure_sequcence | disclosure_sequ-

收稿日期: 2011-05-24; **修回日期**: 2011-06-27 **基金项目**: 国家"863"计划资助项目(2006AA01Z147);江苏省高技术研究资助项目(BG2005020)

作者简介:平震宇(1975-),男,副教授,硕士研究生,主要研究方向为信息处理、信息安全(pingzhenyu@163.com);李培峰(1972-),男,副教授,博士,主要研究方向为中文信息处理;朱巧明(1963-),男,教授,博士,主要研究方向为中文信息处理技术、Web 信息处理、嵌入式系统.

cence

disclosure::= Sourecepeer ↑ credential ↓ Destinationpeer | policy_condition

policy_condition::= True|False|conditional_expression

credential::= peer. credential_name(term,…,term)

term::= peer|value

peer::= variable|peer_name

value::= variable|string

variable::= x|y…

规则(rule)包括规则头和规则体,(discloseure ←)即规则头。如果规则体为空,表示规则头是一个事实。例如,Alice ↑ C_0 ↓ Bob 表示 Alice 授权 C_0 给 Bob。规则体中 Alice ↑ C_1 ↓ Bob 表示 Bob 从 Alice 处接收到 C_1。

凭证(credential)被用来描述主体的属性,以证明主体满足对方要求的身份断言。例如,凭证 University. isStudent(Alice),University 是凭证的发行者,Alice 是主体,isStudent 是凭证的名称。一个凭证可以拥有多个实体。可以用变量来表示凭证的名称或节点的名称。

披露(disclosure)是请求方(Sourecepeer)向资源方(Destinationpeer)提交证书和访问控制策略的过程。

披露序列(disclosure_sequcence)。一个协商过程包括很多元披露。采用二个谓词来将元披露组合成复杂的披露序列。∧连接谓词。例如,$d_1 \wedge d_2$,表示应同时满足 d_1 和 d_2 的要求。∨选择谓词,仅需满足 d_1 或 d_2 的要求。

设规则 $S_0 \uparrow C_0 \downarrow D_0 \leftarrow S_1 \uparrow C_1 \downarrow D_1, S_2 \uparrow C_2 \downarrow D_2, \cdots, S_n \uparrow C_n \downarrow D_n$ 是 Alice 授权策略中的一条规则。对于一个披露 $S_i \uparrow C_i \downarrow D_i$, $i \in [0,n]$,S_i、D_i 必须一个是 Alice。当规则体不为空时,S_0 必须是 Alice。如果凭证 C_0 的颁发者不是 Alice,规则体也不为空,C_0 必须是规则体中 C_i 之一。Alice 在披露其他人的凭证之前必须先接收到这个凭证。规则体中出现的变量必须在规则头中出现,经过实例推演后叫做元披露。

当披露的源和目标是同一个单元时,称为单披露。例如,Alice ↑ C_0 ↓ Alice,表示 Alice 拥有凭证 C_0,如果凭证 C_0 的颁发者不是 Alice,则表示 Alice 已接收凭证 C_0。如果披露的源和目标不是同一个单元,则称为远程披露。如果授权规则头是一个远程披露,则它是一个释放控制规则。例如,Alice ↑ Bob. trusts(Carrie) ↓ Diana ← Bob. trusts(Carrie),如果 Alice 知道 Bob 信任 Carrie,则 Alice 将这个事实告诉 Diana。Alice ↑ Bob. trusts(Carrie) ↓ x ← Bob ↑ Bob. trusts(Carrie) ↓ Alice ∧ Carrie ↑ Bob. trusts(Carrie) ↓ Alice,如果 Bob 与 Carrie 都告诉 Alice "Bob 信任 Carrie",则 Alice 将这个事实告诉任何人。

1.3　披露序列

Winsborough 等人提出 ATN 概念的同时,还相应定义了 ATN 的抽象模型,将双方实体间的信任建立抽象为一条信任凭证披露序列,模型抽象出了信任建立过程的状态表示。

