安全 ARP 的 Clark-Wilson 模型化*)

陈小岩[1] 贺也平[2] 徐梓耀[2] 邓灵莉[2]

(中国科学技术大学 合肥 230026)[1] (中国科学院软件研究所 北京 100080)[2]

摘 要 ARP 协议漏洞严重威胁着 TCP/IP 的安全,一些基于对称或非对称密钥机制的安全 ARP 协议被相继提出。本文介绍了 ARP 协议攻击的原理和几个最出名的基于对称或非对称密钥机制的安全 ARP 协议,引入 Clark-Wilson 商业模型对 ARP 的完整性状态进行了分析,把改进协议 Clark-Wilson 模型化,在模型化的过程中找到了它们不能通过 Clark-Wilson 商业模型验证规则的关键点,并根据 Clark-Wilson 商业模型提出的经典场景,给出了相应的攻击场景。

关键词 ARP,安全 ARP,Clark-Wilson 模型,完整性

Clark-Wilson Modeling of Secure ARP

CHEN Xiao-Yan[1] HE Ye-Ping[2] XU Zi-Yao[2] DENG Ling-Li[2]

(University of Science and Technology of China, Hefei 230026)[1] (Institute of Software, Chinese Academy of Science, Beijing 100080)[2]

Abstract Vulnerabilities in the ARP protocol became a threat to TCP/IP security. Countermeasures to these vulnerabilities based on Symmetric-Key Cryptography or Asymmetric-Key Cryptography are proposed recently. In the present paper, the principle of ARP attacks is analyzed, and the most popular secure ARP protocols are discussed. Clark-Wilson commercial model is introduced to analyze the integrity of ARP. While applying Clark-Wilson commercial model to the ARP integrity policy, all of the secure protocols failed to pass the rules of Clark-Wilson model. With the classical scenes of Clark-Wilson model, corresponding attack scenes are presented.

Keywords ARP, Secure ARP, Clark-Wilson model, Integrity

1 引言

随着计算机技术和互联网技术的不断推广应用,网络逐渐成为人们日常生活中不可缺少的部分。通过网络人们可以完成浏览信息、收发邮件、远程信息管理、与外界进行电子商务交易等活动。但是,由于网络的开放性、资源的共享性、联结形式的多样性、终端分布的不均匀性以及网络边界的不可知性,网络中必然存在众多潜在的安全隐患。随着基于局域网的病毒和木马的传播,ARP 漏洞的问题日趋严重。

2 ARP 攻击

IPv4 中的 ARP[2](Address Resolution Protocol),即地址解析协议,负责网络逻辑 IP 地址和网卡物理 MAC 地址(Medium Access Control)之间的转换。将网络层(IP 层,即 ISO/OSI 中的第三层)的 32 位 IP 地址解析为数据链路层(MAC 层,即 ISO/OSI 中的第二层)的 48 位(特殊网络除外)MAC 地址,建立 IP 和 MAC 之间的一一对应关系。

当网络中一台主机要向另一台主机或者路由器发送数据时,发送方必须知道接收方的 MAC 地址。如果发送方没有在本地的 ARP 缓冲中找到接收方的 MAC 地址,就需要广播 ARP 请求。ARP 请求中包含了接收方的 IP 地址。当接收方接收到了这个请求,就会做出 ARP 应答,应答中就包含了应答方的 IP 地址和 MAC 地址(用〈IP, MAC〉对表示)。为了避免每次数据发送之前都需要进行 ARP 请求的广播,发送方会将查询得到的结果保存到本地的 ARP 缓存中,并以老化机制加以维护。

由于 ARP 协议的设计初衷是为了方便数据传输,设计前提是在网络绝对安全的情况下进行工作。然而,这种设计前提只存在于互联网发展的初期,现在几乎不存在了。ARP 协议是一个无状态的协议,没有任何认证过程,非常脆弱[3,4]。目前的攻击主要有以下四类:

(1)地址冲突攻击[5]

