ELIZABETH ZWICKY

brute force and ignorance

Elizabeth has been involved with Internet security, voluntarily or involuntarily, since the Morris worm in 1989, but retains hope.

Zwicky@otoh.org

VARIOUS NON-SECURITY BLOGS I READ have been busily urging people to choose good passwords, partly because of the *New York Times* [1] and its coverage of the stupidity of 32 million passwords stolen from RockYou. Now, I wouldn't want to discourage you from choosing a good password. In fact, I think it's a good habit to get into. Go long; stuff some punctuation into the middle; have a good time!

But, honestly, it's a strange thing to worry about based on the RockYou data. The RockYou story goes something like this: RockYou offers services that connect a whole pile of different social networking sites. They had an SQL injection bug. This revealed the contents of not only their main user database, but also the stored information they used to connect to other sites on behalf of users—including passwords for RockYou and other sites, each and every one stored in the clear. RockYou's response to this was, to say the least, underwhelming, although under pressure they did inform users that perhaps it might be a good idea for them to change their passwords.

Meanwhile, Imperva, a security company, laid their hands on RockYou's stolen data, did some analysis of the cleartext passwords, and sent out press releases about the shockingly poor passwords people have chosen, and the success brute force attacks would have against them. This was followed by the wave of admonishments I noted earlier, exhorting people not to choose these terrible passwords.

And, indeed, the data suggest that the passwords were terrible. "123456" was the most popular password, and it was dauntingly popular, accounting for nearly 1% of the passwords. But, you know, it doesn't really matter how useful a brute force attack would have been. Sure, with 683 attempts per account (by Imperva's calculations, which I have no reason to doubt), you could have compromised 10% of the accounts. But that's a lot more effort than it took the attackers to compromise *all* the accounts, with a bonus helping of accounts on other sites. The strength of people's passwords at RockYou was totally irrelevant, and the strength of their third-party passwords was only relevant for those people cunning enough not to hand them over to RockYou.

But, you say, not every Web service is designed by people who are better at fluffy kitten pictures than securing passwords; some of them have already

been broken into and now know something about security. Surely at those sites, password strength is good for something other than saving you from public ridicule that ought to have been directed at the people who set free your password in the first place. Well, maybe. But probably not.

The economics of brute force attacks depend greatly on the environment. Brute force is absolutely the way to go if you're attacking a password you have on disk and can fiddle with in the privacy of your own computer. But if you have to try brute force across a wire against a public Web site, you are pitting yourself directly against the site's security. There are two possibilities there. Perhaps the site won't notice, but in that case, it's run by clueless goons, and there's a good chance that the same effort could be invested into attacks with much better payoffs; that was definitely a win for the attackers at RockYou, and it's neither the first nor the last site to have that sort of experience.

And perhaps the site will notice, in which case it's the black hats against the white hats, locked in battle. It's not a battle the white hats can ever win, but they can effectively slow down brute force attacks a lot. Disabling an account altogether is not their only option; they can delay login attempts, they can selectively disable access from individual IP addresses or blocks or specific browser types or cookies, they can insist that the password be changed, they can try to verify that there's a human making login attempts, they can temporarily disable an account, they can send warnings to a contact address, they can arbitrarily change the login process when there are multiple attempts . . . the possibilities are endless.

Meanwhile, the black hats have several fronts where they can pit their cleverness against much weaker opponents. For instance, instead of trying to brute force passwords, they could try to phish for them; there, the white hats are still fighting, but the immediate point of contact is the user, usually a much easier target. Or, the black hats can go attack other Web sites. The effort of breaking into RockYou not only yielded all the RockYou passwords, it also turned up a pile of passwords to other sites, a pile much larger than you could have gathered by attacking the other sites directly.

Brute force attacks against big Web services still exist, of course; attackers are not, on the whole, any brighter than defenders, and old ineffective practices are still rampant on all sides. But on Web services, brute force attacks aren't a major threat, and the current stupidity of passwords isn't enough to skew the economics towards them. There is some level of password stupidity at which brute force starts paying off, and it would be good not to get there, but if you have to pick one lesson to learn from RockYou, it would be, "Don't give away your password." Better yet, learn two lessons; the other one is, "Use different passwords at different sites."

Meanwhile, if you're registering at a site you don't much care about, and you use reasonable passwords at the sites you do care about, why, you have my permission to use "123456" as a password. That way, when the site hands it over on a platter to the miscreants of the Internet, you won't have compromised a password you have some fondness for.

REFERENCE

[1] Ashlee Vance, "If Your Password Is 123456, Just Make It HackMe": http://www.nytimes.com/2010/01/21/technology/21password.html.