第33卷 第18期 计 算 机 工 程 2007年9月
Vol.33 No.18 Computer Engineering September 2007
·安全技术· 文章编号：1000—3428(2007)18—0170—02 文献标识码：A 中图分类号：TP393.08

基于ECC的iSCSI-SAN安全模型设计

刘 明，苏锦海
(解放军信息工程大学电子技术学院，郑州 450004)

摘 要：具有带外存储虚拟化结构的iSCSI-SAN存在安全隐患：一方面，暴露在IP网络上的存储资源容易遭到假冒身份者的非法访问；另一方面，在网络上直接传输的明文存储数据面临着被网络攻击者监听的安全威胁。该文基于椭圆曲线密码体制ECC设计了适合该网络存储结构的安全模型，该模型通过提供双向认证机制防止假冒身份攻击，通过在认证过程中协商一次性会话密钥并对存储数据进行加密保证存储数据的传输安全，从而提高了存储系统的安全性。

关键词：iSCSI；ECC；SAN；网络存储；存储虚拟化

Design of Security Model of iSCSI-SAN Based on ECC

LIU Ming, SU Jin-hai
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】iSCSI-SAN with out-band storage virtualization has some security hidden dangers: one is the storage resource exposed at IP network, which is vulnerable to forgery attack. The other one is the storage data transmitted on IP network, which faces the security threat of network sniffer. Based on ECC, a security model suited to above-mentioned network storage structure is designed, which provides two-side authentication to prevent forgery attack and encryption mechanism to ensure the security of storage data transmission. Consequently, the security of storage system is enhanced.

【Key words】iSCSI; ECC; SAN; network storage; storage virtualization

目前，构建基于iSCSI具有带外存储虚拟化结构的存储区域网(storage area network, SAN)是网络存储[1]的新兴技术，具有广泛的应用前景，但由于这种拓扑结构的开放性，存储资源直接暴露于IP网，大量数据面临着IP网上的各种攻击，安全问题亟待解决。因此，如何根据存储结构特点设计高效的安全机制，从而提高存储系统的安全性，具有一定的现实意义。

1 基于iSCSI的带外存储虚拟化结构及其安全问题

1.1 iSCSI协议

iSCSI[2]即Internet SCSI，是一种在TCP/IP协议网络上，将SCSI数据块映射成网络数据包进行数据块传输的标准。iSCSI协议模型与工作流程如图1所示。

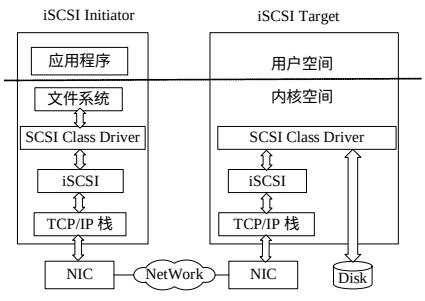

图1 iSCSI协议模型

在图1中，始发端的应用程序发出命令：在一台SCSI存储设备上保存或索取数据。文件系统对这个请求命令进行处理并将这个请求转换为一条或多条SCSI命令，然后这些命令被传送给iSCSI软件层或接口卡。命令和数据在这里被封装成iSCSI数据包，再由TCP/IP栈将它分为适于网络传输的网络数据包，最后通过网络接口卡(network interface card, NIC)将数据包在网络上传送。在目标端，TCP/IP栈将带有iSCSI报头的网络数据包组合并交于iSCSI软件层或接口卡，解析为原始封装的SCSI命令和数据后，将SCSI控制命令和数据发送到相应的SCSI存储类驱动并驱动磁盘驱动器执行请求。如果发送的是数据请求的话，数据从磁盘驱动器上取出，然后再封装并发送给发出请求的计算机。

1.2 带外存储虚拟化

iSCSI协议的一个重要应用是构建存储区域网[3]，而存储区域网根据存储管理器的位置不同分为带外存储虚拟化和带内存储虚拟化两类。本文研究具有带外存储虚拟化结构的存储区域网，如图2所示。