依据上述策略语言定义披露序列 Seq[$d_1 \cdots d_n$], $d_i = S_i \uparrow C_i \downarrow D_i$,表示 S_i 披露凭证 C_i 给 D_i,d_{i+1} 发生在 d_i 之后。如果每个披露 d_i 在其发生时都是安全的,则披露序列是安全的。如果 Seq[$d_1 \cdots d_n$]是安全披露序列,那么存在一个对于 d_1 的安全披露序列,这个序列不超过 $i(1 \leqslant i \leqslant n)$ 个披露。

对于披露 d = Alice ↑ C ↓ Bob,存在一个安全披露序列,意味着如果披露按照披露序列 S 中给定的顺序发生,那么资源拥有者 Bob 最终可以安全地授权 Alice 访问资源 C,而不与任何其他单元的授权策略冲突。

对于元披露 d = Alice ↑ C ↓ Bob,如果 d 在 Alice 的知识库中或者可以通过推演规则推导出来,则它是解锁的,否则是锁定的。如果披露 d 通过 Alice 从其他节点接收到的披露 $d_1 \cdots d_n$ 而解锁,则称 $d_1 \cdots d_n$ 解锁 d。如果规则 R 的实例 r 中,d 是规则头,e 是 r 中的规则体,则称 e 是 d 的相关披露。如果元披露在它发生时已解锁,则称它是安全的。例如,Alice ↑ C ↓ Bob 在 Alice 知识库中是解锁的,则 Alice 可以安全地披露凭证 C 给 Bob。

1.4　推演规则

a)实例推演。如果规则 $R \in P_A$, P_A 为节点 A 的知识库,通过该变量定义域上的一个常量或者标志符取代规则 R 中出现的同一个变量,推导出 R 的一个实例。

b)知识库。如果 $B \uparrow d \downarrow A$,则 $A \uparrow d \downarrow A$。

c)假言推理。如果规则 $D_0 \leftarrow D_1 \wedge D_2 \wedge \cdots \wedge D_n \in P_A$, P_A 为节点 A 的知识库,D_i 是事实,$i \in [1,n]$,则推导出 D_0。

例如,规则 Alice. trusts(x) ←Bob. trust(x),假设 Bob 信任 Diana 并已将这个事实告诉 Alice,在 Alice 知识库中有 Bob ↑ Bob. trusts(Diana) ↓ Alice。运用上述推演规则,可以得到 Alice. trusts(Diana)。

1.5　策略语言实例

以下例子将说明策略语言的使用方法。Alice 需要向保险公司(IC)购买汽车保险,她想知道保险公司的信用评级,如果保险公司的信用评级不小于 AAA,则 Alice 向其购买保险。保险公司需要 Alice 提供其驾驶记录以及信用评级。Alice 需要授权保险公司向车管局(DMV)以及信用咨询公司(CB)查询其相关信息。保险公司将根据 Alice 的驾驶记录与信用评级决定是否接受她的购买请求。

保险购买者 Alice 的协商规则:

1) Alice ↑ Alice. request_purchase(IC,Creditrating) ↓ IC←Ture

2) Alice ↑ Alice. grant(IC,DMV,CB,Credential_DrivingRecord(Alice,IC,DMV),Credential_Creditscore(Alice,IC,CB)) ↓ IC←IC ↑ IC. requestInfo(IC. Creditrating,Alice. DrivingRecord,Alice. Creditscore) ↓ Alice ∧ IC. Creditrating > = AAA

3) Alice ↑ Alice. cancel(IC) ↓ IC←IC ↑ IC. requestInfo(IC. Creditrating,Alice. DrivingRecord,Alice. Creditscore) ↓ Alice ∧ IC. Creditrating < AAA

4) Alice ↑ Alice. Purchase(IC) ↓ IC ← IC ↑ IC. accept(Alice) ↓ Alice

保险公司 IC 的协商规则:

