Understanding Password Database Compromises

Dennis Mirante **Justin Cappos**

Department of Computer Science and Engineering

Technical Report
TR-CSE-2013-02
9/13/2013

Understanding Password Database Compromises*

Dennis Mirante
dennis.mirante@gmail.com

Justin Cappos
jcappos@poly.edu

Department of Computer Science and Engineering
Polytechnic Institute of NYU

Introduction

Despite continuing advances in cyber security, website incursions, in which password databases are compromised, occur for high profile sites dozens of times each year. Dumps of recently stolen credentials appear on a regular basis at websites like pastebin.com and pastie.com, as do stories concerning significant breaches. As a result of these observations, we chose to examine this phenomenon.

A study was undertaken to research information posted on the web concerning recent, high profile website intrusions, wherein user login credentials and other data were compromised. We searched for the party responsible for the incursion, the attack mechanism utilized, the format in which the login data was stored, and the location of any password dumps pilfered from the site. News stories from trade related journals, press releases from the victim company, hacker sites, and blogs from individuals and companies engaged in security analysis were, in particular, searched in order to find related information. A total of thirty four breaches were researched. It should be noted that some dumps, previously published, no longer exist. This is due to either the affected parties taking action against the site posting them, expiration of the allowed posting period, or removal by the original poster. An effort was made to locate copies of these files, sometimes to no avail. In those cases, details concerning the contents of the dumps were collected from published reports about them.

Summary of Findings

As a result of this study, several things are patently clear:

1. Many websites are not following best security practices. According to many posts dealing with password security, good storage practice would dictate the use of bcrypt or PBKDF2 hash algorithms, a salt, and a large number of rounds. The use of salts prevents attackers from using shortcuts. It forces the attacker to brute force the hashes one at a time, instead of attacking them as a group.

* This work was supported in part by the NSF (under grant 0966187). The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of any of the sponsors.

Some sites chose to completely ignore these recommendations. Plenty of Fish (hacked January 18, 2011), Sony Online Entertainment (hacked June 2, 2011), the UN (hacked around November 30, 2011), Yahoo (hacked July 12, 2012), Billabong(hacked July 13, 2012), and Barracuda Networks (hacked July 24, 2013), stored their passwords in plaintext. The hackers had to expend no effort to obtain them.

Other sites used ineffective hashing and no salting. For example, LinkedIn (hacked June 6, 2012), which used unsalted SHA1 and eHarmony (hacked June 5, 2012), which utilized unsalted MD5, both had their compromised passwords cracked within hours of being posted. Rick Redman, a consultant with Kore Logic Security, was quoted in an ars technia posting as having cracked about 55% of the approximately 6.5 million dumped LinkedIn hashes in 24 hours. Trustwave's SpiderLabs Blog reported that they cracked 80% of eHarmony's 1.5 million hashes in 72 hours. Sites like the InsidePro Forum (belonging to a company offering "password recovery software", referred to in many postings as a Russian Hacking site), pastebin.com, and http://pastie.org had files containing plaintext versions of most of the passwords within days. LinkedIn and eHarmony were skewered in the literature for their failure to at least use a salt, as pure hashes have been known to be easily cracked using rainbow tables for many years. In yet another case, the Australian Broadcasting Company, using SHA1, with no salt, had 53% of their close to 50,000 passwords cracked in 45 seconds (Troy Hunt).

While absolutely no information on how the passwords were stored could be found in 26.5% of the cases, we found 11.8% reported passwords were “Hashed and Salted”, 5.9% used salted MD5, 14.7% used unsalted MD5, 11.8% used salted SHA1, while unsalted SHA1, SHA256 salted, crypt(3) salted, and bcrypt each accounted for 2.9%. Plaintext use was noted in 17.6% of the site breaches.

2. **Stopping well known attacks would go a long way.** In the largest percentage of cases (~35.3%), the entity that was victim of the security breach chose not to disclose the attack mechanism. This might be due to several reasons, two of which one might speculate to be: a. the cause could not be determined because audit logs identifying the steps the attacker took were destroyed in the attack -or- b. the cause was determined and all possible exploit holes could not be found and plugged and the victim did not want to advertise the method for others to try to exploit.

SQL injection accounted for ~29.4% of the attacks, the most prevalent mechanism for disclosed attacks. SQL injections attacks were used in stealing user credentials from Adobe (November 13, 2012), Yahoo (July 12, 2012), Nvidia (July 2012), UN (November 30, 2011), Sony Online Entertainment (June 2, 2011), Sony PlayStation Network (April 17 -19, 2011), Plenty of Fish (January 18, 2011), and widely believed to have been used in attacking LinkedIn (June 6, 2012), Billabong (July 13, 2012), and Gamingo (July 7, 2012). In a blog posted on his website (Feb 7, 2013), Bruce K. Marshall, who has researched password security for over a decade, stated "SQL injection attacks appear to be the primary supplier of database dumps containing passwords". He also stated that 97% of these dumps were from sites that used PHP and speculated that "the popularity of the language has led to the rapid deployment of PHP sites

and PHP-based content management systems by people who lack an education in web application security".

Account hijacking (~14.7%), wherein access was obtained via stolen account credentials, is the second most prevalent attack methodology. Plundered login credentials, which most times include a username consisting of an email address, are used to victimize other sites. For example, the Japanese Club Nintendo site was attacked (June 9, to July 4, 2013) via brute force with login credentials stolen from other sites. Over 15,000,000 attempts were made with 23,926 successful. Obviously, 23,926 users ignored the recommended practice of using a different password for each site. Neither did the employee of Simple Machines, whose admin login credentials, stolen from another website, were used to enter the site on July 20, 2013. The admin privileges allowed the intruder to dump the site's user database. Phishing schemes, using stolen email addresses garnered from hacked user databases, typically follow a website's user database heist, yielding more compromised user credentials.