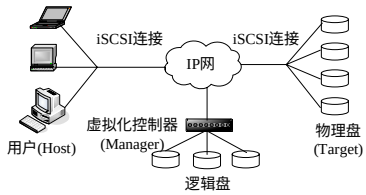

图2 基于iSCSI的带外存储虚拟化

在这种存储结构中，目标存储设备Target是带有SCSI硬盘的存储服务器，用户Host是磁盘上数据的使用者或拥有者，存储虚拟化控制器Manager是具有管理功能的服务器，一方面负责对物理设备进行统一管理，另一方面虚拟出逻辑磁盘提供给用户。Manager与Target通过iSCSI连接构成存

作者简介：刘 明(1981－)，男，硕士研究生，主研方向：信息安全；苏锦海，教授
收稿日期：2006-10-08 **E-mail：**wendaoreyue@yahoo.com.cn

储区域网 SAN，并与 Host 并存于 IP 网内，Host 要访问存储设备时，首先向 Manager 发出 iSCSI-login 请求，Manager 查询用户列表，确定用户为合法用户，并将存储设备的实际地址以及访问控制信息发送给用户，然后用户向实际存储设备发出 iSCSI-login 请求，进行数据块传输。通过在 IP 网上直接传输 SCSI 存储命令，存储控制器的带外处理既完成对存储设备的统一管理又不会成为整个系统的瓶颈，使存储系统的性能大大提高。

1.3 存在的安全问题

这种存储结构虽然在存储性能上有很大提高，但整个存储系统却具有以下安全威胁：

(1)身份冒充。网络攻击者既可以伪装成 Host 从存储区域网内非法获取用户的数据，也可以伪装成 Target 使 Host 将大量数据存储到攻击者指定的存储位置。

(2)窃取数据。攻击者可以利用网络监听技术，直接从 Host 与 Target 间的传输通道上获取所有传输数据。

(3)重放攻击。在整个存储系统具有一定的认证机制的情况下，网络攻击者仍然可以通过截获认证数据并重新发送认证数据的方式，骗取存储系统中的数据。

由此可见，基于 iSCSI 的带外存储虚拟化结构虽然在存储性能上有突出的优势，但在实际的应用中却存在着安全危胁。安全问题得不到解决，存储系统的应用就必然受到制约。

2 基于 ECC 的 iSCSI 安全模型

根据存储结构特点，考虑到存储系统既需要进行身份认证又要进行密钥分发与管理，系统采用公钥密码体制[4]比较合适。同时，在公钥密码体制中，椭圆曲线密码体制具有非常大的优越性，在同等安全的情况下，其所需的密钥长度低、计算数据量小，而且在iSCSI协议中起始端与目标端建立TCP连接后，通过iSCSI的Login PDU进行信息交换，提供了对认证算法进行协商的支持。因此，本方案基于ECC进行安全模型的设计。

2.1 椭圆曲线密码体制

椭圆曲线密码体制[5](elliptic curves cryptosystems, ECC)，即基于椭圆曲线离散对数问题的公钥密码体制，最早于 1985 年由Miler和Koblitz分别提出，它是利用有限域上的椭圆曲线有限群代替基于离散对数问题密码体制中的有限循环群后所得到的一类密码体制。椭圆曲线离散对数问题的困难性是所有椭圆曲线密码方案安全性的基础。所谓椭圆曲线离散对数问题(ECDLP)是指：给定义于有限域 F_q 上的椭圆曲线 E，基点 $P\in E(F_q)$，阶为 n，点 $Q\in\langle P\rangle$，寻找一个整数 $l\in[0,n-1]$，使得 $Q=lP$ 的困难性。整数 l 称为 Q 的基于 P 的离散对数，表示为 $l=\log_P Q$。

2.2 安全模型

如图 2 所示，基于 iSCSI 构成具有带外存储虚拟化的存储区域网，基于 ECC 的认证模型如图 3 所示。其中 H 为客户端，M 为存储虚拟化控制器，T 为目标设备。由于 H 在 M 中有注册信息，而 T 由 M 进行统一管理，因此 H-M 间的相互通信以及 T-M 间的相互通信地址是固定的或已知的。这样图中的①、②两个传输通道可分别用预共享密钥确保数据传输安全，而 H 与 T 的通信地址是由 M 发送的，H 与 T 都没有对方的信息，双方互不信任，因此需要双向身份认证和协商一次性会话密钥。整个认证模型分为 3 个过程：(1)H 向 M 发出访问请求；(2)M 分别向 H、T 发送访问权限和用于认证的信息；(3)H 与 T 进行相互认证并协商出一次性会话密钥。

