Dining Cryptographer 安全协议及工程分析

陶志红[1], Hans Kleine B ning[2], 张世琨[3], 王立福[3]
(1. 南京大学数学系, 江苏南京 210093; 2. Paderborn 大学计算机系, D2333095 德国; 3. 北京大学计算机系, 北京 100871)

摘 要: 网络信息安全包括信息内容的加密及通讯的匿名性质. Dining Cryptographer (DC2net) 协议[1,2] 就是一个基于数学不可解特性的基础安全匿名通信协议, 其主要特点是通过提供匿名信息服务来避免恶意攻击. 本文在介绍 DC2net 协议工作原理的基础上, 从工程应用角度给出了如何构建基于 DC2net 协议的分布式安全信息服务, 并对运行时的有关问题进行了研究.

关键词: 安全协议; 形式化分析; 电子商务; Internet 网络; DC2net (Dining Cryptographer net) 协议
中图分类号: TP309. 7 文献标识码: A 文章编号: 03722112 (2005) 022026204

Dining Cryptographer Protocol and Its Engineering Analysis

TAO Zhi2hong[1], Hans Kleine B ning[2], ZHANG Shi2kun[3], WANG Li2fu[3]
(1. Department of Mathematics, Nanjing University, Nanjing, Jiangsu 210093, China;
2. Department of Computer Science, Paderborn University, D2333095, Germany;
3. Department of Computer Science and Technology, Peking Univerisity, Beijing 100871, China)

Abstract: Network Information Security includes context security and the anonymous property of Network Communication. Din2ing Cryptographer (DC2net) Protocol is a famous anonymous communication protocol based on mathematicsally non2solved property. Its main characteristic focuses on that it can avoid being maliciously attacked by providing anonymous information service. After introduce2ing basic DC2net protocol principle, we discuss some problems from engineering view point like how to construct distributed security in2formation service based on DC2net protocol and analyze its run2time problems.

Key words: security protocol; formal analysis; e2business; internet; DC(dining cryptographer)2net protocol

1 引言

随着以网络为平台的电子商务和电子政务应用的普及, 大量网络安全应用协议[5,7,11,12,13,15] 被设计出来. 在这里介绍的是著名 Dining Cryptographer 协议[1,2] 的网络传输方法, 以下将这个网络简称为 DC2net, 我们讨论基于数学不可解特性的安全信息传输问题.

DC2net 协议基本目标就是在信息的发送方, 发送者可以无限制条件地将自己的某些信息发送给 DC- net 中的目标方而其他网络参与者毫不知情, 并且这一点可以用数学方法加以验证. 而接收方则可以在无法让其他参与者追踪的情况下, 不留痕迹地收到有关的信息. DC2net 传输协议的发明者 David Chaum 为了 DC2net 传输协议可以实际运行, 对协议附加了一些条件如关于这个网络传输必须是可靠且按照广播方式进行的, 所有网络参与者都是诚实的, 这些条件确实有助于 DC2net 传输协议的实现. 由于 Dining Cryptographer 方法本质上属于有别于一般基于密钥的加密方法并且可以和后者进行集成, 所以此方法和相关概念一经提出就在业界受到广泛的关注, 许多基于该方法的安全网络传输协议[11~13] 被不断地提出来. 有不少研究人员采用进程代数的理论研究此类协议, 也有作者用纯数学或信息论的方法来研究.

2 Dining2Cryptographer 协议

David Chaum 是通过下面一个具体的例子给出 DC2net 协议的:

/ 三个保密家到他们平时喜欢的三星级酒店的里吃饭, 服务员告诉他们付款规则是采用匿名方式进行的. 其中一个保密家可以为这顿饭付账或者由 NSA(美国国家安全局) 替他们付账. 三个保密家珍重每个人的匿名付账权力, 但是他们疑惑是否由 NSA 来替他们付账. 为了搞清楚谁付账, Chaum 提出下面的协议规则, 该协议预先假设至多只有一个保密家为这顿饭付账:

(a) 每个保密家将一枚硬币向上抛, 硬币落在他和位于其右边的保密家之间, 从而只有他和他右边的可以看到硬币的表面.

(b1) 每个保密家然后大声说出他所见到的二个硬币, 一

收稿日期: 2004203215; 修回日期: 2004204226
基金项目: 国家 863 项目(No12001AA113171); 国家 973 项目(No. 2002CB312006)

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

个是自己抛的另一个是他左边的人抛的, 说出他看到的二个硬币表面图案一样或不一样.

