Pseudonymity

Pseudonymity, a word derived from pseudonym, meaning 'false name', is a state of disguised identity. The pseudonym identifies a *holder*, that is, one or more human beings who possess but do not disclose their true names (that is, legal identities).[1] Most pseudonym holders use pseudonyms because they wish to remain anonymous, but anonymity is difficult to achieve, and is often fraught with legal issues.[2] True anonymity requires unlinkability, such that an attacker's examination of the pseudonym holder's message provides no new information about the holder's true name.[3]

Examples

Although the term is most frequently used today with regard to identity and the Internet, the concept of pseudonymity has a long history. In ancient literature it was common to write in the name of a famous person, not for concealment or with any intention of deceit; in the New Testament, the second letter of Peter is probably such. A more modern example is all of the Federalist Papers, which were signed by Publius, a pseudonym representing the trio of James Madison, Alexander Hamilton, and John Jay. The papers were written partially in response to several Anti-Federalist Papers, also written under pseudonyms. As a result of this pseudonymity, historians know that the papers were written by Madison, Hamilton, and Jay, but have not been able to discern which of the three authored certain papers.

Pseudonymity has become an important phenomenon on the Internet and other computer networks. In computer networks, pseudonyms possess varying degrees of anonymity,[4] ranging from highly linkable *public pseudonyms* (the link between the pseudonym and a human being is publicly known or easy to discover), potentially linkable *non-public pseudonyms* (the link is known to system operators but is not publicly disclosed), and *unlinkable pseudonyms* (the link is not known to system operators and cannot be determined).[5] For example, true anonymous remailer enables Internet users to establish unlinkable pseudonyms; those that employ non-public pseudonyms (such as the now-defunct Penet remailer) are called pseudonymous remailers.

The continuum of unlinkability can also be seen, in part, on Wikipedia. Some registered users make no attempt to disguise their real identities (for example, by placing their real name on their user page). The pseudonym of unregistered users is their IP address, which can, in many cases, easily be linked to them. Other registered users prefer to remain anonymous, and do not disclose identifying information. However, Wikipedia's server logs may enable system administrators to determine the IP address, and perhaps the true name, of a registered user (see Wikipedia:Privacy Policy for a list of the conditions under which such a linkage would be attempted). It is possible, in theory, to create an unlinkable Wikipedia pseudonym by using an Open proxy, a Web server that disguises the user's IP address. However, most open proxy addresses are blocked indefinitely due to the their frequent use by vandals (see Wikipedia:Blocking policy). Additionally, Wikipedia's public record of a user's interest areas, writing style, and argumentative positions may still establish an identifiable pattern.[6]

System operators (sysops) at sites offering pseudonymity, such as Wikipedia, are not likely to build unlinkability into their systems, as this would render them unable to obtain information about abusive users quickly enough to stop vandalism and other undesirable behaviors. Law enforcement personnel, fearing an avalanche of illegal behavior are equally unenthusiastic.[7] Still, some users and privacy activists like the American Civil Liberties Union believe that Internet users deserve stronger pseudonymity so that they can protect themselves against identity theft, illegal government surveillance, stalking, and other unwelcome consequences of Internet use (including unintentional disclosures of their personal information, as discussed in the next section). Their views are supported by laws in some nations (such as Canada) that guarantee citizens a right to speak using a pseudonym.[8] This right does not, however, give citizens the right to demand publication of pseudonymous speech on equipment they do not own.

Pseudonymity and confidentiality

Most Web sites that offer pseudonymity retain information about users. These sites are often susceptible to unauthorized intrusions into their non-public database systems. For example, in 2000, a Welsh teenager obtained information about more than 26,000 credit card accounts, including that of Bill Gates.[9] In 2003, VISA and MasterCard announced that intruders obtained information about 5.6 million credit cards.[10] Sites that offer pseudonymity are also vulnerable to confidentiality breaches. In a study of a Web dating service and a pseudonymous remailer, University of Cambridge researchers discovered that the systems used by these Web sites to protect user data could be easily compromised, even if the pseudonymous channel is protected by strong encryption. Typically, the protected pseudonymous channel exists within a broader framework in which multiple vulnerabilities exist. Pseudonym users should bear in mind that, given the current state of Web security engineering, their true names may be revealed at any time.

Pseudonymity and online reputations

Pseudonymity is an important component of the reputation systems found in online auction services (such as eBay), discussion sites (such as Slashdot), and collaborative knowledge development sites (such as Wikipedia). A pseudonymous user who has acquired a favorable reputation gains the trust of other users. When users believe that they will be rewarded by acquiring a favorable reputation, they are more likely to behave in accordance with the site's policies.[11]

If users can obtain new pseudonymous identities freely or at very low cost, reputation-based systems are vulnerable to whitewashing attacks[12] (also called serial pseudonymity), in which abusive users continuously discard their old identities and acquire new ones in order to escape the consequences of their behavior: "On the Internet, nobody knows that yesterday you were a dog, and therefore should be in the doghouse today." Users of Internet communities who have been banned only to return with new identities are called sock puppets.