1) IC ↑ IC. requestInfo(IC,Creditrating, DrivingRecord,Alice. Creditscore) ↓ Alice←Alice ↑ Alice. request_purchase(IC,Creditrating) ↓ IC

2) IC ↑ Alice . Credential_DrivingRecord(Alice,IC,DMV), ↓ DMV ←Alice ↑ Alice. grant(IC,DMV,CB,Credential_DrivingRecord(Alice,IC,DMV),Credential_Creditscore(Alice, IC,CB)) ↓ IC

3) IC ↑ Alice . Credential_Creditscore(Alice,IC,CB), ↓ CB←Alice ↑ Alice. grant(IC,DMV,CB,Credential_DrivingRecord(Alice,IC,DMV),Credential_Creditscore(Alice, IC,CB)) ↓ IC

4) IC ↑ IC. accept(Alice) ↓ Alice←(DMV ↑ DMV. Send_Drivingrecode(Alice. Drivingrecode) ↓ IC ∧ CB ↑ CB. Send_Creditscore(Alice. Creditscore) ↓ IC) ∧ (Alice. Drivingrecode > Qualified ∧ Alice. Creditscore > Qualified)

车管局的协商规则:

DMV ↑ DMV. Send_Drivingrecode(Alice. Drivingrecode) ↓ IC←IC ↑ Alice . Credential_DrivingRecord(Alice,IC,DMV) ↓ DMV

信用咨询公司协商规则:

CB ↑ CB. Send_Creditscore(Alice. Creditscore) ↓ IC←IC ↑ Alice . Credential_Creditscore(Alice,IC,CB), ↓ CB

2　协商策略

协商策略是协商双方在建立信任关系过程中采取的披露

信任凭证和访问控制策略的方式，规定协商双方什么时候、采用什么样的方式来释放信任凭证和访问控制策略信息。Winsborough 等人[1]提出了两种协商策略：a）积极（eager）策略，要求协商方在接收到协商对端披露的信息后，披露所有可满足访问控制策略保护的信任证；b）谨慎（parsimonious）策略，协商双方在披露足量的访问控制策略后才会披露所需的信任证。积极策略往往会披露过多与信任建立无关的信任证；而在谨慎策略中，协商者从信任标的出发，按照严格受控的方式，通过交换指定的访问控制策略，尽可能地减少无关信任证的披露。这两种协商策略控制的协商交互次数与两方持有的信任证数量呈线性关系。

2.1 基本协商策略

协商过程定义两种类型的消息：（Mesg，ReqMesg）和 ACK。其中，ACK 是应答信息，（Mesg，ReqMesg）表示披露给对方的已解锁的凭证和协商方向另一方请求披露的凭证。协商由资源请求方向资源提供者发生请求开始，信任协商的推进由消息接收方根据接收的消息内容决定下一步发生的消息内容。

对于参与信任协商的节点 P，需要计算得到信息有：a）信任请求方向其请求披露的集合 D_{new}，D_{new} 中的披露是解锁的。b）节点 P 向其他节点的请求但还未被发送的披露集合 Q_{new}。基本协商策略如下：

```
1  BasicStrategy(MESG_Recived, MESG_send, L){
2  m = the latest message in MESG_Recived
3  if m is a disclosure d THEN
4  D_unlocked = all disclosures unlocked by d and other disclosure in
   D_receive
5  D_new = (D_unlock ∩ Q_receive) - D_send, D_unlock
6     else if m is a request for disclosure d then
7        if d is already unlocked then
8  D_new = {d}
9           else
10  D_relevant = all relevant remote disclosures for d
11  Q_new = D_relevant - D_receive - Q_send
12           return {D_new, Q_new}  }
```

