The Case for the Universal Personal Internet Identification: The Case against Internet Anonymity

Nazli Hardy, Ph.D.

Abstract. **Web 2.0, propelled by interactive users who collaborate in the flow of creativity, has brought with it abundant anonymous users (abusers) who cannot be held accountable for their actions and thus are able to perpetuate security threats under their cloak of anonymity. With this lack of accountability, the Web opens itself to the realm of unending and damaging security threats that no amount of anti-virus software or cautiousness can contain. This paper posits that it is essential to have a Universal Internet IDs, like a universal driver's licenses, that represent users accurately and thus holds them accountable for their actions online. The apparent loss of inhibition online is outweighed by the security of accountability and the traceability of cyber crime. The premise is that the Universal Personal ID will, in fact, further encourage freedom of interactivity and the interchange of collaboration and creativity online.**

Index Terms - **Information Security Threat, Social Networks, Anonymity, Web 2.0.**

I. Introduction

2008 will be the year of social malware and spam volumes will continue to grow without limit (Ironport, 2008). The rise of the Internet has been less due to technology and more due to the force of the "ordinary user". The "ordinary" is certainly no indication to the power that it generates. The history of the Internet (Abbate, 1999), stemming from the 1950's and 1960's with the interests of the RAND, the Defense of Department of the United States, and the research support for certain universities ARPANET, actually did little to drive the growth of the internet. It was only in the mid 1990's, when ordinary people discovered the Internet as a means to communicate, that this medium was propelled to it's meteoric rise, from an engine with limited use by an elite few, to one with apparently unlimited use by a global society. In affect, the Internet became a platform for the common man, on a global scale. Internet technologies, in terms of software, hardware, programming and scripting languages are driven by the demand. Thus the concern for information security on the Internet is not new, in fact on any given day and on many given Web sites, there are further descriptions of threats and solutions for information security. Most computer security courses and text books teach the concepts of hardening resources, platform and application security, and all the different types of security threats that exist online, such as distributed denial of service, cross-scripting, SQL injections and freely available software like the key logger (Hardy, 2006).

Manuscript received March 25, 2008. *Nazli Hardy. Department of Computer Science, Millersville University, Millersville, P.A., USA 17551*
Nazli.Hardy@Millersville.edu Tel: 717-872-3666
http://cs.millersville.edu/faculty/profdetails.php?pid=11

This paper posits that a) the threat of Information security is especially prevalent in the Web 2.0 world, for the very same reason that people consider themselves secure (contextually uninhibited); online: anonymity, b) it is the anonymous (and thus unaccountable) users who are as responsible for information security breaches as the tech-savvy hackers. Thus, the paper proposes a Universal Personal Internet ID (UID) that is unique, much like a universal driver's license.

II. The Current State of Internet Security

In 2007 spam volume increased 100%, became more dangerous, and the "self-defending Bot Network" was introduced, reflecting the quality and technical sophistication of the threats and their developers (Ironport, 2008). Some 55% of email users have lost trust in email because of spam (Pew, 2007), usually embedded as cross-site script attacks or as attachments. Viruses, and the associated network congestion, have become so common that they barely made headlines. Virulent variants the likes of "Feebs", and "Storm", are dominating the stage.

The Feebs worm, for example, remains vigilant for outgoing SMTP connections and then injects an infected .zip file which the recipient is more likely to open since it is coming from an apparently reliable source. Naturally anti-virus companies, such as Symantec and Norton have had to redefine their jurisdiction over fighting malware, but the fact remains they are attacking the problem to which the root is never addressed.

The "Storm" group of malware is appropriately named, as it storms users on a peer-to-peer basis by sending seemingly innocuous emails asking the user to open a hard to resist implicating links like "man you have got to tell me where you picked her up. I saw this on the web, it has to be you, check it out yourself" which seems to direct the identified user to a YouTube video. Many would be tempted to click on the link which actually directs them to a storm node (Ironport, 2008). What makes this example of Storm especially relevant to the premise of the paper is that it is reusable (and easily perpetuated) for many kinds of other attacks, particularly when posted on social networks.