(b2) 如果其中的某一个保密家支付了款项, 他就说出相反的结果, 如果他没有支付这顿饭钱他应该照实说出. 这样所有的保密家可以根据他们所说出的情况, 判断出是由 NSA 付账(当不一样为偶数时) , 或他们中的某一个人付账但不知到具体是哪一个0.

David Chaum 介绍的 DC2net 协议只是一个基础性框架结构, 并没有具体介绍协议的技术实现细节. 目前基于 DC2net 工作原理的安全协议如 Onion 协议[11], Crowds 协议[12] 及 Hordes 协议[13] 在信息发送阶段都是源于下面的条件假设和工作原理的.

在具有可靠广播的条件下, 我们讨论一个加密信息发送的基本情况: 假设已经有 n 个保密家参加了发送信息出去的进程, 而且进一步地假定信息的接收方就是其中的某个保密家, 每二个参与通信的保密家之间都有只有他们自己知道的通信密钥对, 由于是用广播方式进行传播, 所以接收者的身份显然是匿名的, 发送者的匿名性由类似上面的办法实现, 下面是具体描述:

让集合 K= (K1, K2, , , Kn) 作为保密家集合并且记(F, Ý) 作为一个交换群, 算符Ý 有组合加密的含义也就是数据集成打包的意思, 协议如下运行:

(a)定位阶段　基本按照圆桌方式进行, 每二个需要通信的保密家需要通信的之间拥有共享的, 仅仅局限于他们之间的密钥即 Ki 和Kj 拥有公共密钥Si, j(= Sj, i) , 我们定义集合 G 由集合K 中的拥有公共密钥的保密家对(Ki, Kj) 组成, 即如果(Ki, Kj) I G 则(Kj, Ki) I G. 更一般而言约定如保密家 Ki 和Kj 之间没有通讯密钥, 我们就认为他们拥有的密钥为零Si, j(= Sj, i= 0) , 这样就可以将集合 G 扩大到拥有全部的保密家对了, 以下我们就采用这个扩充后的概念.

(b) 获得信息发送权　这个阶段如同上面介绍那样作即将看到的情况反说.

(c)信息发送阶段　我们假设由保密家 Ki, 广播信息 M, 他希望这个信息可以被拥有共享密钥的所有保密家或协议参与者所接收.

$$M Ý \underset{P\{P_i,P_j\} I G}{E} S_{i,j}$$

(d)信息接收阶段　接收方可以通过自己的共享密钥得到信息 M, 并过滤调信息 M 的其他加密形式.

DC2net 协议有以下局限性: 需要安全和可靠的广播通道, 这个前提在这里是强制性的. 广播通道的阻塞性, 信息一旦被阻塞那么通讯的基本目的就达不到. 共享密钥的交换问题, 这保证了加密信息只能通过用正确密钥才可以解开. 目前 Onion[11], Crowds[12] 及 Hordes[13] 协议主要是通过代理(proxy) 机制将信息的实际发送者和接收者集合进行空间上的多次隔离, 从而达到隐藏信息目的. 在如何应用 DC2net 协议于工程实现方面上述三个协议都没有给出具体的介绍. 在下一节, 根据 David Chaum 介绍的例子, 我们从工程应用角度给出如何构建基于 DC2net 协议的分布式安全信息服务.

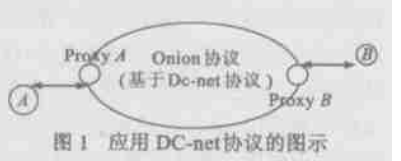


图 1　应用 DC-net协议的图示

3　Dining2Cryptographer 协议的形式化描述和工程实现分析

Dining Cryptographer 协议形式化扩充.

我们让集合 K= {K1, K2, , , Kn} 作为保密家集合围坐在一个大型圆桌上, 每二个保密家之间有一个可以产生随机数的小骰子, 每个保密家可以抛自己右边的小骰子从而产生一个只有他和其右边的保密家才可以看到的随机数, 我们记这个随机数集合为 P= {P1, P2, , , Pn}, 并假设保密家 Ki 通过抛骰子得到的随机数为Pi. 协议的基本原则是一样的, 如果保密家 Ki 没有得到了发送数据的权力, 他就向集合报告他看到的数据差 ai= (pi- pi+ 1) , 反之, 如果是他得到发送数据的权力并发送了数据出去, 他就向集合报告的 ai= (pi- pi+ 1) + 1, 如果没有一个保密家得到发送数据的权力则由集合的管理者发无意义的数据, 现在开始协议的执行:

(a) 如果没有集合 K 中的保密家发送数据, 那么集合得到的数据差总和是

$$\underset{G}{E} a_i = \underset{G}{E} (p_i - p_{i+1}) = 0$$

(b) 如果集合 K 中的保密家Ki 发送数据, 那么集合得到的数据差总和是

$$\begin{aligned}\underset{G}{E} a_i &= (p_1 - p_2) + (p_2 - p_3) + , + (p_i - p_{i+1}) \\ &\quad + 1 + , + (p_n - p_1) \\ &= \underset{G}{E} (p_i - p_{i+1}) + 1 = 0 + 1 = 1\end{aligned}$$

我们可以从数据差总和得知保密家集合 K 中有没有参与者发送信息, 而集合 K 中无法得知是谁发送了数据出去.