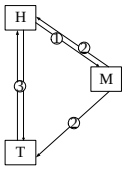

图 3 安全模型

2.3 协议描述

假定 M 与 H 有预共享密钥 k_{MH}，M 与 T 有预共享密钥 k_{MT}，E 为有限域 F_q 上的满足各项安全要求的椭圆曲线，基点 $P\in E(F_q)$，阶 n。椭圆曲线的点的个数为 $\#E(F_q)$，余因子 $h=\#E(F_q)/n$，KDF 是密钥导出函数，Enc_k 为加密函数，用户 H 与 T 相互认证并协商一次性会话密钥，协议描述如下：

(1)H 向 M 发出访问请求

用户 H 向 M 发送访问请求，将用户名 N_h 发送给 M。

(2)M 向 T、H 发送认证信息

1)M 收到请求后，查询用户列表，读取与用户相关的存储设备的 IP 地址 IP_h，端口号 $Port_h$，权限 R_h，其中 R_h 包括分配之后产生的公私钥对的使用期限和可访问存储区，并随机选择私钥 d_H、$d_T\in_R[1,n-1]$ 且 $d_H\neq d_T$，分别计算公钥 $Q_h(x_H,y_H)=d_HP$，$Q_t(x_T,y_T)=d_TP$，用 k_{MH} 对 d_H、Q_t、IP_h、$Port_h$ 以及权限 R_h 加密后将密文 $Enc_{k_{MH}}(d_H+Q_t+IP_h+Port_h+R_h)$ 发送给 H。

2)M 对 d_T、Q_h、用户名 N_h、权限 R_h 用 k_{MT} 加密后，将密文 $Enc_{k_{MT}}(d_T+Q_h+N_h+R_h)$ 发送给 T。T 收到 M 的信息 $Enc_{k_{MT}}(d_T+Q_h+N_h+R_h)$ 后，用 k_{MT} 解密出 d_T、Q_h、用户名 N_h、权限 R_h，并做好认证与密钥协商准备。

(3)T 对 H 进行认证

1)H 收到 M 的信息后，用 k_{MH} 解密

$Enc_{k_{MH}}(d_H+Q_t+IP_h+Port_h+R_h)$

选择随机参数 $k_H\in_R[1,n-1]$，计算：

$k_HQ_t=(x_H,y_H)$，$r_H=\overline{x_H}\bmod n$（$\overline{x_H}$ 为 x_H 的向上取整）

将 r_H、k_H、N_h 根据 IP 地址 IP_h、端口号 $Port_h$ 发送给 T，其中 r_H，k_H 为认证信息。

2)T 收到信息后，根据 N_h 计算：

$X_t(x_T,y_T)=k_Hd_TP$，$v_T=\overline{x_T}\bmod n$

若 H 具有由 M 通过保密通道传输的秘密信息 Q_t，则

$X_t(x_T,y_T)=k_Hd_TP=k_HQ_t$

从而有认证条件：若 $r_H=v_T$ 则认证通过。

(4)H 对 T 进行认证

1)T 对 H 认证通过后，选择随机参数 $k_T\in_R[1,n-1]$，计算：

$k_TQ_h=(x_T,y_T)$，$r_T=\overline{x_T}\bmod n$

将 r_T、k_T 发送给 H，其中 r_T、k_T 为认证信息。

2)H 收到后，计算：

$X_h(x_H,y_H)=k_Td_HP$，$v_H=\overline{x_H}\bmod n$

同上，若 $r_T=v_H$ 则认证通过。

(5)最后 H 与 T 生成共享密钥 k_{HT}

$Q_{ht}(x_{HT},y_{HT})=h(k_H+k_T)d_HQ_t=h(k_H+k_T)d_TQ_h$

$=h(k_H+k_T)d_Td_HP$

$k_{HT}=KDF(x_{HT})$

共享秘密 Q_{ht} 由一次性公钥 Q_h、Q_t 产生，并因每次认证双方选取的随机参数不同而不同，乘以 h 保证 Q_{ht} 的阶为 n 并在群 $\langle P\rangle$ 中。 (下转第 175 页)