第 22 卷 第 1 期 电 子 科 学 学 刊 Vol.22 No.1
2000 年 1 月 JOURNAL OF ELECTRONICS Jan. 2000

Internet/Intranet 互联环境中的安全认证和密钥分配 [1]

孙晓蓉 王育民

(西安电子科技大学 ISN 国家重点实验室 西安 710071)

摘 要 本文提出了解决 Internet/Intranet 互联环境安全性问题的模式，针对不同的 Intranet 的网络结构，提出了适用的安全模式，设计了相应的认证和密钥分配协议，并考虑了协议在开放系统互联 OSI 结构的安全管理问题。协议采用分层机制，在低层采用改进的 Kerberos 协议实现局域网内的认证和密钥分配，而高层的网间认证和密钥分配协议则根据安全模式的不同要求采用单钥体制，或公钥体制来设计。协议能够为 Internet 的各种远程访问提供安全保护。

关键词 因特网 (Internet)，内特网 (Intranet)，认证和密钥分配， OSI 安全结构

中图号 TN913.24, TN918

1 引 言

随着 Internet 的全球化和商业化，引发了 Internet 技术在企业、部门和领域范围内计算机网络的推广应用。这种基于 Internet 体系结构和技术的“内部网络”，简称为 Intranet(内特网)。 Intranet 与 Internet 互联，利用 Internet 的远程访问能力开展电子商务等应用时，首先要解决网络信息安全问题。解决 Internet 的安全问题，本质上是要解决 Intranet 的安全问题。目前，尚无关于 Intranet 的统一的安全标准。各个开发网络产品的大公司纷纷提出自己的安全模式，但每一种模式往往是针对一种特定的环境和用途设计的，不能从整体上解决 Intranet 的安全问题。为了全面地解决 Intranet 的安全问题，本文结合 Intranet 的具体网络配置特点，提出了全面的安全模式，并设计了相应的认证和密钥分配协议，以实现 Internet 上的安全的端-端远程访问。

2 Internet/Intranet 的安全模式

在 Internet/Intranet 环境中，服务器成千上万，网络环境非常复杂。当 Intranet 与外部 Internet 相连时，目前认为最好的保护 Intranet 安全的方法是在 Intranet 与 Internet 之间设置防火墙 (Firewall)。文献 [1] 设计了一种基于防火墙的 Intranet 的安全模式，由于没有全面考虑 Intranet 的网络结构，这种模式很不完善，适用范围受到较大的限制。本节我们针对不同的 Intranet 网络结构，提出相应的、更为适用的安全模式，全面地解决 Intranet 的安全问题。

对于大型的、跨地域的企业或部门，一般是借助防火墙，组建跨公共网的统一的 Intranet。其中，各地的局域网通过防火墙及路由器与总部或其它的局域网互联，如图 1 所示。对于集中于本地 Intranet，可以采用一种结构简单、成本低廉的网络配置模式，如图 2 所示。