Spear-phishing and 3rd party software flaws were tied at ~5.9% each. XSS combined with account hijacking accounted for ~2.9%, while XSS by itself accounted for ~2.9%. According to an HP White Paper, XSS attacks are frequently used to attack web applications. This study found numerous posts related to XSS being used in email hacks, but relatively few in which password databases were stated as ultimately being stolen. Our study found XSS attacks were used in attacking Ubuntu Forums (July 14 and 20, 2013), in Yahoo email hacks (January - April 2012), and may have also been used to hack Billabong (July 13, 2012). Server misconfiguration occurred in ~2.9% of the cases.

3. Hacked websites are moving to two-factor authentication. A malicious party can present a password instead of the correct user. As a result of this, (and, in some cases, to avoid the embarrassment of being hacked a second time) many sites are migrating to two-step authentication or offering it as an option; Linode, Evernote, Twitter, Dropbox, examined in this study, are examples of this. Google, Facebook, Yahoo Mail, PayPal, and most major banking institutions either require its use or offer it as an option. Two-step authentication may involve having the person logging in receiving a message via their cellphone, which must subsequently be typed in to complete the login process or the site displaying an image which the user must scan in via their cell phone and call into the site. It may also involve entering the answers to questions the user selected and answered during either account creation or site enforced maintenance.

Where do we go from here?

Password based authentication continues to be a weak point in Internet security. Sites are increasingly compromised through simple and well known attacks such as SQL injection. Unfortunately, a surprising percentage of sites do not use standard best practices for salting and hashing password data. While users cannot tell if their passwords are protected in an appropriate manner, there are a few simple things users can do to help protect themselves:

1. Two factor authentication mechanisms should be used for major sites when available.
2. Use password managers like 1Password or LastPass to generate strong, per-site passwords. According to work by Troy Hunt, password reuse and poor password strength is still a major problem.

Future research may lead to mechanisms that replace user authentication via passwords. Device-based authentication, using Trusted Platform Modules, coupled with user biometric data, may be the best mechanisms to assure a user is legitimate. However, until this time, websites should take all precautions to ensure the protection and legitimate use of user passwords. Incorporating good practice salting and hashing schemes, SQL injection protection, and multi-factor authentication will go a long way in accomplishing this.

Summary of User Database Compromises

Barracuda Networks (July 24, 2013)
Flaw in Barracuda update servers found by Ephrahim Hegazy, servers misconfigured, usernames and passwords stored in plaintext, vulnerability fixed before exploits could occur. No dumps published.

Simple Machines Forum (July 20, 2013)
Unknown hacker used hijacked admin credentials to log in and steal user database. Passwords SHA1 hashed and 2 byte salted. No dumps published.

Ubuntu Forums (July 14 and July 20, 2013)
Unknown hacker used hijacked moderator credentials and XSS attack to obtain credentials of forum administrator. Those credentials were then used to access the user database. Passwords MD5 hashed and per-user salted. No dumps published.

Apple Developer Site (July 18, 2013)
Ibrahim Balic, security advisor purportedly used XSS attack. No info concerning hashing or dumps published.

Ubisoft (June 28, 2013)
Unknown hacker using stolen credentials. No info concerning password hashing or dumps published.

Nintendo (June 9 to July 4, 2013)
Unknown attackers using brute force attack with credentials stolen from other sites made over 15,000,000 attempts to login. 23,926 successful.

Drupal (May 29, 2013)
Unknown attacker used unidentified third party software flaw to access user database. Company described passwords as "hashed and salted using multiple rounds of hashing based on PHPass". No dumps published.

Reputation (April 30, 2013)
Unknown attacker, unknown attack method, company stated they stopped attack while in progress. Stated "a list of highly encrypted ("salted" and "hashed") user passwords for a small minority of users was accessed". No dumps published.

LivingSocial (April 26, 2013)
Unknown attacker using unpublished mechanism access database. According to company, passwords were hashed with SHA1, using random 40 byte salt. Someone appears to be offering the stolen database for sale: http://countermeasures.trendmicro.eu/dumped-livingsocial-database-offered-for-1-bitcoin/

Linode (April 15, 2013)
Hack The Planet (HTP) used zero day vulnerability in Adobe's ColdFusion. Company said shell passwords stored in cleartext, Linode Manager passwords "salted and cryptographically hashed". Hackers posting, at http://turtle.dereferenced.org/~nenolod/linode/linode-abridged.txt includes links to dump that are no longer valid, and states SHA256 hashing used. No dump found.

Scribd (Week of April 4, 2013)
Unknown hackers using unspecified method accessed user database. Company states 1% of passwords hashed using SHA1 and an unspecified salt. Remainder of passwords encrypted with scrypt. No dumps published.

MusicBrainz (March 29, 2013)
Company in process of converting passwords stored in plaintext using bcrypt with cost of 8. A dump file, which should not have had the converted field in it, was downloaded by an unknown party. No dumps posted.

Evernote (February 28, 2013)
Unknown hackers using unspecified method accessed user database. Official announcement said passwords "hashed and salted". No details on algorithm. Later blog post indicates they use MD5 with unspecified salt. No dumps posted.

Australian Broadcasting Corporation - ABC (February 27, 2013)
Hacker Phr0zebNtst using unspecified method downloaded and posted database to pastebin.com in 10 different files, no longer available. Troy hunt describes posted file structure

and says SHA1 with no salting was used: http://www.troyhunt.com/2013/02/lousy-abc-cryptography-cracked-in.html.

Twitter (February 1, 2013)
Appears Chinese hackers attacked site. No methodology officially published, but spear-phishing attack implied. Company said passwords were "hashed and salted". No details on hash algorithm or salt specified. No dumps posted.

The New York Times (Oct 2012 thru Jan 2013)
Chinese hackers performed spear-phishing attack, resulting in installation of malicious remote access tools. Company chose not to stop hackers, but instead studied their methodology. No description of password storage or dumps published.

ProjectWhiteFox (~December 10, 2012)
Team Ghostshell published 1.6 million hacked usernames and passwords from various agencies. They appear as links in http://pastebin.com/agUFkEEa, which are no longer active. Other sources could not be located.

