

动态 IP 环境下 IKEv2 扩展设计与改进

高振栋

(无锡科技学院, 江苏 无锡 214026)

摘要: IKEv2 作为 IKE 的替代者极大地增强了 IPSec VPN 网关之间隧道建立过程的安全性。但 IKEv2 和 IKE 一样都不能在动态 IP 环境下进行密钥交换。介绍了 IKEv2 的协商过程, 在此基础上讨论了文中提出的动态 IP 环境下 IKEv2 扩展方案的设计与改进。经过改进的扩展方案可以很好地适应动态 IP 环境下的协商过程, 扩大了 IKEv2 的应用范围。

关键词: IPSec; IKEv2; SA; 动态 IP

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2008)12-0162-04

Design and Realization of IKEv2 with Dynamic IP Address

GAO Zhen-dong

(Wuxi Professional College of Science and Technology, Wuxi 214026, China)

Abstract: As a replacer of IKE, IKEv2 enhances the safety of the procedure of establishing the tunnel between IPSec VPN gateways greatly. But not only IKE but also IKEv2 can not proceed the key exchange with dynamic IP address. First introduces the negotiation procedure of IKEv2, then discusses the design and realization of IKEv2 extended scheme with dynamic IP address in detail on the base of standard IKEv2.

Key words: IPSec; IKEv2; SA; dynamic IP

0 引言

在现实的网络环境中, 安全问题举足轻重。IKE 协议作为密钥交换协议可以在 VPN 网关之间(不安全的公共网络)建立安全的通讯隧道。IKE 是一种混合型协议, 其复杂性一直受到业界广泛的批评。IKE 还存在易受攻击、功能冗余等不足。目前, IKEv2^[1]作为 IKE 的替代者日益受到业界的普遍关注。

IKE 和最新的 IKEv2 都只能在固定 IP 地址的情况下进行安全关联(SA)的协商, IKEv2 的扩展草案 MOBIKE^[2]虽然提出了相应的扩展方案, 但是草案只是考虑了 SA 协商之后地址改变的情况, 这极大地限制了动态密钥协商机制的应用。为了解决以上局限, 对 IKEv2 协议进行了进一步地扩展, 提出了一种全新的 IKEv2 动态协商过程, 从而提高了协商能力。

1 原有的 IKEv2 协商过程

和 IKE 类似, IKEv2 同样也存在两个协商阶

段^[3]。第一个阶段称为初始交换阶段, 主要协商 IKE-SA, 第二阶段称为协商子 SA 交换阶段, 主要协商 CHILD-SA, 即 IPSec SA。另外, 还有信息交换用来在 IKEv2 协商双方之间通知一些出错、配置、删除等信息。

1.1 初始交换

在第一阶段中协商双方主要进行两次消息交换, 一共 4 条消息交互。第一次消息交换称为 IKE-SA-INIT 交换, 而第二次称为 IKE-AUTH 交换^[4]。

IKE-SA-INIT 交换过程如下所示。

$I \rightarrow R: HDR, SAi1, KEi, Ni$

$I < - R: HDR, SAR1, KEr, Nr, [CERTREQ]$

第一条消息中的 HDR 表示 IKEv2 消息头, SAi1 包含了发起者针对 IKE-SA 的提案建议, 提案中包括加密算法、认证算法、DH 组等内容, KEi 包含了发起者的 Diffie-Hellman 公开值, Ni 则表示发起者的 Nonce 值。

响应者接收到发起者发送的消息后在 SAi1 中选择某种提案形成 SAR1, 并且将 KEr 和 Nr 分别作为响应者的 Diffie-Hellman 公开值以及 Nonce 值发送给发起者。在响应消息中, 响应者还可以包含可选的证书请求载荷发送给发起者。

收稿日期: 2008-04-14

基金项目: 江苏省自然科学基金项目(BK2004039)

作者简介: 高振栋(1976-), 男, 江苏无锡人, 硕士, 讲师, 研究方向为计算机网络。

IKE_SA_INIT 交换完成之后,协商双方可以计算种子密钥 SKEYSEED 以便得到 7 个其他秘密:SK_d,SK_ai,SK_ar,SK_ei,SK_er,SK_pi,SK_pr。