[1] 1998-05-28 收到， 1999-02-28 定稿

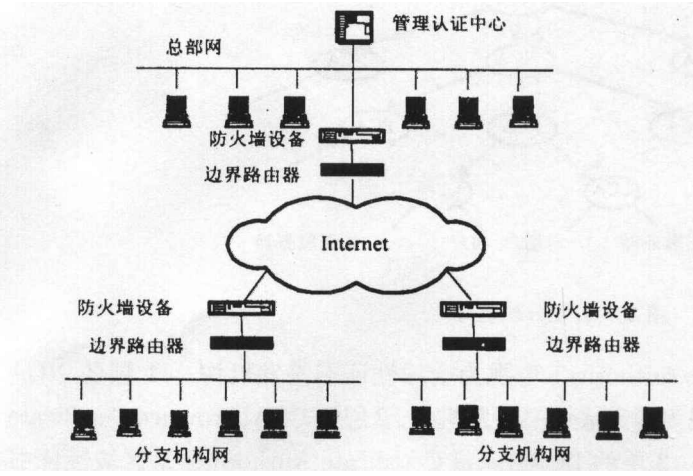

图 1　跨公共网的 Intranet

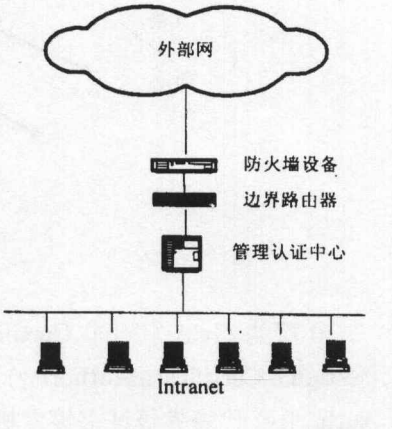

图 2　集中于本地的 Intranet

图 2 所示的 Internet/Intranet 互联环境比较简单。由于 Intranet 局域网与外部网的利益不一致，可以采用这样的安全模式：在 Intranet 网络内部建立网内认证服务器，支持对网络内部用户的认证和会话密钥分配；在防火墙设备中增加网间认证服务器，支持不同的 Intranet 间的相互认证和密钥分配，防止来自外部网络的攻击。我们将这种模式称为模式 1 。

图 1 的 Intranet 是由几个局域网通过公共网互联建立的，防火墙系统主要用来防范来自外部 Internet 的攻击。而在 Intranet 网络内部，各个子网的利益一致，而且整个 Intranet 中的子网数目有限，因此， Intranet 各子网之间的远程访问，可以采用一种简单的安全模式，即各子网的认证服务器相互之间共享一个秘密密钥，以实现子网间的认证和密钥分配，即模式 0 。当 Intranet 各子网内的用户对外部 Internet 进行远程访问时，可以采用两种安全模式：一种是采用上述模式 1 ，在各子网防火墙设备内设置网间认证服务器，通过它所提供的代理服务，进行远程访问；另一种是由总部网统一管理 Intranet 的外部远程访问，子网内用户的远程访问请求经过网内认证服务器加密上溯至总部网，通过设置在总部网管理中心的网间认证服务器的代理服务，进行远程访问，即模式 2 。

上述安全管理模式主要依赖于网络的认证和密钥分配协议，要建立 Intarnet 之间的安全通信，首先要在 Intranet 间建立相互信任的关系，这就要求在通信之前通信双方进行身份认证。由于 Internet 网络环境复杂，要真正实现 OSI(Open System Interconnection) 安全体系结构 [2] 中的对等实体认证，就必须在 Internet 上建立公证机构。

3　端－端认证和密钥分配协议设计

3.1 公钥分配架构

在 Internet/Intranet 互联环境中，单一的公证机构无法满足网络需求。借鉴文献 [3, 4] 的思想，我们提出了适于 Internet/Intranet 互联环境、可全球扩展的分层式公钥分配架构，如图 3 所示。

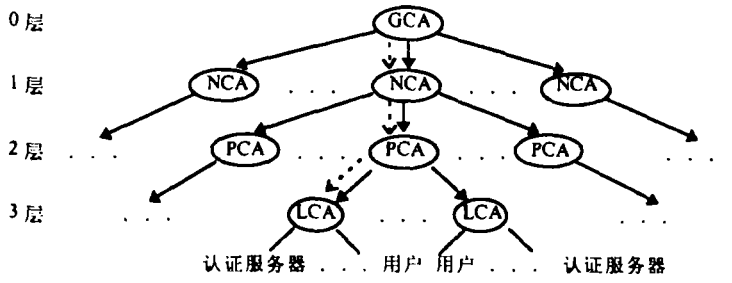

图 3 公钥分配架构

0 层的 GCA(Global Certificate Authority) 可视为全球性证书签发机构， 1 层的 NCA (National Certificate Authority) 可视为国家级证书签发机构, 2 层的 PCA(Province Certificate Authority) 代表省级证书签发机构， 3 层的 LCA(Local Certificate Authority) 是区域性证书签发机构。以图 3 中虚线箭头所指路径为例，给出各级 CA 签发的证件样式。

首先定义符号： $\mathrm{PK}^{(l)}, \mathrm{SK}^{(l)}$: l 层 CA 的公钥和私钥； $\mathrm{ID}^{(l+1)}$: l 层 CA 为 $l+1$ 层实体分配的身份代号； $\mathrm{C}^{(l+1)}$ ： l 层 CA 为 $l+1$ 层实体签发的公钥证书； $\mathrm{sign}(X;Y)$ ： 用密钥 X 对消息 Y 进行签名； $h(\bullet)$ ： 单向函数； cert-M ： 持证者 M 的证件链。

