SEVILLE JUNE2007 SPAIN
19th Annual FIRST Conference

FIRST 2007

Identity Management Systems: the forensic dimension

Peter Sommer

London School of Economics

LSE

SEVILLE JUNE2007 SPAIN
19th Annual **FIRST** Conference

FIRST 2007

Private Lives and Corporate Risk

this year's theme

Let’s explore a Paradox…

- Identity Management Systems have to be robust enough to have evidential value in legal proceedings
- Identity Management Systems have a close relative – called Surveillance Methodologies
- The everyday activities of Digital Forensics may expose activities – and hence potentially invade privacy – in ways never intended by designers of IMSs and law policy makers

Where we need to get to

- Nature of IMSs
  - ➔ and their weaknesses
- Nature of Digital Forensics
  - ➔ and digital forensics research
- Applicable Law and regulation
- Understanding the Paradox

Identity Management Systems

- Enabling Technology
- Management System
- Framework of Policies, Regulations and Law

Identity Management Systems

Enabling Technology

- Uniquely to identify some-one to whom "privileges" can be granted
  - ➔ Something you know, hold, are, do; location
    - Passwords
    - Tokens, RFID
    - Biometrics
    - Specific terminal
- Means to recognise unique identifier, allocate privileges associated with credentials presented
  - ➔ Operating System + Database + Applications

Identity Management Systems

Management System

- Access Control List
  - ➔ Authenticate against database
  - ➔ Grant privileges against criteria to provide authorisation
  - ➔ Authoritative Reissue, Aging, Revocation
- Tokens, RFID
  - ➔ Authenticate against database
  - ➔ Grant privileges against criteria to provide authorisation
  - ➔ Authoritative Reissue, Aging, Revocation
- Biometrics
  - ➔ Authenticate against database
  - ➔ Grant privileges against criteria to provide authorisation
- Specific terminal
  - ➔ Usually deployed in combination with one of the above

Identity Management Systems

Framework of Policies, Regulations and Law

- Policies:
  - ➔ what are the overall needs, purposes and requirements of IMS?
  - ➔ what unwanted side-effects need to be avoided?
- Regulations, Law:
  - ➔ eg compliance with Data Protection, Human Rights, Employment, Surveillance, Business Records, laws, audit and desirable standards, compliance

Types and Purposes of IMS

- IMS for account management, implementing authentication, authorisation, and accounting,
- IMS for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour
- IMS for user-controlled context-dependent role and pseudonym management.

Types and Purposes of IMS

IMS for account management, implementing authentication, authorisation, and accounting

- Used by large organisations for access control to computer systems and networks, etc
  - Inter-company, purchasing systems, ISPs, banks
- eg conventional user-name/password access-control systems, single-sign-on systems, some forms of public key infrastructures

Types and Purposes of IMS

IMS for profiling of user data by an organisation, e.g. detailed log files or data warehouses which support e.g., personalised services or the analysis of customer behaviour

- eg, activity tracking, use of cookies, facilities, "market info/CRM" systems – Amazon, many online retailers, Google, Ebay, cookie deployers – adriver, adclick, hitslink, webstats, doubleclick

Types and Purposes of IMS

IMS for user-controlled context-dependent role and pseudonym management.

- Not many practical examples – but where user presents an “identity” limited to the immediate needs of the transaction

Types and Purposes of IMS

The pro-privacy advocates prefer IMSs that are:

- Limited to the immediate needs of the specific transaction in hand – “credential not identity”
- Do not give more information than is needed
- Give the user control over each transaction
- Use a federated strategy – interoperability or linkage of different IMSs, where needed and where agreed

IMSs: points of vulnerability

Enabling Technology

- Something you know, hold, are, do; location
    - Passwords, Tokens, Biometrics
- Passwords
    - → Overlooked, stolen, password files cracked
- Tokens
    - → Stolen, copied/compromised,
- Biometrics
    - → Biometric reader weakened, compromised,
- Specific Terminal
    - → Terminal hardware identity compromised

In general: eavesdropping on communications links, man-in-the-middle attacks

IMSs: points of vulnerability

Enabling Technology

- Means to recognise unique identifier, allocate privileges associated with credentials presented
- Failure at point of issue: incorrect credentials accepted when password/token issued, biometric linked to individual identity
- Failure / compromise of database of validating data against presentation of credentials
- Failure of database/other technology in granting privileges against credentials
- Failure properly to handle re-issue of lost credentials, age and re-issue passwords/tokens, fully to revoke obsolete credentials

