Research on Attacking Method against the PXE Protocol

Zhitao GUAN, Wenchao CUI, Shuai YUAN, Jietao HE
School of Control and Computer Engineering, North China Electric Power University, Beijing, China
Email: guanzhitao@126.com

Abstract: PXE protocol is a popular remote boot protocol nowadays. The designers focus mainly on the simplicity and convenience of the PXE protocol, but they take less consideration on security issues. There maybe some hidden risks of PXE, so the network attack to PXE is possible to happen. One possible attack approach against the PXE protocol is introduced in this paper. Firstly, the attack principle is stated. Secondly, the simulation process of the attack is described, and the possible results are analyzed. Finally, the protection strategies dealing with such kind of attack method are proposed on the basis of analyzing the potential attacks.

Keywords: PXE protocol; network attacks; remote boot

一种针对 PXE 协议的网络攻击方法及防护策略研究

关志涛，崔文超，袁　帅，何杰涛
华北电力大学控制与计算机工程学院，北京，中国，102206
Email: guanzhitao@126.com

摘　要: PXE 协议是目前流行的远程启动协议，但由于其在设计时主要考虑了简单性和方便性，对安全性考虑不足，留下了一定的隐患，存在受到网络攻击的可能。本文介绍了一种可能的针对 PXE 协议的攻击方法，说明攻击原理，模拟攻击过程，并分析了可能造成的后果。针对该安全隐患，在详细分析潜在危害的基础上，提出了应对这种攻击方式的防护策略。

关键词: PXE 协议；网络攻击；远程引导

1 引言

远程启动协议是指为计算机提供从网络下载启动程序镜像，并引导计算机启动的一类网络协议，它的功能主要有[1]：

- 远程新系统引导，为没有安装操作系统的计算机提供安装新操作系统的能力[2,3,4,5]；
- 紧急远程引导，当本地计算机所安装的操作系统发生异常时，从远程进行引导，进行修复；
- 远程启动，为无本地存储能力的计算机提供操作系统，也就是我们常说的无盘工作站[6,7,8]。

远程启动协议从早期的 BOOTP，DHCP 发展到现在的 PXE（Preboot Execution Environment），为用户提供了越来越丰富的功能，不但能远程启动 DOS 这样的单机操作系统，也能够启动 Windows 及 Linux 这样的全功能系统，在许多场合得到了广泛的应用。但是，这类协议在通讯过程中，为了满足简单性的需要，对安全性问题考虑不够充分，为网络攻击提供了可能性。本文将对攻击 PXE 协议的方法进行初步的研究。

2 PXE 协议分析

PXE 协议是由 Intel 公司于 2000 年提出的远程启动协议，目前已得到了包括 Intel，3COM 等主流厂商的支持，成为 Intel 架构计算机（主要是个人计算机）的标准远程启动协议。它建立在一系列已经广泛使用的网络标准基础上，包括 TCP/IP，DHCP 及 TFTP，通过下列三种技术，为远程启动提供了可靠保证：

- 获取本机网络地址及下载启动镜像的协议；
- 固化在网卡硬件中的一套 API，可供启动程序或 BIOS 调用；
- 启动网卡硬件中固化的 PXE 协议的一种标准方法。

PXE 协议的工作过程如图 1：

* 华北电力大学校内基金支持（200822042）

PXE 协议在使用中分客户端与服务器端两方，客户端首先使用扩展的 DHCP 协议，从服务器端获得本机的 IP 地址及启动程序镜像存放的服务器地址；接着，客户端使用 TFTP 协议从启动服务器下载启动镜像；最后，客户端使用启动镜像进行启动。

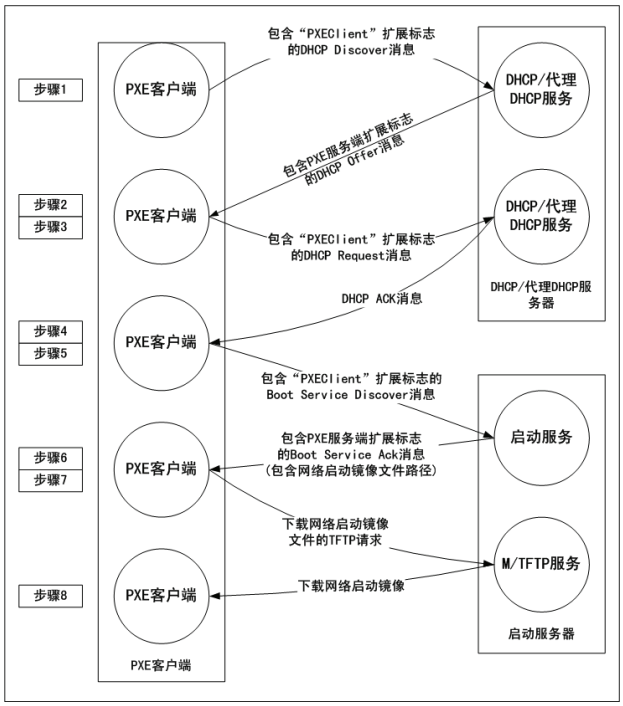

Figure 1. Working process of PXE protocol
图 1. PXE 协议工作过程

3 攻击原理

目前支持 PXE 协议的网卡已经非常普遍，主要的网卡生产厂商及主板生产厂商都开始在他们的新产品中支持 PXE 协议，而一些老式网卡也可以通过使用新版 BOOT ROM 的方式支持 PXE 协议。