这是一类最简单的 ARP 攻击。向被攻击机器发出包含与被攻击机器相同的 IP(或 MAC)的 ARP 报文,被攻击机器就会以为局域网上存在相同 IP(或 MAC)的机器,一些操作系统实现便发出 IP(或 MAC)冲突警告,并中止网络连接。

(2)拒绝服务攻击[5]

这类攻击的实现也非常简单。攻击者只需要向被攻击者发送〈IP_i, MAC_j〉对的 ARP 报文,其中 MAC_j 为伪造的 MAC 地址,被攻击者将把〈IP_i, MAC_j〉写入自己的 ARP 缓存。以后被攻击者发往 IP_i 的所有报文将发往伪造的 MAC_j,对被攻击者的 DoS 攻击便形成了。如果 IP_i 是网关的话,被攻击者将无法正常访问外部。

(3)嗅探攻击[5]

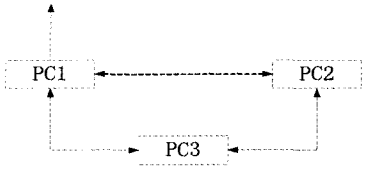

图 1 嗅探攻击

这类攻击也仅仅复杂一点。如图 1,攻击者 PC3 和被攻

*)科技部攻关项目(编号 2005BA113A02)、发改委项目"安全系统软件产业化"资助。**陈小岩** 硕士研究生,主要研究方向为系统软件和信息安全;**贺也平** 研究员,主要方向为安全操作系统;**徐梓耀** 博士研究生,主要研究方向为系统软件和信息安全;**邓灵莉** 博士研究生,主要研究方向为系统软件和信息安全。

击者 PC1、PC2 在同一个局域网中，图中的虚线为攻击前 PC1 和 PC2 之间的直接通信线路。PC3 向 PC1 持续发送〈IP2，MAC3〉对的 ARP 报文，向 PC2 持续发送〈IP1，MAC3〉对的 ARP 报文。PC1 将把发送到 PC2 的报文发送到攻击者 PC3 的网卡 MAC3，PC2 将把发送到 PC1 的报文发送到攻击者 PC3 的网卡 MAC3。PC3 再做转发，便实现了对 PC1、PC2 之间通讯的嗅探，攻击后的通信线路如图 1 中的实线所示。

(4)伪造地址攻击[1]

伪造地址攻击为本人的创新技术，实现起来也不算复杂。PC3 在对 PC1(网关)、PC2 实施了嗅探攻击后，PC3 利用虚拟网卡技术和包转发技术使 PC3 的高层应用透明地使用 PC2 的地址连接网络。实施攻击后，PC3 在不需经过 PC2 允许、完全不影响 PC2 正常使用的情况下，双方同时用 PC2 的 IP 连接网络。PC2、PC3 在完全透明的情况下共用同一个地址，而事先无需在被攻击机器上做任何设置。

相比于前三种 ARP 攻击，伪造地址攻击的危害更显而易见：基于局域网 IP 地址的安全认证将不再受保护，基于 IP 地址的网络计费服务面临着巨大的挑战，黑客的痕迹随时可以抹去。

可以毫不夸张地说，ARP 协议漏洞带来的安全威胁已经超过了它的灵活性和实用性。

3 安全 ARP

抵御 ARP 攻击最直接的办法是做〈IP，MAC〉对绑定。而做〈IP，MAC〉对绑定实质上就是否决、废弃了 ARP 协议，给局域网的灵活性带来很多不便。为了解决这个问题，有人提出了基于对称加密或非对称加密的安全 ARP 协议，希望能从根本上解决 ARP 的安全问题。

Gaoda 和 Huang 提出了一种基于对称加密的安全 ARP[6]。一台安全服务器上维护着所有的〈IP，MAC〉对，所有的 ARP 请求、应答都在客户机和服务器之间进行。用户凭与服务器共享的密钥，可以通过 Invite、Accept 报文来声明自己的〈IP，MAC〉对。