交互信息存放在集合 $MESG_{Recived}$ 中，m 为当前最新信息，如果 m 是一个披露 d，则由披露 d 解锁的凭证以及当前接收到的凭证存放在集合 D_{unlock} 中。由于不需要披露未被请求的凭证，相同的凭证也无须向同一节点发送两次，因此 $D_{new}=(D_{unlock}\cap Q_{receive})-D_{send}, D_{unlock}$ 中存放所有已解锁的凭证，$Q_{receive}$ 是请求方请求的凭证，$D_{unlocked}\cap Q_{receive}$ 是可以发送给请求方的凭证，减去已发送给请求方的凭证 D_{send} 得到 D_{new}。

如果消息 m 是一个请求，如果被请求的披露 d 是解锁的，则 $D_{new}=\{d\}$，否则需要计算与披露 d 所有相关的披露集合 $D_{relevant}$，P 将向其他节点发送请求 Q_{new}，$Q_{new}=D_{relevant}-D_{receive}-Q_{send}$，节点 P 发送 Q_{new} 到相关节点用于解锁 d。最后节点 P 发送 D_{new} 与 Q_{new} 到相关节点。

2.2 基本协商策略的安全性与完备性

基本策略具备安全性和完备性。策略安全性是指如果协商过程中每个披露都安全则策略安全。若协商双方运用协商策略时披露的序列均是安全的，则协商策略具备安全性[8]。在基本策略中凭证披露发生在第 5 行与第 8 行，在这两个时刻凭证均已解锁，先前的披露序列上所有的凭证也均被解锁，所以基本策略是安全的。

若协商方运用协商策略将理论上能达到成功的协商都能找到一个安全披露序列，则称该策略具备完备性。下面使用数学归纳法证明基本策略具备完备性。

假设？d = Alice ↑ C ↓ Bob 是 Bob 在协商中的原始请求，d 的安全披露序列长度是 S。

a）$S=1$ 时协商成功。也就是 d 在协商开始时已经是解锁的，当 Alice 在处理请求？d 时（在第 7 行处）满足解锁条件，直接将 d 加入集合 D_{new} 回复给 Bob，本次协商成功。

b）假设 $S=k$ 时协商成功。考虑 $S=k+1$ 时，如果 d 这时已解锁，则协商成功。假设 d 还是被 $\{d_1,d_2,d_i,\cdots,d_m(1\leqslant i\leqslant m)\}$ 锁的，Alice 在其知识库中的规则实例为 $d\leftarrow d_1\wedge d_2\wedge\cdots\wedge d_m\wedge d_{m+1}\wedge\cdots\wedge d_{m+m'}$，其中 $d_m\wedge d_{m+1}\wedge\cdots\wedge d_{m+m'}$ 是已经可以从 Alice 本地知识库推导出的。Alice 将发送（$d_1\wedge d_2\wedge\cdots\wedge d_m$）到相应的节点，这个过程可以认为是原始请求 d_i 的一个子集。d_i 是安全披露序列其长度最大为 k，也就是说，d_i 的子集同样也协商成功。Alice 将逐个解锁（$d_1\wedge d_2\wedge\cdots\wedge d_m$），最终解锁 d，将其发送给 Bob。

2.3 完整协商策略

如果协商过程中具备安全披露序列则基本策略可以保证协商成功，但是如果本次协商不具备安全披露序列，请求方将无法得到其原始请求的应答，导致无法决定何时宣布本次协商失败，因此当无法提供被请求的披露时需要向披露请求方发送拒绝信息。由于系统中有多的节点参与协商，有可能导致协商处于死锁。例如，Alice 是否披露 d_1 取决于 Bob 是否披露 d_2，Bob 是否披露 d_2 取决于 Carrie 是否披露 d_3，Carrie 是否披露 d_3 又取决于 Alice 是否披露 d_1。这时协商各方都无法决定是否拒绝请求方，协商死锁。当死锁发生时，协商各方既不发送也不接收信息，协商终止。考虑没有死锁发送的情况，在协商过程中参与协商的节点是有限的，基本策略不重发信息，每个请求或者披露只可能发送一次，所以整个协商过程中可能发送的请求和披露同样也是有限的，基本策略总能够有效终止。当协商终止时，协商发起方最初的请求还没有被允许，则可以宣布本次协商失败，也就是说判断协商是否失败，可以通过判断协商是否已经终止来实现。

