



Password security: past, present, future (with strong bias towards password hashing)

Solar Designer <solar@openwall.com>

<http://www.openwall.com>

May 2012

1960s to early 1970s: plaintext password storage

Early time-sharing systems

- CTSS

- ▶ "one afternoon [...] any user who logged in found that instead of the usual message-of-the-day typing out on his terminal, he had the entire file of user passwords"

Fernando J. Corbato, "On Building Systems That Will Fail", 1991 (Turing Award Lecture)

(The problem was a text editor temporary file collision, "early 60's" to "1965" by different sources.)

- TENEX had a character-by-character timing leak exacerbated by paging
- "The UNIX system was first implemented with a password file that contained the actual passwords of all the users"

Robert Morris and Ken Thompson, "Password Security: A Case History", 1978

Besides, some typewriters would print the password being typed unless manually prevented from doing so.

Early 1970s - Multics: non-cryptographic hashes

Attempted one-way transformations, but no "true" cryptographic hashes yet

- "Multics User Control subsystem stored passwords one-way encrypted [...] I knew people could take square roots, so I squared each password and ANDed with a mask to discard some bits."
- After successful break by the Air Force tiger team doing a security evaluation of Multics in 1972-1974, "we quickly changed the encryption to a new stronger method"

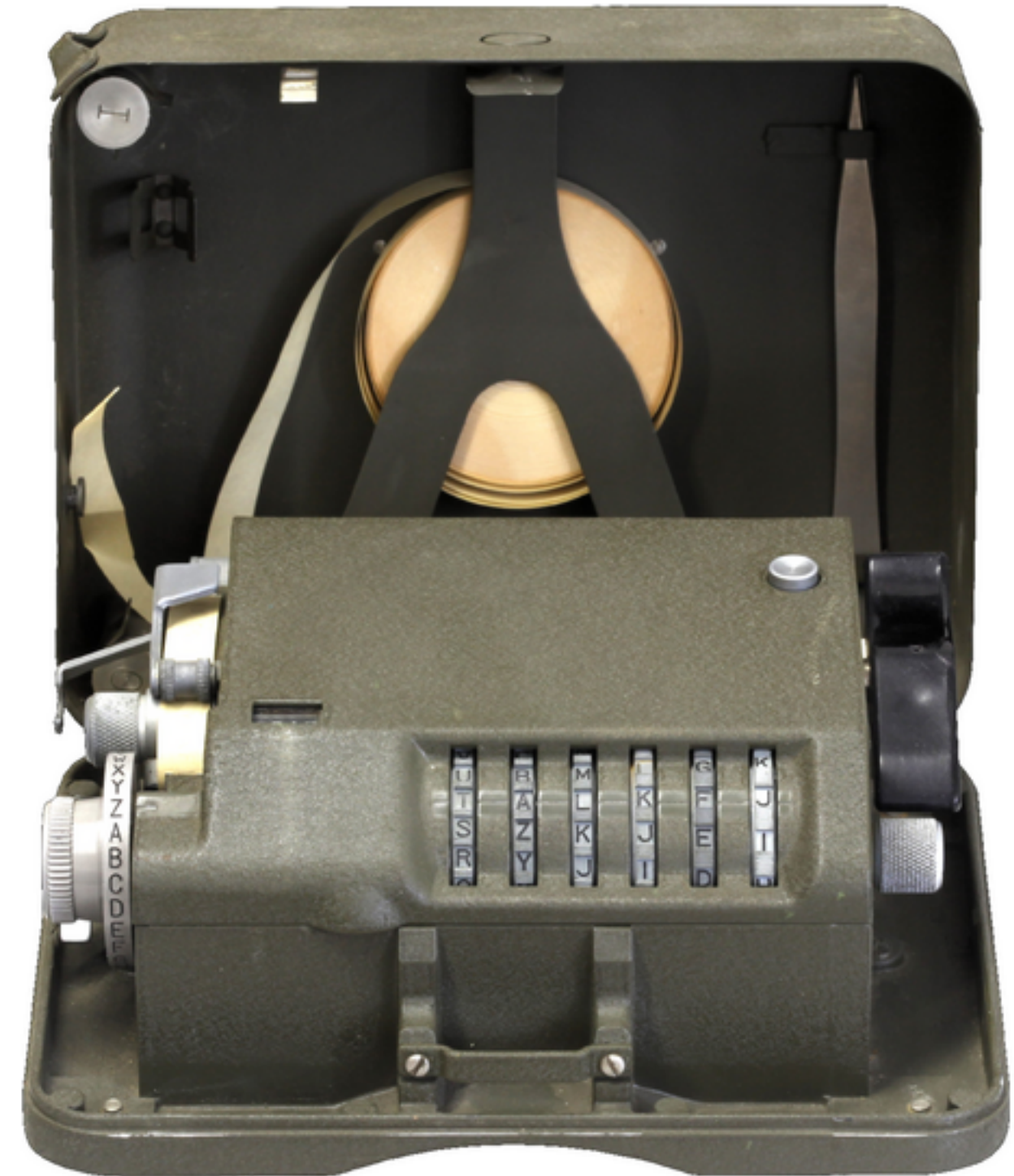
Tom Van Vleck, "How the Air Force cracked Multics Security", 1993 (with later updates)

Early 1970s - Unix: weak cryptographic hash

crypt(3) of Unix up to 6th Edition inclusive reused code from an "encryption program [that] simulated the M-209 cipher machine used by the U.S. Army during World War II. [...] the password was used not as the text to be encrypted but as the key, and a constant was encrypted using this key."