Adobe (November 13, 2012)
Egyptian hacker, ViruS_HimA, using SQL injection, obtained MD5 hashed with no salt database. Dump posted on pastebin.com contained 644 records to assert breach was real. That dump is no longer available. Partial dump containing 230 records is at http://www.sendspace.com/file/lox8oe.

Dropbox (circa Jul 18, 2012)
An unknown hacker using login credentials stolen from other sites obtained access to an employee account, which contained a project document holding email addresses. These email addresses were used in a phishing scam on Dropbox members to secure their login credentials. No dumps published.

Billabong (July 13, 2012)
An attack by the WikiBoat collective, possibly using XSS or SQL injection, obtained database containing plaintext passwords, which was posted on codepaste.net site. Dump no longer available.

Yahoo (July 12, 2012)
An attack by D33DS Company, using union-based SQL injection, was used to obtain the password database, which can be found at http://thepiratebay.sx/torrent/7436152/.

Yahoo email hacked from Jan - April 2012, by unknown hackers, using WordPress exploit, XSS, and malicious JavaScript. No password dumps or other information available.

Yahoo Japan pre-empted an attack on May 16, 2013 before user data could be hijacked. No attack mechanism or dumps published.

Formspring (July 11, 2012)
Unidentified hackers using an undisclosed hack method accessed the development server. Password information dumped online was SHA-256 hashed with random salts. Dump could not be located nor could further info on salt.

Android Forums (July 9, 2012)
Unidentified party accessed compromised server hosting website and account data. Company was unsure if database downloaded. No description of password handling, attack methodology, or dumps found.

Nvidia (circa early July, 2012)
SQL injection attack by Team Appollo. 800 of ~400,000 raw MD5 hashes with no salt can be found at http://pastebin.com/G21ytATD. Hackers said they would post rest later, never did.

Last.fm (June 7, 2012)
2 attacks schemes published at same time. 1.Chinese hackers using phishing scheme harvested login info. 2. MD5 hashed passwords with no salt dumped on an unidentified Russian hacker site. Dump appears to have been posted long before company made aware of it. Dump could not be located.

LinkedIn (June 6, 2012)
Speculated SQL injection attack by unknown hackers resulted in 6.5 million SHA1 unsalted password hashes posted in InsidePro.com forum. Dump available at http://thepiratebay.sx/torrent/7334168/Linkedin_SHA1_passwords.

eHarmony (June 5, 2012)
Unknown hackers using undisclosed (widely believed to be SQL injection) attack posted 1.5 million MD5 unsalted password hashes at the InsidePro Forum. Dump can be found at https://defuse.ca/blog/cracking-eharmonys-unsalted-hashes-with-crackstation.

Gamingo (February 2012, Password Dump Showed Up On July 7, 2012)
A hacker calling himself 8i4ry_Munch3r, using an undisclosed (thought to be SQL Injection) attack, posted link on the InsidePro Forum to MD5 hashed and unsalted passwords. Link no longer valid. Cracked and uncracked portions of original dump can be found in files posted in the forum:
http://forum.insidepro.com/viewtopic.php?t=15447&postdays=0&postorder=asc&start=15.

UN (~ November 30, 2011)
TeaMpOisoN, using an undisclosed (thought to be SQL injection) attack method, downloaded and dumped plaintext usernames and passwords, available at http://pastebin.com/rfB0efDk.

Sony Pictures (June 2, 2011)
LulzSec group used SQL Injection attack to obtain and dump user information on their website (which no longer exists). A partial dump can be found at: http://torrents.thepiratebay.org/6443601/Sownage.6443601.TPB.torrent.

Sony Online Entertainment (May 2, 2011)
LulzSec group using undisclosed (thought to be SQL injection) attack method obtained old database that had not been used sing 2007 and dumped it on their site (which no longer exists). Sony claimed passwords were "hashed and salted". No specifics on hash algorithm or salt available. Neither is dump.

Sony PlayStation Network (Between April 17 and 19, 2011)
LulzSec group, using SQL injection attack, obtained and dumped password database online. Dump could not be found. At the time, Sony stated passwords were "transformed using a cryptographic hash function".

Plentyoffish (Jauary 18, 2011)
SQL injection attack, purported to be by Chris Russo, resulted in unauthorized user database access. All information, including passwords, in plaintext. There is controversy as to whether or not this was a real breach. No dump published.

Gawker (December 11, 2010)
Gnosis group, using an undisclosed attack method, obtained user database containing crypt(3) passwords hashed with 12 bit salts. Stolen data, including passwords, can be found here: http://thepiratebay.sx/torrent/6036976/.

Details of User Database Compromises

Baracuda Networks (July 24, 2013)
A vulnerability in Barracuda update servers was found that allowed access to all employee login credentials. It was found by an Egyptian security advisor, Ephrahim Hegazy. The servers were misconfigured and stored password information within the web directory, rather than outside of it. All username, password information was stored in plaintext. The vulnerability was fixed before any exploits could occur:
http://thehackernews.com/2013/07/Barracuda-network-Password-disclosure-vulnerability_24.html

Simple Machines Forum (July 20, 2013)
Credentials stolen from another website were used to log in to an administrator account. Admin privileges permitted the hacker to dump the site's user database, which includes passwords, personal messages, and other information. All users were advised to change their passwords:

http://www.simplemachines.org/community/index.php?topic=508232.0

In the news and updates section of the website pertaining to the breach, it was stated that the passwords in the database were SHA1 hashed and 2 byte salted:
http://www.simplemachines.org/community/index.php?action=search2;search=sha1;topic=508232
and
http://www.simplemachines.org/community/index.php?action=search2;search=salt;topic=508232
discuss the SHA1 and salt use.

No dumps or other information could be found online.