(1) 公证机构 GCA 采用 RSA 算法 [5] ，产生公钥、私钥对 $(\mathrm{PK}^{(0)}, \mathrm{SK}^{(0)})$ 。再选择大素数和 GF(P) 上的本原元 α ，将 P, α 在网络中公开。GCA 为 NCA 签发公钥证件： $\{\mathrm{PK}^{(0)}, \mathrm{C}^{(1)}\}$ 。

(2) NCA 负责为 PCA 签发公钥证件： $\{\mathrm{PK}^{(0)}||\mathrm{PK}^{(1)}, \mathrm{C}^{(1)}||\mathrm{C}^{(2)}\}$ 。

(3) PCA 负责为 LCA 签发公钥证件： $\{\mathrm{PK}^{(0)}||\mathrm{PK}^{(1)}||\mathrm{PK}^{(2)}, \mathrm{C}^{(1)}||\mathrm{C}^{(2)}||\mathrm{C}^{(3)}\}$ 。

(4)LCA 负责为认证服务器 AS 签发公钥证件: $\{\mathrm{PK}^{(0)}||\mathrm{PK}^{(1)}||\mathrm{PK}^{(2)}||\mathrm{PK}^{(3)}, \mathrm{C}^{(1)}||\mathrm{C}^{(2)}||\mathrm{C}^{(3)}||\mathrm{C}_{AS}\}$ 。

并为 LCA 辖区的用户签发公钥证件: $\{\mathrm{PK}^{(0)}||\mathrm{PK}^{(1)}||\mathrm{PK}^{(2)}||\mathrm{PK}^{(3)}, \mathrm{C}^{(1)}||\mathrm{C}^{(2)}||\mathrm{C}^{(3)}||\mathrm{C}_u\}$ 。

以 $\mathrm{C}^{(1)}$ 为例说明证件样式： $\mathrm{C}^{(1)}$= 有效期， $\mathrm{PK}^{(1)}$, $\mathrm{ID}^{(1)}$, $\mathrm{sign}(\mathrm{SK}^{(0)}; h(\mathrm{ID}^{(1)}, \mathrm{PK}^{(1)}$, 有效期)) 。

证件链的签发是不在线脱机 (off-line) 的，即不包括在实时认证协议中，可以用一个简化的样式来表示： Cert-M: GCA>>NCA, NCA>>PCA, PCA>>LCA, LCA>> M 。

收到通信对方的证件链后，接收者首先判断双方共同信赖的 CA 处于哪一层，如果是位于 LCA 层，仅需利用 LCA 的公钥对 LCA>> M 进行验证，如果是位于 PCA 层，则对 PCA>> LCA, LCA>> M 进行验证。以此类推，直到采用 GCA 的公钥对整个证件链进行验证。

3.2 协议设计原则

端-端协议的设计采用分层机制。为了避免过多地改动网络的原有配置，在端-端认证协议的低层可充分利用网络已有的认证协议。本节设计了一种改进的 Kerberos 协议作为低层网内认证和密钥分配协议的基础。改进的 Kerberos 认证协议采用公钥体制来进行用户初始登录，获得访问许可票据和随机阶段性密钥，以后的认证操作按正常的 Kerberos 协议进行。

为了实现基于安全模式 0 的用户认证，在低层采用上述改进的 Kerberos 认证协议实现网内认证，在高层采用单钥体制实现子网间的认证，并采用时间校准参数来帮助 Intranet 网

内的时钟同步。外地子网的认证服务器可以作为改进的 Kerberos 认证协议的一个应用服务器，这样端-端认证协议就可以看作是改进的 Kerberos 协议的扩展。

对于模式 1，采用改进的 Kerberos 协议作为网内认证和密钥分配协议的基础；考虑到 Internet 发展的动态性，为了便于网间认证服务器的密钥管理，高层网间的认证和密钥分配协议采用 Diffie-Hellman 密钥交换技术 [6] 来设计，主要由网间认证服务器来实现，并采用随机数技术来保证网间交互信息的新鲜性，克服网间时钟同步的困难性。网间认证服务器同样也可以看作是改进的 Kerberos 协议的应用服务器。

