带有分级访问控制的安全组通信实现方案*

苏 铭, 刘 刚
(解放军信息工程大学信息工程学院, 河南 郑州 450002)

摘 要: 带有分级访问控制 (HAC) 的安全成组通信 (SGC) 是指一组成员根据所拥有的特权等级不同而分为若干个分组, 高级的分组成员可以收到并破译低一级分组成员的信息, 但反之则不被允许。提出了改进的基于中国剩余定理的安全组通信方案, 该方案不仅支持安全分级控制, 还具有以下一些特点: 隐藏分级以及接收者的身份, 对发送信息者以及信息进行验证; 为接收者直接获取信息密钥提供一种方法。

关键词: 安全组通信; 分级访问控制; 中国剩余定理
中图分类号: TP183 文献标识码: A 文章编号: 0529-6579 (2004) S2-0172-04

带有分级访问控制的安全成组通信是指一组成员根据所拥有的特权等级不同而分为若干个分组, 高级的分组成员可以收到并破译下一级分组成员的信息, 但反之则不被允许。HAC 通常要使用密码学技术[1], 也就是说, 密钥在访问权的控制中具有极其重要的地位。如果高级的分组成员拥有或者能够得到分组成员的密钥, 那么该高级分组成员则有权访问低一级分组成员的信息。基于密码学的带有分级访问控制的安全成组通信技术主要分为两大类: ①非独立密钥方案[2,3], 在该方案中, 所有分组密钥都直接来自其上一级组的密钥。这样, 间接来自于它的祖先密钥 (然而与之相隔的上级密钥则没有直接关系); ②独立密钥方案[4]。所有的分组密钥都是独立的, 然而上级组成员可以通过一些预先计算的参数计算出下级组成员的密钥。

在本文中, 我们所提出的方案属于第二种方案, 也就是, 独立密钥方案。该方案的基础是中国剩余定理 (CRT)。在这个方案中, 所有的分组成员都可以独立地选择或修改自己的密钥, 这是一个非常重要的安全因素[4]。另外, 该方案还具有以下的一些特点: ①隐藏分级和接受者身份; ②对发送信息者以及信息进行验证; ③无论发送者距离上层接收者的层级有多远, 接收者都可以直接获取发送者的信息密钥。隐藏分级是一种很好的特性, 因为分组知道越少的分级信息, 系统也就越安全, 插入或删除分组也就越容易。同时, 可以免去管理分级信息的开销。隐藏发送者身份在以下几种情况下非常有用: ① 不允许外人 (非组内成员) 知道接收者的身份; ② 不允许发送者知道接收者身份; ③ 发送者难以知道接收者的身份。称这个方案为基于中国剩余定理的分级访问控制。在本文中, $E_k(x)$ 表示利用密钥 k 进行公共密钥加密; 而 $\{x\}_k$ 表示使用 k 进行私有密钥加密。

1 基于中国剩余定理的分级访问控制方案

1.1 组成及其初始化

在方案中有一个组控制器 (GC), 分组 G_i, 对每个分组 G_i 有一个分组控制器, 也记为 G_i。组控制器有一对公共和私人密钥 (P_{GC}, S_{GC}), 其中 P_{GC} 为公共密钥。每一个分组 G_i 也有, 记为 (P_i, S_i)。组控制器实施以下任务: 保证组间整个结构的稳定性; 随机产生一些成对的互质的数 N_0, N_1, N_2, …, N_m; N_0 是公开的, 剩余的 N_i 是秘密的, 也就是, 上级组 G_i 通过公开密钥 P_i 对 N_i 进行加密; 对每一个分组 G_i, 存在一个正整数 N_i 由等式 (2) 定义。GC 用 CRT 运算法则计算出 COM_CRT_i (见等式 (1)) 和 N_i, 并将 N_i, COM_CRT_i 和 N_i 安全的反馈给上级组 G_i。定义 $\{G_{i_1}, G_{i_2}, \cdots G_{i_k}\}$ 为分组 G_i 的所有祖先集合。全等系统 (1) 和等式 (2) 分别定义 COM_CRT_i 和 N_i。

$$\begin{aligned} COM\_CRT_i &\equiv E_{P_j}(K_i) \bmod N_{i_1} \\ COM\_CRT_i &\equiv E_{P_{i_2}}(K_i) \bmod N_{i_2} \\ &\cdots \\ COM\_CRT_i &\equiv E_{P_{i_k}}(K_i) \bmod N_{i_k} \end{aligned} \quad (1)$$