随后进行的 IKE_AUTH 交换使用前面协商得到的 IKE_SA 中包含的加密、认证算法以及密钥进行保护,并且使用认证载荷对已经结束的 IKE_SA_INIT 交换过程进行认证,最终协商得到第一个 CHILD_SA,即 IPsec SA。如下所示,IKE_AUTH 交换过程中的 2 条消息是由 IKEv2 消息头 HDR 以及一个加密载荷组成,在这个加密载荷中包含了身份载荷(ID)、可选的证书载荷(CERT)以及证书请求载荷(CERTREQ)、认证载荷(AUTH)、安全关联载荷(SA)、流量选择载荷(TS)等。SK{}表示被包含的载荷均被相应方向的 SK_e 和 SK_a 加密和认证保护。

I → R: HDR, SK{IDi, [CERT,][CERTREQ,]
[IDr,]AUTH,SAi2,TSi,TSr}

I ← R: HDR, SK{IDr, [CERT,]AUTH,SAr2,
TSi,TSr}

1.2 协商子 SA 交换

这一交换过程作为有额外的 IPsec SA 或完美向前保密(PFS)需求时的一种交换类型,对应原有 IKE 协商的第二阶段,它可由任一协商方在初始交换完成之后发起。如下所示,该交换包含了两条消息,第一条消息发送 SA 提案,交换 Nonce 和流量选择符 TSi 和 TSr。第二条消息对 SA 提案和流量选择符进行响应,交换 Nonce 值,同时能根据 PFS 的需要可选地进行 Diffie-Hellman 交换^[5]。

I → R: HDR, SK{[N], SA, Ni, [KEi], [TSi, TSr]}

I ← R: HDR, SK{SA, Nr, [KEr], [TSi, TSr]}

一次 CHILD_SA 协商可以得到 4 个安全关联,即进入 ESP SA、进入 AH SA、外出 ESP SA、外出 AH SA。

1.3 信息交换

在 IKEv2 协商过程中,协商双方可能希望互相传递某些控制信息或者通知某些特定事件,而信息交换就是为了完成此类消息交互而设计的。信息交换必须在初始交换完成之后进行,并且由协商得到密钥保护。如下所示,协商双方分别交换了可选的通知载荷(N)、删除载荷(D)、配置载荷(CP)等携带控制信息的载荷数据^[6]。

I → R: HDR, SK{[N,][D,][CP]}

I ← R: HDR, SK{[N,][D,][CP]}

2 扩展的 IKEv2 协商过程

以上介绍的是标准的 IKEv2 协商过程,它是在保

持原有 IKE 大部分特性的基础之上改进、发展而形成的新一代 IKE 密钥协商协议。

如图 1 所示,本课题提出的 IKEv2 扩展方案在密钥协商双方之间引入了具有固定 IP 地址的协商第三者。这个协商第三者作为 IP 服务器专门存放各个参加 IKEv2 协商的 VPN 网关或者移动客户端主机当前使用的 IP 地址。每个参加协商的网关或者移动客户端首先通过安全可靠的协议通讯在 IP 服务器中注册自己当前的 IP 地址,并取得同组的各上线网关或者客户端的当前 IP 地址。接下来发起通讯的这一方,同样通过可靠的协议交互获得对等端网关的 IP 地址,开始进行 IKEv2 协商以建立相应的 VPN 隧道并进行通讯。

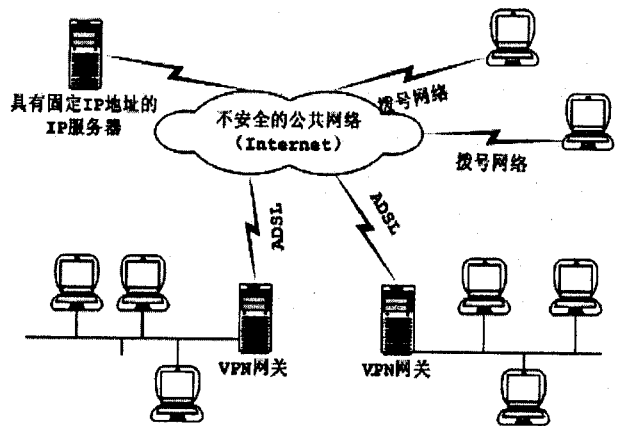


图 1 动态地址 VPN 系统

2.1 数据结构改变

为了适应动态 IP 地址环境,原有的相关数据结构需要进行相应的改动和扩展。首先为每个 VPN 网关或者移动客户端分配一个标识自己身份的 ID 号 (HOST_ID),然后再为它们颁发一个与各自 HOST_ID 号码绑定的数字证书,即这些数字证书中存在各自的 HOST_ID,定义如下:

```
{
    int id; /* 原有证书中包含的 ID */
    int host_id; /* 新增加的 HOST_ID */
    .....
}
```