对于模式 2，协议设计以基于模式 1 的端-端协议为基础。由于用户的远程访问请求上溯至总部网的网间认证服务器，需要增加分支机构网和总部网认证服务器之间的信息交互。

下面协议描述中，[•] 表示公钥加密，{•} 表示单钥加密。

用户初始登录

网络内部用户 A 采用公钥体制向网内认证服务器初始登录，获得访问许可票据和随机阶段性密钥 K_a。

(1) 用户向局域网网内认证服务器发出入网申请，提交其公钥证件和随机数 N_1。A→AS: Cert-A, N_1。

(2) 服务器首先验证用户 A 的证件链的有效性。验证通过后，服务器为用户生成访问许可票据 TGT，同时产生阶段性随机数密钥 K_a、时钟校准参数 Time 和签名函数，用 A 的公钥加密后回送给 A。TGT=sign(SK_{AS}; h(AS, A, 有效期, N))。

AS→A: [Cert-AS, N_1, K_a, 有效期, sign(SK_{AS}; $h(N_1, K_{a,tgs})$), Time]PK_A, {TGT}K_a。

(3) 用户 A 收到消息后，用私钥解密。验证 AS 证书和签名的有效性，验证通过后，向用户 AS 回送认可信息，并存储 K_a 和 TGT。

初始登录完成用户在认证服务器的注册。因无需键入口令，避免了口令的一切不安全性。由于 TGT 有使用期限，用户需要每过一定时间重新初始登录，用户的访问密钥经常更换，一次泄漏不会造成太大的危害，提高了协议的可修复性 [7]。

实时认证

基于模式 0 的认证和密钥分配协议如图 4 所示，具体描述如下。

(1) 用户 A 产生认证符 $Au_a = h(K_a, \mathrm{A}, \mathrm{address}_a, \mathrm{time}_1)$，将消息 $M1$=TGT, {B, time_1, Au_a}K_a 发送给 AS_a，申请远程访问服务。

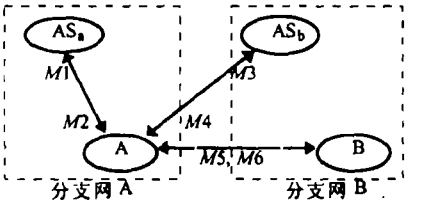

图 4　基于模式 0 的认证和密钥分配协议

(2) ASa 验证 TGT 的有效性。如有效则用 K_a 解密并验证认证符 Au_a，判断 A 是否合法。如 A 是合法的，AS_a 为 A 和认证服务器 AS_b 分配会话密钥 $K_{\mathrm{A,\,AS}_b}$，并签发给 A 访问 AS_b 的票据 $T_{\mathrm{A,\,AS}_b} = \{\mathrm{AS}_b, \mathrm{A}, \mathrm{address}_a, \mathrm{time}_2, K_{\mathrm{A,\,AS}_b}\}K_{\mathrm{AS}_{ab}}$，发送 $M2 = \{\mathrm{AS}_b, K_{\mathrm{A,\,AS}_b}, \mathrm{time}_2, T_{\mathrm{A,\,AS}_b}\}K_a$ 给 A。

(3) 用户 A 解密 $M2$ 得到 $K_{\mathrm{A,\,AS}_b}$，产生认证符 $\mathrm{Au}_{\mathrm{A,\,AS}_b} = h(K_{\mathrm{A,\,AS}_b}, \mathrm{A}, \mathrm{address}_a, \mathrm{time}_3)$，发送消息 $M3 = T_{\mathrm{A,\,AS}_b}$, {B, $\mathrm{time}_3, Au_{\mathrm{A,\,AS}_b}$}$K_{\mathrm{A,\,AS}_b}$ 至 AS_b。

(4) AS_b 解密 $T_{\mathrm{A,\,AS}_b}$，得到 $K_{\mathrm{A,\,AS}_b}$。验证 $K_{\mathrm{A,\,AS}_b}$ 的新鲜性，再解密出 B 和 $Au_{\mathrm{A,\,AS}_b}$，验证认证符。AS_b 为 A 和 B 分配一个会话密钥 K_{ab}，并产生票据 $T_{a,b} = \{\mathrm{A}, \mathrm{B}, \mathrm{time}_4, K_{ab}\}K_b(K_b$

