第 42 卷 第 6A 期
2015 年 6 月

计 算 机 科 学
Computer Science

Vol. 42 No. 6A
June 2015

# 基于 USB-Key 的 iSCSI 身份验证安全加固

郭 燕[1,2] 李永堂[1] 李春杰[1,2]

(中国科学技术大学软件学院 苏州 215123)[1] (中国科学技术大学苏州研究院 苏州 215123)[2]

**摘 要** 主要介绍了 iSCSI 身份认证中的安全措施及其不足,讨论其面对的安全风险,并针对协议身份验证实现中出现的问题提出了改进方案。考虑了在用户名和密码丢失的情况下,如何通过结合 USB-Key 的方式改进身份认证方案 CHAP,提高 iSCSI 协议的安全等级和稳定性。实验结果证明,使用 USB-Key 的 CHAP 认证可以有效地解决多点登录,并有效提高安全等级。

**关键词** iSCSI,USB-Key,网络存储

**中图法分类号** TP311.56 **文献标识码** A

## Improved iSCSI Authentication Based on USB-Key

GUO Yan[1,2] LI Yong-tang[1] LI Chun-jie[1,2]

(School of Software Engineering, University of Science and Technology of China, Suzhou 215123, China)[1]

(Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou 215123, China)[2]

**Abstract** The iSCSI authentication method CHAP was introduced and analyzed, especially its security risks. Cases such as leakage of username and password were considered, and improvement was proposed. Experiments demonstrate that CHAP with USB-key can effectively prevent multi-initiators logging in with same username/password pair, and the security level and stability of iSCSI are significantly improved.

**Keywords** iSCSI, USB-Key, Network storage

## 1 背景

在信息时代,企业的业务数据量快速增加,对数据存储的需求爆炸性增长,数据管理和保存的复杂度不断增加。为了应对越来越高的存储要求,人们提出各种解决方案。如直接附加存储 DAS(Direct-Attached Storage)、网络附加存储 NAS(Network Attached Storage)和存储区域网 SAN(Storage Area Network)。DAS 是将存储设备通过小型计算机系统接口 SCSI(Small Computer System Interface)直接连接到一台服务器,成本低,配置简单,缺点是传输距离存在限制,且服务器本身容易成为瓶颈。NAS 相当于一台网络文件服务器,NAS 连接在 TCP/IP 网络上,易于安装和部署,缺点是存储访问是文件级的,因此它的性能和扩展性取决于 NAS 支持的文件系统。SAN 将域中一台或多台主机链接到存储设备的专用网络,代表是光纤通道(Fiber Channel),其安全性好、速度快,缺点是架构成本过高。

2003 年 2 月 11 日互联网工程任务组(Internet Engineering Task Force,IETF)通过了由 IBM 和思科共同发起的 iSCSI(Internet SCSI)[1] 标准。iSCSI(互联网 SCSI)是一种在 Internet 协议网络上进行数据块传输的标准。它提供机制可以在 IP 协议上层运行 SCSI 指令集,实现了 SCSI 和 TCP/IP 协议的连接,使其能够在高速千兆以太网上进行路由,到达存储位置。它的出现解决了开放性、容量、传输速度、兼容性等问题,同时也提供了远高于基于光纤 SAN 的性价比。

但另一方面,ISCSI 相比于 SAN 或者 SCSI 存在更多的安全风险。SCSI 存储设备直接连接在主机上,基于光纤通道的 SAN 使用专用网络,两者面临的安全风险很小,不需要专门考虑存储方面的安全性。而 iSCSI 使用了 TCP/IP 网络进行数据传输,将面临着网络传输中数据被窃听、篡改等多种安全风险[4,5,8]。

## 2 iSCSI 工作原理和安全机制

### 2.1 iSCSI 工作原理

SCSI 是物理上连接计算机和周边存储设备并在进行数据传输的一套标准,支持块级访问,是一种通用磁盘技术。iSCSI 是针对 SCSI 协议提出的运行于 TCP 层之上的传输协议。iSCSI 由启动器、目标器构成,iSCSI 启动器从应用程序内部接收 SCSI 的 I/O 请求,将其封装为 iSCSI PDU,加上 TCP/IP 包头,通过 TCP/IP 网络将其传送到 iSCSI 目标器,iSCSI 目标器通过 SCSI 处理,将这一请求传送到目标存储设备。从 SCSI 设备获得数据后,将数据和响应封装为 iSCSI PDU,再通过 TCP 连接返回 iSCSI 启动器,解析出数据和响应。

iSCSI 协议允许多个启动器或目标器共存,启动器可以访问多个目标器,不同的启动器可以访问同一个目标器。为了防止攻击者非法访问目标器中资源,iSCSI 自带两种安全