III. The Nature of Web 2.0

Web 2.0, is a social and collaborative generation of Web technology that encourages and draws from the free and uninhibited nature of information flow. Web 2.0 is highly interactive and designed to draw from input of information, much of it personal in nature. Examples are wikis, blogs, and social networks. At a Web 2.0 Conference in 2004, Media Labs and Tim O'Reilly formulated a sense of Web 2.0 versus Web 1.0 (Table 1). This concept has since blossomed to a full-fledged Web 2.0 cyber life, with exciting interactivity

and propagation of knowledge and discourse, but also with severe security implications. The roots of these are rarely addressed in Computer Science circles, even though the technical answer lies firmly there.

Web 1.0	**Web 2.0**
DoubleClick	Google AdSense
Ofoto	Flickr
Britannica Online	Wikipedia
Personal Websites	Blogging
Publishing	Participation/ Comments
Content management systems	wikis
Directories (taxonomy)	Tagging ("folksonomy")

Table 1: Web 1.0 vs. Web 2.0

IV. The Misleading Feature of Anonymity

It can be argued that anonymity is what keeps the user somewhat secure. We can "crawl" and "surf" and "roam" around the World Wide Web under the (deceptively) invisible guise of anonymity. After all we can create scores of email addresses for communications, none of which necessarily bear our actual names, we can leave "anonymous" comments, and we can redefine our identities as with screen names such as "beautifulBlonde2007" or "savvyExec142" or even one reflecting a lofty career goal with "soulSinger". Personally I would go with "BeautifulSavvySinger" any day, but the sad fact remains this wishful Internet ID has nothing to do with the reality for which I am actually accountable. The example given here is fairly harmless, however the factor of accountability is the foundation around which the premise of this paper exists. With the lack of accountability of the Web, we are opening up the realm of unending and damaging security threats that no amount of anti-virus software or cautiousness will solve.

Web 2.0 enables anyone with access to the Internet to have a Web presence. An "anyone" who is easily anonymous and as easily unaccountable for their actions.

Features of the Web 2.0	**The Impact**
The user feels unreachable due to "anonymity"	Provision for unaccountability
The Internet appears to be intangible, and thus unreal	Provision for unaccountability, disregarding the realm of conscience
The Internet is accessible on a global scale	Greater reach and propagation for unaccountability
The speed of connection allows almost real time interaction/ commenting	Faster reach and propagation for unaccountability
Scale of searchability	Broader access to unaccountability

Table 2: The Impact of Anonymity

Lest this sounds like a position on moral proprietary and conscience, the author is an avid advocate for the free flow of information and the equality of access that the nature of the Web 2.0 generates. However, the lack of accountability demotes both the accuracy of information and the equality that should be attributed to all persons. The proposed UID can engender both by enforcing accountability of words and actions.

V. Blogs, Wikis, and Social Networks

This paper focuses on blogging, wikis, and social networks, amongst the several Web 2.0 features. Blogging websites, such as blogspot.com and wordpress.com have readily become a meeting place of creativity where bloggers write about their craft and then connect with bloggers of similar interest world-wide using features such as "blogroll" and links of interests. In fact the blogging community has become a close knit group providing information and support to each other. In many ways, it is ideal global forum that gives a feeling that "the world belongs to those who blog". There are blogs that exist purely for marketing products, while others are connected to online stores, newspapers or research groups to further allow the editors to discuss a product or topic in their own words.

Wikis, the most famous example being Wikipedia, is the epitome of egalitarianism. Everyone can contribute, and anyone can edit content. In fact since its creation in 2001, Wikipedia has since grown to over 5.7 million user-contributed articles and 250 languages. Despite the general concern over the quality of the user-contributed articles (McHenry 2004), Wikipedia has generally received respectable to high marks for accuracy, particularly in the sciences (Read 2006; Giles 2005).