* 收稿日期: 2004-09-11
作者简介: 苏 铭 (1974 年生), 女, 博士研究生; E-mail: mingsu@sohu.com

$$N_i = N_{i_1} \cdots N_{i_2} \cdots N_{i_k} \quad (2)$$

每一个分组 G_i 都对 6 元组 (P_i, S_i, K_i, N_i, COM_CRT_i, N_i) 赋值。K_i 是 G_i 的数据密钥, 用来加密数据信息。P_i 是 G_i 的公共密钥, 而其他五个元素则是不公开的。除了知道分组的 6 个元素, 每个组内成员 j 都有属于自己的公共密钥和私有密钥 (p_j, s_j)。

这里 COM_CRT_i 包含了 G_i 所有的上级组子群中的 P_{i_j} 和 N_{i_j} 信息。然而 G_i 并不知道它的祖先是谁。并且即使 N_i 包含了其上级组的 N_j, G_i 无法从 N_i 中获得这些 N_j, 因为将结果分割成特定的因子和特定的顺序是非常难的 (该问题被称之为 *NP* 完整性), 所以分级是完全隐藏的。

1.2　数据通信

无论何时, 拥有 ID_j 身份的 G_i 组的成员 j 发送信息 M, 它将执行下面的工作:

(1) 使用 K_i 将 M 加密, 也就是 $\{M\}_{k_i}$;

(2) 在 K_i 下计算出 $\{M\}_{K_i}$ 经过加密后的 MAC, 也就是 MAC_{k_i} ($\{M\}_{K_i}$), 在此, MAC 可以是任何一个已知的信息验证码, 例如 MD5。

(3) 建立一个完全对等系统

$$CRT_i \equiv COM\_CRT_i \bmod N_i$$

$$CRT_i \equiv E_{S_j}(MAC_{K_i}(\{M\}_{K_i})) \bmod N_0 \quad (3)$$

(4) 运用 CRT 运算法则计算出 CRT_i。CRT_i 包括所有上级组密钥的信息、MAC 和发送者的签名。

(5) 广播 (或多点传输) 三元组 (ID_j, CRT_i, $\{M\}_{K_i}$)。

当接收者接收到(ID_j, CRT_i, $\{M\}_{K_i}$) 时, 将执行以下的工作:

(1) 计算 $x = CRT_i \bmod N_0$。

(2) 使用 j 的公共密钥将 x 解密, 得到 $MAC_{K_i}(\{M\}_{K_i}) = E_{P_j}^{-1}(x)$, 这里 E^{-1} 表示与 E 相对应的解密运算式。

(3) 如果接收者在 G_i 中, 它将使用自己的 K_i 计算 $MAC_{K_i}(\{M\}_{K_i})$。如果接收者在任何一个 G_i 的祖先子群 G_{i_j} 中, 它将先计算

$$CRT_{i_j} = CRT_i \bmod N_{i_j}$$

和将 CRT_{i_j} 解密得到

$$K_i = E_{S_{i_j}}^{-1}(CRT_{i_j})$$

然后在 K_i 下计算 $MAC_{K_i}(\{M\}_{K_i})$。否则, 接收者将忽略这些信息。

(4) 比较上述的 2 个 MACs。如果 2 个 MACs 相等, 那么发送者和发送的信息都将通过验证。接收者使用 K_i 将信息解密。否则, 这信息就不是发给该接收者, 或者信息在传输过程中就已经被修改过了。因此, 接收者会丢弃这条信息。

1.3　动态密钥管理

在带有层次访问控制的安全组通信中, 有两个动态层: 一层是低级动态层, 在该层中, 每个成员可以加入或离开某个分组, 这由分组控制器管理, 依存于分组密钥管理协议。高级动态层包括以下操作: 加入/插入一个新的分组, 去除一个已有的分组, 合并两个分组, 分裂一个分组并修改分组密钥。所有这些在 CRTHACS 中都比较容易实现。例如, 当一个新的分组 G_i 进入了分级系统, *GC* 通过等式(1) 计算出 G_i 的 COM_CRT_i, 将 COM_CRT_i, N_i, N_i 发送给 G_i。如果 G_i 有下层分组的话(也就是 G_i 被插进一个分级系统中), 那么 *GC* 也需要重新计算出 G_i 的所有下级分组成员的值, 从而使 COM_CRT 能包括 G_i 的公共密钥 P_i 和相对应的 N_i 的信息。所有的其它分组都不受影响。