本文受国家基金委:基于任务行为特征分析的热敏感操作系统技术研究(61272131)资助。

郭 燕(1981—),女,博士,讲师,主要研究方向为信息安全、高性能计算,E-mail:guoyan@ustc.edu.cn;李永堂(1989—),男,硕士生,主要研究方向为信息安全;李春杰(1977—),男,副研究员,主要研究方向为嵌入式系统。

措施：认证和加密。认证主要是在 target 和 initiator 之间做身份认证，加密则是对传输的 TCP/IP 数据包进行加密保护。我们主要讨论认证方案。

### 2.2 iSCSI 身份认证

iSCSI 支持 4 种身份认证的方法：kerberos、简单公钥机制(SPKM)、secure remote password 以及提问握手认证协议 CHAP[2]。CHAP 认证协议简单高效，是目前 IP SAN 领域最常用的安全机制，几乎所有的 iSCSI 实现都支持 CHAP 认证。

CHAP 可为两个通信实体提供双向的认证，单向认证过程如图 1 所示。首先由启动器发起认证请求，将自己支持的散列算法表发送给目标器。然后，由目标器选择一个散列算法，发送一个通信序列号以及挑战数给启动器。当启动器收到消息后，采用收到的序列号、挑战数和密码以选择验证方选择的散列算法进行散列，将散列的结果回复给目标器。目标器则从数据库中取出用户密码，将序列号和挑战数一起进行散列，如果散列结果和从启动器收到的相同，则认证通过，否则，认证失败。双向认证的过程则类似，由启动器验证目标器。

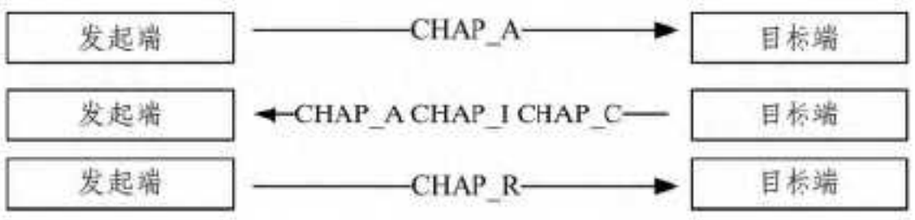


图 1 CHAP 流程图

其中，CHAP-A 是按优先级排列的散列算法，CHAP-N 是名字，CHAP-I 是通信标识符，CHAP-C 是挑战数，CHAP-R 是回复。

### 2.3 CHAP 认证安全问题

使用以上认证方法，CHAP 可以防止重放攻击，同时也防止了密码明文在网络中传输。它的优点是原理简单，不需要其它额外的认证服务器，认证过程中的计算量很小，效率高。但缺点也很明显，首先 CHAP 密钥以明文形式存放，存在安全隐患，如攻击者可利用操作系统漏洞获得此口令；其次，当 CHAP 在未加密的信道中传输时，很容易受到离线词典攻击。攻击者在获得用户口令后，可以冒充用户身份，进行数据访问。也即，用户密码安全性比较脆弱[3]。

另外，经过对多种开源 iSCSI 目标器实现进行验证，iSCSI Target 端对 CHAP 认证不进行区分[7]，即若 A 发起者向 C 目标端发起认证请求并认证成功之后，B 发起者以同样的用户名和密码(目标端只设置有一个用户名和密码的情况下)也可以再次向 C 目标端发起认证并能够认证成功。这种情况下，iSCSI 的表现是不稳定的，A 和 B 都能访问 C 建立的磁盘，但是写入功能表现不稳定。也就是说，iSCSI 本身不能拒绝已经经过身份认证并登陆成功的用户再次在异地进行身份认证并登陆成功。

因此，使用现有的 CHAP 身份认证方案，存在用户密码泄露的可能，而在用户密码泄露之后，即使在用户成功登录的情况下，攻击者也可以登录，使得用户的数据安全和通信面临着极大的风险，不适合在对数据安全要求较高的场合使用。