由于 PXE 协议在查找 DHCP 服务器的过程中，并没有对 DHCP 服务器的真实性进行验证，从而使攻击者有可能通过假冒 DHCP 服务器的方法，向客户机传送错误的启动镜像程序，从而实现对客户机的攻击。

实际的攻击方法可以有三种：

3.1 网络中使用 PXE 协议时

当网络中存在多台 DHCP 服务器的时候（可能包含攻击者所建立的 DHCP 服务器），PXE 客户端对于

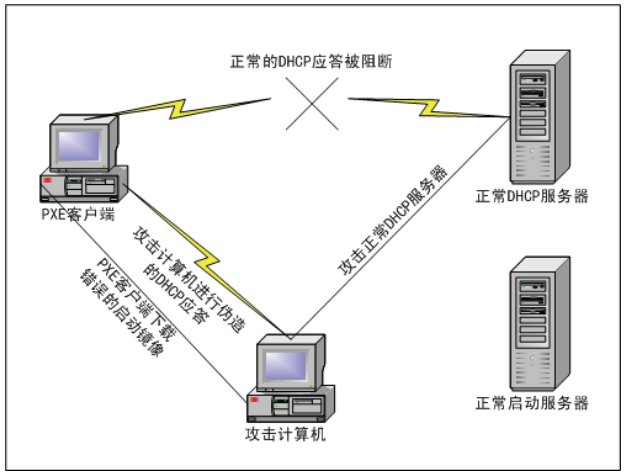

Figure 2. Attacking method to PXE protocol
图 2. PXE 协议攻击图示

收到的多个 DHCP 应答时应该采用哪个并没有明确选择方法，通常使用最先得到的响应。这就给攻击造成了一定的可能性。当网络中的计算机使用 PXE 协议启动时，如一个包含多台无盘工作站的网络，攻击者可以通过：1）采用 DoS 之类的攻击使原有 DHCP 服务器停止响应，而用自己的 DHCP 服务器进行应答；2）或仅仅使自己的 DHCP 服务器能够较快的应答，使 PXE 客户端使用攻击者伪造的 DHCP 应答。

接下来，无盘工作站在启动时会从攻击者的计算机中下载启动程序镜像，并使用此镜像启动计算机。攻击者可以很方便地将启动程序修改为对 PXE 客户端计算机进行攻击的程序，如伪造正常操作系统的登录界面，盗取用户密码等。

3.2 对于松散的网络环境

目前许多计算机在安装过程中，缺省的启动顺序设为了网卡启动，而很多的使用者并没有发现这个问题。因为在正常使用过程中，网络上没有配置 DHCP 服务器，网卡启动会在超时后自动转为由本地设备启动，不会带来什么不良后果。校园网环境就是这样一种比较松散的局域网环境，许多机器位于不同的地理位置，但却可能属于同一网段，如笔者在所使用的校园网环境中，就经常可以在所使用的计算机中收到其它计算机启动时发出的 PXE 扩展的 DHCP 请求。

如果有攻击者在这样的网络中任何一台计算机上安装具有攻击作用的 DHCP 服务程序及启动程序镜

978-1-935068-10-5 © 2010 SciRes.

像，利用用户的大意，就可以攻击其使用的计算机，格式化硬盘等。

3.3 在用户关机离开的时候进行攻击

目前的很多计算机都具备通过网卡唤醒功能（WOL），这项功能本来是为了方便对计算机的管理，但却可能被攻击者利用。攻击者可以在用户关机离开时，通过网络唤醒其它计算机，再利用 PXE 协议进行攻击，而这种攻击可能是用户无法查觉的。

4 模拟攻击方法

当对象 X 有更新操作发生时，更新扩散策略分为两种情况：

Linux 操作系统是由 GNU 组织发布的开放源码操作系统，由于它代码的公开性，任何人都可以进行修改，目前已经出现许多非常小的 Linux 运行环境。本文以修改的 Linux 操作系统作为攻击程序，简单介绍这种攻击方法的可行性。