协商终止判断可以借鉴 Dijkstra-Scholten 终止检测算法[9]。Dijkstra-Scholten 算法检测集中式基本计算的终止性，基本算法的初始进程 P 在检测算法中起着特殊的作用。当基本算法交互 M 条信息时，检测算法至多交互 M 条控制信息，在控制信息和基本信息方面达到了很好的平衡。对于 P 向 q 发送的每一条消息，算法中 q 只向 P 发送一次控制消息。完整协商策略通过简化 Dijkstra-Scholten 算法的信号模式，设计了简化的应答模式结合基本策略算法来检测协商终止，完整协商策略如下：

```
1  FullStrategy(MESG_Recived, MESG_send, L){
2  m = the latest message in MESG_Recived
3  Mes = Null
4        if m is a data message then
5  Mes = BasicStrategy(MESG_Recived, MESG_send, L)
6        else
7  Mark Mes_i as ACKed (Mes_i ∈ MESG_send)
8        Sig = Null
9        Rev = the set of data messages that P received and has not
         Acked
10        if all data messages that P sent have been Acked OR P is the
          originator
11           Sig = Ack message for every message in Rev
12           else
13           Sig = Ack message for every message in Rev ,except the
```

one with the earliest receipt time.
14　return Mes and Sig　}

节点 P 所发送的信息 Mes_i,为其添加 ACK 属性,当接收到 Mes_i 的应答信息后标记为 ACKed。协商策略确保每个发送的消息应该并且只接收到一次应答消息。节点如果发送的所有消息都得到了应答并且节点接收到的信息也都发送了应答消息,则节点状态为终止,否则状态为活动。当节点 P 接收到一个消息 m,如果 m 是数据消息则使用基本策略计算其应该回复的数据消息 Mes,如果 m 是应答信息则标记其相应的先前发送的消息 Mes_i 的 ACK 属性为 ACKed。Sig 为 P 将要发送的应答信息集合,节点 P 已经接收到数据消息但还没有回复应答的信息存放在集合 Rev 中,如果节点 P 发送的消息都已回复 ACKed 或者 P 是协商发起者,则 Rev 中的所有消息都需要回复 ACK 信息,否则需要去除最早接收到的那个数据消息。最后发送数据消息集合 Mes 和应答信息集合 Sig。完整协商策略同样具备安全性和完备性。

3　结束语

自动信任协商技术解决了跨多安全域隐私保护、信任建立等问题,成为一个崭新的研究领域,其研究和应用在国际上备受关注。本文在整理、归纳现有文献中所出现的概念、定义的基础上,定义了两个以上参与方时信任协商的策略语言、安全披露序列、完整协商策略,讨论了协商策略的安全性、完备性等关键概念。本文的协商策略是一种积极策略,披露所有可满足访问控制策略保护的信任证。任何一种新技术从它的诞生、发展到被广泛接受都需要进行不断的探索和实验,随着物联网与云计算的飞速发展,对可信协作的需求越来越迫切,需要对信任协商技术继续展开更深入的研究。

参考文献:

[1] WINSBOROUGH W H, SEAMONS K E, JONES V E. Automated trust negotiation[C]//DARPA Information Survivability Conference and Exposition. New York: IEEE Press,2000:88-102.

[2] LI N H, MITCHELL J C, WINSBOROUGH W H. Design of a role-based trust management framework[C]//Proc of the 2002 IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society Press, 2002:114-130.

[3] LI N H, WINSBOROUGH W H, MITCHELL J C. Distributed credential chain discovery in trust management[C]//Proc of the 8th ACM Conference. 2001:156-165.

