View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Strathclyde Institutional Repository

University of Strathclyde Glasgow

Strathprints Institutional Repository

Poulter, Alan and Ferguson, Ian and Mcmenemy, David and Glassey, Richard James (2009) *Question: where would you go to escape detection if you wanted to do something illegal on the Internet? Hint: shush!* [Proceedings Paper]

Strathprints is designed to allow users to access the research output of the University of Strathclyde. Copyright © and Moral Rights for the papers on this site are retained by the individual authors and/or other copyright owners. You may not engage in further distribution of the material for any profitmaking activities or any commercial gain. You may freely distribute both the url (http://strathprints.strath.ac.uk/) and the content of this paper for research or study, educational, or not-for-profit purposes without prior permission or charge.

Any correspondence concerning this service should be sent to Strathprints administrator: mailto:strathprints@strath.ac.uk

http://strathprints.strath.ac.uk/

Question: Where would you go to escape detection if you wanted to do something illegal on the Internet? Hint: Shush!

Alan Poulter, Ian Ferguson, David McMenemy and Richard Glassey

SAFE Group, Department of Computer and Information Sciences

University of Strathclyde, Glasgow

Abstract

The background to this paper is the introduction of public access IT facilities in public libraries. These facilities have seen recorded instances of misuse alongside weaknesses in checking identities of users and in explaining Acceptable Use Policies (AUPs) to users. The FRILLS (Forensic Readiness of Local Libraries in Scotland) project, funded by the Scottish Library and Information Council, attempted to survey the situation in Scottish public libraries and develop a forensic readiness logging regime for use in them. There is in depth discussion of the use of logging in public library computer facilities.

Keywords: Public libraries, Public access IT facilities, computer misuse, forensic readiness, logging

1. Introduction

The answer to the question posed by this paper is: your local public library - hence the ‘Shush’ clue, which is the stereotypical warning most often issued against bad behaviour in a library. Public libraries are usually seen as oases of peace and quiet, where one reads the local newspaper, scours the returned books trolley for popular local reads, and researches family history or an assignment for school or college. They have not been seen as providing a channel for bad behaviour on the Internet.

The services public libraries offer have been updated in line with the growth of the Internet. Back in the 19th century, when public libraries began, they were seen as ‘street corner universities’, providing access for all to a wide range of published content. In the late 1990s, because of the rise of the Internet, public libraries were given public access computers, which could be used for tasks like word processing, but were increasingly used for Internet access. In the UK free public access to IT facilities was enshrined in the development of the ‘Peoples Network’, the brand name chosen for the startup round of funding. The ‘Peoples Network’ project has been evaluated and was found to have been a vital element in addressing the ‘digital divide’ in society by offering IT facilities to those that did not have them at home. In all developed countries, a significant part of the population (around 25%) has no computer/Internet access at home or work. This figure does not seem to be decreasing.(1,2*)*

Access to a computer in a public library is usually free, although demand may require advance booking. One normally needs to be a member of the public library, that is possess a library card. When signing on, one is asked to read an acceptable use policy (AUP), normally couched in the form of a contract, and one must accept that AUP, by clicking a button, to use any public library computer. The AUP is presented to a user each time they logon. A standard AUP will set out legal requirements for proper computer use and also possibly local requirements: for example chat sites might be ruled out as their use is seen as a waste of a limited public resource. AUPs are normally enforced by observation of user activities by library staff, either by shoulder surfing or screen shadowing using packages like NetLoan. Public libraries are ultimately controlled by local Councils, so their computer facilities are normally run by Council IT departments. These departments normally impose a level of filtering, blocking certain sites from Council employees and, by extension, members of the public using computers in public libraries. Finally, computers in libraries are normally set up to erase or hide each user's activities from other users. Librarians, following on from the tradition of offering user privacy by not making available book loan records, do not make available any logs of user sessions on their public access computers either. This is seen as an ethical imperative and part of professional practice.

However, it might be assumed that there is consistency in IT access procedures in public libraries across the UK, as well as consistent application of AUPs and consistent and visible policies about Internet filtering. These assumptions were investigated by a small research project, 'Open Gateway or Guarded Fortress', which was the recipient of the 2006 Elsevier/Library and Information Research Group Award (3). This project utilised 'mystery shopping' testing and visited 14 different UK library authorities (eight English; four Scottish; two Welsh). Where possible neighbouring libraries were visited; the hypothesis being that two libraries that were close but under a different local authority control could conceivably be visited by the same people and thus any differences in service would be noticeable to the users. The same researcher visited all 14 libraries, and the scenario given was that he was not a library member but wished to access his email using the library computers. The researcher had no means of proving his address or identity, carrying only credit and charge cards, as would most people.