是 B 与 AS_b 共享的随机阶段性密钥)。将消息 $M4 = \{B, address_b, K_{ab}, T_{a,b}, time_4\}K_{A,AS_a}$ 传给 A。

(5) A 解密得到 B 的地址、K_{ab} 和 $T_{a,b}$，产生 $Au_{ab} = h(K_{ab}, A, address_a, time_5)$，向 B 传送消息 $M5 = \{Au_{ab}, time_5\}K_{ab}, T_{a,b}$。

(6) B 解密 $T_{a,b}$ 得到 K_{ab}，并检验票据的有效性。检验通过，再解密得到认证符，验证其正确性。如正确，则允许 A 的访问，传消息 $M6 = \{time_5 + 1\}K_{ab}$ 给 A。否则，拒绝 A 的访问。

该协议实现网间认证和密钥分配时，采用了时戳技术。跨地域 Intranet 网络，可以由总部网的认证服务器每隔一段时间向各个子网发送时间校准参数，来维持整个 Intranet 的时钟同步。

基于模式 1 的认证和密钥分配协议如图 5 所示，描述如下。

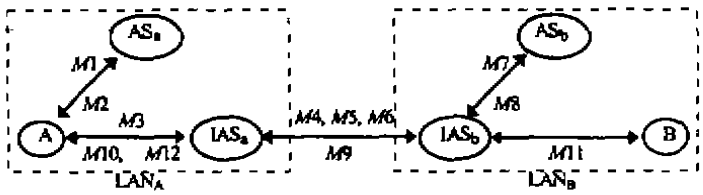

图 5 基于模式 1 的认证和密钥分配协议

设网内认证服务器 AS 与网间认证服务器 IAS_x，共享一个秘密钥 K_{IAS_x}。

(1) $A \xrightarrow{M1} AS_a$: $\{B, time_1, Au_a\}K_a, TGT$. $(Au_a = h(K_a, A, address_a, time_1))$.

(2) $AS_a \xrightarrow{M2} A$: $\{K_{A,IAS}, time_2, T_{A,IAS}\}K_a$. $(T_{A,IAS} = \{IAS_A, A, address_a, time_2, K_{A,IAS}\}K_{IAS_a})$.

(3) $A \xrightarrow{M3} IAS_a$: $\{B, time_3, Au_{A,IAS}\}K_{A,IAS}, T_{A,IAS}$.$(Au_{A,IAS} = h(K_{A,IAS}, A, address_a, time_3))$.

(4) $IAS_a \xrightarrow{M4} IAS_b$: $IAS_a, address_{IAS_a}$, $S_{IAS_{ab}} = \alpha^{N_{IAS_{ab}}} \bmod P$.

(5) $IAS_b \xrightarrow{M5} IAS_a$: $\{Cert - IAS_b, S_{IAS_{ba}}, sign(SK_{IAS_b}; h(S_{IAS_{ab}}, S_{IAS_{ba}}))\}K_{IAS_{ba}}$.

(6) $IAS_a \xrightarrow{M6} IAS_b$: $\{Cert - IAS_a, B, sign(SK_{IAS_a}; h(S_{IAS_{ab}}, S_{IAS_{ba}}))N_{IAS_a}\}K_{IAS_{ab}}$.
$(S_{IAS_{ba}} = \alpha^{N_{IAS_{ba}}} \bmod P,\ K_{IAS_{ba}} = S_{IAS_{ab}}^{N_{IAS_{ba}}} \bmod P,\ K_{IAS_{ab}} = S_{IAS_{ba}}^{N_{IAS_{ab}}} \bmod P)$.

(7) $IAS_b \xrightarrow{M7} AS_b$: $IAS_b, \{A, B, time_1'\}K_{IAS_b}$.

(8) $AS_b \xrightarrow{M8} IAS_b$: $\{K_{ab}, time_2',\ T_{a,b}\}K_{IAS_b}.(T_{a,b} = \{A, B, time_2', K_{ab}\}K_{b,tgs})$.