M-209B, cryptography collection of the Swiss Army headquarters

Photograph by Rama, Wikimedia Commons, licensed under CeCILL v2 and CC-BY-SA-2.0-FR



Early 1970s - Unix: too fast and not salted

The problems were understood before 7th Edition (1978)

- "The running time to encrypt one trial password and check the result turned out to be approximately 1.25 milliseconds on a PDP-11/70 when the encryption algorithm was recoded for maximum speed."
- "It takes essentially no more time to test the encrypted trial password against all the passwords in an entire password file, or for that matter, against any collection of encrypted passwords, perhaps collected from many installations."

Late 1970s - Unix: DES-based crypt(3)

Unix 7th Edition crypt(3) is a cryptographic one-way hash function built upon the DES block cipher

- "DES is, by design, hard to invert, but equally valuable is the fact that it is extremely slow when implemented in software."
 - ▶ Much faster software implementations of DES were devised later
- "the algorithm is used to encrypt a constant [,which] can be made installation-dependent."
 - ▶ First known mention of local parameterization?
- "Then the DES algorithm is iterated 25 times"
 - ▶ First known use of password stretching?

Late 1970s - Unix: password strength checking

- "The password entry program was modified so as to urge the user to use more obscure passwords."
 - ▶ First known use of automated proactive password strength checking?
- "Salted Passwords": "when a password is first entered, the password program obtains a 12-bit random number [...] and appends this to the password typed in by the user." "When the user later logs in to the system, the 12-bit quantity is extracted from the password file and appended to the typed password."
 - ▶ First known use of salts with password hashing?

Late 1970s - Unix: salting

- Salting "does not increase the task of finding any individual password, starting from scratch, but now the work of testing a given character string against a large collection of encrypted passwords has been multiplied by 4096 (2^{12})."
 - ▶ With uniform distribution, there are ~3740 unique salts in 10,000 password file entries
- "it becomes impractical to prepare an encrypted dictionary in advance."
- "It becomes nearly impossible to find out whether a person with passwords on two or more systems has used the same password on all of them"

Late 1970s - Unix: "The Threat of the DES Chip"

- "Chips to perform the DES encryption are already commercially available and they are very fast."
- In crypt(3), "one of the internal tables of the DES algorithm [...] is changed in a way that depends on the 12-bit random number. The E-table is inseparably wired into the DES chip, so that the commercial chip cannot be used."
 - ▶ Except for hashes on which the 12-bit salt happens to be zero

Food for thought: what if DES chips were installed into some Unix workstations and servers, and instead of the E-table hack crypt(3) allowed for much higher iteration counts on those systems?

Late 1970s - Unix: salt & hash encoding syntax

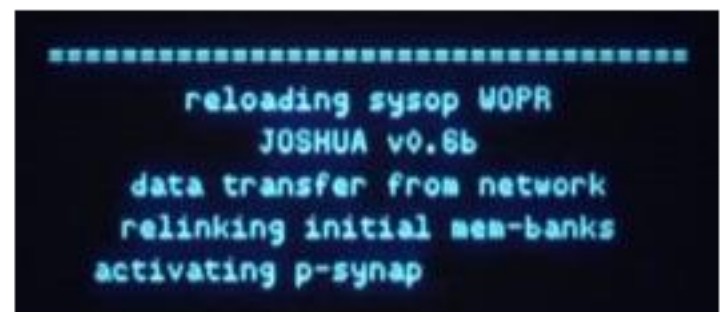
Unix /etc/passwd file excerpt (2.9BSD default, 1983 - but the same hash encoding is used since 7th Edition in late 1970s)

```
wnj:ZDjXDBwX1e2gc:8:2:Bill Joy,457E,7780:/a/guest/wnj:/bin/csh
dmr:AiInt5qKdjmHs:9:2:Dennis Ritchie:/a/guest/dmr:
ken:sq5UDrPlKj1nA:10:2:& Thompson:/a/guest/ken:
mike:KnKNwMkyCt8ZI:11:2:mike karels:/a/guest/mike:/bin/csh
carl:S2KiTfS3pH3kg:12:2:& Smith,508-21E,6258:/a/guest/carl:/bin/csh
joshua::999:2:&:/usr/games:/usr/games/wargames
```

The first two characters are the salt (12-bit), followed by 11 characters of the hash (64-bit).