S-ARP(Secure ARP)[7]用了一种非对称加密机制，每个 IP 有一个私钥。公钥存在安全的权威密钥发布服务器 AKD (Authoritative Key Distributor)中。AKD 上保存了所有客户机〈IP，PublicKey〉的二元组数组。S-ARP 对 ARP 应答做了修改，在包末尾附上时间戳和签名。请求方通过从 AKD 上获得的 IP 对应的公钥，可以验证 ARP 应答是不是该 IP 发出的。

T-ARP(Ticket-based ARP)[8]是另一种基于非对称加密机制的安全 ARP 协议。在 T-ARP 中，采用一个本地票据代理 LTA(Local Ticket Agent)的一对〈公钥、私钥〉来进行验证。所有〈IP，MAC〉对都存放在 LTA 中，每个客户机初始化时都从 LTA 得到一个带有时间戳和有效期的 LTA 签了名的证书。应答方在 ARP 应答末尾附上该票据，请求方通过 LTA 的公钥可以验证该 ARP 应答的有效性。

4 Clark-Wilson 商业模型

ARP 协议漏洞的实质是对 ARP 缓存的写入破坏了完整性。基于这一点，我们引入 Clark-Wilson 商业模型[9]对 ARP 进行分析。

在商务安全领域，Clark 和 Wilson 于 1987 年提出的 Clark-Wilson 完整性策略被认为是真正意义上的完整性目标、策略和机制的起源，可以有效满足企业信息系统所追求的完整性安全需求。

Clark-Wilson 模型是一个完整性的应用级模型，它可以保证商务数据的完整性，提供一个评估商用系统安全性的框架。Clark 和 Wilson 把系统中的数据分为两类：受控数据项(CDI)和非受控数据项(UDI)。CDI 是有完整性保证的对象，UDI 是没有经过完整性策略验证的数据(比如用户的键盘输入)。有两类过程会对数据项进行操作和保护。首先是完整性验证过程(Integrity Certification Procedure，简称 IVP)，来验证数据是否处在一种有效状态(也就是说，它们是用户或者拥有者确信它们未被非可信改变)。第二个过程是转换过程(Transformation Procedure，简称 TP)，或者称为合式事务(Well-formed Transaction)，它使数据项从一个有效状态转换到另一个有效状态。

Clark-Wilson 模型中控制数据完整性的两个主要思想是合式事务和职责分离。

为了确保信息系统满足和保持完整性，Clark-Wilson 模型声明了必需遵循的完整性监视规则作为证明性规则(Certification Rules)，完整性保持规则作为强制性规则(Enforcement Rules)。这些规则为：

规则 1 (C1)IVP 运行时要保证所有的 CDI 处于有效状态。

规则 2 (C2)所有的 TP 必须被证明是有效的，即要维护关系

[TP1，(CDI_a，CDI_b，CDI_c，…)]。

规则 3 (E1)TP 只能操作指定的 CDI。

规则 4 (E2)用户只能通过指定的 TP 访问 CDI，即要维护关系

[UserID，TP1，(CDI_a，CDI_b，CDI_c，…)]。

规则 5 (C3)要验证 E2 中的关系满足职权分离的原则。

规则 6 (E3)系统必须鉴别每个试图执行 TP 的用户身份。

规则 7 (C4)所有 TP 的所有行为信息能证明被只可追加的日志 CDI 记录，可以重构一个操作。

规则 8 (C5)作用于 UDI 上的 TP 能够被证明：要么转化为 CDI，要么被拒绝。

规则 9 (E4)只有能认证实体的代理(管理员)才可以改变实体之间的关系。

5 Clark-Wilson 模型化

要判断一个安全 ARP 的好坏，首先要对 ARP 的目标做一个严格定义，看各个改进版本是否符合，符合了多少。ARP 的目标是：给定 IP 地址，能正确地找到在局域网中对应的 MAC 地址。