While all libraries visited found staff to be extremely helpful, even when access to the Internet was denied, there were occasions when the desire to be helpful was potentially allowing anonymous Internet use. Only two of the 14 libraries visited refused access. However one of these libraries would have happily accepted a bill or official letter as evidence of address, so successful 'dumpster diving' could have resulted in access. Only one pair of libraries offered exactly the same access provisions/AUPs. In only one of the 12 libraries where access was granted did the staff make any attempt to explain their AUP. Indeed, in two of the 12 libraries staff helpfully logged the researcher on to a computer, thus bypassing the AUP!

While this survey revealed that access control was weak, it did not investigate its potential consequences nor possible solutions. Some consequences were known from local experience. For example, apparently searching in Polish would get around filters obscene blocking sites in public libraries in Glasgow, while public library computers in West Lothian were used in a fraudulent online purchase of goods discovered during a police investigation. There are docmented instances of serious misuse. For example, in August 2005, Richard Wartnaby was convicted for downloading nearly 1000 indecent photographs of children in Earlston public library.(4)

Whilst this instance was discovered, many other types of misuse of library IT facilities for hi-tech crime - hacking, identify theft, phishing scams, etc. – may not be. This problem led to the FRILLS project (Forensic Readiness for Local Libraries in Scotland) which was funded by the Scottish Library and Information Council (SLIC) as a part of its 2007 Innovation and Development Fund round of funded projects. The project recognised that whilst library IT facilities are protected and configured with content filters they are not able to record crime. The term ‘forensic readiness’ (FR) describes the technical preparedness for computer investigation in anticipation of a crime. Successful FR would also need suitable staff training and management procedures for routine examination, incident reporting and elevation to enable the proactive seeking out of misuse. Thus FRILLS was to investigate FR for public libraries.

The aims of the FRILLS Project (http://frills.cis.strath.ac.uk) were:

- To create a typology of computer crimes committed on public access computer facilities in general and public library based facilities in Scotland in particular.
- To specify a flexible FR regime which fits the needs and constraints imposed by a variety of library ICT facilities
- To develop management procedures and staff guidelines which will activate/review/terminate FR activity in response to incidents/random checks/regular audits, satisfying privacy legislation and reporting findings to the appropriate external authorities
- To produce a training pack with materials for implementing FR regimes and requisite management policies and guidelines for their use

The remainder of this paper will explore the methodologies used to achieve these aims and the products and outcomes of the FRILLS Project.

2. Computer crime in Scottish public libraries

A detailed, focussed review of the literature on computer crime conducted through public access machines was carried out. Not just academic journals were searched but also publications of the various professional library associations (e.g. CILIP, the Chartered Institute of Library and Information Professionals in the UK, ALA, the American Library Association) and general newspapers (e.g. The Times, The Guardian etc). The intention behind widening the search was to pick up as many examples as possible. There seemed no rationale to restrict the search just to Scottish examples, as location has no effect on computer crime, although Scottish examples were actively sought. Finally, cybercafés were also seen as a potential route for misuse that could be echoed in public libraries and these were included in the literature search.

To supplement the literature review, two online surveys were carried out of Heads of Library Service and of library staff in Scottish public libraries. Both surveys contained similar questions, looking at the effectiveness of AUPs, experience of misuse, how it had been dealt with, and whether training in detection and misuse reporting had been given. Opinions on the FRILLS Project were also sought. As well as these surveys, four Library authorities (Falkirk, Fife. Perth, Renfrewshire) volunteered to participate as potential trial sites, and a selection of library staff at these sites were interviewed, using questions derived from the online questionnaires.

The literature review found substantial evidence of misuse of public library computer facilities, typically involving pornography or child pornography. Misuse in cybercafés exhibited a very similar profile to that of misuse in public libraries. For example, the EasyInternet cyber café in the centre of Glasgow had been used by a customer to distribute child pornography [ref5]. There were other forms of misuse. For example, EasyInternet cyber cafés had also been sued for £210,000 for allowing customers to download music illegally [ref6].

The detection and resolution of misuse had caused instances of severe stress for library staff involved. For example, in a Welsh library a staff member had been sacked for refusing to serve a user who had served a ban for viewing pornography [ref7]. An ongoing case in the United States involves a probationary staff member being sacked for giving police the name of a user allegedly viewing pornography, after being told to follow library procedures first. The user was a person with a very low educational level who may not have been aware of the nature of his actions [ref8].