IMSs: points of vulnerability

Management System

- System fails to perform as specified; emergency measures lack adequate security
- Access Control List / Validation database, compromised
- Data accessed – unauthorised or *ultra vires*
- Data released *ultra vires*
- System poorly protected and breached from outside
  - Logically / Physically
- Corruption within management personnel

- ***Data aggregated with other sources ….***

IMSs: points of vulnerability

In general: anything based on ICT will be subject over time to *erosion*

- What once worked well becomes weakened by:
  - ➔ Prolonged Technical Examination
  - ➔ Spread of information about vulnerabilities fast and easy over the Internet
  - ➔ Increasing computer power makes brute force attack more feasible – Moore’s Law variant
  - ➔ Falling computer costs makes brute force attack more feasible
  - ➔ “Esoteric” hardware/software/technology becomes widely available

Forensic Computing

Most presentations are along the lines of:

- What computer forensics can deliver
  - ➔ Hard disk analysis
  - ➔ Network data capture and analysis
- How to do computer forensics
- Protocols and Procedures

For our purpose I want to look at the nature of Research in Forensic Computing

Aims of Digital Forensics

- To identify sources of evidence
- To acquire evidence
- To preserve evidence
- To analyse evidence
- To identify non-obvious sources of evidence

How to Acquire Evidence

- By pre-planning – system design
  - Access Control Systems
  - Audit logs
  - Serialing of transactions
  - Authentication of People, Files, Transactions
  - Digital Finger-printing of documents, logs, etc
- Forensic Computing
  - Unintended “digital footprints”
  - Evidence identification
  - Evidence Preservation
  - Evidence Analysis, often based on reverse-engineering of OS, apps, etc

History of Computer Evidence

- 1950s-1980s: print-out as evidence
  - Practicalities of production
  - Admissibility
- 198x >: data recovery on hard-disks
  - Techniques
  - Forensic Reliability
  - Interpretation
- 198x >: network forensics
  - Analysis of Log Files
  - Capture of data in transmission
  - Forensic Reliability
  - Interpretation

History of Computer Evidence

- 199x >: data recovery on hard-disks
  - ➔ Reverse engineering to understand artefacts
  - ➔ Growth of integrated commercial forensic analysis products
- 199x >: telecoms, ISP data
- 199x>: protocols, warrants for seizure of many sorts of digital data
- 200x>: analysis of PDAs, cellphones, cameras, MP3 players, digital cctv

History of Computer Evidence

Post 9/11: LE-friendly surveillance legislation:

- increases range of data that can seized
- increases circumstances in which data can be seized
- data retention regimes

Aims of Digital Forensic Research

- To identify potential sources of digital evidence, chiefly unintended artefacts
  - ➔ Eg configuration, temporary files, date-and-time stamps, deleted but recoverable data
- To examine and analyse them
- To derive, by the use of reverse engineering and testing, rules which describe their behaviour
- To produce convenient tools which enable these findings to be used during investigations

Aims of Digital Forensic Research

Motivations:

- To solve a problem within a particular investigation
- Geek Fun
- To develop a commercial product
- To improve one’s academic standing
- *To give Law Enforcement an advantage?*

Digital Forensic Research

Hard-disk based:

- Recovered Files
  - ➔ Deleted, modified files – goes to intent
- MSOffice “properties” / metadata
  - ➔ May show authorship, revisions
- Internet cache
  - ➔ Shows patterns and history of Internet usage – goes to intent, state of mind
  - ➔ Search engine requests
- OS set-up
  - ➔ Accounts, passwords, may show authorship
- System Registry (Windows)

Digital Forensic Research

- System Restore Points
- P2P software artefacts, database and logging files
- Chat software artefacts, database and logging files
- Exif Data
- LNK files
- Thumbnails – thumbs.db etc
- Email headers
- Desktop indexing artefacts