把 ARP 协议 Clark-Wilson 模型化，CDI 为符合系统规定的完整性状态的〈IP，MAC〉对，UDI 为不符合系统规定的完整性状态的〈IP，MAC〉对。IVP 为验证〈IP，MAC〉对的进程，TP_i 为用户 i 更改〈IP，MAC〉对的进程。下面将逐个分析 CDI 两个要素在 ARP 中的体现。

ARP 中声称更改 IP 分为两种：一种是善意地更改 IP，例如 DHCP 动态分配的地址；一种是恶意地更改 IP 为网络上合法用户的 IP。这两种更改 IP 有明显的区别：善意地更改 IP 所声称的 IP 必然是当前网络上不存在的；相反，恶意地更改 IP 所声称的 IP 必然是当前网络上存在的，或者是曾经在网络上存在且有利用价值的。

同样，ARP 中声称更改 MAC 也分为两种。一种是善意地更改 MAC，例如用户更换一块新的网卡；一种是恶意地更改 MAC 为网络上合法用户的 MAC。善意地更改 MAC 所声

称的MAC必然是当前网络上不存在的。相反，恶意地更改MAC所声称的MAC必然是当前网络上存在的，或者是曾经在网络上存在的且有利用价值的。这里有一点要注意的是用户A更换一块B卸下来的网卡，这种情况并不违背我们的模型分析。因为严格地说，网卡从B卸下来是需要做撤回MAC工作的。在B执行了撤回工作后，A便属于善意地更改MAC了。

一个严格的、实用的ARP环境应该允许善意的更改IP、MAC，而杜绝恶意地更改IP、MAC。有了这个前提，完整性状态就可以定义为：当前数据库（包括在线的和离线的）满足且仅满足，不存在同样的IP且不存在同样的MAC。

下面，我们对传统ARP和几种安全ARP协议Clark-Wilson模型化。

5.1 传统的ARP

传统的ARP是无状态、没有任何认证机制，完全没有完整性状态的概念，也就是说规定的完整性状态就是任意状态，不满足C1，也就失去了Clark-Wilson模型的前提。

5.2 A Secure Address Resolution Protocol

规则1 C1可以满足。由于初始状态为空，不存在冲突的〈IP，MAC〉对，系统处于有效状态，因此IVP可以保证从一个所有CDI有效的状态开始运行。

规则2 C2无法满足。没有有效的措施来保证TP更改的正确性。在这种改进协议里，服务器没有对〈IP，MAC〉对进行检查，假定了注册用户不会做恶意欺骗，不会破坏系统的完整性状态。也就是说，TP的有效性是通过对注册用户的信任来保证的。

顺着这个逻辑，我们可以推出一种攻击。TP可以用自己和服务器共享的秘密值来声明错误的〈IP，MAC〉对。也就是说，注册用户可以牺牲自己的信任来达到攻击的目的，或者说，如果用户中了木马或是操作失误，系统的完整性状态就会受到破坏。

因此，这个安全ARP方法不能通过Clark-Wilson模型的验证，也不能保证ARP的安全性。

5.3 S-ARP

规则1 C1可以满足。由于初始状态为空，不存在冲突的〈IP，MAC〉对，系统处于有效状态。因此IVP保证可以从一个所有CDI有效的状态开始运行。

规则2 C2不能满足。用户的私钥是与IP对应，而不与MAC对应的，因此，用户的签名仅仅保证了CDI中IP的正确性，但不能保证CDI中MAC的正确性。所以，用户利用自己的私钥，可以对一个正确的IP和一个伪造的MAC进行签名。IVP不能证明TPi对CDI的操作是有效的。

通过上述分析，可得出一类攻击："嫁祸攻击"。用户A可以向当前局域网的机器（当然不包括B）要求数据传输服务，然后声称自己的MAC更改成了B的MAC，如果其他机器相信A的话，B便需要承受其他所有用户送来的大量数据。

S-ARP已经算是设计得最好的一种安全ARP协议了，但仍然不能通过Clark-Wilson模型来进行验证，其漏洞的本质是CDI的完整性状态没定义好。在S-ARP中，定义的完整性状态为：当前数据库（包括在线的和离线的）满足且仅满足，不存在同样的IP。结果，导致其不允许善意的更改IP，而允许恶意地更改MAC。

