ARP协议的描述与TLA验证

李 元，吴 勇，李 祥
（贵州大学 计算机软件与理论研究所，贵州 贵阳 550025）

摘 要：随着计算机网络的发展，网络的安全性日益受到人们的关注。ARP攻击是一种非常专业化的网络攻击方式，它会给网络管理员增加很大的负担，破坏主机数据，窃取主机信息。Lesilie Lamport提出了一种新的逻辑，即行为时序逻辑(TLA)理论体系，运用这种逻辑对软件或协议系统进行建模，在一定程度上减少了由于状态空间爆炸带来的压力，它能在一种语言中同时表达程序与属性。文中介绍了ARP协议，用基于行为时序逻辑TLA的建模语言TLA+对ARP协议进行建模分析。构造了一个ARP欺骗的攻击者模型，用基于TLA的模型检测工具TLC对其进行验证并找出一条攻击者路径。

关键词：ARP协议；ARP欺骗；行为时序逻辑
中图分类号：TP393.08 **文献标识码**：A **文章编号**：1673-629X(2010)06-0163-04

The Description and Validation of ARP Protocol Based on TLA

LI Yuan, WU Yong, LI Xiang
(Institute of Computer Software and Theory, Guizhou University, Guiyang 550025, China)

Abstract: With the development of computer network, more and more people are paying attention to the security of network. The ARP attacking is a very special mode of network attacking, it will destroy the data of host computer. In recent years, a foreign researcher, Lesilie Lamport, puts forward a new logic: temporal logic of actions(TLA), modeling the concurrent system to put to use this logic can relieve the pressure caused by the state space exposion to some extent, it can express process and attributes in a language at the same time. Introduce ARP protocol. Specify the ARP protocol with TLA+ based on the temporal logic of actions and validate it with TLC and find a path of attacker.

Key words: ARP protocol; ARP spoofing; TLA

0 引 言

网络上的计算机是通过IP地址通信，但是IP地址是位于网络层的逻辑地址，计算机之间要进行数据交换就必须知道它的物理地址，ARP协议的功能就是将逻辑地址转换成物理地址。因此ARP的协议的安全就显得非常重要。现在针对ARP协议进行攻击最常用的一种方式是ARP欺骗，在这种攻击方式下，攻击方可以通过伪造ARP请求与应答更新目标主机的ARP缓存从而骗过目标机，使目标机的数据包发给攻击者。攻击者就可以对截获的数据包的内容进行分析从而破解目标机的信息。

1 ARP协议

网络上计算机之间的通信是通过IP地址。IP地址是一个逻辑地址[1,2]。通过IP地址就可以找到目标网络，但是一个网络内部的计算机之间进行最终的数据交换是经过物理MAC地址。通过MAC地址就能识别具体的一台主机，这时就需要ARP协议把需要通信的目标主机的IP地址解析为与之对应的硬件物理地址。

2 ARP攻击

ARP攻击主要是基于ARP缓存表动态刷新的弱点，攻击者非法篡改目标机ARP缓存表，使目标主机无法正常工作的行为。攻击者可以很容易地将目标主机中IP地址对应的MAC地址改成根本不存在的地址，这样计算机就会往这个根本不存在的地址发送数据包，导致目标机无法接收到数据包，中断了主机与外界网络的通信[3,4]。

3 行为时序逻辑TLA

TLA[5]是由学者Lesilie Lamport提出的一种新的逻辑，即行为时序逻辑，运用这种逻辑对软件或协议系

收稿日期：2009-09-27；**修回日期**：2009-12-28
基金项目：美国GeneChiu基金资助项目(GFC2006-001)
作者简介：李 元(1974-)，男，实验员，研究方向为计算机网络；李祥，教授，研究方向为信息安全、计算复杂性、模型检测。