Ubuntu Forums (July 14 and July 20, 2013)

Email addresses, usernames, and passwords for 1.82 million accounts were exposed. The passwords were hashed using MD5 and a per-user cryptographic salt was used. This scheme is considered by experts to be an inadequate means of password protection:
http://arstechnica.com/security/2013/07/hack-exposes-e-mail-addresses-password-data-for-2-million-ubuntu-forum-users/

A combination of configuration settings in the software used to enable the forum and a compromised moderator account allowed the attacker to obtain administrator access and download the email addresses, user names, and passwords for all the accounts. A postmortem by Canonical, the company that administers the site, indicates an XSS attack was used to obtain the credentials of the forum administrator. The forum administrator looked at an announcement page, which was modified by the attacker using the moderator's account:
http://blog.canonical.com/2013/07/30/ubuntu-forums-are-back-up-and-a-post-mortem/

So far, none of the data has been published. The attacker has not been identified.

Apple Developer Site (July 18, 2013)

A Turkish security advisor claims he found 13 bugs and notified Apple, who took the site down. Details in:
http://www.theguardian.com/technology/2013/jul/22/apple-developer-site-hacked

In subsequent posting, the security advisor, Ibrahim Balić, claims he could access names, Apple IDs/email addresses, and user IDs through a “simple unescaped injection attack”, a Cross Site Scripting attack (XSS).

The same site questions his story in a later article:
http://www.theguardian.com/technology/2013/jul/26/apple-developer-site-hack?view=mobile

So does: http://mytechblog.com/2013/07/apple-developer-website-hacked-what-happened/

Apple has not released any information as to the method used for the attack. Some of the website's information, such as credit cards, was encrypted, and not subject to compromise, as per an email sent out to registered developers and described in: http://www.geek.com/apple/apples-developer-portal-hacked-company-announces-security-overhaul-1562877/

Apple, however, was not able to rule out whether or not names, mailing addresses, or email addresses were accessed. They refused to identify the attack method, whether or not law enforcement has been notified, and whether or not potential suspects have been identified.

The method utilized to encrypt data was not identified.

No password dump could be found online.

There is a video posted on YouTube that shows individual text files containing apple userid information being opened and displayed. This video does not appear to have been originally generated by Balic. It, and several others like it, appear to contain excerpts from the original video posted by Balic, which was subsequently removed: https://www.youtube.com/watch?v=gW7lfCand4Q

The site was reported to be back up on 08/11/13: http://www.pcmag.com/article2/0,2817,2422955,00.asp

Ubisoft (June 28, 2013)

Hack exposed user names, encrypted passwords, and email addresses for potentially up to 58 million users. Hack was initiated using stolen credentials: https://support.ubi.com/en-GB/FAQ.aspx?platformid=60&brandid=2030&productid=3888&faqid=kA030000000eYYxCAM

Ubisoft no released no details concerning the algorithm or salt (if any) used to hash the passwords.

No mechanism for the attack was identified, other to say stolen credentials were used.
No dumps or other information could be found online.

Nintendo (June 9 to July 4, 2013)

The Japanese Club Nintendo site was attacked via brute force by unknown attackers. Login credentials stolen from other sites were used to gain access. Over 15,000,000 attempts were made with 23,926 being successful. Nintendo realized the attack was in progress after observing a huge number of login errors and reset the affected user's passwords:

http://hothardware.com/News/Hacked-24000-Club-Nintendo-Accounts-Compromised/
and
http://nakedsecurity.sophos.com/2013/07/09/nintendo-cracks-after-month-long-15-5-million-strong-hacker-bombardment/

The accounts experiencing illegal access had the user's names, addresses, phone numbers, and email addresses compromised:
http://threatpost.com/brute-force-attack-on-nintendo-fan-site-yields-data-on-25k

No information concerning where the login information used in the attack originated from could be found.

Drupal (May 29, 2013)
Breach occurred via third-party software installed on Drupal.org servers. Exposed information included usernames, email addresses, and salted and hashed passwords using multiple rounds of hashing based on PHPass, as well as country for a subset of the users. All user passwords were reset:
https://drupal.org/news/130529SecurityUpdate#faq

No perpetrators were identified.
No specific hashing algorithm or description of the salting was disclosed.
No attack methodology was disclosed.
No dumps or other information could be found online.

Reputation (April 30, 2013)
In an email sent out to its customers, the company stated that they stopped an attack while it was in progress. Personal information including names, emails, physical addresses, phone numbers, date of birth, and other information was hacked. They also stated that "a list of highly encrypted ("salted" and "hashed") user passwords for a small minority of users was accessed". Even though they claimed the passwords were highly unlikely to ever be decrypted, they reset the passwords of all users to preclude unauthorized access. The text of the email can be found in a blog post found on authentication firm Stormpath's site:
https://www.stormpath.com/blog/reputationcom-loses-user-passwords-emails-and-addresses

No perpetrators were identified.
No hashing algorithm or description of the salting was disclosed.
No attack methodology was disclosed.
No dumps or other information could be found online.

LivingSocial (April 26, 2013)

50,000,000 customers were impacted by the exposure of customer names, email addresses, birth dates and encrypted passwords:
http://allthingsd.com/20130426/livingsocial-hacked-more-than-50-million-customer-names-emails-birthdates-and-encrypted-passwords-accessed/

As per the following announcement issued by LivingSocial, the passwords were hashed with SHA1, using a random 40 byte salt. After the attack, they switch from SHA1 to bcrypt:
https://www.livingsocial.com/createpassword

No attack methodology was disclosed.

