ICS 35.040
L 80

中华人民共和国国家标准

GB/T 32213—2015

信息安全技术　公钥基础设施 远程口令鉴别与密钥建立规范

Information security technology—Public key infrastructure—Specification for remote password authentication and key establishment

2015-12-10 发布　　2016-08-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院软件研究所、中国科学院研究生院、中国电子技术标准化研究院。

本标准主要起草人:张立武、冯登国、张振峰、高志刚、荆继武、张严、王鹏翩、李强、段美姣、高能、陈星。

引　言

目前，基于口令的实体鉴别技术是应用最广泛的鉴别技术，并且可以预见在未来的相当长时间内还将作为一种重要的鉴别技术存在。这一方面是因为口令容易记忆、不需要额外的载体，使用方便；另一方面基于口令的鉴别协议通常简单高效，适用于用户量巨大的信息系统。然而，由于口令一般由可打印的 ASCII 字符组成，选择空间较小，因此安全的基于口令的鉴别协议的设计和实现较为困难。更为不利的因素是用户通常会选择能方便记忆且易于使用的具有特定意义的单词或者词组作为口令，更容易遭受字典式攻击的影响。因此，在构建基于口令的鉴别系统时选择安全的口令鉴别协议变得尤为重要。

非对称密码学的发展为基于口令的身份鉴别和密钥建立协议的构造提供了一种新的方向。通过结合非对称密码学和口令可以构造更安全的口令鉴别密钥建立协议，并能提供抵抗离线蛮力攻击、抵抗字典式攻击、前向安全性等重要安全性质。本标准选取了数个经过广泛理论分析和应用验证的协议，定义了这些协议的数学基础、协议流程。本标准为基于口令鉴别系统的设计和开发提供了参考。

信息安全技术　公钥基础设施
远程口令鉴别与密钥建立规范

1　范围

本标准定义了基于非对称密码技术实现远程口令鉴别与密钥建立的数学定义和协议构造。

本标准适用于采用基于口令鉴别与密钥建立技术的鉴别系统的设计和开发。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 18238.3—2002　信息技术　安全技术　散列函数　第3部分：专用散列函数

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

口令穷举/蛮力攻击　password exhaustive attack/brute-force attack

通过尝试口令所有可能的值，以获取实际口令，并实施违反信息安全策略的行为。

3.2

口令破解　password crack

成功的穷举/蛮力攻击口令及口令相关秘密数据或者成功攻击一个基于口令的密码系统。

3.3

多重散列　iterated hash

重复多次使用散列函数对输入进行散列计算的方法。

3.4

低等级口令　low grade password

易于受口令穷举/蛮力攻击的口令。

3.5

连带口令公钥　password-entangled public key

从口令和私钥计算得出的公钥。

3.6

口令限制私钥　password-limited private key

从口令计算得到的私钥，该私钥的随机性完全来自于口令，并且其随机性受口令随机性的限制。

3.7

口令限制公钥　password-limited public key

从口令限制私钥生成的用于验证口令正确性的数据。