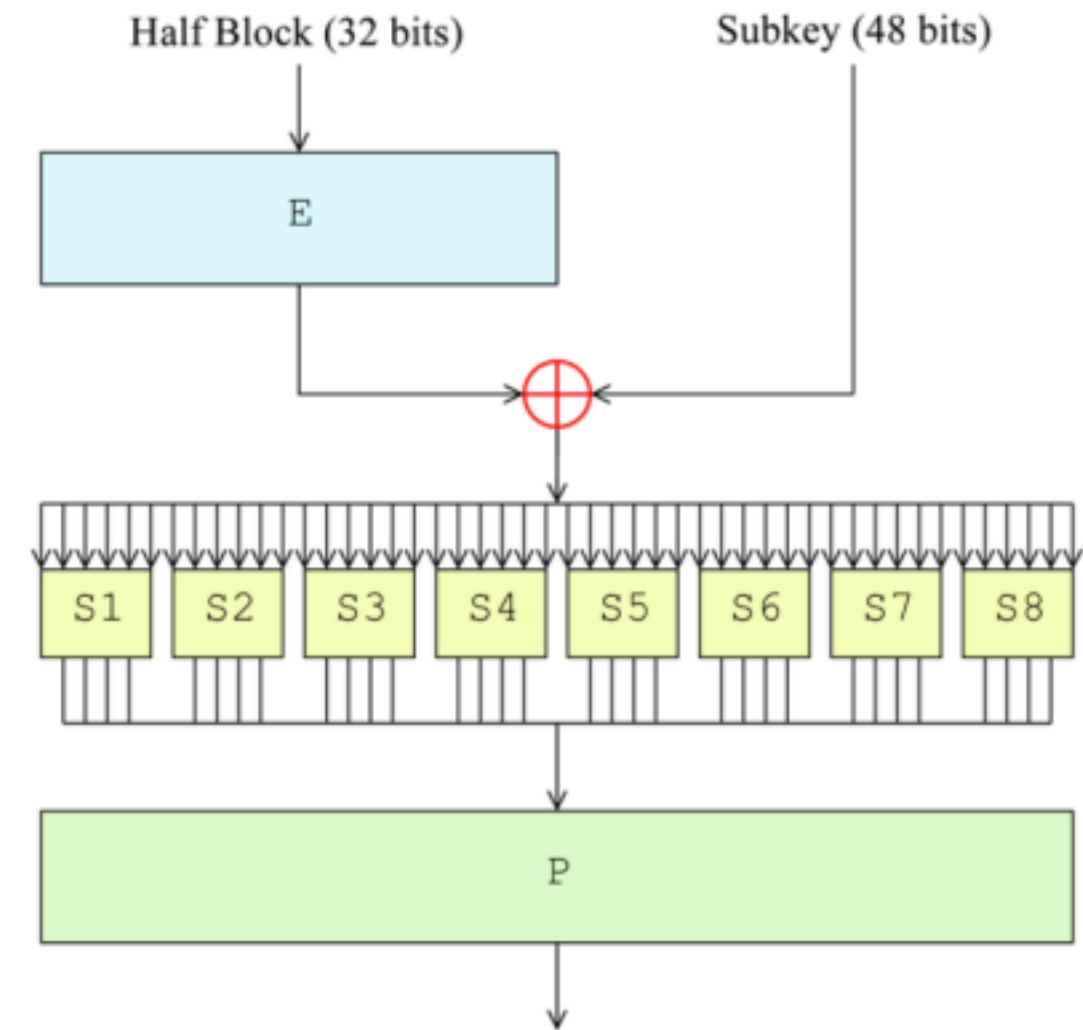
The WarGames movie came out in 1983, featuring war dialing and more.

"Joshua" is a backdoor password in the movie.



Why was DES slow in software?

- Each S-box uses only 6 bits and produces 4 bits
 - ▶ Typical CPUs have much wider word size (16- to 64-bit, then even wider SIMD)
- Possible optimizations (late 1980s)
 - ▶ Spread the 6 and 4 data bits throughout up to 64-bit words to save on other overhead (E and P lookups, shifts to produce array indices)
 - ▶ Do two S-box lookups at once (12-to-8)
 - It is usually not practical to go further (combined tables become too large for fast access)
- Wasteful even with the above optimizations



This diagram illustrating one round of DES has been released into the public domain by its author, Matt Crypto

1980s: no progress on the defense side?

- "A Fast Version of the DES and a Password Encryption Algorithm" by Matt Bishop, 1987
 - ▶ Speeds up crypt(3) by a factor of 10 to 20 through the use of larger/combined lookup tables (up to 200 KB total) and other optimizations
- Morris worm (1988) uses its own semi-fast implementation of DES-based crypt(3) to crack passwords on local accounts
 - ▶ 9 times faster on a VAX 6800 (45 passwords/second), needs only 6 KB
- Ultrix crypt16: poor attempt to overcome the 8-character limitation
- VMS introduces its own plethora of fancy password hashes

Late 1980s to 1990s - Unix: password shadowing

- "Password shadowing first appeared in UNIX systems with the development of System V Release 3.2 in 1988 and BSD4.3 Reno in 1990."

Wikipedia

- Shadow Password Suite by Julianne Frances Haugh, 1988+
- It took many years for the various Unix-like systems, individual Linux distributions, etc. to catch up (although a few were pretty quick)

Password hashes were moved out of `/etc/passwd` and into file(s) not readable by regular users. Typical filenames are `/etc/shadow` (SysV and others) and `/etc/master.passwd` (BSD), although some "trusted" systems use per-user files under `/tcb` or `/etc/tcb`.

In 2001, Openwall GNU/*/Linux made use of per-user shadow files under `/etc/tcb` to reduce privileges of the password-changing program, `passwd(1)` - something those "trusted" systems did not do

Early 1990s: password security tools

- COPS by Dan Farmer
 - ▶ A local security auditing tool for Unix systems
 - ▶ Includes detection of poor passwords as one of the features
- Crack (for Unix) by Alec Muffett
- Cracker Jack (for DOS and OS/2) by The Jackal
- goodpass.c, and later CrackLib by Alec Muffett
 - ▶ "to be wired into "passwd" & "yppasswd", etc."
- npasswd, etc. with proactive password strength checking included

Early 1990s: LM and NTLM hashes

- LAN Manager uses a particularly weak password hashing method ("LM hash") in its authentication protocol
 - ▶ Passwords are case-insensitive
 - ▶ An up to 14-character password is split after the 7th character and the two halves are used as DES encryption keys
 - ▶ The two password "halves" may be cracked separately, just like with crypt16 and bigcrypt, but much faster (no salt, shorter, case-insensitive, no iterations)
- Windows NT stores LM hashes, along with MD4-based NTLM hashes
 - ▶ Cracking the weaker LM hashes is usually enough
 - ▶ NTLM hashes are also a step back as compared to Unix crypt(3): no salt, no iterations