While a search for a password dump was unsuccessful, someone appears to be offering the file for sale in a posting dated April 27, 2013, on the pastebin.com site. The veracity of this post has yet to be confirmed:
http://countermeasures.trendmicro.eu/dumped-livingsocial-database-offered-for-1-bitcoin/

Linode (April 15, 2013)

This company, a privately owned cloud hosting entity, was hacked by a group named Hack The Planet. Credit card information and passwords were exposed:
http://www.zdnet.com/vps-host-linode-issues-customer-wide-password-reset-7000014057/

Linode reported that it uses public and private key encryption to store credit card information and that the private key is also encrypted using a passphrase that is not stored electronically. It also reported that some shell passwords were stored in clear text and reset those accounts. It also cancelled API keys that may have set by the users. It also stated that Linode Manager user passwords were "salted and cryptographically hashed, but provided no detail concerning the salt or hash algorithm used. The hackers were able to gain access via two zero day vulnerabilities in Adobe's ColdFusion application server:
https://blog.linode.com/2013/04/16/security-incident-update/

The vulnerabilities were fixed in Adobe's APSB13-10 hotfix:
http://www.adobe.com/support/security/bulletins/apsb13-10.html

Code that exploits the vulnerabilities can be found here:
http://www.exploit-db.com/exploits/24946/
and here:
http://cxsecurity.com/issue/WLB-2013040074

The hackers disputed Linode claims about the credit card information being safe:
http://www.theregister.co.uk/2013/04/16/linode_breach/

The hackers indicated in their posting, referenced in the previous link, that SHA256 was used to hash the passwords. The link to the database file listed in the posting is no longer available: http://turtle.dereferenced.org/~nenolod/linode/linode-abridged.txt

On May 2, 2013, Linode announced two-step verification as an optional protection device for Linode accounts:
https://blog.linode.com/2013/05/02/linode-manager-two-step-auth/

No dumps or other information available.

Scribd (Week of April 4, 2013)

Usernames, emails, and passwords for all users (estimated to be 50 to 100 million) were exposed. 1%, of the users were affected. The passwords of those users were encrypted with SHA1 plus a salt. The passwords of the remainder of the 50 million users were encrypted with scrypt. Only the passwords of the 1% were reset and notifications sent to them to change their password on this and other services:
http://thenextweb.com/insider/2013/04/04/scribd-reveals-it-was-hacked-this-week-informs-less-than-1-of-its-users-their-passwords-were-compromised/

Scribd did not consider the passwords encrypted with scrypt compromised:
http://www.zdnet.com/up-to-1-million-scribd-user-passwords-may-have-been-compromised-7000013595/

No mechanism for the attack was identified. No dumps or other information available.

MusicBrainz (March 29, 2013)

MusicBrainz was in the process of converting their passwords, previously stored in plaintext to hashed form using bcrypt with a cost of 8. They were converting all their passwords using a converter program that would run over several days. A backup dump file intended to be public, contained the hashed password data because of a programming error. The backup dump was subsequently downloaded by an unknown party. As a result, all users were required to change their passwords:
http://blog.musicbrainz.org/2013/04/05/potential-security-leak/

In a posting on April 22, 2013, the company refuted some reports that it was attacked or compromised. It stood by its original post that the backup file accidently contained the hashed passwords:
http://blog.musicbrainz.org/2013/04/22/server-update-2013-04-22-and-a-notice-regarding-passwords/

No dumps or other information could be found online.

Evernote (February 28, 2013)

Passwords on system were hashed and salted as per:
http://krebsonsecurity.com/2013/03/evernote-forces-password-reset-for-50m-users/ and an email sent by Evernote to its users:
http://pastie.org/6369874

No details were released by Evernote to detail HOW the passwords were hashed and salted. However, one of Evernote's blog posts from May 17, 2011 intimates they use MD5:
http://blog.evernote.com/tech/2011/05/17/architectural-digest/
Evernote subsequently taking greater security measures as per:
http://www.pcworld.com/article/2029996/evernote-pushes-awareness-raising-software-updates-after-hack-attack.html

Evernote subsequently added two factor authentication using smartphone as per:
http://www.techhive.com/article/2040313/evernote-adds-two-factor-authentication-other-security-features-after-hack-attempt.html

No password dump could be found online. No potential suspects have been identified.

Australian Broadcasting Corporation - ABC (February 27, 2013)

Site attacked by a hacker using the Twitter handle of Phr0zenMyst. Personal details, including user names, ip addresses, email addresses, location, postcodes, and hashed passwords were posted on the internet. Hacking was done in response for ABC interviewing a controversial Dutch anti-Islam politician:
http://www.smh.com.au/it-pro/security-it/fifty-thousand-exposed-in-abc-website-hack-20130227-2f5j9.html

The database was dumped to 10 different files, listed in a pastebin.com file. An attempt to download these files was unsuccessful, as they were no longer available:
http://pastebin.com/J3ceSWMw

Information, other than passwords, was in plaintext. The following post, along with others found, presents the record structure of the database that was dumped. It (they) also state that SHA1 hashing was used, and no salting was done. It took 45 seconds to decode 53% of the passwords:
http://www.troyhunt.com/2013/02/lousy-abc-cryptography-cracked-in.html
No mechanism for the hack was identified. No other dumps or information available.

Twitter (February 1, 2013)

Twitter reset the passwords for the accounts of 250,000 users after user information, which included usernames, email addresses, and hashed and salted passwords that may have been compromised. They did this after identifying unauthorized attempts to access user data:

http://www.eweek.com/security/twitter-resets-250000-user-passwords-after-cyber-attack/

While not directly implicating anyone in the attack, Twitter indicated that the attack followed a pattern similar to the one that occurred on the NY Times. From this statement, it was inferred that the attack was carried out by Chinese hackers, most likely using a similar spear-phishing attack:
http://rt.com/news/twitter-accounts-hacked-compromised-282/

Twitter announced in May that they would implement two-step verification to cut down on phishing schemes and account hijacking:
http://www.foxbusiness.com/technology/2013/05/22/twitter-adopts-extra-security-layer-in-response-to-recent-attacks/

No specific hashing algorithm or description of the salting was disclosed.
No attack methodology was specifically disclosed.
No dumps or other information could be found online.