(9) $IAS_b \xrightarrow{M9} IAS_a$: $\{B, address_b, K_{ab}, T_{a,b}, N_{IAS_a} + 1\}K_{IAS_{ba}}$.

(10) $IAS_a \xrightarrow{M10} A$: $\{B, address_b, K_{ab}, T_{a,b}, time_4\}K_{A,IAS}$.

(11) $A \xrightarrow{M11} B$: $\{Au_{ab}, N_a\}K_{ab}, T_{a,b}$.

(12) $B \xrightarrow{M12} A$: $\{N_a + 1\}K_{ab}$.

(1)—(3) 用户 A 向 AS_a 提出远程访问申请。AS_a 对 A 进行认证后，为 A 和 IAS_a 分配会话密钥 $K_{A,IAS}$，将 $K_{A,IAS}$ 传送给 A，并利用票据业务传送给 IAS_a。(4)—(6) IAS_a

和 IAS_b 相互认证并采用 Diffie-Hellman 密钥交换技术产生会话密钥 $K_{IAS_{ab}}$。(7)—(10)IAS_b 代替 A 向 AS_b 申请访问 B。AS_b 为 A 和 B 分配会话密钥 K_{ab}，并签发 A 访问 B 的票据 $T_{a,b}$。K_{ab} 和 $T_{a,b}$ 经 IAS_a 和 IAS_b 转发给 A。(11)—(12) 用户 A 和 B 之间的密钥传递和相互认证。

在 Intranet 局域网内的认证中采用了时戳技术来防止重放攻击；在 Intranet 网间认证中，采用随机数来保证网间交互信息的新鲜性，克服 Intranet 间时钟同步的困难性。

对于模式 2，网间认证服务器设置在总部网的，当用户申请远程访问时，AS_a 要将 A 的请求上溯至总部网的 AS_h；而在访问网中，由于对 B 的访问票据是由 AS_b 签发的，总部网 AS_v 要将对 B 的访问申请转发给 AS_b，如图 6 所示。

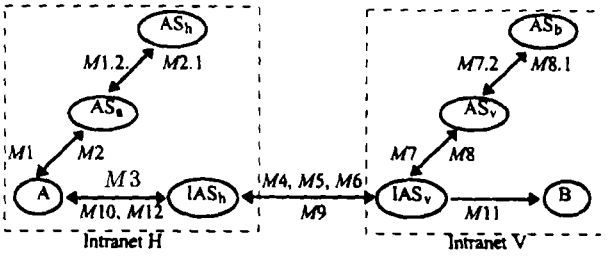

图 6　基于模式 2 的认证和密钥分配协议

由于 AS_a 需要将 A 的请求上溯至总部网的 AS_h，而对 B 的访问许可票据仍然由 AS_b 签发，因此需要增加 AS_a 和 AS_h 的信息交互过程 $M1.2$ 和 $M2.1$，以及 AS_v 和 AS_b 之间的信息交互过程 $M7.2$ 和 $M8.1$。

设 AS_a 与总部网 AS_h 之间共享密钥 K_{ah}，IAS_h 与总部网 AS_h 之间共享密钥 K_{hh}；AS_b 与 AS_v 之间共享密钥 K_{bv}，IAS_v 与 AS_v 之间共享密钥 K_{vv}。

(1) $A \xrightarrow{M1} AS_a$: $\{B, time_1, Au_a\}K_a, TGT$。

(1.2) $AS_a \xrightarrow{M1.2} AS_h$: $AS_a, \{A, 时间\}K_{ah}$。

(2.1) $AS_h \xrightarrow{M2.1} AS_a$: $\{K_{A,\,IAS}, time_2, T_{A,\,IAS}\}K_{ah}.(T_{A,\,IAS} = \{IAS_h, A, address_a, K_{A,\,IAS}, time_2\}K_{hh})$。

(2) $AS_a \xrightarrow{M2} A$: $\{K_{A,\,IAS}, time_3, T_{A,\,IAS}\}K_a$。

(3) $A \xrightarrow{M3} IAS_h$: $\{B, time_4, Au_{A,\,IAS}\}K_{A,\,IAS}, T_{A,\,IAS}$。