Early 1990s: BSDi configurable iteration count

- BSDi BSD/OS extends DES-based crypt(3) with proper support for long passwords, configurable iteration count stored along with each hash (the "J9.." below corresponds to 725 iterations), and 24-bit salt

```
_J9..saltLSQbyJrHIzg
```

- HP-UX, OSF/1, Digital Unix bigcrypt: poor attempt to fix crypt16
 - ▶ Still possible to crack the 8-character "halves" separately

```
y3hOhMyjWl8ZgRrZfS5BcgqE  
winniethepooh
```


Mid 1990s: FreeBSD fixed iteration count

- FreeBSD MD5-based crypt(3) by Poul-Henning Kamp, 1994
 - ▶ Long passwords, 1000 iterations of MD5 (not configurable), up to 48-bit salt
 - ▶ "On a 60 Mhz Pentium this takes 34 msec" (source code comment)
 - A password cracking optimized reimplementation later ran 5 times faster (also on original Pentium)
 - ▶ In late 1990s, adopted by most Linux distributions and Cisco IOS

`1longsalt$0QgNqdKo00f5to4mPrBB3.`

- "How should a password algorithm be designed today? I'd use iterated, salted, locally-parameterized SHA or MD5 [...] I'd use an iteration count stored with the hashed password"

Steven M. Bellovin, Bugtraq mailing list posting, 1995

1995-1997: QCrack - crypt(3) precomputation

- During precomputation, each candidate password (typically a dictionary word or the like) is hashed with all 4096 possible salts. Then one byte is written out per hash (thus, 4 KB per candidate password)
- On a Pentium 120 MHz that would do ~1 1000 c/s with John the Ripper, having a 1 GB (an entire hard drive or tape) of QCrack-precomputed partial hashes would save at most 1 day of computation during an attack
- Usually not practical, but illustrates precomputation attacks prior to the advent of rainbow tables

Although there are anecdotes of people having used tapes with pre-computed DES-based crypt(3) hashes before, QCrack written in 1995-1997 by The Crypt Keeper appears to be the only generally available tool of this nature

1997: bitslice DES

- "A Fast New DES Implementation in Software", Eli Biham, 1997
 - ▶ "This implementation is about five times faster than the fastest known DES implementation on a (64-bit) Alpha computer, and about three times faster than than our new optimized DES implementation on 64-bit computers. [...] view the processor as a SIMD computer, i.e., as 64 parallel one-bit processors computing the same instruction."
 - ▶ ~100 gates per S-box
- "Reducing the Gate Count of Bitslice DES", Matthew Kwan, 1998+
 - S-box expressions released in 1998, technique presented in 1999, paper posted online many years later
 - ▶ 51 to 56 gates per S-box on average depending on available gates

The gate count was further reduced in later years by Marc Bevand (45.5 using Cell's "bit select" instruction), Dango-Chu (39.875, ditto), Roman Rusakov (32.875 with "bit selects", 44.125 without)

Why is bitslice DES faster?

- A single instance of DES uses at most 12 bits per machine word
 - when doing 12-to-8 dual S-box lookups, which also typically exceed the size of L1 data cache
- With bitslicing, we compute e.g. 64 instances of DES in parallel on a 64-bit CPU - making full use of every bit in the 64-bit machine words
- We could compute multiple non-bitsliced instances of DES side-by-side and more fully use the machine word width in this way, but this requires support for vectorized array lookups for efficient implementation
 - ▶ In 2000s, some CPUs got SIMD permute instructions that are potentially usable: PowerPC AltiVec VPERM, Cell SHUFB, Intel SSSE3 PSHUFB, AMD XOP VPERM
 - ▶ 2013+: Intel Haswell microarchitecture is expected to include AVX2 VSIB (gather)

1998: validation vs. cracking speed ratio

Bitslice DES made it apparent that even an attacker possessing only the same kind of CPU that is used by the defender (such as in an authentication server) has a speed advantage resulting from the inherent parallelism of password cracking (test many passwords)

- ▶ "You can increase the iteration count, but you're limited with the validation time. [...] it is important to make sure that the best implementation of the same hash, but optimized for cracking (multiple keys at a time), is not much faster than the password validation function."
- ▶ "One-way hash choice: make sure it can't be made faster by a bitslice implementation, or mixing the instructions from two separate hashes (for higher issue rate). That is, the function should have a lot of natural parallelism, so that we can exploit it all in the validation function."

Solar Designer, "bitslice & crypt(3) choice", comp.security.unix posting, 1998

1990s: new concepts

- Key derivation function (KDF)
- Key stretching (password stretching) was formally defined and studied
 - ▶ J. Kelsey, B. Schneier, C. Hall, and D. Wagner, "Secure Applications of Low-Entropy Keys", 1997
 - ▶ A related concept became known as "strengthening" (throw salt away), but stretching ended up winning
- Passphrase
 - ▶ In PGP, S/Key, SSH, encrypted filesystems

1990s: network sniffing

- Non-switched Ethernet (10BASE2, 10BASE-T) was prevalent
- Network protocols typically transmitted passwords in the clear
 - ▶ This has started to change in mid-1990s
- A common attack was sniffing of passwords via a machine (such as a compromised server) on the same Ethernet segment with the target server or with some of the users
- This has contributed to the rise of more advanced authentication methods

1990s: alternative authentication methods

Some of these are an improvement, but they are susceptible to offline password guessing attacks on certain authentication material anyway:

- Challenge/response pairs
 - ▶ What may be worse, common protocols such as POP3 APOP are poorly defined, requiring that plaintext-equivalents be stored on the server, even though this could be avoided
- Kerberos: TGTs, AFS user database
- S/Key, OPIE: skeykeys file
- SSH: passphrase on private key
- SRP: verifiers

Thus, passwords (or passphrases) are not going away, and proper password hashing or key derivation remains relevant even if as a component of other authentication schemes

Other uses of passwords

A password or passphrase is also used to protect things such as:

- Encrypted home directories, filesystems, full disks
 - ▶ FileVault, EFS, TrueCrypt, LUKS/dm-crypt, eCryptfs, ...
- Archives (WinZip, RAR, ...)
- Wireless networks (WiFi WPA-PSK)
- PGP secret keys
- Mac OS X keychains, other "password vaults"

This will also keep passwords/phrases and decent KDFs relevant for many years to come

1996-2000: more password security tools

- John the Ripper by Solar Designer (later also by project contributors)
 - ▶ "Incremental mode" orders candidate passwords for decreasing estimated probability considering trigraph frequencies, yet is able to search a keyspace exhaustively given enough time
 - ▶ Takes advantage of 64-bit CPUs, MMX, bitslice DES (1998+)
- pam_passwdqc by Solar Designer
 - ▶ An alternative to pam_cracklib, with support for passphrases
 - ▶ Later became passwdqc tool set co-authored by Dmitry V. Levin
- L0phtCrack by L0pht Heavy Industries
 - ▶ Cracks LM and NTLM hashes used by Windows NT

Effect of hash type and password policy

passwdqc vs. KoreLogic's DEFCON 2010 contest passwords

- Of the MD5-based crypt(3) hashes, teams cracked 33%
 - ▶ passwdqc with default policy would permit 3.5% of cracked or 1.1% of all
 - When a user's desired password is rejected, the user would not always pick a password that would not get cracked. Estimate: 1.9% would be crackable.
 - ▶ Of the uncracked passwords, passwdqc would reject 45% and permit 55%
- Of the NTLM hashes, teams cracked 94%
 - ▶ passwdqc with default policy would permit 35% of cracked or 33% of all
 - Estimate: 53% would be crackable.
 - ▶ Of the few uncracked passwords, passwdqc would reject 14% and permit 86%

To withstand offline attacks, both a decent hash type and a decent password policy should be used at once

Late 1990s: OpenBSD bcrypt

- "We present two algorithms with adaptable cost -- eksblowfish, a block cipher with a purposefully expensive key schedule, and bcrypt, a related hash function."

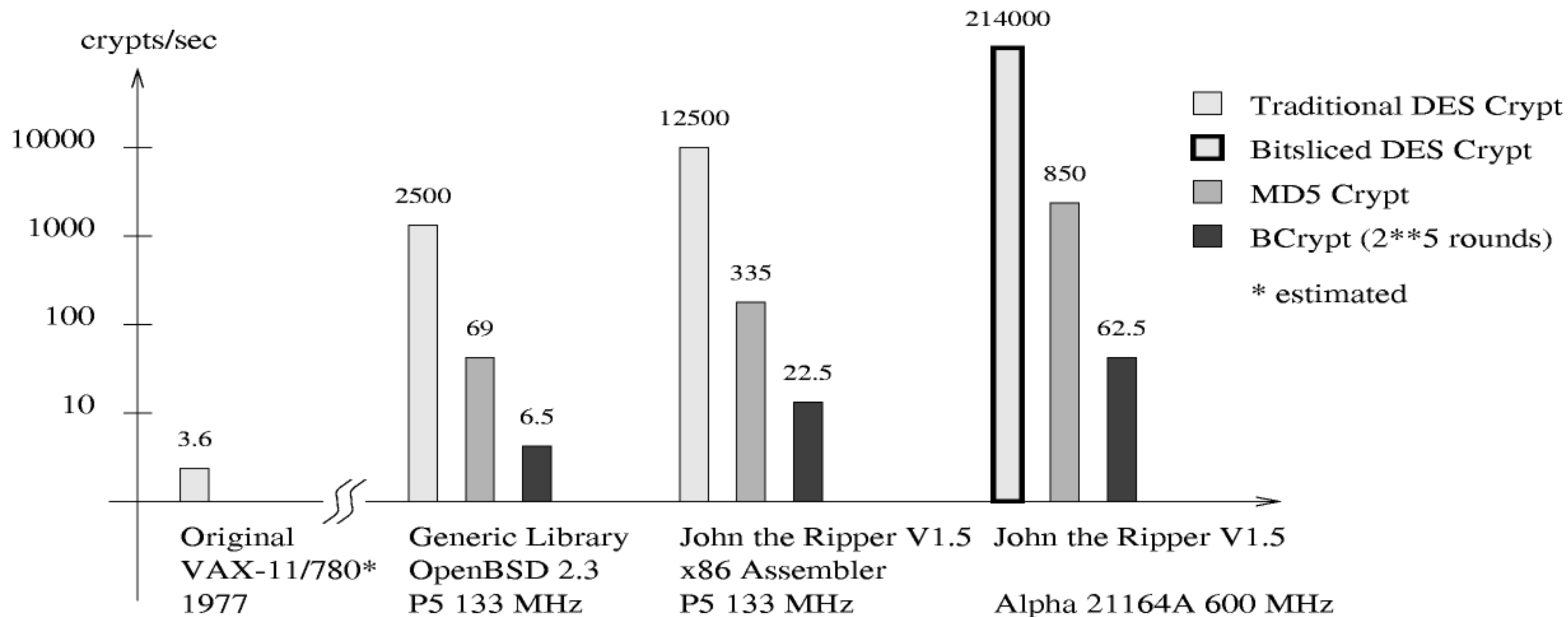
Niels Provos and David Mazieres, "A Future-Adaptable Password Scheme", The OpenBSD Project, 1999