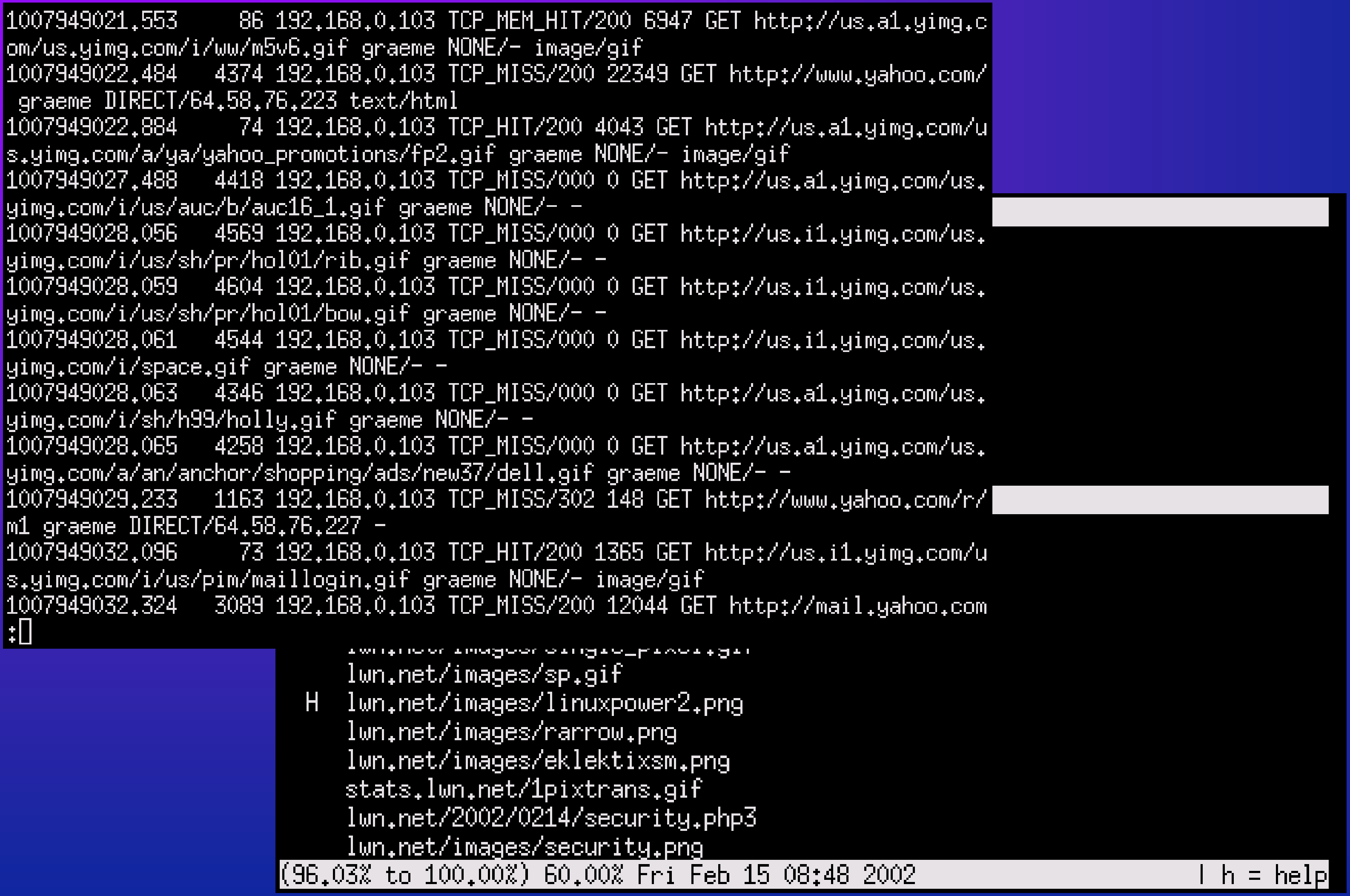
Digital Forensic Research

3rd party logs:

- Web logs
- IDS logs
- Remote service anti-virus logs
- Telco logs, landline, cell, ISP
- ISP RADIUS logs

Aim is to audit activity, seek corroboration and hence identify specific individuals