(4) $IAS_h \xrightarrow{M4} IAS_v$: $IAS_h, address_{IAS_h}, S_{IAS_{hv}}$。

(5) $IAS_v \xrightarrow{M5} IAS_h$: $\{Cert-IAS_v, S_{IAS_{vh}}, sign(SK_{IAS_v}; h(S_{IAS_{hv}}, S_{IAS_{vh}}))\}K_{IAS_{vh}}$。

(6) $IAS_h \xrightarrow{M6} IAS_v$: $\{Cert-IAS_h, B, sign(SK_{IAS_h}; h(S_{IAS_{hv}}, S_{IAS_{vh}})), N_{IAS_h}\}K_{IAS_{hv}}$。

(7) $IAS_v \xrightarrow{M7} AS_v$: $IAS_v, \{A, B, time_1'\}K_{vv}$。

(7.2) $AS_v \xrightarrow{M7.2} AS_b$: $AS_v, \{A, B, time_2'\}K_{bv}$。

(8.1) $AS_b \xrightarrow{M8.1} AS_v$: $\{K_{ab}, time_3', T_{a,b}\}K_{bv}.(T_{a,b} = \{A, B, K_{ab}, time_3'\}K_{bv})$。

(8) $AS_v \xrightarrow{M8} IAS_v$: $\{K_{ab}, time_4', T_{a,b}\}K_{vv}$。

(9) $IAS_v \xrightarrow{M9} IAS_h$: $\{B, address_b, K_{ab}, T_{a,b}, N_{IAS_h}+1\}K_{IAS_{vh}}$。

(10) $\mathrm{IAS}_h \xrightarrow{M10}$A: $\{\mathrm{B}, \mathrm{address}_b, K_{ab}, T_{a,b}, \mathrm{time}_4\}K_{\mathrm{A,\ IAS}}$.

(11) $\mathrm{A}\xrightarrow{M11}$B: $\{\mathrm{A}u_{ab}, N_a\}K_{ab}, Ta, b$.

(12) $\mathrm{B}\xrightarrow{M12}$A: $\{N_a + 1\}K_{ab}$.

3.3 协议安全管理

当前提出的密钥分配协议基本上都没有考虑与 OSI 安全结构相结合的问题， W.Fumy 在文献 [8,9] 中指出了这方面存在的问题，并提出了四种建议。根据 W.Fumy 的建议，我们对上述的认证和密钥分配协议的安全管理问题进行了初步探讨。

在 OSI 安全结构中，有许多协议，如 ISO-8073/8473 、 TCP/IP 等都是在网络层或以上的网络层次上执行的，端-端安全加密通常在传输层的底层执行。事实上，应用于网络上层加密的密钥不能在网络下层来分配和协商，而且密钥分配协议必须在执行安全加密协议需要加密密钥时才能执行，因此，考虑将低层认证和密钥分配协议放置传输层的底层。网络中，许多通信协议都提供一些冗余数据空间用于通信双方的协商。Intranet 网络采用 TCP/IP 协议， TCP 协议中建立了三轮握手，而且协议中的冗余空间可以根据需要增加，因此，利用 TCP 报头的冗余字段实现两个 TCP 通信、实体之间的密钥分配是比较容易的，而且对计算复杂度较高的基于公钥体制的密钥交换更为有利 [10] 。因此考虑利用通信协议的冗余来实现网间认证和密钥分配协议。

4 协议安全性分析

在上述协议中，用户和认证服务器的公钥证书是由公证机构签发的。除了公证机构之外，任何人均不了解公证机构的私钥，因此公钥证书不能被公证机构之外的任何人伪造或篡改。

协议中，用单钥算法证实认证密钥携带者的身份。攻击者不了解用户的秘密密钥，不能伪造认证符来假冒用户。公钥签名算法用来证实网间认证服务器的身份，攻击者不知道认证服务器的私钥不能伪造签名。签名的使用还可以有效的防止中间人攻击 [11] 。

在协议中， $N_{\mathrm{IAS}_{ab}}$, $N_{\mathrm{IAS}_{ba}}$, N_{IAS_a}, $N_{\mathrm{IAS}_{hv}}$, $N_{\mathrm{IAS}_{vh}}$, N_{IAS_h}, N_a 均为随机数，每次执行方案都需要改变一次。即使攻击者截获了某些消息，也不能利用它们来假冒协议中的任何实体进行欺诈，因此协议可以防止重放攻击。

