

NIST 特别出版物 800-118

企业口令管理指南

NIST

**National Institute of
Standards and Technology**

Technology Administration
U.S. Department of Commerce

国家标准和技术研究所的建议

**Karen Scarfone
Murugiah Souppaya**

计算机安全

国家标准和技术研究所
信息技术实验室
计算机安全处

Gaithersburg, MD 20899-8930

2009 年 4 月



美国商务部
部长: Gary Locke

国家标准和技术研究所
副所长: Patrick D. Gallagher

目录

执行摘要

1 介绍

- 1.1 权限
- 1.2 目的和适用范围
- 1.3 适用对象
- 1.4 篇章结构

2 口令和口令管理概述

3 抑制针对口令的威胁

- 3.1 口令捕捉
 - 3.1.1 保存
 - 3.1.2 传输
 - 3.1.3 用户的知识和行为
- 3.2 口令猜测和破解
 - 3.2.1 猜测
 - 3.2.2 破解
 - 3.2.3 口令的强度
 - 3.2.4 用户口令挑选
 - 3.2.5 本地管理员口令挑选
- 3.3 口令替换
 - 3.3.1 忘记口令的恢复和重置
 - 3.3.2 对保存的账号信息和口令的访问
 - 3.3.3 社会工程
- 3.4 使用被攻破的口令

4 口令管理解决方案

- 4.1 一次登录技术
- 4.2 口令同步
- 4.3 本地口令管理
- 4.4 不同口令管理技术的比较

附录 A 设备和其他硬件口令

附录 B 术语表

附录 C 缩略语