模拟攻击环境由两台计算机组：一台运行 Linux 操作系统的服务器模拟攻击计算机，运行 ISC dhcp-3.0 软件提供支持 PXE 的 DHCP 服务；运行 tftp-hpa 软件提供 TFTP 服务。另一台安装有支持 PXE 协议网卡的计算机模拟 PXE 客户端计算机，并将启动顺序设为网卡优先。

4.1 攻击计算机的配置

PXE 客户端在工作过程中，需要三个二进制文件：启动镜像、Linux 内核和 Linux 根文件系统。启动镜像文件是可执行程序，它向用户提供简单的控制界面，并根据用户的选择，下载合适的 Linux 内核以及 Linux 根文件系统。PXELinux 提供的 pxelinux.0 原本是为利用 PXE 协议远程启动 Linux 操作系统设计的启动镜像，由于本文的攻击程序也是采用 Linux 实现的，因此在模拟攻击中也可以使用。通过配置可以取消 pxelinux.0 运行时与用户的交互，保证攻击的进行。

Linux 内核以及 Linux 根文件系统构成了一个操作系统环境，可以对系统资源进行访问。为了达到攻击的目的，需要对使用的 Linux 操作系统进行定制，具体方法可以参考 Linux 文档。最终的 Linux 内核可以去除大量不需要的功能，如网络功能、USB 功能等，只需要具有访问硬盘的能力即可。目前的个人计算机硬盘基本都为 IDE 接口，这种接口最多只能使用 4 块硬盘，在 Linux 操作系统中表示为：/dev/had，/dev/hdb，/dev/hdc，/dev/hdd。因此在不知道 PXE 客户端计算机具体配置的情况下，攻击程序也可以通过简单的查询访问到实际的硬盘。接下来修改系统启动脚本，加入想实行的攻击命令，如格式化硬盘等。制作根文件系统的方法请参考 Linux 文档，此处不再赘述。

在攻击计算机中，将 pxelinux.0、Linux 内核文件、Linux 根文件系统三个文件安装在服务器 TFTP 服务软件指定的位置，并配置 DHCP 服务程序及 TFTP 服务程序。

4.2 攻击过程及结果

首先运行攻击计算机，接着启动 PXE 客户端计算机。攻击过程是：

1) PXE 客户端计算机首先通过 DHCP 服务器得到启动镜像文件名（pxelinux.0）及其位置；

2) PXE 客户端计算机通过 TFTP 协议下载 pxelinux.0 并运行；

3) Pxelinux.0 也通过 TFTP 协议下载 Linux 内核文件及 Linux 根文件系统；

4) 启动 Linux 内核。

在实际模拟中，这种攻击方法成功地格式化客户端计算机的硬盘，造成数据丢失。

上述过程中步骤 1 及步骤 2 是由 PXE 协议实现的，而之后的过程则是由 pxelinux.0 程序及 Linux 完成的。这种方法主要的好处是方便，不需要攻击者编写大量的代码。在真实环境中，攻击者也可能不采用这样的过程，而是直接在启动镜像中就加入攻击代码，省去了再次下载 Linux 内核及根文件系统的过程。

5 结论

综上所述，我们可以看出，远程启动协议一方面给计算机的管理带来了很大的方便；另一方面，如果使用时不加注意，也可能被利用进行破坏。因此管理人员及使用者应该注意下列几点：

- 在确实要使用 PXE 协议的网络中，管理人员应该经常检查有无陌生的 DHCP 服务器在网络上工作；
- 无盘工作站的使用者一定要注意系统启动时的情况是否正常，如果发现启动过程异常，及时向管理人员汇报；
- 个人计算机的使用者如果不需要使用网络

启动功能，一定不要在设置中使用网卡成为第一启动设备。

致　谢

本课题研究由华北电力大学校内基金支持（基金号：200822042）。

References (参考文献)

[1] Intel Corporation, Preboot Execution Environment (PXE) Specification, 1999.

[2] Xiaojun Du, Kai Gent, Qiuhong Wu. Principles and Applications of Linux Automated Install Based on PXE [J]. Communication Technology, 2008, 41(8): 137-138.

[3] QIU Jianxin, MA Shixia. The Application And Dissection Of Automated Linux Install Through Network [J]. Microcomputer Applications, 2005, 26(6): 760-764.

[4] YAN Ge, ZHENG Yi-feng. The Design And Application Of Automated Linux Install Through Network [J]. Journal of Zhangzhou Teachers College (Natural Science), 2006(4): 45-49.

[5] Li Huaigang, Qiu Jianxin. The realization and principle of linux's install through network [J]. Computer Applications and Software, 2006(9):109-111.

[6] Yu Xi-zhong. The organization and application of the diskless workstations [M]. 2001.

[7] Wang Chunhai, Wang Qun. The newly illustration of diskless workstation and terminals configuration and application. Post&Telecom Press. 2001.

[8] Wang qin, Ganyu, Wang zhenglin. The organization and management of the diskless workstations [M]. TSinghua university press. 2002.