协议采用基于公钥技术的初始登录，有效地避免了口令猜测攻击。用户的身份和地址信息在实时认证时加密后传输，这样可以隐藏用户的真实身份，防止攻击者对用户的跟踪，实现匿名传输。

协议在 Intranet 局域网网内和 Intranet 各子网间认证时采用单钥体制，实现简单，速度快； Intranet 和外部 Internet 之间的认证采用公钥体制，有利于整个 Internet 网络和分布式环境的结构简化，并可以极大地消除域间的某些不安全因素，提高网络的整体安全性。

5 结束语

本文对 Internet/Intranet 互联环境的安全模式进行了讨论，根据不同的 Intranet 网络配置，分别提出了相应的解决安全性问题的安全模式，并设计了相应端-端认证和密钥分配协议。协议采用分层式设计，考虑了与 OSI 的安全结构相结合的问题，低层的密钥分配协议改进 Kerberos 协议，在执行加密协议的网络层次上实现；高层的密钥分配协议采用单钥体制或 Diffie-Hellman 密钥交换技术，利用通信协议的冗余来实现。采用文中的安全模式，在企业或部门的网络向 Intranet 转型时，低层则可以采用网络原有的认证协议，只需要对网络客

户机的应用软件稍作修改，并增加一个网间认证服务器，并在数据库中增加一些网间认证服务器的密钥．协议可以在各种远程访问中建立 Intranet 间的端-端保密通信，保证 Internet 上电子商务的安全进行．

参 考 文 献

[1] 徐胜波，王新梅．Internet 网络环境中认证和密钥分配的研究．通信学报，1997, 18(12): 83–88.

[2] ISO 7498-2, Information processing system–Open system intercomnection reference model, security architecture, 1988.

[3] Draft Recommendation X.509, The Directory-Authentication Framework, Version 7, Glouccester.

[4] Chokhani S. Towards a national public key infrastructure. IEEE Comm. Mag., 1994, 32(9): 70–75.

[5] Rivest R, Shamir A, Adleman L. A method for obtaining digital signature and public key cryptosystems. Comm. of ACM., 1978, 21(2): 120–126.

[6] Diffie W, Hellman M E. New direction in cryptography. IEEE Trans. on IT, 1976, IT-22(6): 644–654.

[7] Hwang T, Ku W. Reparable key distribution protocols for internet environments. IEEE Trans. on Comm., 1995, COM-43(5): 1947–1949.

[8] Fumy W. (Local area) Network Security. Computer Security and Industrial Cryptography, Lecture, Notion Computer Science, EAST Course, Belgium: 1991, 211–226.

[9] Fumy W, Leclerc M. Integration of key management protocol into the OSI architecture. Proc.of CS'90: Symposium on Computer Security, Fondazione Ugo Bordoni: 1991, 151–159.

[10] Diffie W. Security for the DoD transmission control protocol. Proc. of Crypto'85, Springer LNCS 218, 1986, 108–127.

[11] Diffie W, Van Oorschot P C, Wiener M J. Authentication and authenticated key exchange. design, code and cryptography, 1992, 120–126.

SECURE AUTHENTICATION AND KEY DISTRIBUTION PROTOCOLS FOR INTERNET/INTRANET ENVIRONMENT

Sun Xiaorong　　Wang Yumin

(*National Key Laboratory on ISN of Xidian University, Xi'an* 710071)

Abstract　In this paper, the solutions to the security issues of Internet/Intranet environment are proposed, and authentication and key distribution protocols are presented, which can be incorporated into the OSI (Open System Interconnection) architecture. The protocol adopt modified Kerberos authentication protocol at the lower sublayer, and design authenticated key exchange protocols using symmetric or asymmetric cryptosystem at the upper sublayer for different solutions. The protocols can be used for remote access applications, thus it is benefit to security manage of Intranet.

Key words　Internet, Intranet, Authentication and key distribution, OSI security architecture

孙晓蓉：　女，1972 年生，博士生，研究方向为通信网的安全保密．

王育民：　男，1936 年生，教授，博士生导师，长期从事信息论、信道编码、密码学以及通信网的安全等方面的研究．