基于地址加密的移动 IPv6 绑定更新认证研究

王 彬[1,2] 刘东苏[1]

(西安电子科技大学 西安 710071)[1] (西安理工大学 西安 710048)[2]

摘 要 移动 IPv6 协议将为下一代互联网中提供有效的移动接入支持。本文对移动 IPv6 的主要安全问题进行了分析,讨论了现存解决方案中存在的问题,提出了一个基于地址加密的移动 IPv6 绑定更新认证方案。最后,对方案的安全性进行了分析。本方案使用了公钥加密算法,但不要求公钥基础设施(PKI)的支持,并可对抗假冒攻击等常见攻击方法。

关键词 移动 IP,绑定更新,认证

A Study of Authentication of Mobile IPv6 Binding Update Based on Address Encryption

WAGN Bin[1,2] LIU Dong-Su[1]

(Xidian University, Xi'an 710071)[1] (Xi'an University of Technology, Xi'an 710048)[2]

Abstract Mobile IPv6 enables a mobile node to access network at any location in next generation Internet. This paper analyzes the main security problems of mobile IPv6 protocol, discusses the problems occurred in the current solving schemes, and proposes a binding update authentication scheme of mobile IPv6 based on address encryption. Finally, a security analysis of the scheme has been made. This scheme is used public key cryptosystem, but it is not need the support of public key infrastructure (PKI), and can confront popular attacks, such as impersonation attack.

Keywords Mobile IP, Binding Update, Authentication

1 引言

在移动 IPv6[1]中提供了一种路由优化机制,允许任通信结点(CN)向任何移动结点(MN)直接路由数据包。当 MN 接收到一个从家乡代理通过隧道转交的一个数据包,就初始化一个路由优化协议。MN 向 CN 发送一个绑定更新(BU)消息,其中包含了 MN 的家乡地址(HoA)与转交地址(CoA)。CN 将该信息存储在绑定更新高速缓存中,告诉 CN 以后要发往 HoA 的消息将发送到 CoA。这样,MN 与 CN 之间传输的数据包将不需经过家乡代理,实现直接路由。

根据移动 IPv6 的路由优化机制,攻击者 C 可以在某个地址向 B 发送一个虚假的 BU,声称 A 移动到某一地址。如果通信结点 B 相信了该 BU,则将它以后发往 A 的消息直接发送到 C。因此,C 可以截获发给 A 的数据包,并伪装为 A 与 B 进行通信。另外攻击者还可以随意伪造一个 BU 中的 CoA,干扰 B 与 A 之间的通信,实施 DoS 攻击。

因此,为保证 IPv6 路由优化机制的安全实施,必须对 BU 进行认证,即 MN 与 CN 之间的身份认证和 BU 的完整性认证。

2 相关工作

为解决 IPv6 路由优化机制中存在的安全问题,已经提出了以下的一些解决方法:

T. Aura 提出了一种基于返回路由能力测试的 BU 认证[2]。协议中要求 MN 必须向 CN 返回一个由 CN 发送到其 HoA 的值 Ko,CN 验证 MN 能否从其 HoA 收到消息,可防止 DoS 攻击。该方案的安全性在于,CN 必须验证 MN 能否从其家乡代理接收到 Ko。对攻击者来说,要伪造 BU,则必须有能力截获 Ko,因此使得大量潜在的威胁急剧减少。但该方案不能完全排除假冒攻击。

P. Nikander 等人提出了一种基于返回双重路由能力的 BU 认证协议[3],CN 收到来自 MN 的绑定更新初始化请求后,分别要向其 HoA 和 CoA 各发送一条消息,要求由两条信息中的信息生成密钥,并使用该密钥对绑定更新消息进行加密。攻击者只有同时截获两条消息,才能计算出加密密钥。由于两条消息经过了不同的路由,攻击者很难同时截获。但该方案同样存在两条消息被截获的风险性。