由于在动态 IP 地址环境下,原有的 IP 地址已经不能准确表示各方的身份,所以在内核中的安全关联数据库(SAD)和安全策略数据库(SPD)中所有主机的 IP 地址修改为分配的 HOST_ID,网段的 IP 地址改为该网段 VPN 网关的 HOST_ID。

另外,在新引入的 IP 服务器内核中增加一个 ID 与 IP 地址的映射数据库,文中称之为 ID-IP 数据库,简称 IDPD。

载荷中的发送者的 HOST- ID 以及当前 IP 地址,然后利用内核通讯机制写入内核中的 IDPD 中,以便后续的使用。

(4) 与之建立 VPN 隧道的 VPN 网关列表。

各个 VPN 网关或者

扩展 IKEv2 配置载荷中的配置属性的种类，增加以下新类型：

(2) CURRENT_IP_ADDRESS 用于表示配置载荷传送的是协商方当前的 IP 地址信息。

IP 服务器接收到提交消息后,提取出包含在配置

[illegible]

图 2 配置载荷(CP)的格式

各个 VPN 网关向 IP 服务器注册 IP 地址之后, VPN 网关的 IKEv2 守护进程向作为响应方的 VPN 网关的 IKEv2 守护进程发起进行 IPSec SA 的协商请求。但是,在动态 IP 地址的网络环境下,对方网关的 IP 地址是不固定的,所以响应方网关必须向 IP 服务器索取发起者当前的 IP 地址。考虑到与服务器的通讯是在公网上进行,为了保障通讯过程的安全性,它们之间的通讯采用在提交阶段协商的 IKE-SA 进行保护。

首先定义一个新的 IKEv2 载荷类型,即 IP 地址载荷。格式如图 3 所示。

[illegible]

图 3 IP 地址载荷格式

图 3 中的 ID 域为该 IP 地址载荷发送方的 HOST_ID, 当前 IP 地址则为对应的 IP 地址。

如下所示, IKEv2 协商发起者使用 IKE_SA 中的密钥保护传送给 IP 服务器的数据。IDi 和 IDr 分别表示发起者和发起者索要地址的协商对方的身份载荷, 其中包含了各自的 HOST_ID。IPr 表示包含协商对方当前 IP 地址的 IP 地址载荷。

$$I < -R:HDR,SK\{IP_r\}$$

IP 服务器接收到发起者的请求后,使用 PF_KEY 内核通讯机制根据 IDr 查询内核中的 IDPD 得到对应的 IP 地址,然后将信息反馈给发起者。同时,将 IDi 和 IDr 记录在 IDPD 中,以便响应者地址发生改变后能够通知发起者。

发起者得到协商对方的 IP 地址后,便向协商对方发起 IKEv2 协商请求。如下所示,在第一条消息中增

加了证书载荷,这个证书载荷中包含了分配给发起者的 HOST_ID。

$I \rightarrow R: HDR, SA_i, KE_i, Ni, [CERT_i]$

$I \leftarrow R: HDR, SA_r, KE_r, Nr, [CERTREQ]$

响应者接收到发起者的 HOST_ID 后,向 IP 服务器发送请求要求根据发起者的 HOST_ID 查询发起者当前的 IP 地址,这样,IKEv2 发起者和响应者之间的协商就被转化成固定 IP 地址的情况,后续的协商过程和标准的 IKEv2 类似。