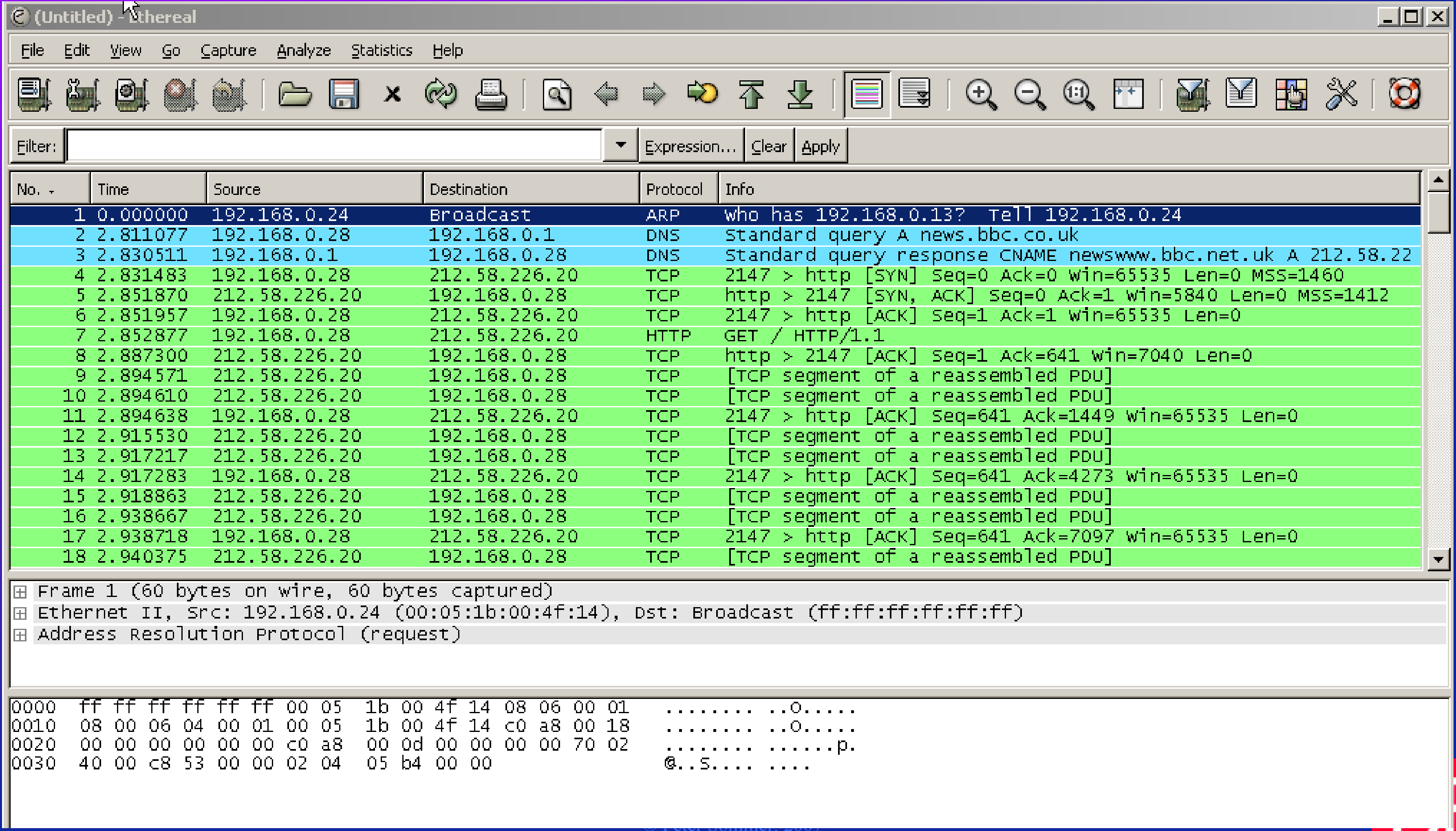
Squid Logs



```
1007949021.553     86 192.168.0.103 TCP_MEM_HIT/200 6947 GET http://us.a1.yimg.c
om/us.yimg.com/i/ww/m5v6.gif graeme NONE/- image/gif
1007949022.484   4374 192.168.0.103 TCP_MISS/200 22349 GET http://www.yahoo.com/
 graeme DIRECT/64.58.76.223 text/html
1007949022.884     74 192.168.0.103 TCP_HIT/200 4043 GET http://us.a1.yimg.com/u
s.yimg.com/a/ya/yahoo_promotions/fp2.gif graeme NONE/- image/gif
1007949027.488   4418 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/us/auc/b/auc16_1.gif graeme NONE/- -
1007949028.056   4569 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/rib.gif graeme NONE/- -
1007949028.059   4604 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/us/sh/pr/hol01/bow.gif graeme NONE/- -
1007949028.061   4544 192.168.0.103 TCP_MISS/000 0 GET http://us.i1.yimg.com/us.
yimg.com/i/space.gif graeme NONE/- -
1007949028.063   4346 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/i/sh/h99/holly.gif graeme NONE/- -
1007949028.065   4258 192.168.0.103 TCP_MISS/000 0 GET http://us.a1.yimg.com/us.
yimg.com/a/an/anchor/shopping/ads/new37/dell.gif graeme NONE/- -
1007949029.233   1163 192.168.0.103 TCP_MISS/302 148 GET http://www.yahoo.com/r/
m1 graeme DIRECT/64.58.76.227 -
1007949032.096     73 192.168.0.103 TCP_HIT/200 1365 GET http://us.i1.yimg.com/u
s.yimg.com/i/us/pim/maillogin.gif graeme NONE/- image/gif
1007949032.324   3089 192.168.0.103 TCP_MISS/200 12044 GET http://mail.yahoo.com
:
```

```
       lwn.net/images/single_pixel.gif
       lwn.net/images/sp.gif
    H  lwn.net/images/linuxpower2.png
       lwn.net/images/rarrow.png
       lwn.net/images/eklektixsm.png
       stats.lwn.net/1pixtrans.gif
       lwn.net/2002/0214/security.php3
       lwn.net/images/security.png
(96.03% to 100.00%) 60.00% Fri Feb 15 08:48 2002                     | h = help
```