- ▶ Configurable iteration count (encoded as base-2 logarithm), 128-bit salt
- ▶ In 2000 and later, adopted by Openwall GNU/*/Linux, ALT Linux, OpenSUSE and made available as a non-default option on other *BSDs and Solaris

```
$2a$08$128bitsalt22charslong0lHvsqGDe2t1XUwNgAVQ82BcG8Q8dWfu
```

- 8-to-32 variable S-boxes, so uses 32 bits per machine word only
 - ▶ Would need scatter/gather (or at least gather) to overcome that

Late 1990s: crypt(3) speed comparison



Niels Provos and David Mazieres, "A Future-Adaptable Password Scheme", The OpenBSD Project, 1999

May 2012: modern crypt(3) cracking speeds

Since 1999

- crypt(3) cracking speeds for all flavors discussed so far have increased by a factor of 50 to 200 per CPU chip (for the fastest code and CPUs)
- Configurable iteration counts do help to compensate for that, although system defaults tend to be rather low to support a wide range of hardware and usage scenarios (e.g., bcrypt is typically used at costs only 8 to 32 times larger than the "2⁵ rounds" baseline used in 1999 benchmarks)
 - ▶ Cracking speeds increase more rapidly than single password validation speeds
- AMD Radeon HD 7970 "Tahiti" GPU provides an additional boost of a factor of 5 for DES and 20 for MD5 (but none for bcrypt so far - may change)

Late 1990s to 2007(+?): web apps use raw MD5

"Web apps" started to appear, usually written in PHP, so indeed they directly used PHP's `md5()` function for password hashing.

PHP also offers `crypt()`, but those hashes were not sufficiently portable between systems (in 1990s, some Unix-like systems could lack DES-based `crypt(3)` because of US export regulations, and PHP is not Unix-only). This may be too complicated an explanation, though. Chances are that those web apps' developers simply did not know the options.

- ▶ No password stretching: Cracking speeds for one hash are about 1000 times higher than those for FreeBSD's MD5-based `crypt(3)`.
- ▶ No salt: Effective cracking speeds (`{account, password}` combinations tested per second) for non-targeted attacks against large raw MD5 hash databases are even higher (times the number of hashes), precomputed hash tables may be used.

2003: rainbow tables

- "As an example we have implemented an attack on MS-Windows password hashes. Using 1.4GB of data (two CD-ROMs) we can crack 99.9% of all alphanumerical passwords hashes (2^{37}) in 13.6 seconds"

Philippe Oechslin, "Making a Faster Cryptanalytic Time-Memory Trade-Off", 2003

- ▶ Martin Hellman's time-memory trade-off (1980) enhanced and applied to password hashes
- Storage needs are a lot lower than for QCrack's naive approach
- Nevertheless, infeasible with large random salts
- Each hash being cracked requires extra processing
 - ▶ With a very large number of saltless hashes it may be quicker not to use rainbow tables, but instead to hash each candidate password and compare against all hashes being cracked e.g. with large yet in-memory bitmaps and hash tables for $O(1)$ comparisons cost

2007+: web apps move to phpass

- phpass is an easy to use PHP password hashing class
 - ▶ phpass would use bcrypt if available (CRYPT_BLOWFISH in PHP), and if not then fallback to BSDi-style extended DES-based hashes (CRYPT_EXT_DES in PHP), with "a last resort fallback to MD5-based salted and variable iteration count password hashes implemented in phpass itself (also referred to as portable hashes)"
- phpass has started to see some adoption by major web apps (WordPress, phpBB3, and Drupal) in 2007, which has helped further adoption
 - ▶ Not surprisingly, many of them chose to force the use of the "portable hashes", which unfortunately make less efficient use of the server's CPU

phpass was originally written during a security audit of an Openwall client's "web app" in 2004 in response to the findings (so that they could replace their weak password hashing). It was released publicly in 2005.

phpass portable hashes

The portable hashes are very simple, which was key to phpass' acceptance. More elaborate "portable hashes" would likely not be accepted; this may be something to try for a next generation phpass now that the foot is in the door.

```
$P$BsaltsaltW41DSqbN0VQv0GUtYyhFv.
```

In this example, "B" means 2^{13} or 8192 iterations. The salt is 48-bit.

phpBB3 uses 2048 iterations, WordPress uses 8192 (but these hashes are compatible with each other). Drupal 7 uses a revision of these hashes with MD5 replaced by SHA-512, the prefix changed to "\$S\$", and iteration counts at 16384 and beyond (increasing between releases).

2007+: password cracking on GPUs

- Pioneered by Andrey Belenko of Elcomsoft
 - ▶ Initially for NTLM, LM, and raw MD5 hashes, achieving speeds of over 100M per second
Beyond reach of existing software on CPUs at the time (except for Cell)
- Andrey and others improved the speeds and implemented other attacks
 - ▶ 2010: Whitepixel by Marc Bevand achieves 33.1 billion passwords/second against a single raw MD5 hash on a sub-\$3000 4x AMD Radeon HD 5970 computer (8 GPU chips)
 - ▶ 2012: oclHashcat-lite by atom does 10.9 billion on a single HD 6990 card (two GPU chips)
 - ▶ 2011: oclHashcat-plus by atom made GPUs usable for a full set of password cracking attacks on a wide variety of hashes (both "fast" and "slow" ones)
- John the Ripper is catching up with GPU support
 - ▶ 2011, 2012: more limited in GPU support than oclHashcat-plus, but Open Source

2007: SHA-crypt in glibc 2.7+

Introduced for political rather than technical reasons

- "Security departments in companies are trying to phase out all uses of MD5. They demand a method which is officially sanctioned. For US-based users this means tested by the NIST."