Social networks such as Facebook.com, and MySpace.com were initially predominant on college campuses and now have become a commonplace for reconnecting with old friends, keeping in touch with colleagues, and making new friends via old friends. Common groups and widget applications sew together these social portals.

What is common to all of the above is the ability for users a) to create an identity based on an email and b) to leave comments and feedback (though there are measures to limit and monitor these) **anonymously**. It is this anonymity that encourages candid, free, unchecked, balanced and imbalanced, thoughtful and thoughtless comments.

Sites such a ratemyprofessors.com allow students to anonymously leave comments about their professors; good and bad. In many cases, it crosses the boundary of commenting on the course and the professor's ability to teach and veers into the students' personal opinion of the professor. The site allows professors to respond rebut – but not anonymously. The professors necessarily have to maintain professionalism because their comments are not anonymous, whereas the students or even other colleagues can anonymously and without accountability leave any comment. Clearly there is an imbalanced ground between anonymous and identified users of the Internet.

VI. The Advantages of Anonymity is its Disadvantage

Arguably there are benefits of the interactive and easily accessible nature of the Web. Anyone can have a Web presence and have their say. Anyone can easily market their products and creativity. Certainly bloggers in prohibitive governments like China and Saudi Arabia are forced to assume aliases to save themselves from being prosecuted for stating their opinions.

However, anonymity does not solve the underlying problem. Anonymity in fact propagates the problem by allowing the problem to exist. So in effect the advantage of anonymity is its disadvantage.

VII. The Disparity of Identification

The basic security threats posed on the Web and in particular, on Web 2.0 can be placed in 3 categories that apply to the user community: personal, professional, and financial. In each case, we see that the security threats exist due to the disparity of anonymity and the availability of actual information on people.

Facebook users have information such as name, current status, hometown, political views (Fig 1). In addition, email addresses, likes and dislikes, hobbies and activities and other personal information are listed. Although not all of this information is compulsory, most legitimate users prefer to portray themselves accurately since friends and colleagues view these pages. They choose to be accurate because in identifying themselves there is an immediate legitimacy. For example, the author of the paper will not state herself to be anything more than she is because her friends and colleague know who she is and thus she is forced to be accountable.

Likewise the author's information on a blogspace (Fig 2) has to be accurate because it is linked to her professional and personal pages and she is (necessarily) accountable the information and comments I make.

On Facebook and Blogger, it is certainly possible to restrict the access of the information to only friends, or to certain people, or only people who belong to the same networks as the user, or it is accessible to everybody. So, it is very possible for an "anonymous" user on the same network to view all the information about a legitimate user as well the information and photos of their friends, using a false (and this anonymous) userid.

IP addresses are easily traceable, for example in the constantly edited Wikipedia, IP addresses are logged. However, IP addresses do not carry the same weight in accountability as does the name and thus one is more likely to feel unaccountable for the IP address as one is to one's own identity. This is clear by the amount of vandalism (and consequent correcting) on wikis. Additionally, it is possible to spoof or block IP addresses, making it impossible to track a user. IP addresses are also not helpful when a user is logging on from a public machine.

An unknown user or party can anonymously create a pictogram of a "legitimate" user from their Web presence – a "webgram". Since certain professionals necessarily have to represent themselves and their history accurately (Fig 3), there is transparency (and thus accountability) in their related Web actions. If all else were equally transparent, then there would be no issue because of the forced accountability all round. However, due to the discrepancy of those who have the luxury of being "anonymous' there is a clear disadvantage to the transparent user who becomes a clear target in a open ground of spam, worms, viruses, and all other malware by the unaccountable anonymous user.

Personal information like date of birth and hometown is easy to obtain online. Mother's maiden name is not too hard to decipher with the personal information people post. Therein lays the foundation for identity theft. Granted such information should be guarded always and not given out; they can easily be divulged in conversation with mutual friends.