协商结束后,参加协商的 VPN 网关各自将协商好的 IPsec SA 通过 PF_KEY 通讯机制写入内核中的安全关联数据库中,以便以后再次使用。

2.4 地址通知机制

VPN 网关注册 IP 地址后由于某种原因,自身的 IP 地址可能再次发生变化。另外,网络、VPN 网关可能出现故障以至无法正常通讯,这可能导致使用过时的安全关联从而降低了系统的安全性。为此,扩展方案提供一个选项,允许管理员根据具体情况设置各个 VPN 网关每隔一个时间周期便向 IP 服务器提交自己当前使用的 IP 地址,消息交互和提交阶段一样。考虑到网络通讯效率,IP 服务器第一次接收到 VPN 网关提交的地址后必须发送反馈消息,但是对于后续的消息,只要提交的地址没有发生改变,服务器便可以不用发送反馈消息。另外,如果某 VPN 网关提交的地址发生变化,IP 服务器便会根据 IDPD 得知和该网关进行

IKEv2 协商的所有 VPN 网关,也就可以通知这些 VPN 网关,以便它们做出相应的处理。

3 结束语

提出了针对 IKEv2 的扩展设计与实现,使 IPsec VPN 网关可以不必限制在固定 IP 环境下进行隧道建立,扩大了 VPN 的应用范围,与扩展前的 IKEv2 具有更广阔的应用前景。

参考文献:

- [1] Microsoft C. Kaufman. RFC4306. Internet Key Exchange (IKEv2) Protocol[S]. 2005.
- [2] Kivinen T, Tschofenig H. RFC4621. Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol[S]. 2006.
- [3] 陈卓,张正文. Internet 密钥交换协议 IKEv2 研究[J]. 计算机应用与软件, 2008, 25(2): 269-270.
- [4] 韩旭东, 汤隽, 郭玉东. 新一代 IPsec 密钥交换规范 IKEv2 的研究[J]. 计算机工程与设计, 2007, 28(11): 2549-2552.
- [5] 杜春燕, 周晓东, 陆建德. 一种基于 IKEv2 的 IPsec 远程访问实现方案[J]. 电脑与电信, 2007(9): 4-6.
- [6] Lari I A, Jorma Y, Pekka L. A Proposal to Improve IKEv2 negotiation[C]//Emerging Security Information, Systems, and Technologies, 2007 International Conference. Valencia, Spain: [s. n.], 2007: 169-174.

(上接第 161 页)

具有伪造 II 地址的报文可能发生在 Internet 上的任何区域。因此要设置 IP 地址伪造就需要在 Internet 的各级网络采用包过滤技术,报文构造方式设置相应的过滤规则,以截获这些伪造 IP 地址的报文,解除 IP 的欺骗^[5]。

3.3 解除信任关系

从 TCP 通信过程中,可以看出,两个主机之间的通信主要是通过它们 IP 地址建立起来的认证机制,那么解除这种认证关系,取而代之的是一种基于加密的可信第三方安全协议的认证机制,以增强身份鉴别功能。

3.4 防止序列号被猜测

TCP 序列号猜测成功的关键在于,系统为每个连接产生的初始序列号 ISN 不具有随机性。因此,采用新的 ISN 序列号生成技术,同时对生成的 ISN 进行 HASH 映射,增加序列号的随机和保密性。

3.5 增加认证机制

正常情况下的两个计算机的数据通信过程中,增

加两方通信的认证机制,周期性地作一次身份认证,以防在数据传送过程的身份冒认出现。

4 结束语

文中做了 TCP 的三次握手协议的安全漏洞的分析及基本实现,针对性地分析了为解决这种综合网络攻击而采用的几种防范措施,为网络安全防预提供了可行的方法。

参考文献:

- [1] 黄发文,徐济仁,陈家松. 计算机网络安全技术初探[J]. 计算机应用研究, 2002, 19(5): 46-48.
- [2] Wright G R, Stevens W R. TCP/IP 详解 卷 2: 实现[M]. 陆雪莹等译. 北京: 机械工业出版社, 2000.
- [3] 吉文华, 于汇敏. 防 Dos 攻击的算法的分析和实现[J]. 计算机应用, 2003, 23(6): 90-91.
- [4] 寺田真俊, 菅岛信. TCP/IP 网络安全篇[M]. 王庆译. 北京: 科学出版社, 2003.
- [5] 蔡敏, 叶震, 徐吉斌. 协议分析技术在入侵检测中的应用[J]. 计算机技术与发展, 2007, 17(2): 239-241.