Detecting and deterring public computer misuse: the FRILLS project

•Presentation for the SLIC AGM and IDF showcase, 5/11/8

What is FRILLS?

- FRILLS = Forensic Readiness for Local Libraries in Scotland
- Research Team:
  - Alan Poulter
  - Ian Ferguson
  - Richard Glassey
- http://frills.cis.strath.ac.uk
- Plus a large cast of questionnaire respondees and interviewees – to whom many thanks are due!

Proposal outline

- “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.”

Specific aims

- create a typology of 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

Methodology

- Carry out literature reviews of computer misuse via public access IT (libraries and cybercafes) + computer forensics tools
- Carry out online survey of Heads of Library Service, Library IT Managers, and library staff regarding computer misuse they had experienced
- Interview Heads of Library Service and Library IT Managers at volunteer pilot sites for their perspective/needs/situation
- Develop and test an FR logger with pilot sites

Literature review of computer misuse

- Found evidence of misuse of public access facilities, typically involving pornography or child pornography.
- Misuse in cybercafés exhibited a very similar profile to that of misuse in public libraries:
  - e.g. the main EasyInternet cyber café in Glasgow had been used by a customer to distribute child pornography.
- Other forms of misuse:
  - e.g. EasyInternet cyber cafés had been sued for £210,000 for allowing customers to download music illegally
- The detection and resolution of misuse had caused severe stress for library staff involved:
  - e.g. in a Welsh library a staff member had been sacked for refusing to serve a user who had served a ban for viewing pornography
  - e.g. in the United States a probationary staff member was sacked for giving police the name of a user allegedly viewing pornography, after being told to follow library procedures first.

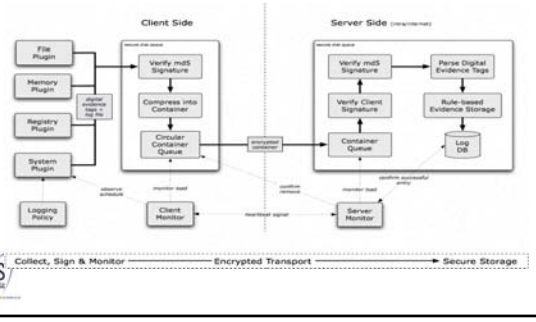
Staff experience of computer misuse

- Broad agreement that Internet access should not be monitored – but many library staff were aware of misuse and in favour of controls
- Checking for misuse e.g. via URL history was extremely unpleasant to do
- The more checking was done, the more misuse was found'
- Acceptable Use Policies (AUPs) breached e.g. porn, chat, IM, Bebo, letterhead forgery and more
- AUPs written in English "legalese", difficult to enforce/explain, not kept up to date, problem of defining 'unacceptable content', not in minority languages
- No standard recording of misuse

Create a flexible FR logging system

- Focused on Windows XP + Explorer + Office as core logging targets – problem of variety of other targets
- Browser/chat logging would get core coverage as main areas of reported abuse
- Logging would not record user passwords on external systems
- Minimise software development by reusing existing freeware tools
- Use XML to develop a structure for log files
- Developed the Autonomous Logging Framework (ALF)
- Implications for network traffic and long-term storage of log records

ALF (Autonomous Logging Framework)



Work with pilot sites to develop FRILLS

- The response from IT Services to the technology survey was extremely poor
  - It was by necessity extremely detailed in its questioning
  - Some Council IT operations were outsourced, which did not help data gathering
- Some Council IT staff were interviewed:
  - to them public access IT in libraries was very much a service 'add-on' and not a core offering
  - they appeared to be doing some logging of access for misuse checking themselves. However they were not willing to allow ALF to be used on their networks.
  - tried to simulate a library IT setup in our Lab but could not afford Deep Freeze license

Outcomes: Service issues

- Need for a standard AUP, centrally updated, available in a large number of languages?
- Need for more checking of user understanding of AUPs? (e.g. online tests)
- Need for a standard procedure and set of penalties for dealing with misuse?
- Need for a central register of misuse cases?
- More advice on Internet privacy and data security could be offered to users?

Outcomes: Logging issues

- Uses:
  - 'non-ID' drop-in access
  - wifi access
  - to avoid confrontations with users in cases of suspected misuse
  - to give users an authenticated record of their session
  - non-filtered access
- Technical:
  - Suspect, but cannot prove, that hacking is going on
  - Implementation needs to be flexible enough to met a wide variety of local use scenarios
  - How might the unpleasant task of checking logs for evidence of misuse be automated?
  - How robust is the logging against expert interference?