R. Deng 等人提出了一个基于公钥的认证协议[4],其主要特点是使用了由家乡链路发布的公钥证书,证书中主体姓名为家乡链路子网前缀,并将公钥与 MN 的 HoA 绑定。每个家乡链路有一个公钥/私钥对,并从 CA 获得一个公钥证书 PKC。该协议主要的问题是需要有一个可信的 CA 为家乡链路发布公钥证书,而目前尚无一个全球的 CA 解决方案。

3 新的方案

A. Shamir 在 1984 年提出了基于 ID 的加密机制[5],D. Boneh 等人在 2001 年设计出了一个实用的基于身份的加密方案(IBE)[6]。在此基础上,结合 IPv6 路由优化机制及现有安全解决方案中存在的问题,笔者进一步提出了基于地址加密的移动 IPv6 绑定更新认证方案。

其将 MN 的转交地址 CoA 作为 MN 的公钥,密钥生成中心(KGC)由家乡代理(HA)承担,负责为 MN 生成与 CoA 对应的私钥,并产生系统参数。

主要思路如下:

王 彬 博士研究生,讲师,主要研究方向为网络通信、Internet 应用;刘东苏 教授,主要研究方向为网络安全、移动通信系统安全。

3.1 系统初始化

HA 首先完成系统参数的选择，并生成主密钥，算法如下[6]：

1)选定一个安全参数 $k\in Z^+$，生产一个素数 q，两个群 G_1 和 G_2，以及一个双线性映射 $\hat{e}:G_1\times G_1\rightarrow G_2$，选择一个随机数生成器 $P\in G_1$；

2)选择一个随机数 $s\in Z_q^*$，设 $P_{pub}=sP$；

3)选择两个 HASH 函数 $H1:\{0,1\}^*\rightarrow G_1^*$，$H2:G_2\rightarrow\{0,1\}^n$；

系统参数为：$params=\langle q, G_1, G_2, \hat{e}, n, P, P_{pub}, H1, H2\rangle$；

主密钥为：$s\in Z_q^*$。

3.2 MN 私钥生成协议

当 MN 移动到一个新的外地链路后，将得到一个新的转交地址 CoA。MN 需要其家乡代理为其生成新 CoA 对应的私钥，并获得用于加解密的系统参数 params。MN 与 HA 之间的信息传输都用双方的共享密钥 $K_{MN\text{-}HA}$ 保护，共享密钥的获得可通过 IPSec 实现。