Dining Cryptographer 协议的工程实现分析

我们安排系统维护着二个很大的相对运动广播数据环: OUT 和IN 环, 分别包含的是向外发送或接收的数据. 环上分别有很多小的数据存储箱 Oboxi/ Iboxi, 用于存储保密家计划向外发送或接收的数据, 我们可以记集合 OUT= {Obox1, Obox2, , , OboxN}, IN= {Ibox1, Ibox2, , , IboxN}, 这里我们假设 OUT 环和IN 环分别拥有N 个数据存储箱.

系统容许每个协议参与者 Ki 可以向OUT 环的数据存储箱写数据, 也可以从 IN 环的数据存储箱取数据, 考虑到具体情况在实现时有附加规定. 为了提高公正性, 系统随机设置了许多观察员其等同于协议参与者的基本角色, 不真正地参与数据发送和接收, 仅仅用来保证协议的参与者不被完全串通的目的. 所以考虑到这类的观察员的存在, 集合 K 的成员数 n 要超过实际参与该协议的实体数目. 这样我们就可以来讨论保密家集合 K= {K1, K2, , , Kn} 成员之间的通信问题. 作为一个双向运行的网络数据传输协议我们假设有二个保密家 A 和B 希望互相发送信息为A y B: MessageOa 和 B y A: Mes2 sageOb, 他们拥有共享密钥为 Sab(= Sba) .

(a)定位阶段　我们也称之为加入 DC2net 环阶段, 严格

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

地讲这个阶段是由如下步骤组成. 预约: 保密家 A 预约 B 要参加通信并交换通讯密钥, 这个过程需要有个条件, 即保密家 A 知道 B 且 B 也知道 A. 可以认为在茫茫人海中保密家 A 可以通过类似广播或公共信息版 BBS 方式用一定的加密信息方式通知保密家 B 要求对话. 加入: 要彼此通信的保密家 A 和 B 共同加入到保密家集合中来, 并且将他们之间公共密钥也交换完成. 有不少研究者在这里采用级连[11,12]或递归方法[13]来完成共享密钥的传递过程, 一些传统上的通信握手协议可以集成到这里来. 保密家 A 和 B 对 DC2net 环的加入还意味着和系统交换了事务密钥以及建立固定联系和基本身份隐藏步骤, 在这里我们简化成保密家 A 和 B 已经在一系列的必要步骤后加入到了 DC2net 协议环结构中, 并且记得他们此时已经变为: Ay K_{i0}, By K_{j0} 了.

(b) 获得信息发送权 系统此时产生一个随机数集合 $P = \{P_1, P_2, \cdots, P_n\}$, 此时假定共有包括观察员在内共 n 个协议参与者, 并且按照 Dining Cryptographer 方法进行分布. 系统负责保证每个参与者 K_i 只可以看到二个随机数 P_i 和 P_{i+1}, 同时系统采取一系列调度算法来保证每个 K_i 都可以在一定时间范围内获得信息发送权, 直接可以将令牌协议的部分机制集成进来, 并由系统负责当分配给 K_i 有信息发布权时, 系统自动地对 $a_i = (p_i - p_{i+1})$ 进行加 1 处理.

(c) 信息发送阶段 保密家 A 此时也就是 K_{i0} 拿到了信息发送权, 在系统的统一时钟同步控制下, 将用密钥 Sab 加密的信息 MessageOa 放入 OUT 环上的, 此时恰好就在他手边的比如 Oboxi 号信箱, 当然将数据放入到信息 OUT 环也有所规定. 要和系统交换某些只有系统才能识别的信息, OUT 环上信息由系统来维护并且所有参与者无权修改. 系统在容许 K_{i0} 发送信息时自动使得 Oboxi 信箱里没有其他正在使用的信息.

