

Source: Les Fraser

Version V0.2/27.05.2008

Document for:

| | |
|-------------|---|
| Decision | |
| Discussion | x |
| Information | |

Social Networks - Problems of Security and Data Privacy Background Paper

CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among Informatics Professionals in recognition of the impact that Informatics has on employment, business and society. CEPIS -which represents 37 Member Societies in 33 countries across greater Europe- has agreed on the following statement:

1 Introduction

Security within IT systems/services has evolved and continues to evolve as technology changes. From a business perspective, the old certainties that came with internally managed systems and well defined system boundaries are already eroded by the need to permit access to services by home and remote workers, by the complexity of creating integrated national and even international systems to service the entire enterprise, and by the emergence of a strong third-party service industry which brings a need to extend some aspects of the corporate networks and services to include service companies upon whom business depends. The Internet is now a key business tool but its integration into the business network brings different security challenges. From the perspective of a private citizen, the security risks of IT have increased enormously as we enter the broadband era.

Until now the security model, however much it has changed and evolved has been based upon the principle of the fortress: that the outer defences must be maintained and the danger kept at bay. Internal security within the IT system was a separate and clearly defined issue. Whether as a citizen or a business, your security could be controlled using anti-virus/anti-malware filters to prevent access by hostile code, and firewalls together with ever-stronger authentication processes to control and prevent access by hostile systems/people.

2. Issue

The Internet is changing and the use we make of it is evolving. The growth of social networking concepts which provide more personal and interactive uses of the internet are beginning to change the nature of the security model. We need to recognize this change and develop approaches that are compatible with this technology.

Background

When the Internet was a repository of fairly static information, risks were based around the download of information and material you didn't want, and the possibility of a hostile entity using the Internet conduit to gain illegitimate access to internal services. In general, the Internet and in particular the web, was based upon the exchange of static information - you place information on a web page, and I read it.

With obvious exceptions, (the exchange of music via peer-to-peer networking, for example) the ability to interact with an organisation via web-based protocols was usually limited to transaction-based activity executed through the completion of pre-defined information. (Buy a book from Amazon, or complete your tax return online, for example.) This transaction information was usually collected at the perimeter of the network, and as an individual you were in contact only with an outer web server.

New web-based technologies based upon what some call 'social software' and businesses tend to call "collaborative software" or "Web-2" are much more interactive and operate on a personal rather than corporate level, and so bring with them a different set of risks. Definitions of what these terms mean are many and inconsistent, but in general terms the following may suffice:

Web2.0 is the logical evolution of the Internet to permit the connecting of people to each other and to permit individual control over their interaction;

"Social Software" applies to web-enabled software programs which allow users to interact with and share information with other users;

"Collaborative Software" applies to a subset of social software that enables collaborative work functions. The underlying concepts are often similar, and the distinction between "business" and "social" programs or services is often not clear.

Technology is slowly changing the way people and organisations relate to each other. More and more, the Internet may drive their social life. Web-2 developments will permit greater interaction with the customer, but on the customer's terms. The ability of the individual to personalise the information presented to him is a key factor.

There are many social networking sites which permit you to create a personal profile, advertise your interests, and inform the world of what you are doing. Some, such as 'friends reunited' have a specific purpose in bringing together those who were once classmates. Others inevitably will be dating sites and bring together those who are seeking intimate friendship. Many such as Facebook or MySpace for example, are intended to enable you to keep in touch with friends and family. Whatever the underlying purpose, they will allow you to upload a personal image profile on the web, to send/receive messages, to chat via online chat rooms, and share files and photographs.

Other interactive sites may let you inform the world of your movements. Twitter poses the question 'What am I doing Now?' as its byline, and permits you to tell the world what you are up to. Another lets you post where you are in the world, and tells you whether any of your acquaintances are also in town at the same time. There are hundreds of other similar sites springing up on the web. People who are very involved in these sites may also have a personal 'blog' site and will certainly participate in a number of online chat facilities to keep in contact with friends.

Businesses can and do make use of the same technology, to scroll through online CV profiles looking for prospective new staff for example, or use a corporate 'blog' to promote the company's products and services, or offer online chat sites to provide interactive assistance to customers, and so on.

Social networking sites on the Internet can be categorised according to their main purpose, as follows:

(a) Contact sites

Sites such as *Linkedin*, *PLAXO*, or *Friends Reunited*, whose primary purpose is to share contact details and provide links permitting others to access the details of friends and contacts. They are used by both individuals and organisations to keep track of contacts and to widen their contact base through exploiting the links to 'friends of friends'.