2　方案改进

为了防止最近出现的基于 GCD 计算的攻击, 我们对前面提到的方案进行了改进。

下面先简单说明一下基于 GCD 计算的对我们的方案的可能的三种攻击。这些攻击有可能暴露分级的信息。

(1) 在方案中, CRT_i 与信息相关, 但是 COM_CRT_i 是独立的, 尤其从等式 (3) 得到任何 CRT_i 的两个实例, 由于 N_i 的多样性而不同。因此, 根据来自相同分组 G_i 的 2 个以上的信息, 攻击者 (G_i 以外) 可以从获得 N_i 的信息, 根据是由于

$$CRT_{i_j} - CRT_{i_k} \equiv 0 \bmod N_i$$

所以, $\gcd(CRT_1 - CRT_2, CRT_1 - CRT_3)$ 除尽 N_i。如果攻击者获得多个 CRT_{i_j}, 就可以提炼出 N_i 的信息。

(2) 分组 G_i 可以通过计算 $\gcd(N_i, COM - CRT_i - E_{P_j}(K_i))$ 来计算出他的祖先 G_j, 因为 G_i 可以处理 COM_CRT_i 和 N_i, 并计算 $E_{P_j}(K_i)$。

(3) 如果 2 个分组 G_i 和 G_j 勾结, 则他们可以通过计算

$$\gcd(CRT_1 - E_{P_k}(K_i), CRT_j - E_{P_k}(K_j))$$

获得他们公共的祖先 G_k。

针对这3 种攻击，对前面提到的方案进行了改进，主要归纳为下面 3 个方面：

① 从 CRT_i 中将带符号的 MAC 移走，将带符号的 MAC 作为分离的项，这样 CRT_i 就可以与信息独立出来，这样可以防止第一种攻击。

②移走 COM_CRT_i，并使用新的 CRT_i 来替换。而且新 CRT_i 由 GC 计算得到。GC 将 CRT_i 送给 G_i，而不是 COM_CRT_i，N_i。这样 G_i 可以直接使用 CRT_i，而不需要知道 N_i，这样就可以防御第 2 种攻击。

③ 根据全等系统(1) 将与分组 G_{i_k} 对应的 $E_{P_{i_k}}(K_i)$ 的公共加密替换为私有密钥加密 $\{K_i\}_{K_{i_k}}$，这样由于 G_i 不知道 K_k，所以 G_i 就不能计算出他的祖先分组 G_k 相关的 $\{K_k\}_{K_k}$。这样就防止基于 GCD 的第3 种攻击。实际上，这个修改对第 2 种攻击也比较有用，因为 $E_{P_j}(K_i)$ 不包含在 COM_CRT_i 中。

3 安全和性能分析

我们的方案是具有安全性的，因为分组数据密钥独立存在，没有分组 G_i 可以通过自己的数据密钥猜到或计算出其他分组 G_j 的数据密钥。分组 G_i 能够计算出次级分组 G_j 的数据密钥的唯一方式是获得 N_i 和 S_i 的值，这里 N_i 和 P_i 被包含在 G_j 的 COM_CRT 值内。N_i 和 S_i 为 G_i 的私有密钥，其他的组是无法获得 N_i 和 S_i。所以非法的组是不能获得分组 G_j 的数据密钥的。

关于此方案的性能，有 3 个比较复杂的地方需要考虑：空间、时间和通信复杂性。

空间复杂度主要分成两类进行计算，一类是访问控制结构或组成员，另一类是表示密钥 (P_i，S_i，K_i)，描述 P_i，S_i，K_i，N_i，$COM-CRT_i$ 和 N_i 所用的空间。前者表示需要一般的整数，例如 32 位的整数。而后者则需要一个大的整数，通常是1 024 bit。所以前者可以被忽略。假设大整数为 L。