The New York Times (Oct 2012 thru Jan 2013)

Attributed to Cyber attack from China, thought to be due to the paper publishing an investigative report on October 25, concerning business dealings that garnered billions of dollars for the relatives of China's prime minister, Wen Jiabo. Accomplished by installation of malware that performed spear-phishing attack. Email containing malicious links or attachments sent to employees that installed remote access tools. Attackers used university computers used by Chinese military to attack US military contractors previously. Details:
http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html?pagewanted=all&_r=0

The paper purportedly chose NOT to immediately stop the hackers, but instead studied their methodology to help build better defenses against future cyber attack:
http://www.csoonline.com/article/728083/lesson-learned-in-cyberattack-on-the-new-york-times

ProjectWhiteFox (~December 10, 2012)

Team Ghostshell published 1.6 million hacked user's usernames and passwords. They came from many sources including the military and other government institutions, law firms, financial firms, the aerospace industry, NASA, etc. The information was published to promote freedom of information and concurrent with an ITU meeting taking place to discuss Internet management:
http://www.forbes.com/sites/andygreenberg/2012/12/10/hacker-group-touts-1-6-million-password-dump-to-protest-un-internet-regulation/

The hacked information was posted on pastebin.com site: http://pastebin.com/agUFkEEa
This file contains Team Ghostshell's rational for the attacks as well as links to the hijacked account information posted on three mirror sites: slexy.org, privatepaste.com, ant github.com.

Attempts to access these files to determine attack methodology or examine the user account data were unsuccessful, as these files have either been subsequently removed or the permitted posting period has expired.

Adobe (November 13, 2012)

An Egyptian hacker, calling himself ViruS_HimA, broke into Adobe's Connectusers.com forum and made off with the account details of 150,000 users:
http://news.softpedia.com/news/Adobe-Confirms-Hack-Shuts-Down-Connectusers-Forum-307070.shtml

Prior to Adobe confirming the attack, experts from the security firm Sophos examined the posted hashes, which were hashed using MD5, with no salt:
http://nakedsecurity.sophos.com/2012/11/15/cracked-passwords-from-alleged-egyptian-hacker-adobe-breachegyptian-hacker-allegedly-breached-adobe-leaked/

The pastebin post where the hacker published 644 records to prove the breach was real has been removed. It is described here:
http://www.zdnet.com/adobe-suspends-connect-user-forum-after-apparent-hack-7000007440/

The attacker claimed the attack was accomplished using SQL injection:
http://www.darkreading.com/attacks-breaches/adobe-hacker-says-he-used-sql-injection/240134996

A partial dump of the originally posted file, containing 230 records can, can be found at:
http://www.sendspace.com/file/lox8oe

Dropbox (circa Jul 18, 2012)

Dropbox became aware of this issue when they began to receive complaints from site members that email accounts only used for Dropbox were being spammed. Dropbox's investigation found that unknown hackers used usernames and passwords stolen from other sites to log into Dropbox. One of the accounts breached this way belonged to an employee. The employee account contained a project document with user email addresses that were used to spam Dropbox members. In addition, these stolen usernames and passwords were used to attempt logins to the Dropbox site, with some success.
As a result of this, Dropbox announced their intention to use two factor authentication in their announcement of what went on issued July 31, 2012, which can be found on this page of the Dropbox blog:
https://blog.dropbox.com/page/4/?page=%2Fsecurity-update-new-features%2F

Dropbox implemented a time based, two-step verification method in August 2012:
http://krebsonsecurity.com/2012/08/dropbox-now-offers-two-step-authentication/

No perpetrators were identified.
No dumps or other information specifically concerning the affected accounts could be found online.

Billabong (July 13, 2012)

The user names (email addresses) and passwords of up to 35, 000 users were stolen by the WikiBoat collective and 21,000 of them were posted on the codepaste.net site. The file is no longer available. All of the information was in plaintext:
http://news.softpedia.com/news/Billabong-Hacked-Over-20-000-Clear-Text-Passwords-Leaked-281131.shtml

While the specific mechanism for the attack was not published, security researcher Troy Hunt enumerated many issues with Billabongs site, including disposition towards XSS and SQL injection attacks:
http://www.troyhunt.com/2012/07/heres-why-we-keep-getting-hacked-clear.html

Yahoo (July 12, 2012)

Accomplished by D33DS Company. Hackers retrieved and published unencrypted account details (emails and passwords) for 450,000 user accounts. Accounts belonged to VOIP service Yahoo Voices:
http://www.huffingtonpost.com/2012/07/12/yahoo-hack-d33ds-company_n_1667359.html

D33DS Company announce the leak in a twitter post which no longer exists:
(https://twitter.com/denjacker/status/223148408800690176)

They also prefaced the password dump they published with a statement indicating the attack was a union-based SQL Injection attack. The entire dump file can be downloaded via bit torrent from:
http://thepiratebay.sx/torrent/7436152/

Yahoo email continues to be hacked. It was hacked 4 times in four months, starting in January, exploiting a buggy version of WordPress on the Yahoo Developers Blog, as well as cross-site scripting flaws and malicious JavaScript:
http://siliconangle.com/blog/2013/04/30/yahoo-mail-hacked-again-serious-questions-raised-about-its-ability-to-protect-users/

The initial January hack was purported to use an XSS exploit perpetrated by a lone hacker who posted a video on YouTube, which was subsequently removed because it violated YouTube's policy on depiction of harmful activites:
http://thenextweb.com/insider/2013/01/07/yahoo-mail-users-hit-by-widespread-hacking-xss-exploit-seemingly-to-blame/

There are still complaints about email accounts continuing to be hacked now:
http://www.wowt.com/news/headlines/E-mails-Recently-Hacked-Most-Of-Them-Yahoo-Accounts-212367331.html

No password dumps or other information available.

The usernames of 22 million people may have been stolen from Yahoo Japan on May 16, 2013. Passwords reportedly were not stolen. The attack was pre-empted by disconnecting the company's servers from the internet:
http://www.wired.co.uk/news/archive/2013-05/20/yahoo-japan-hacked

No mechanism for the attack was published. No dumps or other information available.