Network Logs



```
No. -  Time      Source          Destination     Protocol Info
     1 0.000000  192.168.0.24    Broadcast       ARP      Who has 192.168.0.13?  Tell 192.168.0.24
     2 2.811077  192.168.0.28    192.168.0.1     DNS      Standard query A news.bbc.co.uk
     3 2.830511  192.168.0.1     192.168.0.28    DNS      Standard query response CNAME newswww.bbc.net.uk A 212.58.22
     4 2.831483  192.168.0.28    212.58.226.20   TCP      2147 > http [SYN] Seq=0 Ack=0 Win=65535 Len=0 MSS=1460
     5 2.851870  212.58.226.20   192.168.0.28    TCP      http > 2147 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1412
     6 2.851957  192.168.0.28    212.58.226.20   TCP      2147 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
     7 2.852877  192.168.0.28    212.58.226.20   HTTP     GET / HTTP/1.1
     8 2.887300  212.58.226.20   192.168.0.28    TCP      http > 2147 [ACK] Seq=1 Ack=641 Win=7040 Len=0
     9 2.894571  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    10 2.894610  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    11 2.894638  192.168.0.28    212.58.226.20   TCP      2147 > http [ACK] Seq=641 Ack=1449 Win=65535 Len=0
    12 2.915530  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    13 2.917217  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    14 2.917283  192.168.0.28    212.58.226.20   TCP      2147 > http [ACK] Seq=641 Ack=4273 Win=65535 Len=0
    15 2.918863  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    16 2.938667  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
    17 2.938718  192.168.0.28    212.58.226.20   TCP      2147 > http [ACK] Seq=641 Ack=7097 Win=65535 Len=0
    18 2.940375  212.58.226.20   192.168.0.28    TCP      [TCP segment of a reassembled PDU]
```

```
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: 192.168.0.24 (00:05:1b:00:4f:14), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊞ Address Resolution Protocol (request)
```

```
0000  ff ff ff ff ff ff 00 05  1b 00 4f 14 08 06 00 01   ........ ..O.....
0010  08 00 06 04 00 01 00 05  1b 00 4f 14 c0 a8 00 18   ........ ..O.....
0020  00 00 00 00 00 00 c0 a8  00 0d 00 00 00 00 70 02   ........ ......p.
0030  40 00 c8 53 00 00 02 04  05 b4 00 00               @..S.... ....
```