## 3 基于 USB-Key 的 CHAP 加固

为了解决用户名密码泄露以及多点登陆的问题，进一步保护本系统的安全，本文提出了一种基于 USB Key 的 CHAP 认证方案。

### 3.1 USB Key 和公钥认证

USB Key 是一种 USB 接口的智能加密硬件存储设备，小巧易用，具备了数据加解密、数字签名、访问控制等多种安全功能，广泛应用在安全等级要求较高的场合。USB Key 内置智能卡芯片，存储用户的公私钥对，使用内置的算法实现对用户身份的认证，同时保证用户私钥存在密码锁中不能导出，保证了用户认证的安全。每个 USB Key 还有一个个人识别码(Personal Identification Number，PIN)，使用时必须要知道这个 PIN 值才可以访问内部功能，并且 PIN 码输入错误有限制次数，超过限制次数 USB Key 将被锁定再不能使用。所以 USB Key 的安全由硬件设备本身和 PIN 码双重保护[6]。

非对称密码算法中，加密和解密使用两个不同的密钥，并且理论上无法从一个密钥得出另一个密钥。使用一个密钥进行加密，只有另一个密钥才能解密。使用公开的密钥进行加密，只有私钥拥有者才能解密，保证了信息的安全；如果公钥可以成功解密，则可以证明加密者持有私钥，从而证明了身份。因此，在应用中一般使用公钥加密，保护信息安全；使用私钥签名，验证信息来源。

### 3.2 CHAP 认证加固

用户使用 USB Key 作为硬件辅助，在原有 CHAP 认证的基础上，增加 USB Key 的验证加固，解决 iSCSI 身份认证过程中可能面临的安全风险。安全加固后的认证仅对原有的 CHAP 认证过程做较小的改动，具体流程如下：

1. iSCSI 启动器向目标器发起身份验证请求；

2. 目标器选择散列算法，生成通信序列号以及挑战数，发给启动器；

3. 修改 iSCSI 启动器程序，启动器向目标器发出〈序列号，挑战数，密码〉散列值(AB)之前，使用 USB Key 中的私钥进行签名，然后发出签名后的值(XY)；

4. 修改 iSCSI 目标器程序，修改后的 iSCSI 目标器接收到来自 iSCSI 启动器的数据(XY)后，查出本地明文密码和序列号以及挑战数做摘要，然后将摘要和签名一起作为参数进行验签；

5. 如果验签通过，则认证通过，否则认证失败。

通过使用 USB Key 进行 CHAP 认证加固，即使在用户名和密码泄露的情况下，如果不能获得用户的 USB Key，那么将不能通过身份验证。在增加了 USB Key 保护以后，攻击者只有在同时获得用户名密码、USB Key，以及用户 USB Key PIN 三方信息的时候，才能冒充合法用户登录成功，大大增加了攻击难度，同时也解决了目标器端对认证不稳定的问题。

## 4 实现与测试

常见的发起端有 open-iscsi 和 Windows Initiator，分别应用在 Linux 和 Windows 平台下。open-iscsi 作为发起端程序，将网卡虚拟为一个 iSCSI 卡，接收发送 iSCSI 报文，从而实现发起端和目标端之间 iSCSI 协议和 TCP/IP 协议传输。采用该软件作为发起端基本不用额外开销，成本极低。

目标端使用较多的是 IET(iSCSI Enterprise Target)和 SCST(generic SCSI target subsystem for Linux)，它们都实现了 iSCSI 协议，并且 iSCSI 的管理程序在用户态实现，实际的数据传输在内核态，不受用户空间调用。为了达到较好的表现，SCST 需要对内核打补丁，以支持 TCP/IP 的零拷贝技术，

SCST 中的数据在目标端和后端设备间都是零拷贝的，不需要额外的内核空间。

在实验过程中，iSCSI 客户端启动器使用的是 open-iscsi-2.0.873[9]，服务器端目标器使用的是 iSCSI Enterprise Target(iet)[10]，客户端和服务器端都运行于 ubuntul3.04。USB Key 购于海泰方圆公司。

针对文中讨论的两种安全问题，分别在 Windows 系统和 Linux 系统中进行了测试。

1. 攻击者在获得了用户名和密码，但是没有用户 USB Key 的情况下，进行登录，如图 2 所示，结果显示登录失败。


图 2 Windows 中攻击者登录失败

2. 攻击者在获得了用户名和密码，合法用户正常登录的情况下，进行登录，结果显示登录失败，而合法用户的通信不受影响。

图 3 显示在用户输入正确的用户名和密码后，登录成功。此时，窃取了用户名和密码的攻击者在另一台电脑上进行登录，图 4 显示攻击者登录失败，合法用户的使用不受影响。

```
# iscsiadm -m discovery -t sendtargets -p 10.6.12.62:3260
10.6.12.62:3260,1 iqn.foo.example.chap.enhance
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.authmethod --value=CHAP# iscsi-
adm -m node -T iqn.foo.example.chap.enhance -o update --
name node.session.auth.username --value=lee
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.password --value=123456789011
# iscsiadm -m node -T iqn.foo.example.chap.enhance -p 10.6.
12.62:3260 -l
Logging in to [iface: default,target: iqn.foo.example.chap.enhance,
portal: 10.6.12.62,3260]
Login to [iface: default,target: iqn.foo.example.chap.enhance,por-
tal: 10.6.12.62,3260] successful.
```

