Overview

1. Public access IT facilities in public libraries
2. “Open Gateway or Guarded Fortress” project
3. FRILLS project (“Forensic Readiness for Local Libraries in Scotland”)  
4. Conclusions

1.1 Background - public libraries

- The “People’s Network” – government initiative to put in public access machines into all public libraries and offer free access to the Internet
- New direction for public libraries to address the ‘digital divide’ issue:
  - Offer free IT use/Internet access
  - Offer IT training
  - Offer online/CD/DVD courses
- But chiefly used for email/chat, surfing, games etc.
1.2 Public libraries – IT facilities

- Run by local authority IT Departments
- Users required to agree to an Acceptable Use Policy (AUP)
- Monitoring by observation or access management packages (NetLoan), which also erase user sessions
- Use of web filtering
- Professional issues with censorship and monitoring
- Evidence of serious misuse e.g. child porn

2.1 “Open Gateway or Guarded Fortress” project – LIRG Research Prize

Assumptions:
1. Consistency of service access and quality in public libraries across the UK
2. Rigorous and consistent application of AUPs
3. Clear and visible policy about Internet filtering
4. Consistent front-end with:
   - Wide range of information sources (local and Internet)
   - Novice Internet Guide

2.2 ‘Gateway or Fortress’ research methodology

- Unobtrusive testing (mystery shopper) visiting 14 different UK library authorities (8 English; 4 Scottish; 2 Welsh)
- Where possible neighbouring authorities were visited (logic being users may interact with both and expect equality of service provision)
- Same mystery shopper visited all 14 library services. Rubric: “I am not a member of this library, please can I use your computers to check my email.” No ID was shown beyond credit/debit cards
2.3 ‘Gateway or Fortress’ access results

- Only one pair of libraries used same interface, AUP and filter list
- Only two of the 14 libraries refused access because of a lack of acceptable ID (i.e. address)
- In only one library did staff make any attempt to explain the AUP and what the responsibilities of the user were
- In two libraries, staff logged the researcher onto the system themselves, thus bypassing the AUP entirely

2.4 ‘Gateway or Fortress’ service results

- Only one library provided a novice Internet guide
- No consistency in Internet filtering, two libraries blocked nothing on the check list (chat, email, Social networking, sexual health, dating, downloading and gambling) others blocked varying sites – one library used fake 404 errors
- Most commonly blocked were chat sites (50%), an advice site for gay teenagers (33%) and the gambling site (33%)
- No explanation of data/session retention, no security advice

3.1 FRILLS project (“Forensic Readiness for Local Libraries in Scotland”)

- “Aims to develop simple, low-cost techniques to provide a basic forensic readiness (FR) regime for public access ICT facilities, in order to deter misuse of those facilities by better detection of misuse”
- “Successful FR needs suitable staff training and management procedures for routine examination, incident reporting and elevation to enable the proactive seeking out of misuse whilst offering privacy.”
- Funded by the Scottish Library and Information Commission (SLIC), see: http://www.frills.cis.ac.uk
3.2 FRILLS: aims

- create a typology of computer misuse of public access computer facilities
- specify a flexible FR regime which fits the needs and constraints imposed by a variety of library ICT facilities
- develop management procedures to activate/review/terminate FR activity, satisfy privacy/freedom of access and report findings to the appropriate authorities
- produce a training pack with materials for implementing FR regimes and requisite management policies

3.3 FRILLS: methodology

- Literature reviews of computer misuse via public access IT + computer forensics tools
- Online surveys of Heads of Library Service, Library IT Managers, library staff regarding computer misuse
- Interviews with Heads of Library Service, Library IT Managers
- Work with pilot sites to develop FRILLS

3.4 FRILLS: computer misuse

- Two main types:
  - Breaching AUPs e.g. porn, chat, IM, Bebo
  - Breaking the law, e.g. child porn
- AUPs written in English “legalese”, difficult to enforce/explain, not standard, not kept up to date, problem of defining ‘unacceptable content’
- No standard recording of misuse. In principle access should not be monitored/filtered – but many library staff were aware of misuse and in favour of controls
3.5 FRILLS: Specify a flexible FR regime

- Focused on XP + Explorer + Office as core logging targets – problem of variety of other targets
- Logging would not record user passwords on external systems
- Logging would offer levels, from none on up
- Minimise software development by reusing existing freeware tools
- Use XML to develop a structure for log files

3.6 FRILLS: Autonomous Logging Format

4.1 Conclusions: Implementation

- Each implementation would have to be different because of:
  - Technical set up/dealing with local IT provider
  - Local policies with regard to checking, reporting and imposing penalties
- Uses of logging: non-ID access, one-person libraries, out of hours access (wifi), ‘precautionary warnings’ of behaviour near AUP limit
4.2 Conclusions: Issues

- Management:
  - lack of standards for AUPs, for checking, reporting and dealing with misuse

- Technical:
  - Overhead of logging in terms of network traffic – could logs be stored in a remote central repository?
  - How to automate analysis?
  - How robust is the logging against expert interference?

ANY QUESTIONS?