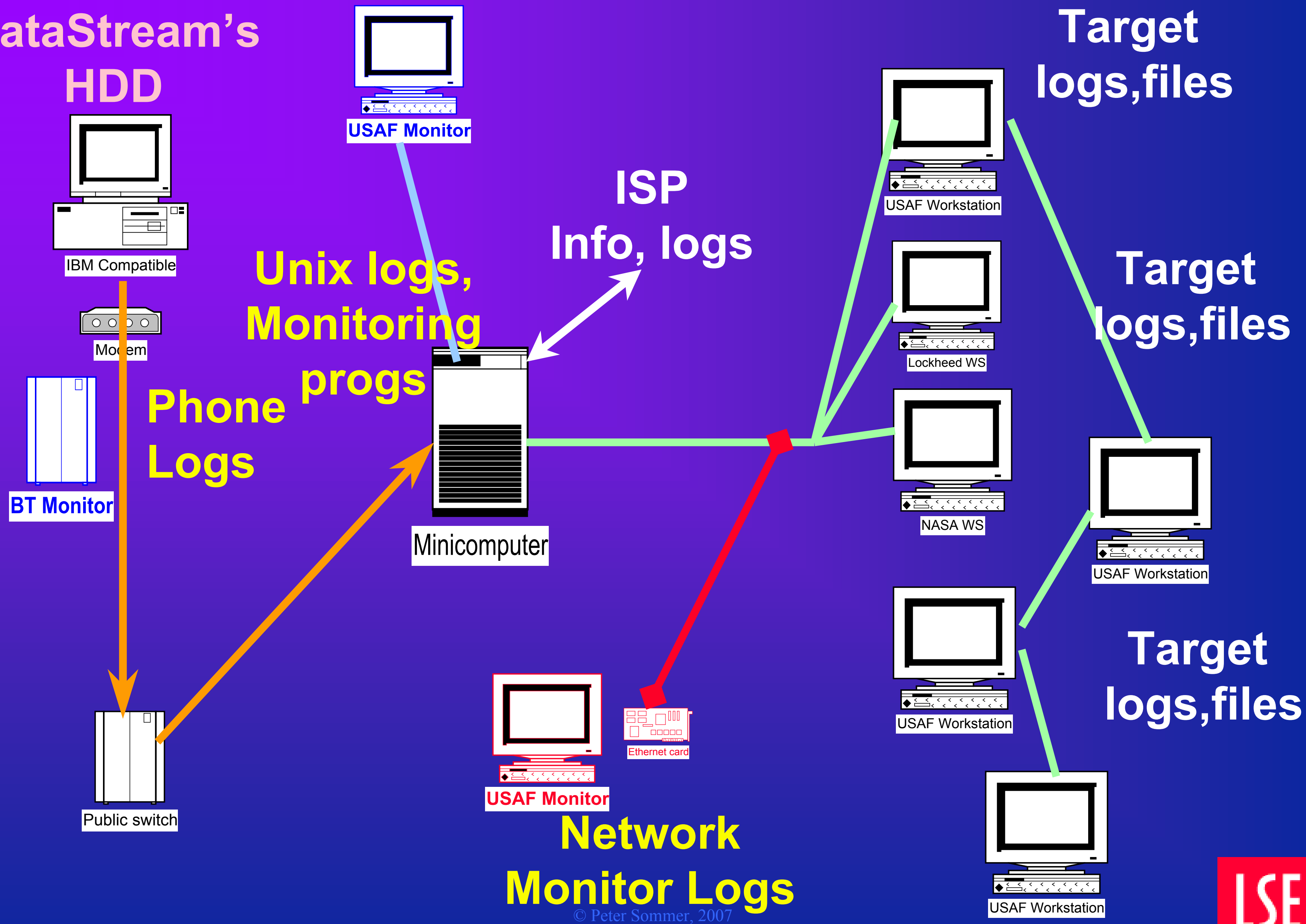
Digital Forensic Research

Interception

- Who contacted whom, when, for how long – and what was said.
- Forensics: how do you do this practically and with integrity-checking?
- Law: how do you do this legally?
  - ➔ Special case of UK – s17 RIPA 2000 restrictions; but you can get similar results via hard-disk examination

Practical Investigations

- Multiple streams of evidence to build a detailed picture
- Corroboration from several weak streams



ataStream's HDD

Unix logs, Monitoring progs

ISP Info, logs

Phone Logs

Target logs,files

Target logs,files

Target logs,files

Network Monitor Logs

Forensic Research and IMSs

- Can we get more than was intended from the enabling technology?
- Can we get more than was intended from the Management System?
- Can we analyse the audit trails in unintended ways?
- Can we do so legally?

Data Protection Principles

Personal Data :

1. processed fairly and lawfully
2. only obtained for one or more specified and lawful purposes
3. adequate, relevant and not excessive
4. accurate and up to date
5. not kept longer than necessary
6. processed in accordance with rights of data subjects

Data Protection Principles

7. Appropriate measures against unauthorised and unlawful use
8. Non-transference outside EU

Exemptions:

National Security, crime, taxation, health, education, social work, regulatory activity, journalism, research, history, statistics, legal proceedings

Human Rights Tests

UDHR 1948

- Art 12: arbitrary interference with privacy
- Art 13: freedom of movement
- Art 8: effective remedies for violation of fundamental rights

Violation Tests

- Necessity
- Proportionality

Forensic Research and IMSs

- Can we get more than was intended from the enabling technology?
  - Reveal identity?
  - Collect identity without obvious trace?
- We can get warrants for one purpose but then use the data for others?