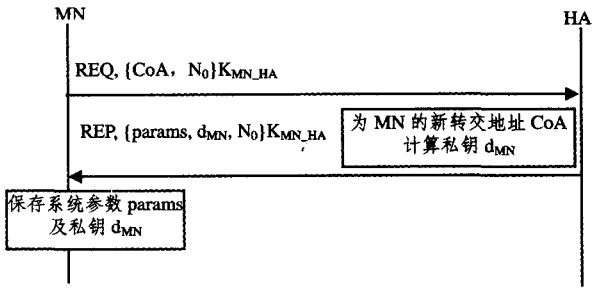

图 1 MN 私钥生成协议

协议过程如图 1 所示。其中：REQ：私钥生成请求消息；REP：私钥生成应答消息；N_0：MN 生成的随机数，用于消息的新鲜性保护。

MN 私钥 d_{MN} 的生成算法：

1) 计算 $Q_{CoA}=H1(CoA)\in G_1^*$；

2)计算 $d_{MN}=sQ_{CoA}$。

3.3 绑定更新认证协议

当 MN 要与某个通信结点 CN 进行通信时，运行图 2 所示绑定更新认证协议。

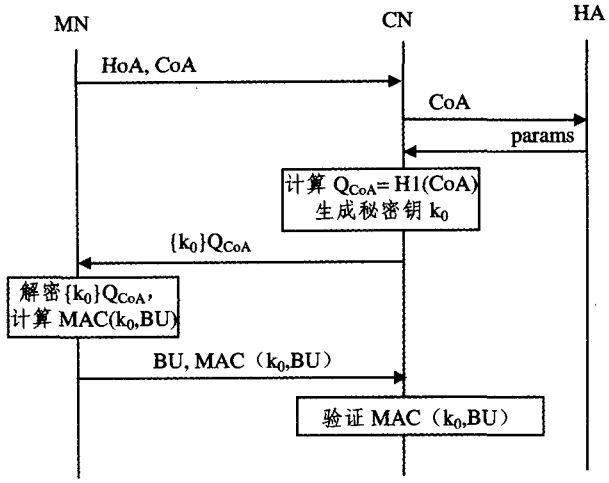

图 2 绑定更新认证协议

MN 首先向 CN 发送绑定更新初始化请求，包括自己的转交地址 CoA 和家乡地址 HoA。CN 接收到 MN 的初始化请求后，要向 MN 的家乡代理获取系统参数 params，并对生成的秘密钥 k_0 进行。加密算法如下：

1) 计算 $Q_{CoA}=H1(CoA)\in G_1^*$；

2)选择随机数 $r\in Z_q^*$；

3)计算密文 $C=\langle rP, k_0\oplus H2(g_{CoA}^r)\rangle$，

其中 $g_{CoA}=\hat{e}(Q_{CoA}, P_{pub})\in G_2^*$。MN 收到加密消息后，用自己的私钥进行解密，得到秘密钥 k_0。解密算法如下：

假设密文 $C=\langle U, V\rangle$，其中 $U=rP$，$V=k_0\oplus H2(g_{CoA}^r)$，

计算 $k_0=V\oplus H2(\hat{e}(d_{MN}, U))$。

秘密钥 k_0 用于保护绑定更新 BU 的完整性，并实现对 MN 身份的认证。

4 安全性分析

(1)MN 私钥生成协议中 MN 与 HA 之间的相互认证与私钥 d_{MN} 的安全传输依赖于双方共享的密钥 $K_{MN\text{-}HA}$，而 $K_{MN\text{-}HA}$ 的协商可通过 IPSec 实现。同时，引入随机数 N_0，可实现消息的新鲜性保护，有效的防止的重放攻击。

(2)绑定更新认证协议中 MN 身份的认证依赖于 HA 为 MN 产生的公钥/私钥对 Q_{CoA}/d_{MN}。CN 用 MN 的公钥 Q_{CoA} 加密消息 k_0，因此只有合法的 MN 才能正确解密并得到 k_0。

(3)绑定更新消息 NU 的保护依赖于 MN 与 CN 之间共享的会话密钥 k_0。CN 收到 MN 发送的消息 BU，MAC(k_0，BU)后，重新计算 MAC(k_0，BU)，若与收到的消息相等，则认为认证成功。

结束语 基于地址加密的移动 IPv6 绑定更新认证方案较好地解决了 MN 与 CN 之间的身份认证和 BU 的完整性认证问题，对比现有安全解决方案，可对抗假冒和密钥截获等常见攻击形式，并避免了对 PKI 支持的要求。该方案在实验环境中进行了模拟测试，将在 CERNET2 环境中进一步进行测试。

参 考 文 献

1 Johnson D, Perkins C, Arkko J. Mobility Support in IPv6. RFC3775, 2004

2 Aura T. Mobile IPv6 Security. http://research.microsoft.com/users/tuomaura/publications/aura-protocols02.pdf

3 Nikander P, Arkko J, Aura T, et al. Mobile IP version 6 Route Optimization Security Design. IEEE Vehicular Technology Conference, 2003,3(10): 2004～2008

4 Deng R, Zhou J, Bao F. Defending Against Redirect Attacks in Mobile IP. In:CCS'02, 2002.12

5 Shamir A. Identity-based cryptosystems and signature schemes. In:Proc. CRYPTO 1984, LNCS vol. 196, Springer, 1984,196: 47～53

6 Boneh D, Franklin M. Identity-based encryption from the Weil pairing. SIAM J. of Computing,2003,32(3):586～615