Ulrich Drepper, "Unix crypt using SHA-256 and SHA-512", 2007 (revised in 2008)

- Configurable iteration count (5000 by default), large salts

Ulrich's SHA-crypt.txt shows some confusion during SHA-crypt design: "the produced output is 32 or 64 bytes respectively in size. This fulfills the requirement for a large output set which makes rainbow tables less useful to impossible" - that's nonsense

```
$6$saltstring$svn8UoSVapNtMuqlukKS4tPQd8iKwSMHWj1/O817G3uBnIFNjnQJuesI68u4OTLiBFdcbYEdFCoEOfaS35inz1  
$6$rounds=10000$saltstringsaltst$OW1/O6BYHV6BcXZu8QVeXbDWra3Oeqh0sbHbbMCVNSnCM/UrjmM0Dp8vOuZeHBy/YTBmSK6H9qs/y3RnOaw5v.
```

SHA-crypt analysis

- SHA-crypt hashes are decent (albeit not a technical improvement), especially the flavor based on SHA-512
 - ▶ Uses 64-bit machine words; not SIMD, though
- SHA-512 is not as GPU-friendly as e.g. MD5, yet is reasonable to attack on current GPUs (2012)
 - ▶ SHA-crypt based on SHA-512 at default rounds=5000 can be attacked at ~11500 c/s on NVIDIA GTX 570 1.6 GHz with a John the Ripper patch by Claudio Andre
 - ▶ bcrypt at "\$2a\$08" (256 iterations), which is default on some systems and is achieving similar validation speed to the above, can be attacked at ~680 c/s on AMD FX-8120 3.1 GHz (combined speed for 8 threads) with John the Ripper; no speedup from GPUs yet (but this may change)

2009: sequential memory-hard functions

Defense against specialized hardware (ASICs, FPGAs, GPUs)

- "We introduce the concepts of memory-hard algorithms and sequential memory-hard functions, and argue that in order for key derivation functions to be maximally secure against attacks using custom hardware, they should be constructed from sequential memory-hard functions."

Colin Percival, "Stronger key derivation via sequential memory-hard functions", 2009

- ▶ General-purpose computers spend more die area on memory (RAM, caches) than on computation logic (ALUs, vector units) inside CPUs
- ▶ RAM is about as expensive to implement in cracking-optimized hardware, whereas computation logic is cheaper to implement in a specialized and massively-parallel fashion (avoiding the overhead on instruction decode, out-of-order execution, etc.)

2009: scrypt

- The scrypt KDF accepts three parameters tunable "according to the amount of memory and computing power available, the latency-bandwidth product of the memory subsystem, and the amount of parallelism desired".
- As defined, scrypt uses Salsa20/8 core as its main cryptographic primitive, which makes efficient use of up to 128-bit SIMD vectors
 - ▶ It might be possible to use wider SIMD vectors when p is greater than 1
- A variation of scrypt based on another cryptographic primitive is possible (e.g., to please those requiring NIST-approved cryptography)
 - ▶ Alternatively, it may be shown that scrypt's cryptographic security is achieved by its initial use of PBKDF2 with SHA-256, whereas further processing is "non-cryptographic"

2012: current uses of script

- As KDF in script author's simple file encryption program
- As KDF in Tarsnap, script author's "online backups for the truly paranoid"
- As a proof-of-work scheme in Litecoin, "a coin that is silver to Bitcoin's gold" (after Bitcoin mining became feasible on GPUs and FPGAs only... ASIC, anyone?)
- No crypt(3) encoding syntax is defined for script yet
 - ▶ script author is the FreeBSD Security Officer. He must be really good at resisting the temptation of making the system use his new creation (creature?) before it's "mature"

Late 1990s to 2000+: 2FA goes mainstream

- Many online services and especially banks have started to treat user-targeted attacks such as trojans and phishing seriously
- To this end, they deployed 2-factor authentication where passwords are augmented with one-time codes or another second authentication factor
 - ▶ There's some debate as to whether and which kinds of 2FA are effective against which types of attacks. "Two-factor authentication isn't our savior. It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions. It solves the security problems we had ten years ago, not the security problems we have today."





Bruce Schneier, "The Failure of Two-Factor Authentication", 2005

- Passwords remain relevant as one of the factors: "something you know"



MULTIFACTOR AUTHENTICATION



KNOW	HAVE	ARE	DO
			
Passwords ID Questions Secret Images	Token (Smart) Card Phone	Face Iris Hand/Finger	Behavior Location Reputation

Threat models

- Offline attacks

- ▶ Decent hash type
- ▶ Proper password stretching settings
- ▶ Random per-account salts

With targeted attacks (on few high-value accounts as opposed to lots of low-value ones), salts are of relatively little help, yet they should be used in those cases as well

- ▶ Strict password policy

- Password reuse across sites

- Who is responsible for what?