The social cost of cheaply discarded pseudonyms is that experienced users lose confidence in new users, and may subject new users to abuse until they establish a good reputation. System operators may need to remind experienced users that most newcomers are well-intentioned (see, for example, Wikipedia's policy about biting newcomers). Concerns have also been expressed about sock puppets exhausting the supply of easily remembered usernames. In addition a recent research paper demonstrated that people behave in a potentially more aggressive manner when using pseudonyms/nicknames(due to the effects of Online disinhibition effect) as opposed to being completely anonymous. Proposals have been made to raise the costs of obtaining new identities (for example, by charging a small fee or requiring e-mail confirmation). Others point out that Wikipedia's success is attributable in large measure to its nearly non-existent initial participation costs.

References

[1] May, Timothy C. (1991). The Crypto Anarchist Manifesto (http://www.activism.net/cypherpunk/crypto-anarchy.html).

[2] du Pont, George F. (2001) The Criminalization of True Anonymity in Cyberspace (http://www.mttlr.org/volseven/du pont.html) 7 Mich. Telecomm. Tech. L. Rev.

[3] Post, David G. (1996). Pooling Intellectual Capital: Thoughts on Anonymity, Pseudoanonymity, and Limited Liability in Cyberspace (http://www.cli.org/DPost/paper8.htm). *University of Chicago Legal Forum.*

[4] Froomkin, A. Michael (1995). "Anonymity and Its Enemies (Article 4) (http://www.wm.edu/law/publications/jol/95_96/froomkin. html)". *Journal of Online Law.*

[5] Pfitzmann, A., and M. Köhntopp (2000). " Anonymity, Unobservability, and Pseudonymity: A Proposal for Terminology (http://dud.inf. tu-dresden.de/literatur/Anon_Terminology_v0.23.pdf)". In H. Federrath (ed.), *Anonymity* (Berlin: Springer-Verlag), pp. 1-9.

[6] Rao, J.R., and P. Rohatgi (2000). "Can Pseudonyms Really Guarantee Privacy?" (http://www.freehaven.net/anonbib/cache/ rao-pseudonymity.pdf) Proceedings of the 9th USENIX Security Symposium (Denver, Colorado, Aug. 14-17, 2000).

[7] Clarke, Roger (1998). "Technological Aspects of Internet Crime Prevention." (http://www.anu.edu.au/people/Roger.Clarke/II/ ICrimPrev.html) Paper presented at the Australian Institute for Criminology's Conference on Internet Crime (February 16–17, 1998).

[8] http://www.eff.org/legal/cases/2TheMart_case/20010420_eff_2themart_pr.html

[9]   Reuters News Service (2000). "Report: Hackers Had Gates' Credit Card Data" (http://news.com.com/2100-1017-238427. html?legacy=cnet) (March 26, 2000).

[10]   Katayama, F. (2003) "Hacker accesses 5.6 Million Credit Cards" *CNN.com: Technology (February 18, 2003).* (http://www.cnn.com/2003/TECH/02/17/creditcard.hack/)

[11]   Kollock, P. (1999). "The Production of Trust in Online Markets." (http://www.sscnet.ucla.edu/soc/faculty/kollock/papers/online_trust. htm) In E.J. Lawler, M. Macy, S. Thyne, and H.A. Walker (eds.), *Advances in Group Processes* (Greenwich, CT: JAI Press).

[12]   Feldman, M., S. Papadimitriou, and J. Chuang (2004). "Free-Riding and Whitewashing in Peer-to-Peer Systems." Paper presented at SIGCOMM '04 Workship (Portland, Oregon, Aug. 30-Sept. 3, 2004).

External links

- Anonymity Bibliography (http://www.freehaven.net/anonbib/) Excellent bibliography on anonymity and pseudonymity. Includes hyperlinks.
- Anonymity Network (http://www.tik.ee.ethz.ch/~rennhard/shopaware/) Describes an architecture for anonymous Web browsing.
- Electronic Frontier Foundation (EFF) Anonymity/Pseudonymity Archive (http://www2.cddc.vt.edu/www.eff.org/Privacy/Anonymity/)

Article Sources and Contributors

Pseudonymity *Source*: https://en.wikipedia.org/w/index.php?oldid=550289251 *Contributors*: Aeternus, Ais523, Angela, ArnoldReinhold, Auntof6, Beland, Chulki Lee, DancingMan, David Eppstein, Davidgothberg, Fastfission, Ferkelparade, Graham87, Ground Zero, Guthrie, Heron, HorsePunchKid, HuPi, IceKarma, Jmabel, Jtarragano, KaiAdin, Kevin Steinhardt, Kku, Kotepho, Kzzl, Mardhil, Mellery, Miagirljmw14, Michael Hardy, Mindmatrix, Mmb2006, Modemac, Neep, Nihiltres, Novum, Ntmatter, Nyenyec, Otto4711, Pfaff9, PierreAbbat, Plausible to deny, PullUpYourSocks, Raraoul, Rjwilmsi, Sbacle, Shaddack, Tearanui, Tom harrison, TonyW, Tsikerdekis, Wik, Ww, Zorro CX, 45 anonymous edits

License