统进行建模，在一定程度上减少由于状态空间爆炸带来的压力，它能在一种语言中同时表达程序与属性。

TLA+[6,7]是以 TLA 为基础的系统描述语言，它以模块的形式构造规约，并通过扩展或实例化等方法把多个模块组合以形成更为复杂的规约。TLA+支持多种规约形式，标准形式如 Init/\[][Next]∧Liveness。其中，Init 指初始状态谓词，该公式描述了所有合法的初始状态；Next 指下一状态关系，规定了系统所有可能的动作，是所有变量组成的元组，且 $[Next]_v = Next \vee v'$；Liveness 则是一个时序公式，通过合取各动作的公平性条件来规定系统的活性属性。其实，一个 TLA+规约就是一个简单的数学公式，本质上描述的是一个状态机。

TLA 公式的完整语法定义：

< formula >≜< predicate > | □[< action >]$_{<\text{state function}>}$ | ¬ < formula > ∧ < formulaL > | □ < formula >

< action >≜布尔表达式，由常量符号、变量及带撇号的变量组成；(action通常表现为 $v = \cdots \wedge v' = \cdots$ 的形式，其中 v 表示变量在当前状态下的值，v' 表示该变量在下一状态的值)

<predicate>≜不包含带撇号的变量的<action> |Enabled<action>；

<state function>≜非布尔表达式，由常量符号和变量组成。

TLC 是一个用于找出用 TLA+规约中错误的工具。TLC 只能处理如下的标准形式规约：

Init∧[][Next]$_{var}$∧Temporal

Init 是初始谓词，Next 是下一个状态行为，var 是所有变量组成的元组，Temporal 是一个时序公式，它常常用于规约一种活性情况。

最常用的一个用于检测一个规约中错误的有效的方法就是试图验证这个规约应该满足的属性是否满足。

4 用 TLA+构造 ARP 协议

ARP 协议即地址解析协议[8]，它的主要功能就是获得目标机 IP 地址对应的 MAC 地址。这里主要以 ARP 协议在同一网段的工作为例，利用 TLA 建模并且构造一个 ARP 欺骗[2]。