It is relatively simple for our anonymous spammers to use email addresses, coupled with information about favorite movie and music titles (easily found on profiles) to propagate directed spam or cross-site scripting (security vulnerability which allow code injection by directing users to malicious sites) and phising emails.

Disgruntled and anonymous bloggers who post libelous information about colleagues, professors, or people they feel have wronged them have no accountability, yet, it indirectly jeopardizes careers. Again this is caused by the discrepancy of the legitimate and identifiable person online versus the anonymous person who cannot be held accountable. It always falls on the transparent and "legitimate" Internet user to fight against libel at the risk of appearing defensive and engaging in an unprofessional stance against an irate but anonymous user.

VIII. Existing Security Features of Web 2.0

Many current and improving security measures exist; technologies such as Secure Socket Layer (SSL), digital signatures and envelopes, anti-virus software, authentication protocols such as Challenge-Handshake Authentication Protocol (CHAP), several encryption algorithms – however they do not protect the "social" user of Web 2.0 who drive the technology by the very nature of their interactivity and collaboration.

IX. The Necessity of the Universal ID

Security measures are geared to protect against the anonymous user. This paper proposes eliminating the primary source of the problem by disallowing anonymity by enforcing a universal ID. Imagine people owning homes, and cars, and working at jobs under aliases where they create a fantastical identification for themselves. There would be utter security chaos. In most countries there are ID cards issued by a national authority. These cards are issued only after several forms of other identifiers (6 in the United States) are presented, included a picture form.

X. Features and Implementation of the Universal ID

Just like domain names are issued under the auspices of ICANN, working with regional entities, the issuance of the UID to access the Internet will thwart internet security risks.

The features of the UID will similarly contain name, address, and a unique identifier generated by the issuing body and users are responsible for keeping it safe as they would their credit card numbers. All users log onto the Internet using their ID number. If this is lost, a new one must be issued, just like in the case of credit cards. The inconvenience

is a detractor from people misplacing or sharing their IDs. These numbers have to be renewed periodically just like licenses.

XI. Potential Resistance to the UPID (response in brackets)

(i) Site registration with email confirmation is already a form of UID. *It is not, it is easy to make up an email address with false information.*

(ii) There is significant cost in the formation of a new body to issue licenses. It is a massive task. *Indeed but compared to the ever-increasing cost of fighting against security vulnerabilities, it is minimal. In addition, ICANN can create a parallel body for this.*

(iii) People in non-democratic governments (like China, Myanmar, and Saudi Arabia) rely on anonymity to fight back against anarchy. *True but anonymity itself cannot and does not democratize governments. In addition, every government official also will have to use universal IDs thus furthering accountability by all.*

(iv) There will be no monitoring agent to enforce the proper use of the UID. People can lend each other their IDs. *True, but the ownership will encourage accountability, which is exactly the strength of the UID Just as people are reluctant to lend others their license or credit card because ultimately they are responsible for its use, they will be careful not to misuse their own UIDs*

(v) People will no longer be able to visit certain entertainment sites online anonymously. *This is small price to pay for the security resulting in the disabling senders of phising emails and spam. In addition, they can still visit any site – but they are accountable*

This is moral policing. *No it is only enforcing accountability. People will do only what they are ready to be held responsible and they will be discouraged from actions to which they do not want to associated – thus limiting security vulnerabilities and threats.*

XII. Conclusion

The UID levels the playing field for all users. Anonymous users of the Internet are not only not held accountable, their actions are further enabled by the lack of accurate identifiers. Users of the Internet who represent themselves accurately (by necessity or by choice) are penalized by having to pay the price of securing themselves personally, professionally, and finically because they are accountable for their actions online.

To address the ongoing problem of information and Internet security, the source must be addressed – accountability. Anonymity emboldens users to be and say and do what they normally cannot back up or to which they normally would not associate themselves.