(b) Social Networking Sites

These include sites such as *Facebook*, *MySpace* or even *TWITTER* whose primary purpose is to allow people to provide a 'shop-window' on their life, and to share aspects of their life with others. Although in most cases these are primarily personal sites, other organisations are increasingly exploiting these sites for commercial purposes. Just as an individual may enter an item of news to share with others, a theatre may enter details of a production to share with 'friends of the theatre' or a company may provide details of new products.

(c) Visual Information Sharing sites

A number of sites such as *YouTube* or *Flickr* permit the sharing of video and still photo content. In addition to personal video clips, YouTube does carry product advertisements, instructions for the use of products, and film/TV trailers.

(d) Game and Interactive Virtual Reality sites

Virtual worlds or Metaverses are 3-dimensional virtual realities where an individual may create their own personal avatar and interact with others. There are many interactive worlds in the internet community where people may play games, notably fulfilling a desire to engage in war-games as an orc or an elf, though there are many different simulations available. These are referred to as massively multiplayer online role playing games ([MMORPG](#)). Some are used for entirely social purposes, and have no 'game' as such. These range from children's sites such as *Barbie Girls* or *Club Penguin* (for a list of these see <http://www.360kid.com/blog/?p=25>) to adult-oriented sites such as *Second Life*, which is probably currently the largest and most successful of the social 3-D sites. As its title implies, it permits you to develop an entire 'second life' owning virtual land, setting up virtual businesses, interacting with others to socialize or to cooperate in a virtual 3-D world.

Interactive role-play games are played in real time, and the actions of your character and those around you are controlled by the players themselves. Players will have freedom to do anything they wish to do within the rules and the environment of the virtual world.

Some companies are looking to these sites as a way to reaching the 25-35 year old age group, currently considered the prime age group by marketing people. IBM has hosted matches at the Second Life Wimbledon; the Liverpool Philharmonic Orchestra has staged a live concert in Second Life, a number of pop groups have played virtual concerts. Work within large corporation, such as IBM, into the commercial application of sites like "Second Life" has shown early positive results, (e.g. <http://www.ibm.com/virtualworlds/businesscenter/>).

Initial results suggest that a meeting of people who maintain a presence on Second Life through their "second-life" avatars is more productive than either phone or video conferencing. Building a private virtual reality site was less successful, however, as people become attached to (and in some respects are) their personal avatar, and don't adapt well to another body.

Social Networks - the problem for business

The first difficulty for business is that whilst it may wish to take advantage of these sites and interact with customers, the business cannot either create or control these social sites. The attraction of certain sites (rather than others) to the individual is difficult to determine but it is in part a rather transient peer pressure - everyone must be on Facebook because all their friends are. Tomorrow, the users may migrate *en masse* to another site for no easily discernible reason. The presence of a business may be accepted or ignored depending upon its ability to participate within the rules of the site and its relationship with the site users. But, were a company to try to build its own image of these sites, it would be bound to fail.

The second requires a major change to the business security process - whether users are collaborating with others across an internal network in the creation of a report, or interacting more widely on the internet, these web-based programs require person to person interaction outside of the traditional corporate security model.

Security and privacy issues

The social software which makes the web increasingly useful also permits criminal or malicious activity in unexpected ways. For example:

- (a) Mobile phone technology provides easy and instant digital camera and video facilities, and this can be used maliciously. The filming of an assault and then posting the video on social networking sites is considered to enhance the image of the attacker (at least amongst their peers);
- (b) There have been cases of cyber bullying, misuse and corruption of personal information, the posting of material about an individual by third parties, often of a malicious nature, and publishing of material involving others, without their consent, which can be embarrassing or worse. Photographs of teachers in the classroom may be placed on these sites with uncomplimentary comments, as can photos of girls in