The surveys/interviews carried out in Scotland echoed the literature. While serious incidents were very rare, there were reported instances of misuse, for example unsavoury use of chat/Bebo, letterhead forgery and a minor using a purloined adult library card to access unsuitable material, among others. Library staff found checking for misuse, and dealing with it, extremely unpleasant. All used methods to lock down machines and many had means of remote viewing of user screens. While procedures were in place, some staff perceived differences in their application between different libraries (e.g. in obtaining witness statements) and many wanted more training in this area. There seemed to be no central monitoring of abuse: thus someone banned in one area could potentially shift activity to another**.**

All libraries surveyed used an acceptable use policy. However these had diverged over time from a core model provided when the People's Network was rolled out. Effort therefore had to be expended in duplicating similar updating efforts in other authorities. A minority of responders said that users got no explanation of the AUP. This would be a breach of proper protocol. Others responded that the legalese used in AUPs was impenetrable, especially to users for whom English was not their first language. Many responders thought that AUPs were too easily ignored. In general, surveyed library staff, though wary of misuse and supportive of a logging system which would make monitoring more effective and easier, were extremely concerned that users not be put off by any use of logging software. Privacy of library users was held to be paramount.

3. A flexible forensic readiness tool for public libraries

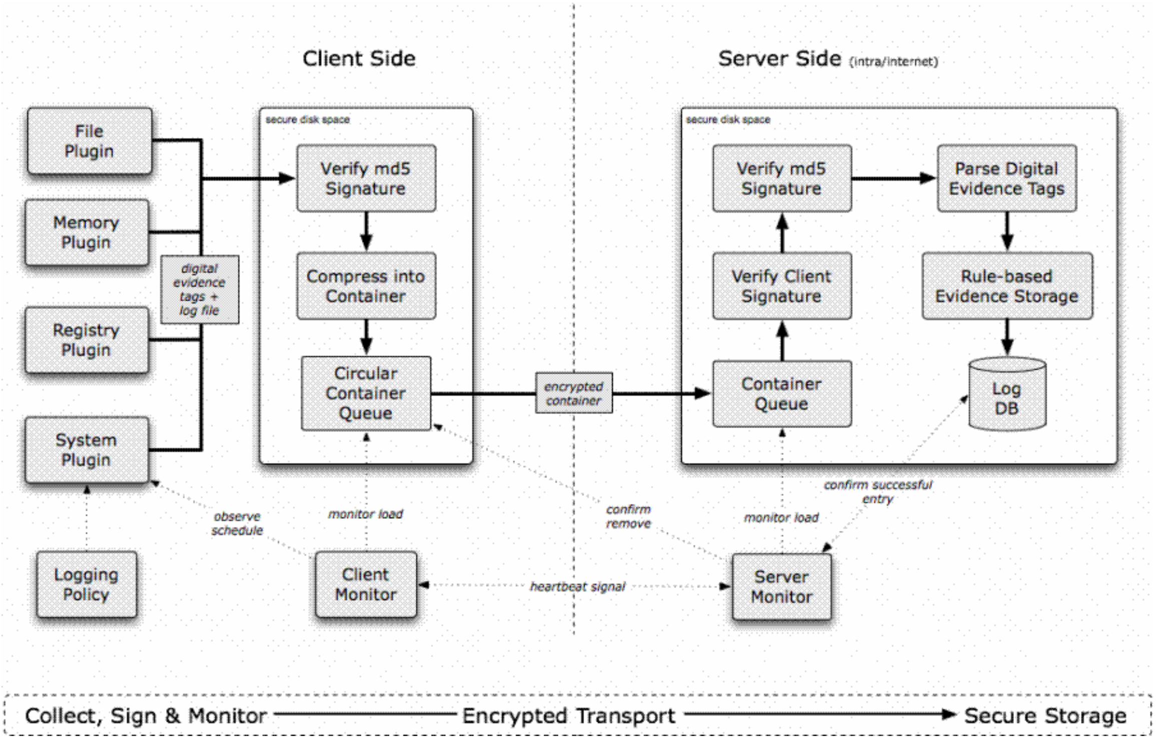
A survey of public library IT managers was attempted but got one response! The survey was lengthy as the intention was to gauge the range of deployment environments and the most commonly-used applications, so it might have put off would-be responders. Some Council IT operations were either outsourced, or in the process of being outsourced, which also did not help. There was no publicly-available overview of Council IT infrastructures.