While the interactivity and collaborative flow of information and creativity of Web 2.0 should be encouraged and further developed, the technology and its users should be protected by anonymous abusers. The legitimate Internet user should not constantly have to guard themselves against errant anonymous users because that negates and inhibits the inherent free flow of online information and creativity.

It is almost impossible to catch cyber criminals because the cloak of anonymity and the maze created by infected "innocent" computers within a botnet that protects them.

The Universal ID is not equivalent to the Internet policing. It only enforces accountability. There is no international moral police that states a user cannot leave comments or post opinions or visit adult websites or even send spam. It only enforces the notion of accountability and takes away the dark cloak of anonymity. However, it does make it easier to track cyber crime, like ID theft that can be traceable by authorities using the access route (including IP) and UID number.

Whatever the administrative problems and difficulties of generating and maintaining universal IDs, the advantages far outweigh them. In many cases, the resistance is akin to the resistance against national IDs. Even though the Internet is an intangible medium, its reach and accessibility necessitates protective measures that address the problem at the root. Anonymity has disengaged the user from the normal sense of accountability that comes with identification.

References

1. Abbate, Janet. *Inventing the Internet*. Cambridge: MIT Press, 1999.
2. Hardy, Nazli, *Course Website for Security*, Millersville University, 2006 Available: http://mucspc.millersville.edu/nmollah/ComputerSecuritySyllabus.htm
3. Ironport Report, *2008 Internet Security Trends*, CISCO & Ironport 2008 Available: www.**ironport**.com/**securitytrends**/
4. Pew Internet & American Life Project, *May 25, 2007 Survey*
5. McHenry, R. 2004. The faith-based encyclopedia. *TCS Daily*, 15 Nov 2004. Available: http://www.techcentralstation.com/111504A.html.
6. Giles, J. 2005. Internet encyclopedias go head to head. Nature 438: 900-901.