通过Clark-Wilson模型的验证，我们可以得出结论：S-ARP也存在安全漏洞。问题的根源是没有定义好CDI的完整性状态。同时，S-ARP也带来一定的限制：用户不能更改自己的IP，更改IP必须同时重新生成公钥/私钥对。

5.4 T-ARP

规则1 C1可以满足。由于初始状态为空，不存在冲突的〈IP，MAC〉对，系统处于有效状态。因此IVP可以保证从一个所有CDI有效的状态开始运行。

规则2 对于C2，作者没有提出一种机制来验证TP是有效的。为了继续用Clark-WilsonN模型进行验证，我们先假定存在一种有效的机制来验证。

规则3 E1无法满足。每个TP都有操作任意CDI的权利，IVP只保证TP提出的CDI在当前有效，而不能限制TP跟CDI的一一对应性。也就是说，如果TP_i先于TP_j提出CDI_j，IVP就允许了TP_i提出CDI_j的合法性而否决TP_j提出CDI_j的合法性。

基于这点分析，不难设计出这样一个漏洞，用户i只要先于用户j提出本该属于用户j的IP或MAC，用户j就失去了提出自己对应的IP或MAC的权利。

规则4 E2是对E1的增强，因此E2就更加不可能通过验证了。在T-ARP，每个用户是对等的，并没有UserID来保证用户指定的TP访问CDI。

所以，T-ARP也不能通过CLARK-WILSON模型的验证。问题的根源是T-ARP中没有分辨每个用户、TP和CDI之间关系的机制，即没能维护[UserID，TP1，(CDI_a，CDI_b，CDI_c，…)]这样一个关系表。

综上所述，目前最著名的安全ARP都没能通过CLARK-WILSON模型的验证，没有达到商业运作的要求。我们利用CLARK-WILSON模型，也确实找出了这几种安全ARP的漏洞。

结论 ARP协议是一个非常重要然而又非常脆弱的协议，新的攻击不断威胁着整个TCP/IP体系。本文利用Clark-Wilson商业模型分析了传统的ARP协议和经典的安全ARP协议，遗憾的是，目前已经提出的几个最著名的安全ARP协议都不能通过Clark-Wilson商业模型的验证。通过对模型化不吻合的关键点的分析，找出了它们的漏洞所在，为下一代的安全ARP设计打下了基础。

参考文献

1 陈小岩. 局域网中透明伪造地址的实现：[内部技术报告]. 中科院软件所

2 Plummer D C. An ethernet address resolution protocol or converting network protocol addresses to 48. bit ethernet address for transmission on ethernet hardware. RFC 826, November 1982

3 Bellovin S M. Security problems in the tcp/ip protocol suite. Computer Communications Review, 1989, 2(19): 32～48

4 Bellovin S M. A look back at security problems in the tcp/ip protocol suite. In: 20th Annual Computer Security Application Conference (ACSAC), December 2004. 229～249

5 Fleck B. Wireless access points and arp poisoning. http://www.cigitallabs.com/resources/papers/download/arppoison.pdf

6 Gouda M G, Huang Chin-Tser. A secure address resolution protocol. Computer Networks, 2003, 41(1): 57～71

7 Bruschi D, Ornaghi A, Rosti E. S-ARP: a secure address resolution protocol. In: Computer Security Applications Conference, 2003, Proceedings, 19th Annual, Las Vegas, NV, USA, 2003. 66～74

8 Lootah W, Enck W, McDaniel P. TARP: ticket-based address resolution protocol. In: Computer Security Applications Conference (ACSAC 2005), 21st Annual. Tucson, Arizona, Dec. 2005. 9

9 Clark D D, Wilson D R. A comparison of commercial and military computer security policies. In: Proceedings of IEEE Symposium on Security and Privacy, Oakland, CA, April 1987. 184～194