- revealing poses, indiscreet pictures at parties etc, and these expose the victim to ridicule;
- (c) Identity theft becomes easier if social networking sites can be mined to provide in-depth information on an individual. Search engines are emerging, which specifically focus on collating personal information from social networking sites. (www.pipl.com for example);
 - (d) Within virtual reality sites, various further issues arise. In part these are to do with the psychology of the sites themselves. People will have a strong bond with their avatar, whether it is the child whose penguin has the bright red scarf or the adult whose alter ego is everything he is not. Even if logically this is a game, events which happen to your avatar may affect you emotionally and this introduces issues such as emotional 'bullying' through social network sites. There are also opportunities to apply behaviour analysis to the avatar of an individual, and this may be quite revealing;
 - (e) Another major issue is the extent to which virtual reality sites allow an individual to screen their real identity. Whilst it allows you to hide behind a virtual identity, it also allows others to do the same, and this may be exploited. You can no longer believe what you see. People are usually trusting in their personal relationships, and may therefore place too much trust in virtual friendships. This may particularly apply to children, as their 'new' friend may or may not be the pre-teen boy or girl she appears to be. A child may be persuaded to divulge information, or to behave inappropriately, by an online 'friend' in a seemingly friendly social environment, and the friend may be a mid-aged paedophile playing a role. Confidence tricksters and other criminal individuals also prey on trusting adults.
 - (f) Real-life crime will inevitably intrude into virtual reality sites if they can. Second Life, for example, allows cash transactions using virtual Linden Dollars, which are negotiable currency and can be bought and sold in real life. Virtual goods can be bought and sold, and therefore theft, fraud, money-laundering etc. become possible. In virtual worlds people can meet and talk, and virtual meetings may be a way of keeping together groups of friends or business colleagues. This is also useful to international terrorist or criminal cells;
 - (g) There are real legal issues in virtual reality sites, which are yet to be resolved. All crime in the real world is reflected in virtual reality worlds too, but there is no legal protection for the virtual citizen against, for example, a theft of money or goods on Second Life. If you are a victim of a crime in a virtual reality site, which jurisdiction will take your theft or fraud seriously?

Social networking sites do carry a great deal of personal information, and the unwary or uninformed user may easily give away a great deal more information than they had intended. From one perspective, you may think that this gives rise to few if any security concerns, as there should be no information on the sites which was not supplied in the first instance by the participants themselves.

However, several issues are emerging, and no doubt there will be others in the future, as people learn to exploit these sites more ruthlessly. The basis of these risks is a failure to recognise the need to modify the rules to deal with the emerging technology. This falls into 2 main areas: personal information and intellectual property.

Personal information which people legitimately place on the web may have been uploaded to be shared amongst friends, but may be exploited by others in various ways.

- (a) Employers are beginning to look at social networking site entries to check on staff behaviour, or as part of a vetting process for employment. Suddenly these cool pictures of you drunk and semi-naked in a bar in Malaga are seen in a different light.
- (b) From a corporate and business perspective, employees of the company may give away information including 'soft' intelligence, such as identities of employees, location of premises, etc., which would assist social engineering attacks against the company.
- (c) Companies concerned with their image may be concerned by adverse publicity for the organisation through the exposure of inappropriate behaviour of company staff, perhaps in working time or perhaps socially outside the working environment.
- (d) As more people use and rely on social networking sites they may become a business conduit, but there is a danger that the company may be accused of inappropriate business practice if business is transacted or agreements made through contacts on social networking sites.

Intellectual property rights are not well defined in this new environment. Material placed on the web will have (in most countries) an assumed copyright of some description, but the definition of this varies from country to country and the ability of the individual to enforce this in an international world is problematic. Personal photographs and other items collected from the web have been used without the owners consent, and the owner may have very little redress. In one case, a holiday photograph was taken from a site and included in a brochure advertising a holiday resort. The media in particular will see this as a legitimate source of background material, and recently in Wales there was concern when the press printed family photographs taken from the Facebook sites of several teenagers who had committed suicide.

What can be done?

The more complex social networking sites (such as Second Life) may need to be looked at from a law enforcement perspective. Some questions should be addressed including:

- Can a crime be committed in a virtual world?
- Under whose jurisdiction might this fall?
- Can evidence of a crime be gathered in a virtual world?
- What will be regarded as legally admissible evidence?
- Is a discussion between avatars in a virtual world legally recognisable, either as a basis of a business deal or as a meeting of terrorist/criminal individuals?

From a corporate perspective, a revised security model which takes into account the sharing of information across social networks is necessary. There are risks in the use of and social networking software, though these are often not well recognised. In particular, the extent to which information passing between individuals using the sites as a conduit, and the extent to which these sites intrude into the corporate network model.

For the individual, the most effective solution remains education of the user to keep him/her alert to what may happen and the precautions which can be taken. We need to make people aware that the Internet is not, in reality, a private place. European-level guidance is needed to inform the citizen of the advantages and of the risks of social networking sites, and to provide an overall awareness, particularly to the young and vulnerable, of the need to be cautious in what they do online.