(d) 信息接收阶段 现在用密钥 Sab 加密的信息 MessageOa 在 OUT 环上 Oboxi 信箱的, 并且被交换到 IN 环的比方说 Iboxt 信箱中. 由于循环机制的作用, 它一次次地经过每个协议参与者的面前. 系统再次为信息接收产生一个随机数集合. 当 K_{j0} 用共享密钥解开此信息后, 完成以下步骤, 在系统作用下对 $a_i = (p_i - p_{i+1})$ 进行加 1 处理, 而其他的 K_i 由于没有相应的通信密钥, 知道这个信息不是发给他的所以不知道具体内容. 我们可以称 E_{ai} 为 Dining Cryptographer 系数, 如果这个数为 1 则表明 A 也就是 K_{i0} 发出的信息已经被接收了, 由于系统只有在某个保密家知道密钥 Sab 情况下才能发出 1 这个信号, 而知道这个密钥的保密家只有 K_{j0} 也就是 B 了. 所以在 A 看来给 B 发送的信息已经被 B 收到了, 同样道理 A 也可以收到 B 发来的信息, 而且这个信息也可以包含下一个通信的新密钥或密钥链, 所以基于 Dining2Cryptographer 方法的网络通讯在原理上得以基本实现.

Dining Cryptographer 协议安全归约的形式化表示.

Dining Cryptographer 协议基于数学和逻辑方面可靠性即: 发送和接收的动作无法被判断出来让集合 $K = \{K_1, K_2, \cdots, K_n\}$ 作为保密家集合, 用逻辑语言描述以下的动作和要求:

保密家 K_{i0} 给 K_{j0} 发出信息, 要求没有其他的保密家知道信息由谁发出, 注意在发送阶段 K_{j0} 也无法知道信息由谁发出, 在接收阶段除 K_{j0} 之外没有其他的保密家知道信息由谁接收, 由于系统采取非同步策略即发送的信息可以在几个时钟周期后传递, 所以即使是 K_{i0} 在看到网络上有接收信息时, 也无法确认就是自己刚才发送的相应信息, 这一点算是理论上的完整性, 我们这里用逻辑公式表示如下:

send 表示发送信息的动作, $send_i$ 表示保密家 K_i 发送信息; receive 表示接收信息的动作, $receive_i$ 表示 K_i 接收信息; $know_i$ 表示保密家 K_i 知道(发送信息或接收信息) 的意思.

我们用逻辑公式表示 Dining Cryptographer 协议的基本原理, 即: 要么没有人发送信息, 要么有人发送但我们不知道是谁发的, 但是只要是有人发就一定有人收到信息, 且没有其他人知道是谁收到这个信息, 即使是发送者也不例外.

首先假设在集合 K 内拥有同样密钥的保密家被认为是同一个对, 我们用 S 表示所有密钥的集合, 则上面的假设可以表示成: 设 Sab(= Sba) 为保密家 K_{i0} 和 K_{j0} 之间的共享密钥, K_i 为任一个集合 K 中知道该共享密钥的保密家, 则 $i = i_0$ 或 $i = j_0$.

要么保密家 K_{i0} 没有发出信息且其他的保密家也没有发送信息:

$$\neg send_{i0} \wedge know_i(\neg send_0 \wedge \cdots \wedge \neg send_n)$$

要么保密家 K_{i0} 发出信息且其他的保密家没有发现: $j \neq i_0$ 为任意的

$$send_{i0} \wedge know_i(send_0 \vee \cdots \vee send_n) \wedge \neg know_i(send_0) \wedge \cdots \wedge \neg know_i(send_j) \wedge \cdots \wedge \neg know_i(send_n)$$

当保密家 K_{i0} 发出信息后, 拥有共享密钥的保密家 K_{j0} 一定能收到该信息:

$send_{i0} \Rightarrow K_{i0}$ 和 K_{j0} 有相同的密钥且 $receive_{j0}$ 并且除了保密家 K_{j0} 自己以外任何保密家不知道谁接收了信息: $i \neq j_0$ 为任意的

$$receive_{j0} \Rightarrow know_i(receive_0 \vee \cdots \vee receive_n) \wedge \neg know_i(receive_{i0}) \wedge \cdots \wedge \neg know_i(receive_j) \wedge \cdots \wedge \neg know_i(receive_n)$$

目前有一些具体研究表明这个问题是可以用 CSP/FDR2, SPIN[8] 或其他模型检测工具加以验证[10], 在我们接下来的一项研究中 (另文发表), 将根据 Halpern 的知识逻辑推理[6] 的一个著名的概念: 公共知识, 在提出匿名形式化定义基础上给出一个可模型检测的证明.

Dining Cryptographer 协议实际运行的几个问题.

