Fact, Fiction and the Internet: Authentication Using Public [Mis]Information

M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

David Harley, BA, CISSP, FBCS, CITP is Director of Malware Intelligence at ESET<http://www.eset.com> and a distinguished and frequent contributor<http://www.eset.com/threat-center/blog/> of intelligent commentary on new developments in information assurance. I am grateful to him for his kindness in allowing us to publish his essay below on an alarming trend.

* * *

In their simplest form, many social networking sites are not much more than online diaries. Whether you’re thinking of Bridget Jones or Adrian Mole, Alan Clark or Samuel Pepys, most of us realize that a diary is just someone’s personal view, and not a reliable source of indisputable information. Most of us except for financial institutions, that is, or so it appears.

In a recent blog post<http://thompson.blog.avg.com/2009/12/now-_this_-is-scary.html>, security expert Roger Thompson<http://thompson.blog.avg.com/about.html> related how an authentication check by his credit card company resulted in their asking him a question to verify his identity, using information publicly available – as opposed to, or in addition to, the use of the sort of information we share with such institutions as “secret questions”, for instance. The required answer in this case concerned the age of Roger’s daughter-in-law, to whom they referred to by her maiden name. The only public resource that Roger could think of that would connect the two of them is Facebook<http://www.facebook.com/>, though other commentators have pointed out that genealogy sites are used in identity checks too.

For a while now, some security researchers have advised people to be economical with the truth when using chatrooms, forums and social-networking sites. Why would you give your true date of birth to a site that doesn’t need to know it and that can’t be trusted to keep it private? Is it a good idea to let all your Facebook friends know you’re on holiday next week when you may not have met them all personally and can’t be sure how much of your information is available to their friends? If you must use your dog’s name as a password (you really shouldn’t be using names for passwords), talking about Fido on Facebook gives a determined attacker a good start along the password guessing route. How much easier is it to harvest information about a target when their place of birth or current home town is public knowledge?

In the security industry, we talk a lot about the dangers of social networking and sharing information that may be valuable to burglars and scammers, or even spies (if you happen to be married to the head of MI some-number-or-other). But it isn’t just about what you do, or information that you give away. Other people can give away information that impacts on you, like that current, dated photo of you next to Niagara Falls that your friend posts to his Facebook page, giving clear notice that you aren’t at home right now.

This latest revelation about how information posted to Websites is being used (or misused) suggests a potential scenario where false information might actually be seen as more valid than true information, simply because it’s “publicly available” and your bank assumes that you – or
someone within your social network – will never lie to a social networking site.

There is probably more misinformation than information in the online world, whether it’s deliberate deception, propaganda, fraud, well-meaning lack of comprehension, or just data that are no longer current. So any instance of an organization relying on the accuracy of data from a wider (more public) range of resources raises concerns about inaccuracy and perhaps even the deliberate poisoning of data. How can individuals keep track of and validate everything that is “known” about them when presumed-valid information is pulled from who knows where? More so, if the organization pulls that information long after it has supposedly already validated you as a customer.

While a bad guy who has access to all the information that a bank has may not need to change it in order to profit from it, there are several scenarios where he might want to. This might include hampering remediation; influencing the presentation of data he can write to even when he can’t read it (a more common situation than one might think); and compromising public data as part of a social engineering attack. The objective could also be to block legitimate access to information as well as or instead of impersonation.

Regulation of data is nowhere near keeping up with the Internet age. The possibility of an organisation using one customer to validate (or invalidate) another poses more awkward ethical and practical issues than most of us have thought of. It might benefit us all to think for a moment about the long-term impact that our next Facebook update or tweet< http://twitter.com/> may have on ourselves or our friends, before we put fingers to keyboard or keypad.

We should also start looking into the practices of organizations which are making ill-considered use of such [mis]information.

* * *

ESET is exhibiting at Infosecurity Europe 2010, the No. 1 industry event in Europe held on 27th – 29th April in its new venue Earl’s Court, London. The event provides an unrivalled free education programme, exhibitors showcasing new and emerging technologies and offering practical and professional expertise. For further information please visit www.infosec.co.uk

* * *

David Harley, BA, CISSP, FBCS, CITP,< http://blog.isc2.org/isc2_blog/authors.html#harley> has been researching and writing about malicious software and other security issues since the end of the 1980s. From 2001 to 2006 he worked in the UK’s National Health Service as a National Infrastructure Security Manager, where he specialized in the management of malicious software and all forms of e-mail abuse, as well as running the Threat Assessment Centre. He joined ESET’s Research team in January 2008 as Research Author, and was appointed Director of Malware Intelligence in August 2008.