图 3 Linux 中合法用户登录成功

```
# iscsiadm -m discovery -t sendtargets -p 10.6.12.62:3260
10.6.12.62:3260,1 iqn.foo.example.chap.enhance
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.authmethod --value=CHAP# iscsi-
adm -m node -T iqn.foo.example.chap.enhance -o update --
name node.session.auth.username --value=lee
# iscsiadm -m node -T iqn.foo.example.chap.enhance -o update
--name node.session.auth.password --value=123456789011
# iscsiadm -m node -T iqn.foo.example.chap.enhance -p 10.6.
12.62:3260 -l
Logging in to [iface: default,target: iqn.foo.example.chap.enhance,
portal: 10.6.12.62,3260]
iscsiadm: Could not login to [iface: default,target: iqn.foo.example.
chap.enhance,portal: 10.6.12.62,3260]:
iscsiadm: initiator reported error(19 - encountered non-retryable
iSCSI login failure)
```

图 4 攻击者使用相同用户名和密码登录失败

结束语 本文讨论了 iSCSI 协议中 CHAP 身份认证方法在使用中的不足，即密码易泄露和允许多点登录，提出了使用 USB Key 对 iSCSI 的身份验证过程进行加固，攻击者必须在同时获得用户密码、USB Key 以及 USB Key 的 PIN 码的情况下才能成功登录，因此大大提高了 iSCSI 身份认证的安全性和稳定性。

## 参 考 文 献


[1] Satran J, Meth K, Sapuntzakis C, et al. Internet Small Computer Systems Interface(iSCSI). IETF RFC 3720, 2004. [EB/OL]. https://www.ietf.org/rfc/rfc3720.txt

[2] Simpson W. PPP Challenge Handshake Authentication Protocol. IETF RFC 1994, 1996. [EB/OL]. https://www.ietf.org/rfc/rfc1994.txt

[3] Leduc G. Verification of two versions of the challenge handshake authentication protocol(CHAP)[J]. Annales des télé communications. Springer-Verlag, 2000, 55(1/2): 20-30

[4] 朱坷. iSCSI 存储系统中的安全性研究[D]. 上海: 上海交通大学, 2007

[5] 刘明. 基于 iSCSI 协议的网络存储安全技术研究[D]. 郑州: 中国人民解放军信息工程大学, 2007

[6] 陈龙辉. 移动 PKI 体系中 SD 安全模块的研究[D]. 北京: 北京邮电大学, 2008

[7] Vishwakarma S, Bagaria S. iSCSI Simulation Study of Storage System[C] // Cambridge, UK, Computer Modeling and Simulation, 2008, 4: 703-707

[8] Alaidaros H M, Rasid M F A, Othman M, et al. Enhancing Security Performance with Parallel Crypto Operations in SSL Bulk Data Transfer Phase[C] // Penang: Telecommunications and Malaysia International Conference on Communications, 2007, 5: 129-133

[9] Aizman A, Yusupov D. Open-iSCSI[OL]. http://www.open-iscsi.org/

[10] iSCSI target[OL]. http://iscsitarget.sourceforge.net/


(上接第 354 页)


[7] Fukui K, Fukunaga S, Tanimoto K. ZigBee technology for low-cost and low-power radio communication systems[J]. Journal Institute of Electronics Information and Communication Engineers, 2005, 88(01): 40-45

[8] 于海斌, 曾鹏, 等. 智能无线传感器网络系统[M]. 北京: 科学出版社, 2006

[9] 金纯, 罗祖秋, 罗凤, 等. ZigBee 技术基础及案例分析[M]. 北京: 国防工业出版社, 2008

[10] 李文仲, 段朝玉. ZigBee 无线网络技术入门与实践[M]. 北京: 北京航空航天大学出版社, 2007

[11] Akyildiz I F, Su W, Sankarasubramaniam Y, et al. Wireless Sensor Networks: A Survey[J]. IEEE Computer, 2002, 38(4): 393-422