DC2net 协议的主要安全特性是通过隐藏通行双方的真实身份, 避开来自网络的恶意攻击的. 所以目前应用 DC2net 协议的通行策略[11~13]就是通过设置代理或多级别代理将通行双方的身份进行隐藏, 而后再置于 DC2net 协议下实施通行. 这里的一个主要问题就是密钥的交换问题, 包括在首次通信及后续通行中. 防止通讯被截听的另一个问题就是通信方在设置代理时也不能就此固定下来, 否则通过通信流量的监测还是可以判断出具体通行双方的身份信息的. 解决这个问题的一种途径就是采用 Onion 协议[11]的多级应用 DC2net 协议的方法, 形象地比喻就是小环置于大环之上运行, 这是目前这个

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

研究领域的一个主要研究课题. 从理论分析角度看, 满足 DC2net 协议的运行环境的公平性如何给使用者以信服的保证, 目前还没有一个明确的结论, 许多研究者[8,10] 正在从事的研究工作或许将会给我们一个满意的结果.

4 结束语

本文在介绍 DC2net 协议原理实例的基础上, 从工程角度给出了如何构建基于 DC2net 协议的分布式安全信息服务, 同时也分析了目前应用 DC2net 协议的几个实验系统如 Onion[11] 等基本工作原理及存在的问题. 源于数学方法的网络信息安全服务相关技术发展非常快, 尽管目前几个实验系统还存在明显的问题, 但可以相信一旦找到比较完善的解决方案将会对网络安全信息服务产生重大影响.

参考文献:

[1] David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms [J]. Communications of the ACM, 1981, 24(2): 84- 88.

[2] David Chaum. The dining cryptographers problem: unconditional sender and recipient untraceability[J]. Journal of Cryptology 1988, 1(1): 65- 75.

[3] E M Clarke, E A Emerson. Design and synthesis of synchronization skeletons using branching time temporal logic[A]. Logic of Programs: Workshop[C]. Yorktoen Heights, NY: Springer, LNCS, May 1981. 131. 52- 71.

[4] C Diot, et al. Deployment issues for the IP multicast service and architecture[J]. IEEE Networks, 2000, 14(1): 78- 88.

[5] Dolev D, Yao A. On the security of public key protocols[J]. IEEE Transactions on Information Theory, 1983, 29(2): 198- 208.

[6] R Fagin, J Halpern, Y Moses, M Vardi. Reasoning about Knowledge [M]. Cambridge MA: MIT Press, 1995.

[7] G Holzmann. Design and Validation of Computer Protocols [M]. Prentice Hall, 1991.

[8] G Holzmann. The spin model checker [J]. IEEE Trans. Software Engineering, 1997, 23(5): 279- 295.

[9] D M Nessett. A critique of the burrows, abadi and needham logic[J]. ACM Operating Systems Review, 1990, 24(2): 35- 38.

[10] R van der Meyden, Kaile Su. Symbolic model checking the knowledge of the dining cryptographers[A], 17th Computer Security Foundations workshop[C]. Asilomar, IEEE, 2004. 281- 291.

[11] M Reed, P Syverson, D Goldschlag. Proxies for anonymous routing[A]. 12th Annual Computer Security Applications Conference[C]. USA: IEEE, December 1995. 95- 104.

[12] M K Reiter, A D Rubin. Crowds: Anonymous for web transactions[J]. ACM Transactions on Information and System Security, 1998, 1(1): 66- 92.

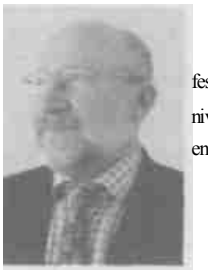
[13] N L Brian, S Clay. Hordes: A Multicast Based Protocol for Anonymity [R]. Dept. of Computer Science University of Massachusetts, 2002.

[14] 卿斯汉. 安全协议的设计与逻辑分析[J]. 软件学报, 2003, 14(7): 1300- 1309.
Qing SH. Design and logical analysis of security protocols[J]. Journal of Software, 2003, 14(7): 1300- 1309.

[15] 卿斯汉. 安全协议 20 年研究进展[J]. 软件学报, 2003, 14(10): 1740- 1752.
Qing SH. Twenty years development of security protocols research[J]. Journal of Software, 2003, 14(10): 1740- 1752.

作者简介:

陶志红　男, 1965 年生, 2003 年 12 月南京大学博士毕业, 目前主要研究方向包括: 基于构件的大规模软件开发(CBSD), 运行时模型检测(Run2Time Model Checking), 可计算建模分析(Computational Modeling Analysis)和构件的并发控制(Component Currency). E2mail: tzh@cs. pku. edu. cn.



Hans Kleine Büning　1948 年生, He is a Professor of Computer Science Department of Paderborn University. His current research interests include software engineering, model checking and artificial intelligence.

© 1994-2010 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net