网络安全的保证——密码*

朱晓琴
(盐城工学院 电气工程系,江苏 盐城　224003)

摘　要:讨论了网络对密码技术所产生的影响,并通过使用实例表明密码技术在安全技术领域的地位不可替代。

关键词:密码技术;网络安全;密钥
中图分类号:TP393.08　　文献标识码:A　　文章编号:1671-5322(2002)02-0068-03

1　密码

随着计算机技术,特别是计算机网络化的迅速普及和发展,使得网上开展的商务交易活动越来越多,如网上购物、网上信息发布、网上金融服务等等。而网上交易的焦点是安全性问题,即保证敏感的信息不被盗窃和篡改、伪造、内部数据不受黑客或病毒的侵袭,交易双方的身份得以确认。这一切需要取决于密码技术,它是保证信息的机密性、完整性及可用性的基本手段,它通过数据加密,消息认证和数字签名等方式,能在不安全的环境下对通信和存储的数据加以保护,以防止任何危及系统安全行为的发生。

从 20 世纪 70 年代中期开始,以数据加密标准 DES 和公钥密码为标志,现代密码技术进入了最富活力的崭新阶段。目前加密技术分为对称加密和非对称加密。信息的加密和解密使用相同的密钥时,交易双方的任何信息都通过这把密钥加密后传给对方。DES 是美国国家标准组织(ANSI)提出的目前广泛采用的对称加密方式之一,共有 56bit(Key-56),其分组长度是 64。非对称加密(公开密钥加密)是指在加密过程中,密钥被分解为一对。这对密钥中的任何一把都可以作为公开密钥通过非保密方式向他人公开,而另一把则作为专用密钥加以保存,公开密钥用于对机密的加密,专用密钥则用于对加密信息的解密[1]。

2　密钥的强度

在现实生活中,每个人都接触过一些安全设备,如保险柜,而有价证券的安全则是真伪的鉴别,这些传统安全机制有不可更改的物理标记及依赖于众所周知的特征。但是随着新技术的不断发展,安全专家的绝技很快为大众所掌握,因此,密码技术越来越被看好。因为其所追求的安全,应是一种客观的,可被证明的安全。即:

a、安全性不仅仅建立在静止不变的物理特征上。

b、安全判别不是只凭经验,还能逻辑地证明。

c、安全强度可无限增加。

下面的例子可证实最后一点。

2.1　身份认证

通过考查自动取款机(ATM)的工作过程,来看一个系统如何实现登录时的身份认证。在使用 ATM 之前,首先要检验用户的身份,即用户向 ATM 输入个人密码 PIN,ATM 经过与系统的联机查询来判断用户是否合法,它是通过静态的 PIN 来鉴别身份,一旦 PIN 被攻击者获悉,就可以进行欺骗了。为了避免这种静态密码潜在的不安全因素,通常采用一种改良的身份认证协议,它的要点是认证过程不传递任何秘密,而是以交换具有随机特征的数据来实现问答,使攻击者无从下手。这就是所谓的问答式协议 C&R(challenge and response)。

* 收稿日期:2001-09-10

作者简介:朱晓琴(1971-),女,江苏盐城市人,盐城工学院讲师。

2.1.1　用户与卡之间的鉴别

a、用户被要求输入 PIN

b、在卡内检验 PIN 正确与否

c、系统内不存储 PIN 及用户可随时改变

d、PIN 加密后存入卡中

2.1.2　卡与系统内的鉴别

a、系统随机提问 :r

b、卡内算出的答案 :$R' = f(K, r)$

c、系统计算 :$R = f(k、r)$

d、比较 R 与 R' 以确定用户的身份,f 为密码函数,K 为密钥

该系统优点 :通过一个简单的协议和密码函数,就可将系统的安全性提高一大步 :即有卡而不知 PIN 仍无法通过检查 ;卡与系统之间的对话是随机的,对窃听者毫无帮助。目前,许多系统都应用 C&R 实现身份认证,例如某些新一代的 IC 卡电话,移动通信系统等。这系统的缺点是,系统同时也掌握用户的密钥 K。