ARP 协议的主要工作过程如图 1 所示。

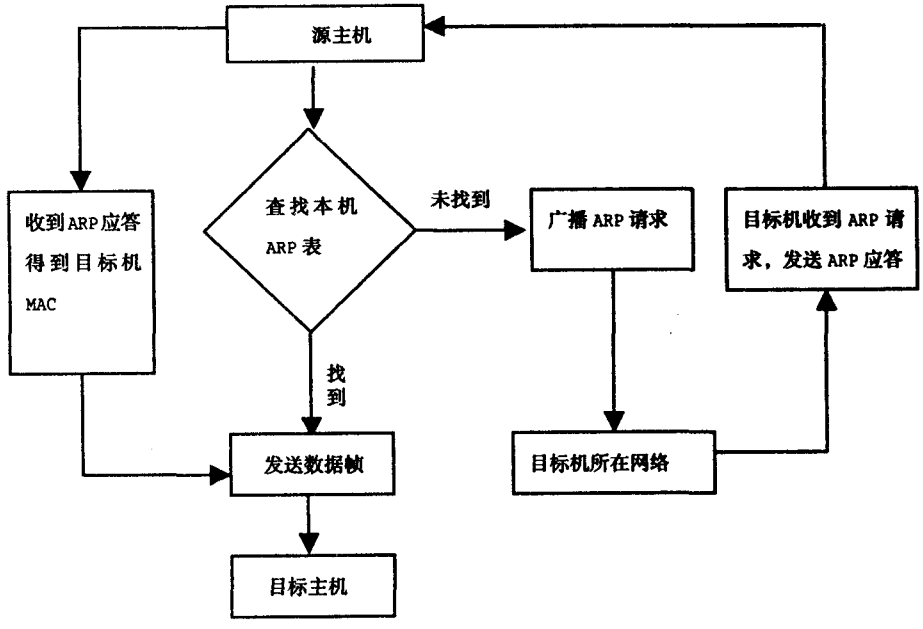

图 1 在同一网段内 ARP 工作原理

在这个协议中主要动作如下：

Detct：查找 ARP 缓存表。

SSend(ipadr)：源主机广播 ARP 请求。

TAWRcv、TBWRcv、TCWRcv、TDWRcv 分别表示网络内的主机 A、B、C、D 收到 ARP 请求。

TASend(repy)、TBSend(repy)、TCSend(repy)、TDSend(repy)分别表示主机 A、B、C、D 发送 ARP 应答。

SRcvR：源主机收到目标机发送来的 ARP 应答。

STSend：源主机给目标机发送数据帧。

TRcvD：目标机收到源主机发送来的数据帧。

这个协议中用到 5 个状态变量：begin，run，K，L，go，chan。

begin 是用来控制协议是否查看 ARP 缓存表；

run 用来控制是否广播 ARP 请求；

K 是一个通道，它用来发送 ARP 请求；

L 是一个通道，它用来发送 MAC 地址；

chan 是一个通道，用来发送数据帧。

有三个常量集合，IP 集合表示 ARP 缓存表，MAC 集合是不在缓存表中的 MAC 地址集合，IPN 集合表示一个网段内的不在 ARP 缓存表中的 IP 地址。

具体 ARP 模型如下：

```
---------- MODULE ARP ----------
EXTENDS Naturals, Channel
CONSTANTS IP, MAC, IPN
VARIABLES begin, run, K, L, go
```

```
KChan = INSTANCE Channel WITH Data <- IPN, chan <- K
LChan = INSTANCE Channel WITH Data <- MAC, chan <- L
----------------------------
vars = <<begin, run, K, L, go, chan>>
ARPInit = ∧ Init /* 初始状态定义 */
∧ begin = 0 ∧ run \in {0,1} ∧ KChan! Init ∧ LChan! Init ∧ go \in {0,1}
ARPTypeInvariant = ∧ KChan! TypeInvariant /* 类型不变量定义 */
∧ LChan ! TypeInvariant ∧ TypeInvariant ∧ begin \in {0,1} ∧ run \in {0,1}
∧ go \in {0,1}
/* 查找 IP 地址为"210.40.7.187 的主机是否在 ARP 缓存表中若存在的话 run 变量值为 0,否则为 1" */
Detct = ∧ begin = 0 ∧ run' = IF "210.40.7.187" \in IP THEN 0 ELSE 1
∧ begin' = 1 ∧ UNCHANGED <<K, L, go, chan>>
SSend(ipadr) = ∧ begin = 1 /* 通过通道 K 广播 ARP 请求 */
∧ run = 1 ∧ KChan ! Send("210.40.7.187") ∧ UNCHANGED <<begin, L, go, run, chan>>
/* run =0 说明要查的 IP 地址在 ARP 缓存中所以直接通过通道 chan 发送数据帧 */
SSendD = ∧ begin = 1 ∧ run = 0 ∧ Send("frame") ∧ UNCHANGED <<begin, L, go, run, K>>
TAWRcv = ∧ begin = 1 /* 目标机"210.40.7.185"收到 ARP 请求 */
∧ KChan! Rcv ∧ go' = IF K.val = "210.40.7.185" THEN 1 ELSE 2
∧ UNCHANGED<<begin, run, L, chan>>
TBWRcv = ∧ begin = 1 /* 目标机"210.40.7.186"收到 ARP 请求 */
∧ KChan! Rcv ∧ go' = IF K.val = "210.40.7.186" THEN 0 ELSE 1
∧ UNCHANGED<<begin, run, L, chan>>
TCWRcv = ∧ begin = 1 /* 目标机"210.40.7.187"收到 ARP 请求 */
∧ KChan! Rcv ∧ go' = IF K.val = "210.40.7.187" THEN 0 ELSE 1
∧ UNCHANGED<<begin, run, L, chan>>