- Online attacks

- ▶ Password policy
- ▶ Per-source rate limiting
- ▶ Additional authentication factors
- ▶ Behavior analysis

Akin to a "spam filter", may reduce success rate of non-targeted attacks (Google does it)

- ▶ User-targeted attacks

Phishing, trojans, client vulnerability exploits

- ▶ Network-based attacks

DNS, routing, MITM, old-fashioned sniffing

- ▶ Server vulnerability exploits

Desirable properties of a future KDF

- These need to be configurable
 - ▶ With settings encoded along with password hashes, etc. - depending on specific use case
- Lots of parallelism within one instance
- Ability to use almost arbitrarily wide SIMD vectors within one instance
- Existing hashes upgradable to higher iteration counts
 - ▶ without knowledge of the plaintext passwords
 - ▶ Maybe to higher memory cost and higher available parallelism as well? - tricky
- Friendly to whatever hardware we have in the defender's system
 - ▶ and to hardware that we might have there in the foreseeable future
- Optionally unfriendly to other kinds of hardware

KDFs unfriendly to hardware we do not have

- This is controversial
 - ▶ Concept pioneered in DES-based crypt(3) being unfriendly to existing DES chips
- If our authentication server only has CPUs and RAM, then the KDF being GPU-unfriendly is a plus
 - ▶ However, future server CPUs might have embedded GPUs or similar (e.g., Intel MIC)
- If we have an FPGA or ASIC in the server, being CPU-unfriendly is a plus
 - ▶ e.g., this may slow down attacks with a botnet, where victims' computers will generally not have specialized hardware
- Multiple blocks friendly to different hardware components that we have
 - ▶ However, complexity is the enemy of security and reliability
- Configurable unfriendliness (set of blocks to use and their weights)

CPU + RAM friendliness

- CPU-friendly

- ▶ 32- or 64-bit integers, SIMD
- ▶ Sequential memory-hard functions
- ▶ "Large" variable S-boxes

However, this prevents use of SIMD until AVX2 VSIB

- ▶ Use of specialized instructions - e.g., AES-NI

- CPU-unfriendly

- ▶ Small S-boxes (variable or/and fixed) - waste machine word bits

Beware of bitslicing and byte permute instructions

- ▶ Bit permutations

Such instructions are to appear in 2013 in non-SIMD form, though

- ▶ Unusual transforms

e.g., integer addition with only partial carry (an adder with some holes punched)

GPU friendliness

- GPU-friendly

- ▶ 32-bit integers, SIMD
- ▶ No/low memory needs
- ▶ Low register pressure

- GPU-unfriendly

- ▶ Exceeding total memory available on typical GPU cards

However, there may be a practical recomputation vs. memory trade-off - in fact, it's deliberate in scrypt

- ▶ Variable S-boxes exceeding fast memory size per thread (work-item in OpenCL parlance)
- ▶ Data-dependent branching

Deep enough tree to make eager execution inefficient

Beware of side-channel leaks

- ▶ CPU-unfriendly algorithms

Small S-boxes, bit permutations, unusual transforms

FPGA/ASIC friendliness

- FPGA/ASIC-friendly

- ▶ Small S-boxes (variable or/and fixed)
- ▶ Bit permutations

- ASIC-friendly

- ▶ Unusual yet simple transforms

e.g., integer addition with only partial carry (an adder with some holes punched)

```
#define pcadd(a, b, mask) (((a) ^ (b)) + (((a) & (b) & (mask)) << 1)) & 0xff)
```

- FPGA/ASIC-unfriendly

- ▶ Sequential memory-hard functions

All of the friendliness examples in this and previous slides assume that sufficient parallelism is available in one instance of a KDF, as suggested before.

Local parameter

- Must contain sufficient entropy
 - ▶ way beyond a typical password or even passphrase
- Hashes are not crackable offline without knowledge of the local parameter
- However, if the local parameter is stored right on the authentication server or in the password database, then it is likely to be stolen/leaked along with the hashes
- Problem: migration of locally-parameterized hashes between systems with different local parameters
 - ▶ Solution: embed a "local parameter ID" in the hash encodings, support multiple local parameters at once

Unreadable local parameter

- When a KDF is at least partially implemented in a dedicated device (e.g., in a hardware security module or even a dedicated server), it becomes possible to embed a local parameter in the device
- If the local parameter is unreadable by the host system (e.g., by a server doing password authentication), this buys us an extra layer of security
 - ▶ Need to have a backup copy - e.g., a cluster of multiple HSMs or/and a piece of paper in CEO's safe

Companies like Google and Facebook could use this approach to substantially reduce the impact of a possible user/password database compromise. Clearly, they can afford to move password hashing onto HSMs or dedicated servers. In fact, they could benefit from hardware acceleration of password hashing.

KDFs in scripting languages (future phpass)

- We're limited in our choice of cryptographic primitives, especially if portability to other scripting languages is desired
 - ▶ MD5 is the most ubiquitous common denominator, but use of SHA-512 is more appropriate by other criteria
- Include parallelism so that we may eventually benefit from it
 - ▶ e.g., when support for next generation phpass hashes gets embedded into PHP proper
- Feed moderately large amounts of data into the available cryptographic primitives so that we save on interpreter or VM overhead
 - ▶ e.g., invoke PHP's SHA-512 implementation on strings that are several kilobytes long - enough to keep the call overhead to a minimum, yet still within L1 cache
- Sequential memory-hard functions may be possible

Need to resist the temptation

Please resist the temptation to customize password hashing in your own web application or the like

- It is too easy to get it wrong
- Having too many different password hash types in active use is undesirable
 - ▶ Difficult to migrate hashes between systems
 - ▶ Existing password security auditing tools are not immediately usable, so administrators of individual installs of your app won't be able to audit the security of their users' passwords

Yet a determined attacker will implement this, then distribute the tool to others

- Further research, experiments, discussions within the community are needed - to arrive at as few next generation KDFs as practical