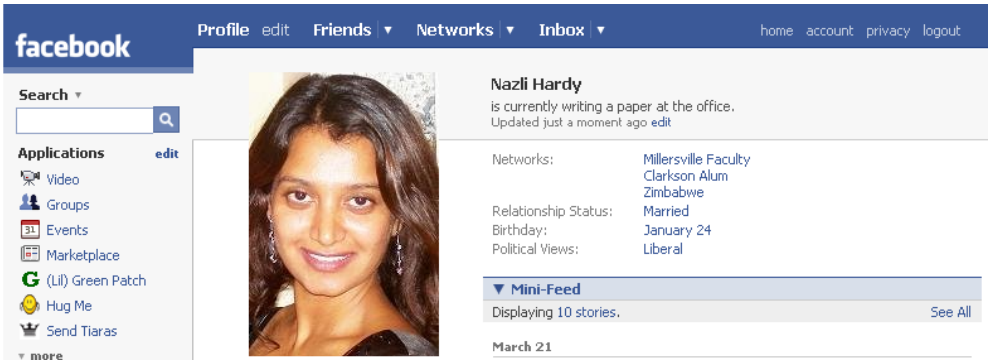

Figure 1: Facebook Profile of the Non-Anonymous Web 2.0 User

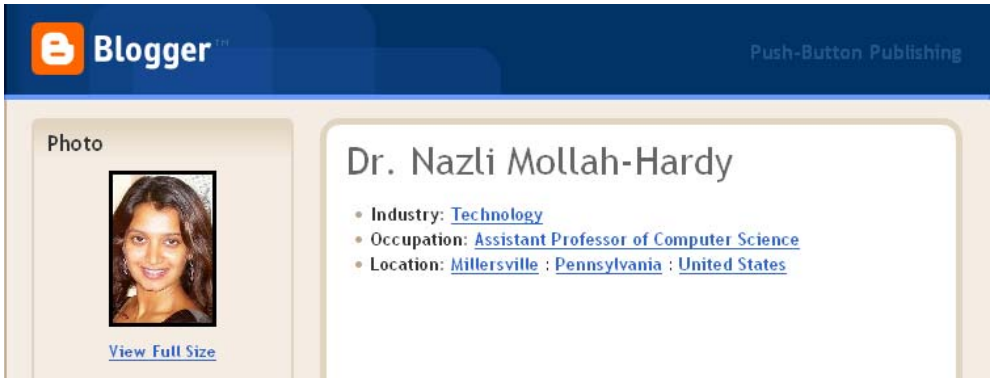

Figure 2: Blogger Profile of the Non-Anonymous Web 2.0 User

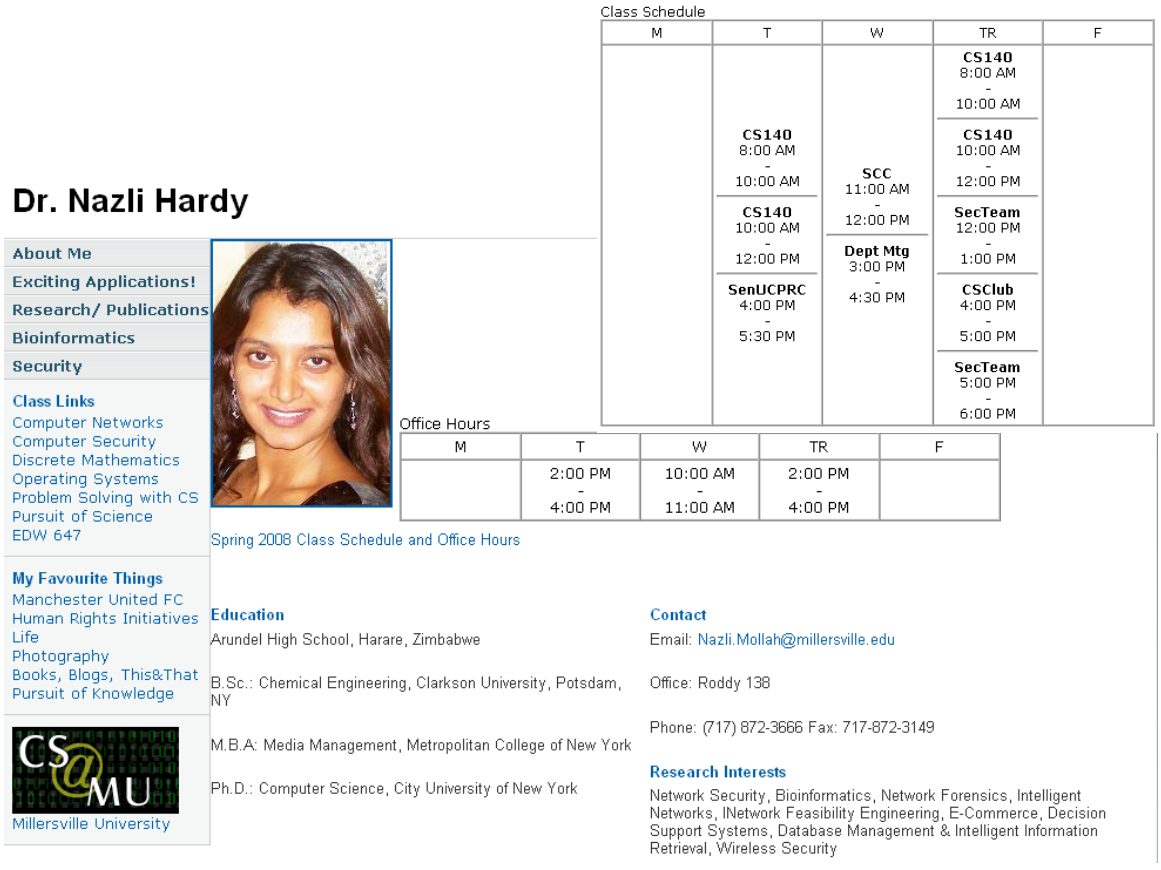

Fig 3: Some Professions Necessitate Accurate Representation of Personal and Professional Identifying Information