[4] SEAMONS K E,WINSLETT M,YU T. *et al*. Protecting privacy during on-line trust negotiation[C]//Proc of the 2nd Workshop on Privacy Enhancing Technologies. Berlin:Springer-Verlag,2002.

[5] YU T, WINSLETT M. SEAMONS K E, *et al*. Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation[J]. ACM Trans on Information and System Security,2003,6(1).

[6] Yu T. Automated trust establishment in open systems [D]. Illinois: University of Illinois, 2003.

[7] De TREVILLE J. Binder, a logic-based security language[C]//Proc of IEEE Symposium on Security and Privacy. Washington DC:IEEE Computer Society,2002.

[8] SEAMONS K E, WINSLETT M, YU T, *et al*. Limiting the disclosure of access control policies during automated trust negotiation [C]// Network and Distributed System Security Symposium. 2001.

[9] DIJKSTRA E W, SCHOLTEN C S. Termination detection for diffusing computations[J]. Information Processing Letters, 1980, 11(1):134-145.

(上接第 289 页)

5　结束语

本文分析了目前存在的网络安全态势评估算法,提出了一种基于多源异构传感器的网络安全态势评估模型及其实现方法。根据态势感知模型实现了相应的原型系统,通过对实验网络环境的分析发现,本文提出的方法不仅能够提供管理者当前网络真实的安全状况,还有助于适时地调整系统安全策略,提高网络整体安全性。

参考文献:

[1] 赖积保,王颖,王慧强,等.基于多源异构传感器的网络安全态势感知系统结构研究[J].计算机科学,2011,38(3):144-149.

[2] YIN Xiao-xin, YURCIK W, SLAGELL A, The design of visflowconnect-IP: a link analysis system for IP security situational awareness [C]//Proc of the 3rd IEEE International Workshop on Information Assurance (IWIA). 2005:141-153.

[3] BATSELL S G, RAO N S, SHANKAR M. Distributed intrusion detection and attack containment for organizational cyber security[EB/OL]. http://www. ioc. oml. gov/projects/documents/containment. pdf, 2005.

[4] LEE S, CHUNG B, KIM H, *et al*. Real-time analysis of intrusion detection alerts via correlation[J]. Computers & Security, 2006,25(3):169-183.

[5] VALDES A, SLONNER K. Probabilistic alert correlation[C]//Proc of the 4th International Symposium on Recent Advances in Intrusion Detection (RAID 2001). London: Springer Verlag, 2001:54-68.

[6] MU C, HUANG H, TIAN S. Intrusion detection alert verification based on multilevel fuzzy comprehensive evaluation[C]//Proc of the 2005 International Conference on Computational Intelligence and Security. Berlin: Springer-Verlag, 2005:9-16.

[7] QIN X, LEE W. Discovering novel attack strategies from INFOSEC alerts[C]//Proc of the 9th European Symposium on Research in Computer Security. [S.l.]:Sophia Antipolis,2004:439-456.

[8] STEVEN C, ULF L, MARTIN W F. Modeling multistep cyber attacks for scenario recognition[C]//Proc of the 3rd DARPA Information Survivability Conference and Exposition. 2003:284-292.

[9] 陈秀真,郑庆华,管晓宏,等.层次化网络安全威胁态势量化评估方法[J].软件学报,2006,17(04):885-897.

[10] 王娟,张凤荔,傅翀,等.网络态势感知中的指标体系研究[J].计算机应用,2007,27(8):1907-1909.

[11] BELTON V, GEAR A E. On a shortcoming of Saaty's method of analytic hierarchies[J]. Omega,1983,11:227-230.

[12] DYE C Y. Joint pricing and ordering policy for a deteriorating inventory with partial backlogging[J]. Omega,2007,35(2):184-189.

[13] LIU Y S, HUANG G S. A new combination rule of evidence theory based on consensus[C]//Proc of International Conference on Machine Learning and Cybernetics. 2005:18-21.