Byteing Off More...

Jeffrey Barlow
Pacific University

Follow this and additional works at: http://commons.pacificu.edu/inter08

Recommended Citation
Byteing Off More...

Rights
Terms of use for work posted in CommonKnowledge.

This editorial is available at CommonKnowledge: http://commons.pacificu.edu/inter08/35
This is a new feature for Interface. We have been interested for some time in drawing reader’s attention to worthwhile discussions on the World Wide Web that are short and can stand alone. It is also our intention to lead readers to useful sources to which they themselves can usually subscribe without charge.

For this month we lead off with an issue currently in the news, part of the "Sarah! Sarah! Sarah!" phenomenon, referring of course to Sarah Palin, the clearly charismatic Republican Vice-Presidential candidate. The event we are following is the hacking of Palin's email account. There is a great deal of material on the WWW about this incident, but we have chosen to follow the thread in successive postings in ComputerWorld because we find them easily accessible and well written. [1]

We are less interested in the contents of Palin's email, which seem, frankly, dull, than in what the rest of us can learn about protecting our own email. After all, few of us pay all that much attention to email security.

The most probable method used—although some doubt this would in fact be effective [2]—was a simple password reset scheme. This amounts to attempting to log into an email account of a second party.

The Internet or service provider is pretty easy to identify for many people, and often scattered across the Internet. Services such as http://www.contactvip.com/ sell access to tens of thousands such addresses. For many of us, simply accessing institutional or company pages would give us such an address—try finding your own, you will very probably be surprised at how easy it is.
The next step is simply to try to log into the second party's account. Many people and some sites utilize the user's email address as the login ID. We already have that....

Now all that remains is the password. After a few failed tries you will almost certainly encounter the "forgotten your password?" screen. Yes? No problem, we can reset the password. But the next step is often to answer a security question: "What is your mother's maiden name?" Your favorite sport? Your dog's name? Etc.

Now back to the web and look the information up. Between corporate bios, Youtube and other Web 2.0 social sites, genealogical sites, blog postings, etc., most information can be found. In Palin's case a small group working together apparently answered three separate security questions in little time.

Answer the question correctly, then reset the password. Viola!

While this might take some limited time on the WWW, this approach would probably work for all but the truly security conscious among us.

What is the solution? Don't use your real mother's name, but the mother you wish you had had, in my case, Lauren Bacall. (Sorry mom.) Or the dog you wish you had had: Lassie! No more worry about falling down wells, or at least of getting out of them! (Sorry Buddy.)

Other good advice is to mix up letters and numbers in your passwords or logons or identifications. Simply doing this will much delay even a major "brute force" attack wherein a large computer or group of computers simply starts trying all possible combinations until the intruder is in. But network security is very likely to have its own safeguards against such attacks, and hopefully they will soon be noticed in any event.

Such passwords can be difficult to remember, so try this simple variant: use whatever English word you are going to use, but systematically
convert some letters to digits. "L" might become "1", "O" becomes "zero" "J" a "6" etc. To remember this system you could also establish simple correspondences once, write it down someplace—the table—not the password, and you are good to go forever.

[1] We have relied primarily upon a posting By Gregg Keizer, "Security researchers ponder possible Palin hacks. There are lots of ways someone could hack her Yahoo e-mail, say experts", found at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115100&intsrc=news_ts_head and also by Gregg Keizer "Update: Hackers claim to break into Palin's Yahoo Mail account It's 'incredibly dangerous' to use a private account, says security expert" found at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9114934

Also useful was Jaikumar Vijayan "Web proxy firm working with FBI to trace Palin e-mail hacker. The webmaster of a Ga. company says he's been asked to save server logs" http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9115099

[2] As indicated in the sources used for this article, some have questioned whether or not a password reset attack could have been successful given the security at Yahoo.com, where the hack supposedly occurred. We, however, as stated above, believe this to have been the probable method utilized.