/* 目标机"210.40.7.189"收到 ARP 请求 */
TDWRcv = ∧ begin = 1 ∧ KChan! Rcv ∧ go' = IF K.val = "210.40.7.189" THEN 0 ELSE 1
∧ UNCHANGED<<begin, run, L, chan>>
/* 目标机"210.40.7.185"发送 ARP 应答其中包括自己的 MAC 地址 */
TASend(repy) = ∧ begin = 1 ∧ go = 0 ∧ LChan ! Send("44-45-53-54-00-00")
∧ UNCHANGED<<begin, run, K, go, chan>>
/* 目标机"210.40.7.186"发送 ARP 应答其中包括自己的 MAC 地址 */
TBSend(repy) = ∧ begin = 1 ∧ go = 0 ∧ LChan ! Send("44-45-53-54-00-28")
∧ UNCHANGED<<begin, run, K, go, chan>>
/* 目标机"210.40.7.187"收到 ARP 请求其中包括自己的 MAC 地址 */
TCSend(repy) = ∧ begin = 1 ∧ go = 0 ∧ LChan ! Send("44-45-53-54-00-36")
∧ UNCHANGED<<begin, run, K, go, chan>>
/* 目标机"210.40.7.189"收到 ARP 请求其中包括自己的 MAC 地址 */
TDSend(repy) = ∧ begin = 1 ∧ go = 0 ∧ LChan ! Send("44-45-53-54-00-21")
∧ UNCHANGED<<begin, run, K, go, chan>>
/* 源主机收到目标主机发送来的应答其中包括 MAC 地址 */
SRcvR = ∧ LChan ! Rcv ∧ L.val = "44-45-53-54-00-36" ∧ Send("frame")
∧ UNCHANGED<<begin, run, K, go>>
/* 目标机收到源主机发送来的数据帧 */
TRcvD = ∧ Rcv ∧ begin' = 0 ∧ UNCHANGED <<run, K, L, go>>
/* 协议的下一个动作 */
ARPNext = ∨ Detct ∨ \E ipadr \in IP : SSend(ipadr) ∨ SSendD ∨ TAWRcv ∨ TBWRcv ∨ TCWRcv
∨ TDWRcv ∨ \E repy \in MAC : TASend(repy) ∨ \E repy \in MAC : TBSend(repy)
∨ \E repy \in MAC : TCSend(repy) ∨ \E repy \in MAC : TDSend(repy) ∨ SRcvR ∨ TRcvD
fairness = ∧ WF_vars(Detct) /* 行为的公平性约束 */
∧ WF_vars(\E ipadr \in IP : SSend(ipadr)) ∧ WF_vars(SSendD) ∧ WF_vars(TAWRcv)
∧ WF_vars(TBWRcv) ∧ WF_vars(TCWRcv) ∧ WF_vars(TDWRcv)
∧ WF_vars(\E repy \in MAC : TASend(repy)) ∧ WF_vars(\E repy \in MAC : TBSend(repy))
∧ WF_vars(\E repy \in MAC : TCSend(repy)) ∧ WF_vars(\E repy \in MAC : TDSend(repy))
∧ WF_vars(SRcvR) ∧ WF_vars(TRcvD)
ARPSpec = ∧ ARPInit ∧ [][ARPNext]_vars ∧ fairness
----------------------------
THEOREM ARPSpec => []ARPTypeInvariant
============================
在其配置文件 tla.cfg 中加入
----------------------------
CONSTANTS IP = {"210.40.7.181", "210.40.7.182", "210.40.7.183", "210.40.7.184"}
IPN = {"210.40.7.185", "210.40.7.186", "210.40.7.187", "210.40.7.189"}
MAC= {"44-45-53-54-00-00", "44-45-53-54-00-28", "44-45-53-54-00-36", "44-45-53-54-00-21"}
```