Since all the volunteer trial sites used Windows XP, Explorer and Office, this was chosen as the target environment for the FR tool. As far as possible, programming was eschewed and re-use of existing facilities/software that recorded and analysed system activity, preferably free and open source (e.g. procmon for XP), was prioritised. Subsidiary objectives for the logging system were:

1) To never record or log user passwords on any system/service
2) To focus on browser logging but also cover chat
3) To store logs in hashed, encrypted form
4) To be able to defend logging activities against those with the expertise to subvert them
5) To accommodate wifi, since libraries were thinking of offering wifi access

6) To be usable 'in reverse' i.e. by those who wanted to ensure maximum user privacy by turning off any and all logging.

XML was used to develop a structure for log files detailed enough for forensic records. Off the shelf packages and some written code were used to build a logging application called the Autonomous Logging Framework (ALF), shown in the diagram below. It creates an encrypted, authenticated XML record of a user session. There are implications for network traffic and long-term storage of these log records.



From interviews with library staff it become clear that IT Services provide the machines and networking for their public access IT, but provide it on their own terms. IT Services exist primarily to provide core systems support, and local IT resources, for Council functions and Council staff. Public access IT is very much a service 'add-on' and not a core offering.

It proved possible to interview one group of Council IT staff. They appeared to be doing some logging of access for misuse checking themselves. However they were not willing to allow non-commercial software to be used on their networks. This refusal to allow use of non-standard software was also met at the other three sites. While this made project goals of deploying, testing and preparing training for logging software impossible, it perhaps reflected their caution about maintaining their service levels. It also proved impossible to set up a mock public library IT facility in our laboratory at the University.

4. Discussion

Although the logging software and architecture embodied in one potential output of FRILLS was not field tested as envisaged, the project itself discovered many flaws in the current system of provision of public access IT facilities in public libraries in Scotland, and, by extension, public libraries elsewhere in the UK and overseas.

A standard procedure for dealing with misuse should be in place and supported by a set of training materials for public library staff. A listing of types and incidents of abuse should be maintained and updated, to spread awareness of new problems. A central listing of currently banned users should be maintained. Without this centralised system, the checking and reporting and punishment for computer misuse, will lack effectiveness. Even if ALF had been deployed throughout public libraries in Scotland, the lack of a centralised reporting and management structure would have severely undercut its effectiveness.

The lack of one canonical AUP for all Scottish public libraries is also telling. One centrally-maintained AUP could be more easily updated over time as new problems or issues are discovered. The centralised incident list (proposed above) would help drive AUP content updating. Centralised) AUP provision would also enable the provision of the AUP in a variety of languages. Attention could also be directed at replacing the 'legalese' currently used with much more plain language. Accessibility issues with a text-only AUP could also be tackled by providing it in other media (e.g. as an MP3 file of spoken text). Finally, the need for user understanding of AUPs could be reinforced in staff training and also perhaps by extra software which would 'pop up' AUP-related questions during a user's session to bring its restrictions to their attention. This software might upset library users intent on completing a task though, so should be used sparingly.

Somewhat ironically, there was a general concern, noted above, that library users had a right to privacy when using the Internet. There are instances of papers in library-related journals, which give advice to librarians on how to remove typical records of activity, like URLs in a browser cache (refs 9, 10). However this advice does not go far enough. It fails to encompass the possibility of Internet activities being recorded outside of the immediate library environment, as user traffic in IP packets traverses the Internet. There ought to be advice available for library users on how to obtain private Internet access via anonymous proxies if they really want browsing to be hidden. There was no sign of encryption packages being offered to library computer users even though they were processing potentially personal data on a public machine in a public location. Generally there seems to be a lack of awareness of security issues amongst both library users and librarians: one interviewee related that a library user had been asking other people for help using a credit card with online shopping! Public libraries would be an ideal venue for imparting information about Internet security, which would tie in well with the 'digital divide' mission which originally inspired the introduction of public access computers in public libraries.

If logging as performed by ALF was permitted in public libraries, it would add to the value of the public access IT facilities. The 'Open Gateway or Guarded Fortress' research report, covered above, revealed the need for, and tacit acceptance of, drop-in user access, whereby anybody, not just registered users of a particular library, could use its computer facilities. If all drop-in usage was logged, by ALF or an equivalent, then this would go a long way towards allowing secure, drop-in access. People really just wanting to check their email when away from home surely would not object to logging.