A strengthening of legislation designed to protect personal information is necessary, and also work to define and then to protect data ownership rights in a web-based environment.

Social networking sites are not going to go away - we are at the beginning of a major change in the way the Internet is used in daily life - and social networking will evolve and become more powerful as a social force in society. CEPIS can encourage Member Societies to take this issue forward within their own communities, and to build upon any EU initiatives and guidance in this area.



Annex I: Virtual Worlds Listed by category

So many worlds, so little time. Not sure where to start? Here are a few recommendations:

Best for Kids

[Disney's Toontown](#)
[Mokitown](#)
[Virtual Magic](#)
[Kingdom](#)
[Whyville](#)

Best for Teens

[Coke Studios](#)
[Dubit](#)
[Habbo Hotel](#)
[The Manor](#)
[The Palace](#)
[Playdo](#)
[Second Life for](#)
[Teens](#)
[The Sims Online](#)
[Sora City](#)
[There](#)
[TowerChat](#)
[whyrobbierocks.com](#)
[Yohoho! Puzzle](#)
[Pirates](#)

Best for 20s - 30s

[Active Worlds](#)
[Cybertown](#)
[Dreamville](#)
[The Manor](#)
[Moove](#)
[Muse](#)
[The Palace](#)
[Second Life](#)
[The Sims Online](#)
[Sora City](#)
[TowerChat](#)
[There](#)
[Virtual Ibiza](#)

Best for Techies

[Active Worlds](#)
[Cybertown](#)
[Muse](#)
[Second Life](#)

Best for Newbies

[Coke Studios](#)
[Dubit](#)
[Habbo Hotel](#)
[Playdo](#)
[The Sims Online](#)
[There](#)
[TowerChat](#)
[Virtual Magic](#)
[Kingdom](#)
[VP Chat](#)
[VZones](#)
[whyrobbierocks.com](#)
[Whyville](#)
[Yohoho! Puzzle](#)
[Pirates](#)

Best for Artists

[Active Worlds](#)
[Cybertown](#)
[Muse](#)
[Second Life](#)
[There](#)
[Worlds.com](#)

Best for Dial-Up

[Coke Studios](#)
[Dubit](#)
[Habbo Hotel](#)
[The Manor](#)

Free Access!

[Active Worlds](#)
[Coke Studios](#)
[Dreamville](#)
[Dubit](#)
[Habbo Hotel](#)
[Mokitown](#)
[Moove](#)
[Muse](#)
[The Palace](#)
[Playdo](#)
[Second Life](#)
[Sora City](#)
[There](#)
[TowerCha](#)
[Traveler](#)
[Virtual Ibiza](#)
[Virtual Magic](#)
[Kingdom](#)
[Voodoo Chat](#)
[whyrobbierocks.com](#)
[Whyville](#)
[Worlds.com](#)
[Yohoho! Puzzle](#)
[Pirates](#)

Mac Access

[Coke Studios](#)
[Dubit](#)
[Habbo Hotel](#)
[The Manor](#)
[Mokitown](#)
[The Palace](#)
[Playdo](#)
[Second Life](#)
[TowerChat](#)
[Virtual Ibiza](#)
[VZones](#)
[whyrobbierocks.com](#)
[Whyville](#)

[Voodoo Chat](#)
[VP Chat](#)
[VZones](#)
[Worlds.com](#)
[Yohoho! Puzzle](#)
[Pirates](#)

Best for Ages 40+

[The Manor](#)
[Moove](#)
[The Palace](#)
[There](#)
[Traveler](#)
[VP Chat](#)
[Voodoo Chat](#)
[Worlds.com](#)
[Yohoho! Puzzle](#)
[Pirates](#)

[Mokitown](#)
[The Palace](#)
[Playdo](#)
[TowerChat](#)
[Traveler](#)
[Virtual Ibiza](#)
[Voodoo Chat](#)
[VP Chat](#)
[VZones](#)
[Whyville](#)
[Worlds.com](#)

[Yohoho! Puzzle](#)
[Pirates](#)

Best for Broadband

[Active Worlds](#)
[Cybertown](#)
[Disney's Toontown](#)
[Dreamville](#)
[Moove](#)
[Muse](#)
[Second Life](#)
[The Sims Online](#)
[There](#)
[Yohoho! Puzzle](#)
[Pirates](#)