Password length limits in history of operating systems and popular web sites

I heard that many years ago for example passwords on linux systems were limited to 8 characters. Or rather, you could type in more than 8 characters, but only the first 8 characters mattered.

Consider the most common operating systems Windows, Mac OS and GNU/linux, or popular websites: What is the history about password policy length.

passwords historical

edited Oct 17 '12 at 8:41
M'vy
6,605 23 54

asked Oct 17 '12 at 8:06
student
501 1 8 15

generally community wiki has been discouraged, as it doesn't really fit SE's model. – Rory Alsop ♦ Oct 17 '12 at 9:58

It was not just linux, but nearly all unix at the time. they all used crypt() and truncated anything past 8 characters. I surprised a lead sysadmin at a national leading payroll company with this fact on his systems are recently as 2005. – jrwren Nov 9 '12 at 17:53

1 Answer

There are a variety of sources out there for this kind of information, but only for individual services or operating systems. It's rather hard to get exact dates and version information on a lot of this, because people still had old versions of software running, or changes weren't documented at the same time they were made. I've done my best to correlate the facts into a single list.

Services

Facebook: No limit (tried up to 1000 characters)
Twitter: No limit (tried up to 500 characters)
Twitter API: No limit.
Windows Live ID / Hotmail: 16 characters. The service is now known as Outlook.com
MySpace: In 2009, there was a 10 character limit. This has been increased, but I've not tested the limits.
LinkedIn: In 2009, there was a 16 character limit. Again, this has been increased. Currently there doesn't seem to be a limit.
Google Accounts / GMail / YouTube: There has never been a limit.
OpenID: No limit.

Mobile

Android: No limits on unlock / device encryption / root passwords.
iOS: No limits on unlock / device encryption passwords. Root password uses old `crypt`, so limit is 8 characters (the rest are ignored). Tested on iOS 4 and 5. (source)
Blackberry: 32 characters (source).
PalmOS: 31 ASCII characters (source). This may have changed since 2001.

Operating Systems

Windows 95 / 98: 14 characters (split into two 7-character hashes)
Windows 2000 / XP / Server 2003: Technical limit is 127 characters. Password change dialog limits to 32 characters. If 14 or less characters are used, the old LanMan hash is used. If 15 or more are used, the newer NTLM hash is used.
Windows Vista / 7 / Server 2008: 127 characters.
Unix (1990s and earlier): 8 ASCII characters.
OS X: No limit. Earlier Apple OS products may have had limits, but these have not been thoroughly investigated or documented.

Linux: Varies between distributions. Old versions have the same problem as Unix, since they use the old DES-based crypt hashes. Most have no limit, since they use a proper hash algorithm. Some have a soft limit of 72, 79 or 127 characters.

Here's a quick rundown of password hashing in some popular distros:

- **Ubuntu:** Early versions use MD5, 8.10 and later use SHA512 with a 64-bit salt.
- **Debian:** 5.0 and earlier used MD5, 6.0 and later use SHA512 with a 64-bit salt.
- **CentOS:** 5.0 and earlier used MD5, 6.0 and later use SHA512 with a 64-bit salt.
- **RHEL:** Old versions used DES-based crypt with 8-character limit. After that, MD5 was used. Changed to SHA512 in version 4.7.
- **Fedora:** Prior to Fedora 9, MD5 was used. Default was changed to SHA256 in Fedora 9, with support for SHA512 available.
- **Arch:** Used to be MD5, was changed to SHA512 in November 2011.

edited Oct 17 '12 at 9:11

answered Oct 17 '12 at 8:46

Polynomial
62.6k 17 155 252

2 Yeah, Linux is probably too generic. I'll dig up some info. – Polynomial Oct 17 '12 at 8:55

1 Added a few popular distros. – Polynomial Oct 17 '12 at 9:12

I just had to recover from Mac OS X Mavericks (10.9.3) which would not let me log back in after setting a 17-character long password. Therefore, I'd have to say that OS X (still) has an effective limit of "less than 17 characters." – Samuel A. Falvo II May 30 '14 at 21:11