Formspring (July 11, 2012)
420,000 encrypted passwords dumped:
http://www.huffingtonpost.com/2012/07/11/formspring-hacked-passwords-leaked_n_1665231.html
and:
http://www.pcmag.com/article2/0,2817,2406967,00.asp

Only passwords were published. No user names or other identifying information was posted. The passwords were SHA-256 hashed and random salted. The attacker gained access into a development server and used it to access account information:
http://www.voiceofgreyhat.com/2012/07/formspring-hacked-420000-password.html

Formspring subsequently implemented bcrypt cryptographic hashes. Portions of the company's blog post, which no longer appears on the site, can be found here:
http://www.itwire.com/your-it-news/home-it/55656-formspring-sprung-with-password-security-breach

How the development server was accessed was not disclosed. No attacker identified. No dumps or other information available.

Android Forums (July 9, 2012)
It was reported on July 10, 2012 that the server hosting the website had been compromised and the user database containing information on 1 million plus accounts was accessed. At the time of the announcement, it was not certain whether or not the user database was downloaded. This database contained usernames, emails, hashed and salted passwords, registration IP addresses, and other info as described in the announcement as posted here:
http://androidforums.com/site-updates-announcements/580371-important-notice-security-breach.html#post4645422

No perpetrators were identified.
No specific hashing algorithm or description of the salting was disclosed.
No attack methodology was disclosed.
No dumps or other information could be found online.

Nvidia (circa early July, 2012)

Up to 400,000 user names, email addresses, hashed passwords, and profile information compromised after an SQL injection attack on Nvidia forums:
http://www.itp.net/589777-nvidia-hacked-user-records-compromised#.Ug6tWW33OPY

In the Nvidia post quoted by the above, Nvidia stated the passwords were "hashed passwords with random salt". A group of hackers, "Team Apollo" claimed responsibility on July 16, and posted Admin information and password hashes (800 of the ~400,000) at:
http://pastebin.com/G21ytATD
They claimed they would post the rest later. Searching failed to find the existence of a subsequent dump.

The passwords posted were raw MD5 hashes with no salt. It appears Nvidia lied:
http://www.techpowerup.com/169112/nvidia-forums-hack-passwords-not-salted.html

A search for a counter statement refuting the Team Apollo disclosure yielded no results.

No other dumps or information could be found online.

Last.fm (June 7, 2012)

Two login credential hacking incidents for this site were published around the same time (June 7). The first one was an attack accomplished by use of a malicious domain registered to a Chinese IP address. Phishing scheme that harvested user login information by sending users a message that they should check out a blog with an associated URL. When they clicked on the link they were directed to a fake last.fm login screen which collected their username and password:
http://countermeasures.trendmicro.eu/phishing-attack-targets-lastfm-users/

The second one was the announcement that Last.fm passwords had been dumped on a Russian hacker site. It appears that the hacking took place months before the announcement and that the login info had been posted on the site for a long time before it was discovered:
http://news.cnet.com/8301-1009_3-57450166-83/how-long-ago-did-the-last.fm-security-breach-happen/?part=rss&subj=news&tag=2547-1_3-0-20
Following post reiterates dumps were posted for a long time prior to Last.fm's announcement:
The passwords were hashed using MD5 and were unsalted. Blog also reiterates that Last.fm database had been available on the net for some time:
http://snurps.blogspot.com/2012/06/breach-update-eharmony-and-lastfm-also.html

No mechanism for the attack was published. No dumps or other information available.

LinkedIn (June 6, 2012)

6.5 million SHA1, unsalted passwords were posted on a Russian based online InsidePro Forum, belonging to a Moscow based company that specializes in "password recovery":
http://arstechnica.com/security/2012/06/8-million-leaked-passwords-connected-to-linkedin/

Other than the passwords, no user names or other data was posted:
http://www.pcworld.com/article/257045/6_5m_linkedin_passwords_posted_online_after_apparent_hack.html

Linkedin was subsequently skewered for its lax password handling:
http://www.h-online.com/security/features/Comment-LinkedIn-and-its-password-problems-1612877.html

The password dump is available at:
http://thepiratebay.sx/torrent/7334168/Linkedin_SHA1_passwords .
In addition, the following blog entry references other depositories where password hash file can be loaded and discusses a method for examining it:
http://bh0kal.blogspot.com/2012/06/is-your-linkedin-password-hacked.html
I was able to download the referenced .zip file from:
http://depositfiles.com/files/8fxr534yx

No mechanism for the attack was identified by LinkedIn, but it is widely speculated to be via SQL injection:
http://nakedsecurity.sophos.com/2012/06/21/linkedin-slapped-with-5-million-class-action-suit-over-leaked-passwords/
and
http://www.business2community.com/tech-gadgets/do-you-have-a-vulnerability-a-look-at-app-security-0361183

eHarmony (June 5, 2012)

1.5 million password hashes stolen and dumped on line at the same Russian forum that published the LinkedIn hashes:
http://www.telegraph.co.uk/technology/news/9316218/LinkedIn-hacker-also-stole-1.5m-passwords-from-dating-site-eHarmony.html

No other user information (user names, emails, etc.) was posted. The case insensitive passwords were hashed using MD5, but were not salted:
http://news.cnet.com/8301-1009_3-57460253-83/analysis-eharmony-had-several-password-security-fails/?part=rss&subj=news&tag=2547-1_3-0-20

An in-depth analysis was performed was published:
http://blog.spiderlabs.com/2012/06/eharmony-password-dump-analysis.html

Hash dump can be found here:
https://defuse.ca/blog/cracking-eharmonys-unsalted-hashes-with-crackstation

No mechanism for the attack was identified. No dumps or other information available.

Gamingo (February 2012, Password Dump Showed Up On July 7, 2012)

In late February 2012, a hacker called 8i4ry_Munch3r hacked this site. On realizing this, the company took the site down for an extended period. In an email, Gamingo stated that usernames and encrypted passwords were stolen and intruders might be in possession of additional personal data. The company instructed all users to change their passwords. A copy of the notice issue on March 1, 2012 can be seen here:
http://otherlandnf.com/content/?news=42

On July 7, a link to a dump of the password hash file was posted on the Russian InsidePro Forum:
http://www.zdnet.com/8-24-million-gamigo-passwords-leaked-after-hack-7000001403/
This is the link to the InsidePro posting. When going through it, it appears that the original dump is no longer available, but uncracked and cracked portions of it, wherein the hash and the password are displayed, may be found in subsequent postings:
http://forum.insidepro.com/viewtopic.php?t=15447&postdays=0&postorder=asc&start=15
The users there were co-operating in decoding the hashes.