Data = {"frame"}
SPECIFICATION ARPSpec
INVARIANT ARPTypeInvariant
= =

5 一个 ARP 欺骗实例

ARP 协议一个最大的弱点就是,一个主机可以接收任何主机发送过来的应答,这就使得允许第三方截获源主机的发送的 ARP 请求,然后将其自己的 MAC 地址发送过去。由于数据帧传送的时候是以 MAC 地址为标准传送,所以此时主机最后传送的数据帧就发送给第三方主机而不是目标机。在模型 ARP 中,加入攻击者行为如下:

ItuderRcv = ∧ begin = 1 ∧ KChan! Rcv
∧ K.val = "210.40.7.187" ∧ go' = 5 ∧ UNCHANGED<<begin,run,L,chan>>
ItuderSend(repy) = ∧ begin = 1 ∧ go = 5 ∧ LChan ! Send("44 - 45 - 53 - 54 - 00 - 99")
∧ UNCHANGED<<begin,run,K,go,chan>>

这两个行为的目的就是攻击者截获源主机的 ARP 请求,然后将自己的 MAC 地址 44 - 45 - 53 - 54 - 00 - 99 发送给源主机,然后源主机就会将数据帧发送攻击者。下面验证一个属性:

[]<>(KChan ! Send("210.40.7.187")) ∧[]<>TRcvD

这条属性是说如果源主机发送 ARP 请求,目的主机最后一定能收到源主机发送来的数据帧。具体用 TLA 描述如下:

- - - - - - - - - - MODULE MCARP - - - - - - - - - -
EXTENDS ARP
Property1 = []<>(KChan ! Send("210.40.7.187")) ∧[]<>TRcvD
THEOREM Spec = > Property1
= =

协议开始运行时 K 通道中的初始值是 210.40.7.185,L 通道中的初始值是 44 - 45 - 53 - 54 - 00 - 00。状态 2 表示查找 ARP 缓存表,状态 3 表示经过查找后发现 IP 地址为 210.40.7.187 的目标机不在 ARP 缓存表内,因此转到状态 3 源主机通过通道发送 IP 地址到通道 K 中。此时 ARP 请求被攻击者截获因此转移到状态 4。状态 5 中,攻击者将自己的 MAC 地址应答通过通道 L 发送给源主机。最后使得源主机无法将数据帧发送给 IP 地址为 210.40.7.187 的目标机。这条路径如图 2 所示。

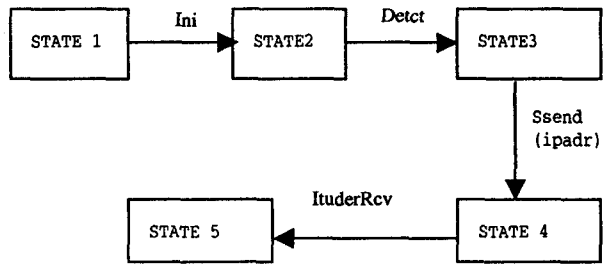

图 2 ARP 攻击路径

这条路径就是攻击者进行 ARP 攻击的路径。

6 结束语

ARP 攻击是一种非常专业化的网络攻击方式,它会给网络管理员增加很大的负担,破坏主机数据,窃取主机信息。文中用了一种新的方式用基于行为时序逻辑 TLA 的系统描述语言 TLA + 对 ARP 协议进行了建模并且通过构造一个 ARP 欺骗实例并找出了一个攻击者路径。

参考文献:

[1] Internet Protocols CSC/ECE 573. The Address Resolution Protocol[R]. USA:N. C. State University,2005.
[2] 吴建平. 高等计算机网络——体系结构、协议机制、算法设计与路由器技术[M]. 北京:机械工业出版社,2003.
[3] Comer D E. 计算机网络与 Internet - 网络应用[M]. 第 3 版. 北京: 清华大学出版社,2002.
[4] 吴 勇, 李 祥. ARP 攻击的分析与防范[J]. 计算机与信息技术,2008(8):7 - 9.
[5] Lamport L. The Temporal Logic of Actions[J]. ACM Transactions on Programming Languages and Systems, 1994, 16 (3):872 - 923.
[6] Lamport L. Specifying Systems[M]. [s.l.]:Addison - Wesley Longman Publishing Co., Inc, 2002.
[7] Lamport L. Specifying Systems The TLA + Language and Tools for Hardware and Software Engineers[M]. [s.l.]:Microsoft Research Addison_Wesley Publishing Version,2002.
[8] Stevens W R. TCP/IP 详解 卷 1:协议[M]. 范建华,译. 北京:机械工业出版社,2005.

(上接第 162 页)

10 - 15.
[23] 周 权,周小东. 基于簇首节点的可信传感器网络路由[J]. 传感器与微系统,2008,27(10):42 - 45.
[24] Song Fei, Zhao Baohua. Trust - based LEACH Protocol for Wireless Sensor Networks[C]//Proceedings of the 2nd International Conference on Future Generation Communications and Networking. Hainan, China:[s.n.],2008:200 - 205.
[25] 张留敏,李腊元,李春林. 一种基于主观逻辑的无线传感器网络可信路由算法[J]. 武汉理工大学学报:交通科学与工程版,2009,33(1):75 - 78.