时间复杂度需要考虑 3 类复杂性：密钥产生，加密和解密，以及 CRT 运算法则的复杂性，我们主要考虑 CRT 运算法则的复杂性，也就是[5]：

$$O(M(kL)\log(k)) + O(kM(L)\log(L))$$

在这里，$M(n)$ 表示两个 n 位二进制长度的整数相乘的运算时间；$O(n)$ 是以 bit 为单位计算而不是字节。将密钥产生时间、加密和解密的时间忽略不计，因为这些时间主要依靠的是所选择的特定的运算法则。

通信复杂度，我们指的是与密钥相关的事物的规模，包括在 GC 和分组之间 (分组控制器与参与者之间) 或分组控制器与次级成员之间的通信 CRT 参数。这里可以分为三类：组控制器 (GC)，分组控制器(G_i) 和参与者(p_j)。主要计算分组控制器和分组成员之间的密钥，也就是 N_i，$COM-CRT_i$ 以及 N_i。与计算空间复杂度类似，通信复杂度也是 $O(HL)$。

下表将对其复杂性进行总结。

	Space	Time	Communication
GC	$O(mHL)$	$O(mM(HL)\log(H)) + O(mHM(L)\log(L))$	$O(HL)$ (GC and G_1/p_1)
G_1	$O(HL)$	Independent of m and H	
p_1	$O(HL)$	$O(M(2L)) + O(2M(L)\log(L))$	

这里 H 表示一个分组所能拥有的最大数目的上级组个数。

4 结 论

在本文中，我们提出了一种新的带有分级访问控制的安全成组通信方案。这个方案中有许多特性，可以概括如下：①最主要的特点是分组的层次和接收方的信息是隐藏的；②发送方的身份可以被鉴定；③MAC 包括在 CRT_i 中，这样可以保证信息的完整性；④每一个分组可以独立的改变它的密钥 K_i，而不影响其他的分组；⑤插入和删除分组只影响它的后继分组；⑥所有的接收方接受后继分组的成员的信息时执行相同的计算，无需考虑后继分组的距离。

通过与其他的加密方案的比较，我们的方案不仅提供了高效的动态的访问控制，而且还具有可测量性、隐藏分级和接收者身份、以及验证用户和信息等特性，从而在许多应用中比较有用。

参考文献：

[1] BIRGET J C, ZOU X, NOUBIR G, et al. Hierarchy-based access control in distributed environment[C]. To appear in the proceeding of the ICC2001 Conference, 2001.

[2] AKL S G, TAYLOR P D. Cryptographic solution to a problem of access control in a hierarchy[J]. ACM Transactions on Computer Systems, 1983, 1(3): 239－247.

[3] CHICK G C, TAVARES S E. Flexible access control with master keys[C]. Cryptology: CRYPTO'89 LICS, 1990, 435: 316－322.

[4] LIN G H. Dynamic key management schemes for access control in a hierarchy[J]. Computer Communications, 1997, 20: 1381－1385.

[5] CHIOU G H, CHEN W T. Secure broadcasting using the secure lock[J]. IEEE Transaction on Software Engineering, 1989, 15(8): 929—934.

Hierarchical Access Control for Secure Group Communication

SU Ming, LIU Gang
(Department of Computing Science the Information and Engineering University, Zhengzhou 450002, China)

Abstract: Secure group communication with hierarchical access control refers to a scenario where a group of members is divided into a number of subgroups located at different privilege levels and a high-level subgroup can receive and decrypt massages within any of its descendant lower-level subgroups; but the converse is not allowed. To propose a improved scheme, which is based on the Chinese Remainder Theorem. The scheme not only enables secure hierarchical control but also provides the following properties: hiding of hierarchy and receivers, authentication of both senders and messages, and a mechanism for the receiver to directly derive the key of a message.

Key words: secure group communication; hierarchical access control

---

(上接第 171 页)

The Application of Semi-fragile Digital Watermark Technology in the MPEG

WANG Lei, WANG Dao-xian, DUAN Xiao-hui
(Department of Electronics, Peking University, Beijing 100871, China)

Abstract: Based on the MPEG-2 video coding standard, some watermark arithmetics used in static image process are introduced to the video watermarking. And the goal is achieved that not tampering with the video quality at the same time of according with the MPEG-2 coding standard, and being tolerant of the transmission distortion and normal image/video processes as well as detecting some intended attacks and sophistication. In addition a digital watermark authentication arithmetic aimed at the MPEG standard is proposed.

Key words: semi-fragile watermark; MPEG; video authentication; gray coding