The passwords were hashed using MD5. Salting was not mentioned and apparently not used:
http://www.theregister.co.uk/2012/07/24/gamigo_password_breach/

A full analysis of the hashed passwords appears here:
http://iqsecur.blogspot.com/2012/08/analysis-of-gamigo-hashes.html
Gamingo did not speak to the mechanism of the attack, but it has been stated elsewhere to be SQL injection:
http://www.business2community.com/tech-gadgets/do-you-have-a-vulnerability-a-look-at-app-security-0361183

No dumps of the entire database could be found. Any that were previously posted had either expired or been deleted.

UN (~ November 30, 2011)

TeaMpOisoN hacked and got hundreds of email addresses, usernames, and plain-text passwords that they dumped onto pastebin.org:
http://www.theregister.co.uk/2011/11/30/un_hack/

These usernames and passwords were stored in plaintext. A dump of them can be found here: http://pastebin.com/rfB0efDk

The attack methodology used to obtain this information was not disclosed. The TeaMpOisoN post taunted the security experts at the UN to figure it out.

In a subsequent post on February 9, 2012, the group published details of the UN's databases and a list of exploitable vulnerabilities within the un.org domain. The urls listed were purported to be vulnerable to blind SQL injection. The post can be found here: http://pastebin.com/ZB4eLVeS

Sony Pictures (June 2, 2011)

LulzSec group responsible. Used SQL injection attack and posted details on the attack and user information, which they claimed was stored in plaintext, on their website (site no longer exists). They claimed to have accessed the information of 1 million users and posted user details for 50,000 users on their website: http://www.bbc.co.uk/news/business-13636704

A torrent of multiple file dumps of some of the pilfered accounts can be found at: http://torrents.thepiratebay.org/6443601/Sownage.6443601.TPB.torrent. The passwords contained within are plaintext.

Sony Online Entertainment (May 2, 2011)

LulzSec group responsible. Information concerning 24.6 million Sony Online Entertainment account holders stolen. Database contained 12,700 non-US credit card numbers, mostly expired or corresponding to deleted accounts. The database had not been in use since 2007: http://online.wsj.com/article/SB10001424052748704436004576299491191920416.html?mod=e2tw

Sony was criticized for leaving old data around and for not providing details on how passwords were protected: http://nakedsecurity.sophos.com/2011/05/03/sony-admits-breach-larger-than-originally-thought-24-5-million-soe-users-also-affected/

Sony did not say what method of protection was used to secure the credit card data, however, they said the passwords were hashed. There was no disclosure on what hashing algorithm was used and whether a salt was used.

No password dumps or other information available.

Sony PlayStation Network (Between April 17 and 19, 2011)

Play Station data center in San Diego attacked. PlayStation Network and Qriocity services were pilfered to obtain personal details from approximately 77 million accounts. Subsequent attacks followed. Personal information reportedly compromised (credit cards). LulzSec group responsible, subsequently caught. Network attacked many times in same period.

Attack was via SQL injection, as published here:
http://www.theatlanticwire.com/technology/2011/12/hacks-mattered-year-hack/46731/

The credit card information stored in their systems was encrypted, while personal data was not:
http://blog.us.playstation.com/2011/04/27/qa-1-for-playstation-network-and-qriocity-services/
Sony later updated their statement to say that, while the stored passwords were not encrypted, they were not stored in plaintext, but were transformed using a cryptographic hash function:
http://blog.us.playstation.com/2011/05/02/playstation-network-security-update/

No description of the hashing method could be found.

No password dumps or other information available, as Sony had the information removed from websites it was posted on.

Plentyoffish (Jauary 18, 2011)

There is controversy concerning how this hack was accomplished. The founder and CEO of the company accused a 23 year old Argentinean, Chris Russo, of performing the hack and trying to extort money:
http://www.tomsguide.com/us/Plenty-of-Fish-hacked-data-breach-mafia-chris-russo-markus-frind,news-9960.html#t212572
More drama ensued when Russo spoke out against the assertions being made against him:
http://business.financialpost.com/2011/01/31/alleged-plenty-of-fish-hacker-speaks-out-claims-he-was-only-trying-to-help/?__lsa=86cf-f265
The attack was carried out via SQL injection. User names, passwords, email addresses, and paypal account information for more than 28,000,000 users were stored in plaintext:
http://thehackernews.com/2011/02/real-story-behind-hacking-of.html

No dumps or related information found online.

Gawker (December 11, 2010)

Hacked by Gnosis group. Root access to Linux based servers allowed access to source code, Gawker's Custom Management system, user password database of 1.3 million users, and other files. The hackers attacked Gawker on the pretext that they found them arrogant and because of a previous feud between Gawker and 4Chan. User credentials, as well as chat logs, and Gawker website source code was posted on the Pirate Bay website and torrents:

http://www.pcworld.com/article/213438/gawker_media_hack_everything_you_need_to_know.html

All stolen data posted by Gnosis can be found here:
http://thepiratebay.sx/torrent/6036976/

The passwords were purportedly DES-based crypt(3) hashed using 12 bit salts. Jon Oberheide posted an analysis of passwords he cracked using the John the Ripper tool:
https://blog.duosecurity.com/2010/12/brief-analysis-of-the-gawker-password-dump/

Joseph Bonneau of the Cambridge University computer lab posted another analysis of the attack, speculating on the methodology used and also indicating that the passwords were hashed using crypt(3) with 12 bit salts. He also stated that the passwords were problematic, as they were truncated to 8 characters due to the small DES key size and there was no support for ascii characters:
http://www.lightbluetouchpaper.org/2010/12/15/the-gawker-hack-how-a-million-passwords-were-lost/

No mechanism for the attack was identified.