2.2　密钥管理

对密钥管理是基于共同保守秘密来实现的,但在一些特殊场合,为避免权力过于集中而采取分散管理,而该管理方法显然存在一个如果管理人员不严会带来严重后果的问题。为此,密码学研究一种所谓的门限体制(threshold schenes)[2],不但可实现密钥分散管理,还能保证人们所期望的各种安全需求。将问题一般化为十一门限体制,它将密钥分解为若干部分密钥并满足 :(1)任意 t 个部分密钥可恢复到完整的密钥 ;(2)t-1 或更少的部分密钥不能导出完整的密钥。下面以 $t = 2$ 为例来考查门限体制的构成。首先设一些简单的几何概念,设 $PG(m, q)$ 是 q 元域 $GF(q)$ 上的 m 一维射影空间,它的点 A 是一些非零 $(m+1)$ 一重 $(a_0, a_1 \cdots a_m)$,$a_2 \in GF(g)$,其中 $(a_0, a_1 \cdots a_m)$ 与 $(\lambda a_0, \lambda a_1 \cdots \lambda a_m)$,$\lambda \neq 0$,表示同一个点 $(m+1)$ 一重 $(a_0, a_1 \cdots a_m)$ 也称作点 A 的齐次坐标。连接点 A 和点 B 的直线 $\overline{AB}$ 由 $(\lambda a_0 + \mu b_0, \lambda a_1 + \mu b_1 \cdots \lambda a_m + \mu b_m)$ 其中 $\lambda, \mu \in GF(g)$ 不全为零。所以,$PG(m, g)$ 中有 $(q^{m+1}-1)/(q-1)$ 个点,每条直线上恰有 $q+1$ 个点。

首先固定射影平面 E,选 E 上的一条直线 l_0,密钥为 l_0 上任意一点 K 。部分密钥是位于经过点 K_0 的第二条直线上 l 的几个点 $K_1, K_2, \cdots K_n$。从任意两个部分密钥可以求出直线 l,进而得到与直线 l_0 的交点,即密钥 K_0,如图 1。

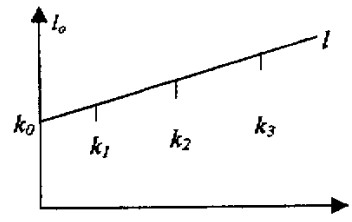

图 1　2 门限系统

Fig. 1　Two-threshold system

而由一个部分密钥导出密钥 K_0 的机会并不比它全盲目地搜索 K_0 的机会更好,其成功的概率不到 $1/q$,此处当 $q = 2^{100}$,攻击者要找到密钥 K_0 几乎是不可能的。

其次,由上述几何模型很容易构造一个认证系统。如确定平面 E 上的直线 l_0 作消费空间,密钥空间是 $E - l_0$。消息 M 在密钥之下的认证码定义为连线 $\overline{MK}$,每次通过检验 l_0 与 $\overline{MK}$ 的交点是否等于 M 来确定消息的真实性,此时就使得入侵者成功的概率达到理论上的最小值 $1/\sqrt{k} = 1/q$,此处 $K = |E - l_0|$ 是密钥的个数。

3　密钥的发展

面对网络信息化环境对安全的迫切需求,以及计算机技术进步对密码安全性的威胁,密码又将如何发展呢?1997 年美国国家标准与技术局(NIST)在全球范围公开征集新一代数据加密标准(AES)。AES 除了保持 DES 的某些好的特征外,分组长度和密钥长度都作了加强,特别是密钥长度为 128,129 和 256 可选。在公钥算法方面,基本上以整数分解(FP),离散对数(DLP)及椭圆曲线离散对数(ECDLP)为基础,前两者求解算法是平方筛法,而后者还未发现亚指数时间算法。

近年来,网络以空前的规模向全球各个角落延伸,这其中也部分得益于光通信技术的成熟,而光通信的理论基础是量子物理。因而随之发展的量子密码学也应运而生,并且其能够达到经典密码学所追求的无条件安全。故量子密码技术也越来越受到人们的关注。

参考文献 :

[1] 陈坚,孙志昂. 跨世纪的数字技术与数字产品[M]. 西安 :西安电子科技大学出版社,1999.

[2] Shamir A. How to share a secret[J]. Comm ACM,1985,22(1):612 - 613.

Roles of cryptographic techniques in Internet security

ZHUO Xiao-qing

(Department of Electronic Engineering of Yancheng Institute of Technology, Jiangsu Yancheng 224003, China)

Abstract: In this paper we discuss the influence caused by Internet on cryptographic techniques, it shows by instances that cryptography plays an unreplaceable role in the field of Internet security.

Keywords: cryptographic techniques; Internet security; cryptographic key

(上接第 7 页)

Current control mode pulse width modulator UC3842 and Its applications

ZHANG Lan-hong[1], CHEN Dao-lian[2]

(1. Department of Electric Engineering of Yancheng Institute of Technology, Jiangsu Yancheng 224003, China; 2. Automation institute of Nanjing university of Aeronautics Astronautics, Jiangsu Nanjing 210016, China)

Abstract: Operation principles and excellent characteristics of Current control mode pulse width modulator UC3842 are introduced, problems of its application which should be paid attention are pointed out., its application in Active - clamp flyback converters is discussed.

Keywords: Current control; pulse width modulate; slope compensation