Forensics and Identity Management Systems

Intended and Unintended Checking of Identity

- Intended:
  - ➔ To grant access
  - ➔ To grant a privilege
  - ➔ To make a payment
- Unintended
  - ➔ To place an individual at a particular location at a particular time
  - ➔ To create a log of activities from which behavioural patterns can be derived

Movement Trails

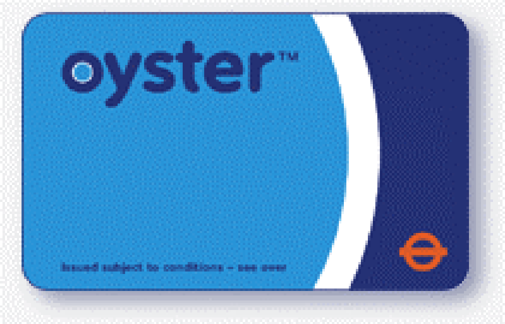
IDENTITY CARD

1. BLUNKETT
2. DAVID
3. 06-06-47 SHEFFIELD
4a. 02-09-03 4b. 01-09-13
5. SECRETARY OF STATE FOR THE HOME OFFICE
6. HOUSE OF COMMONS, LONDON, SW1A 0AA

THIS CARD IS NOT VALID FOR DRIVING

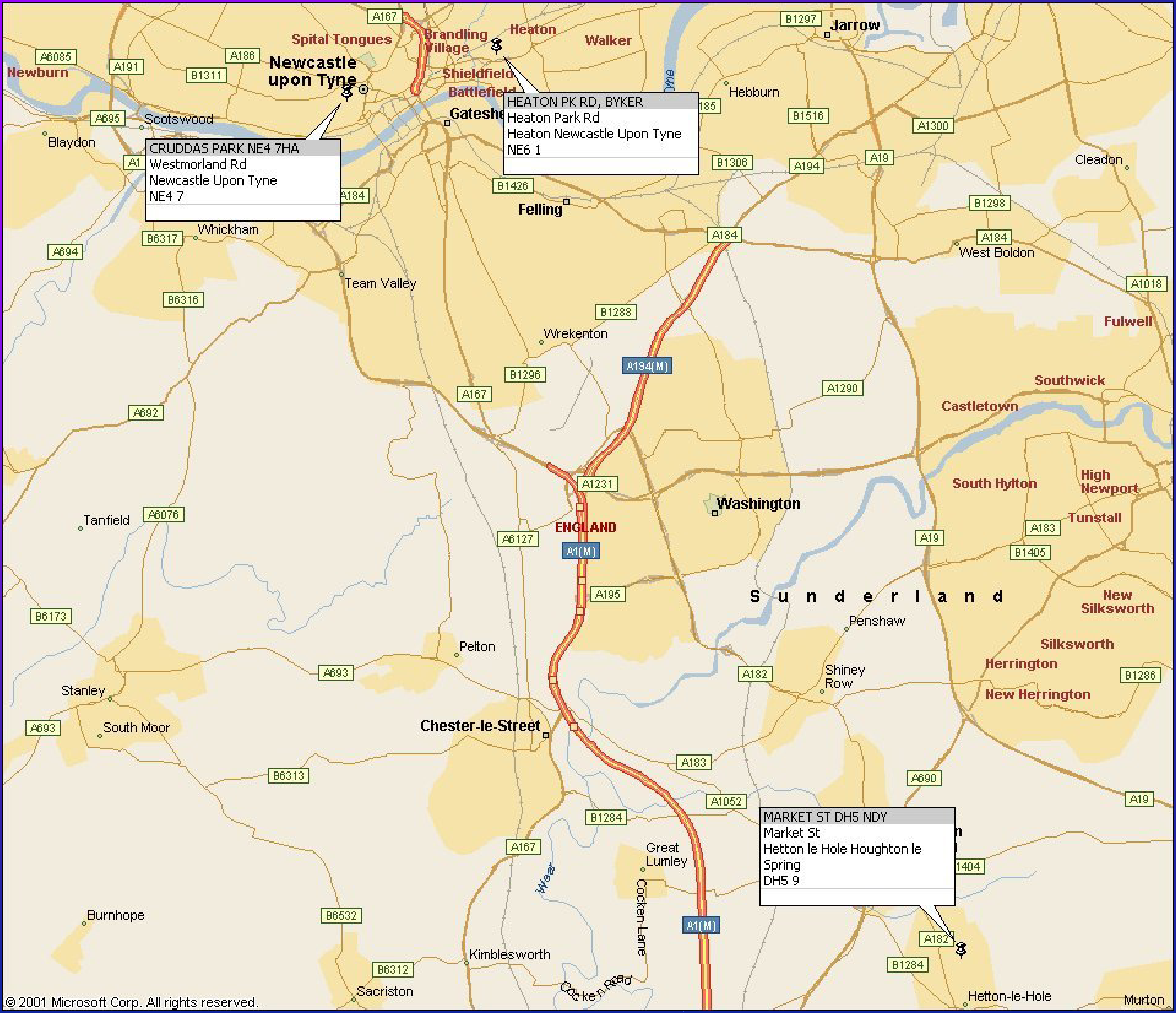
CARD HOLDERS ENTITLEMENTS:

- To play the Race Card
- To remove the automatic right to Trial by Jury
- To charge over-16s £40 for a compulsory ID Card
- To call for the seizure of the homes of cannabis users
- To extend detention without trial
- To muddle justice with politics



Movement Trails

- Bank records
  - ➔ ATM usage
- Credit card records
- Retail store records
- CCTV
  - ➔ Analogue, digital
- Telephone Records
  - ➔ Fixed, Mobile
- (Future) Identity Card usage


CRUDDAS PARK NE4 7HA
Westmorland Rd
Newcastle Upon Tyne
NE4 7
HEATON PK RD, BYKER
Heaton Park Rd
Heaton Newcastle Upon Tyne
NE6 1
MARKET ST DH5 NDY
Market St
Hetton le Hole Houghton le
Spring
DH5 9
Newcastle upon Tyne
Gateshead
Newburn
Spital Tongues
Brandling Village
Heaton
Walker
Jarrow
Shieldfield
Battlefield
Hebburn
Scotswood
Blaydon
Whickham
Felling
Cleadon
West Boldon
Team Valley
Wrekenton
Fulwell
Southwick
Castletown
South Hylton
High Newport
Tunstall
Washington
ENGLAND
Tanfield
Sunderland
New Silksworth
Penshaw
Silksworth
Herrington
Shiney Row
New Herrington
Pelton
Stanley
South Moor
Chester-le-Street
Great Lumley
Cocken Lane
Wear
Burnhope
Kimblesworth
Sacriston
Cocken Road
Hetton-le-Hole
Murton
A1(M)
A194(M)
A167
A6085
A191
A186
B1311
A695
A1
A184
B6317
A694
B6316
A692
A6076
B6173
A693
B6313
B6532
B6312
B1297
B1516
A1300
B1306
A194
A19
B1298
A1018
B1426
B1288
B1296
A1290
A1231
A6127
A195
A182
A183
B1405
B1286
A690
A1052
B1284
B1404
© 2001 Microsoft Corp. All rights reserved.

Forensic Research and IMSs

- Can we get more than was intended from the Management System?
- Can we analyse the audit trails in unintended ways?
- Can we do so legally? If original application for a warrant was valid – how, and at what stage do the courts say that further exploration and aggregation becomes “ultra vires”?

Forensics and Identity Management Systems

Intended and Unintended Audit Trails

- → When was an identity used / presented?
- → Was it accepted / rejected?
- → For what activities was it used?
- → For how long are the records kept?
- → What constraints exist on usage and analysis?
- → What constraints are there on passing on to 3rd parties?

- How are courts to monitor situations where records are kept for too long and data analysed *ultra vires*?

FIDIS type 2 IMSs:

- Cell-site analysis
- Automatic Number Plate Recognition / Traffic Congestion Charging
- Radio-based traffic charging
- Oyster Cards
- Swipe cards for physical access control
- CCTV + facial recognition

FIDIS type 2 IMSs:

- Credit cards – general and specialised: purchases plus locations
- Store Loyalty cards
- Library books taken out
- Medical databases
- Education databases
- Google logs

Broad-based ID cards:

- Leave a trail each time they are presented:
- Locations, movements
- Use of social and medical services

Understanding the Problem

- The everyday activities of Digital Forensics may expose activities – and hence potentially invade privacy – in ways never intended by designers of IMSs and law policy makers
- Practitioners in Digital Forensics do not necessarily set out to breach privacy – their aim is to aid law enforcement
  - → But the effect of their work may be to weaken privacy rights

Understanding the Problem

- Data obtained by LE without warrant remains unusable in court proceedings
- Data held by 3rd parties and then ceded to LE under warrant: provided original warrant is valid, 3rd parties may not be able to restrain subsequent use
- Data obtained by LE with a warrant but used *ultra vires* through technical ingenuity – courts may lack the understanding to forbid its use.
- Position of data aggregation by LE unclear but appears unprotected by courts

Remedies?

- First step is to describe the problem
- Can we frame precise laws?
- Do we grant judges discretion to exclude for “unfairness” or “abuse of process”?
- ????

SEVILLE JUNE2007 SPAIN
19th Annual FIRST Conference

FIRST 2007

Identity Management Systems: the forensic dimension

Peter Sommer
London School of Economics
peter@pmsommer.com
p.m.sommer@lse.ac.uk

LSE