There are other potential 'positive' applications of logging, where it allows extra facilities, rather than just being seen as a form of control. An example, mentioned above, is when a public library introduced wi-fi. Since this could be used outside of normal working hours and/or by library users who are not physically present and observable in a public library, then logging activity on these connections might be a sensible precaution. Some users may want a 'logged' option, a record of their activity, as it would prove what they did/did not do in a particular session. The functional diagram of ALF above, would need to be amended to allow for delivery of a log file to a user, as well as to the repository. Some form of external verification tool would also be needed. Finally, filtering (blocking) of certain Internet sites was also raised as a potential problem by the Open Gateway or Guarded Fortress' research. If a connection was logged, then surely filtering could be turned off as there would be a record of sites the library user had looked it, meaning that any illegal sites the library user accessed, as opposed to those considered unacceptable, could be monitored.

Finally, an issue that was raised in interviews with library staff was the unpleasantness, and personal risk involved, in confronting a library user suspected of misuse. Since many library staff are female and many library mis-users are male, such a confrontation becomes physically dangerous. Some female librarians may work shifts alone in a small public library, which only heightens the risks to them of confrontations over suspected misuse. Thus a logging tool could be used to avoid any confrontations by record suspicious use and then being used later in a more controlled environment to confront a user suspected of computer misuse.

5. Conclusions

We feel that we have opened up a potentially rich seam for research into computer misuse, of various types and severity, in public libraries. We suspect, but have not had the opportunity to prove, that hacking is going on. If technically-naïve users are trying to misuse library computers, trying to bypass filters, to download porn or MP3s, to borrow (or steal) a library card for a false identity, then surely professional hackers have cottoned on to the vulnerabilities in terms of identification and usage tracking that exist in public libraries. A related institution, cybercafés, offer very similar facilities to those in public libraries and we have already raised above serious incidents of misuse in cybercafés. In parts of the world not developed enough to have universal public library access, cybercafés fulfil a very important role in people's lives, as many cybercafé users cannot afford any other form of Internet access. Future studies perhaps should tackle these different institutions together.

Two related areas of research are the automatic analysis of logs and the effectiveness of any form of logging against an expert user. The first topic would be invaluable should logging get taken up generally in public libraries and/cybercafés. Even if logging is only used sparingly then automatic log analysis can remove (or reduce) the time consuming and unpleasant task of log analysis by a human. One feels that any deployment of logging in public computer facilities would be a target for certain elements. How well it would serve to dissuade or block those elements is unknown.

We began this paper with a jocular reference to the image of the librarian. We now feel that the librarian image should change sharply, to accommodate new duties arising from the new computer facilities in libraries and the potential issues arising from their misuse.

We would like to thank the Scottish Library and Information Council for their support of this research.

References

1. Brophy, P. The People's Network: A turning point for public libraries: first findings. London: Resource, The Council for Museums, Archives and Libraries, 2002. 23p

2. Brophy, P. The People's Network: moving forward. London: Museums, Libraries and Archives. 2004. 27p.

3. McMenemy, D. Internet access in UK Public Libraries: notes and queries from a small scale study**.** *Library Review*. 57 (7). 2008. XXpp.

4. Edinburgh Evening News. Jail for father who looked at child porn on school PC. August 10, 2005.

http://edinburghnews.scotsman.com/scotland.cfm?id=1757852005

5. Riley, W. Student Ran Kiddie Porn Ring At Café. The Express (Scottish Edition). October 15. 2005. Pg. 38

6. Cullen, D. EasyInternet abandons CD burning court appeal: pays damages, costs to BPI. The Register. 2003.

http://www.theregister.co.uk/2003/04/09/easyinternet_abandons_cd_burning_court/

7. BBC Library sex surfer gets apology. October 19 2005

http://news.bbc.co.uk/1/hi/wales/south_east/4356316.stm

8. American Library Association Library Worker’s Firing Sparks Firestorm. American Libraries Libraries Direct 4/2/2008. http://www.ala.org/ala/alonline/currentnews/newsarchive/2008/march2008/tularefirestorm.cfm

9. Coombs, Karen Protecting user privacy in the age of digital libraries. Computers in Libraries 25 no6, 200516-20pp

10. Huang, Phil. How You Can Protect Public Access Computers and their Users. 2007 Computers in Libraries 27(5)(May 2007): 16-20.

11. Gitta, S. and Ikoja-Odongo. J.R The impact of cybercafés on information services in Uganda. First Monday. 2003.

http://www.firstmonday.dk/issues/issue8_4/gitta/