Password Hashing Competition

SHA-3 requirements:
secure, **fast**
better than
MD5, SHA-1, SHA-2

PHC requirements:
secure, **slow**
better than
MD5, SHA-1, SHA-2
PBKDF2, bcrypt, scrypt

https://password-hashing.net

Password Hashing Competition

INTRODUCTION / CALL FOR SUBMISSIONS / CANDIDATES / TIMELINE / INTERACTION / EVENTS / FAQ

Introduction

The Password Hashing Competition (PHC) is an effort organized to identify new password hashing schemes in order to improve on
scrypt, etc.), and to encourage the use of strong password protection. Applications include for example authentication to web servic
devices, or key derivation for full disk encryption.

Motivations behind the PHC include:

- The poor state of passwords protection in web services: passwords are too often either stored in clear (these are the services
email after hitting "I forgot my password"), or just hashed with a cryptographic hash function (like MD5 or SHA-1), which expos
brute force cracking methods.
- The low variety of methods available: the only standardized construction is PBKDF2 (PKCS#5, NIST SP 800-132), and there
bcrypt and scrypt.
- A number of new ideas discussed within the security and cryptography communities, but which have not yet led to a concrete

(For more information on the topic of password hashing, a quick and comprehensive introduction is this presentation.)

To identify new password hashing schemes suitable for widespread adoption, the PHC follows the model of focused cryptographic
eSTREAM, or SHA-3 (see the Cryptographic competitions website).

Objective: **portfolio** of schemes, for diverse applications:

- Password hashing for web services
- Key-derivation for FDE
- PIN hashing for mobile platforms
- etc.

Organized by a panel of experts from industry, academia, gov

Engineering challenge:

costly to evaluate (slow, memory-hungry)
for **attackers** (GPUs, FPGAs, etc.)

Theoretical challenge:

prove **lower bounds** on time/space usage,
design **new modes** of operation

Associated events in 2013

Jul 30-31 in Las Vegas, USA *("offensive")*

Dec 2-6 in Bergen, Norway *("academic")*

http://passwordscon.org

Password Hashing Competition

Read the call for submissions on
https://password-hashing.net

Join the mailing list
(discussions-subscribe@password-hashing.net)

Submit before Jan 31, 2014

#pwdhc on Twitter; #phc Freenode chan