Purple Penelope
and UK MOD’s Emerging Strategy for Information Security

Ruaridh Macdonald
Defence Evaluation and Research Agency
Background

- MOD’s future Command Systems need a common operating environment
- Achieved through
  - COTS software
  - Interconnection of systems
- Requires a different approach to security
Current Security Practice

- Multi-level working
  - Some users not cleared to see all information
  - adequate defence against compromise
  - too constraining for honest users
  - based on bespoke software and niche products

- System High Working
  - All users cleared to see all information
  - avoids technical measures
  - hard to police flows between systems
Overview

- Doing it in theory
- Doing it in practice
- Demonstration
- Different types of attack
- Conclusions
The Proposed Solution

- Interconnected Domains
- Labelling
- Role based access control
- Inter-domain transfers sanctioned by people
- Application-oriented accounting and audit
Domains

- A domain is a logical or physical place in a business model where people can work.
- Domain boundaries are chosen to enclose closely related business functions (or data).
The Domain-based Approach

- Considers security from the point of view of the business process, not the implementation.
- Leads to a set of measures better suited to modern computer systems:
  - different measures for different threats
  - discretionary labelling defends against mistakes
Domain Rules

- All members cleared for all data
  - Compartmented or System High Mode

- Small
  - probably no more than 1000 for SECRET systems
  - larger for RESTRICTED, several thousand

- Limit inter-domain data exchange across levels
Domain Rules (continued)

E3 assurance of

- Exclusion of non-members
- Labelling and access control
- Human sanction of inter-domain exchange
- Accountability for inter-domain exchange
- Blocking of unnecessary inter-domain exchange
Labelling

- Mandatory Labelling
  - originator mandates marking for all time
  - access checks compare user’s clearance against marking

- Discretionary Labelling
  - marking can be changed at user’s discretion
  - access checks compare user’s clearance against marking
Purple Penelope

- NT Extensions
  - Discretionary Labelling
  - Filemanager
  - Screen stripe
  - printing
  - floppy disks

- Applications
  - e.g. Notepad, MS Word, MS Access, Netscape

- Currently for NT 3.51
  - PP for NT 4 almost complete
Purple Penelope Mechanisms

- Discretionary Labelling
  - documents, clipboard, databases, messages, printing

- Export Sanction
  - shared filestores, floppy discs, messages

- Role Based Controls (*under construction*)
  - filestore

- Accounting (*planned for future*)
  - shared files
Demonstration of Purple Penelope

Screen stripe appears at the top of the screen

Selected file is SECRET  Clipboard is RESTRICTED

Current application specific label

Separately labelled clipboard
Selected file is SECRET   Clipboard is empty

User’s private filestore
Domain shared filestore (access mediated on user clearance)
You have requested the export of a file to a shared filestore. The file to be exported has the following details:

From: \figaro\francois$\demo files\conf.TXT
To: \FIGARO\registry\shared files\CAN demo files\conf.TXT
Label: CONFIDENTIAL

This operation is audited, and you will be held accountable in the event of a security breach.

WARNING!!!
The unexpected appearance of this dialogue indicates the presence of a virus or Trojan Horse.
In such an event, press ALERT and contact your Security Officer immediately.
BRIEFING REPORT

24-Apr-97

Prepared by PP2 Group of Purple Penelope

2 page(s)

UNCLASSIFIED
Armoured Fighting and Reconnaissance Vehicles within the British Army

**Warrior**

Warrior is an armoured combat vehicle. It is NBC proof, and a full range of night vision equipment is included as standard.

**Weight of Vehicle** 24,500 kg  Restricted

<table>
<thead>
<tr>
<th>Quantity</th>
<th>Armament</th>
<th>Marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>30mm Rarden cannon</td>
<td>Confidential</td>
</tr>
<tr>
<td>1</td>
<td>7.62mm Hughes Chain Gun</td>
<td>Secret</td>
</tr>
</tbody>
</table>

**MS Access as example front end to shared trusted database**
Netscape Test Page 3

Oranges are NOT the only fruit

We can load an unclassified document if we want

Or go back to the restricted one

Support for labelled Web pages
Accounting and Audit

- usually operating system collects accounting information
- Large volume of information
- Cannot establish relevant facts
  - e.g. what data exported.
Traditional Accounting

07:25 start application WordProcessor
10:30 WordProcessor, open for read “Plans.doc”, Secret
10:31 WordProcessor, close “Plans.doc”
16:50 WordProcessor, open for write “Expenses.doc”, Secret
16:51 WordProcessor, close “Expenses.doc”
16:52 downgrade “Expenses.doc” to Unclassified
16:53 print “Expenses.doc” at Unclassified
16:54 delete “Expenses.doc”
18:42 quit application WordProcessor
PP Approach to Accounting

- Application level rather than Operating System
- Easy for user
- Role based
- Export of data
- Possibly archive copies of exported data
Security Architecture

User (private)  Role  Domain (read only)  External
Security Problems

- Outsiders
  - Deliberate/direct attack e.g. hacker
  - Indirect attack e.g. macro virus

- Insiders
  - Accidental release e.g. mislabelling or misdirecting
  - Deliberate release e.g. traitor
Direct Attack

Configuration Control  Firewalls

User  Role  Domain  External

(Countermeasures are italicised)
Indirect Attack

Discretionary Labelling
Role Based Access Control

Configuration Control
Firewalls

User
Role
Domain
External

Export Sanction
Firewalls

(Countermeasures are italicised)

DERA
Accidental Release

Discretionary Labelling

Export Sanction

Firewalls

(User, Role, Domain, External)

(Countermeasures are italicised)
Deliberate Release

User Domain Role External

Accounting & Audit Firewalls

(Countermeasures are italicised)
Current State & Future Work (1)

- **NT4**
  - Port complete apart from Explorer
  - Screen stripe to be made a configurable taskbar

- **Explorer**
  - Bugs in customisation capability

- **Office ‘97**
  - Labelling extensions ported
  - Plans for labelling PowerPoint slides

- **Role Based Access Controls on shared filestore**
Current State & Future Work (2)

- Accounting
  - Done for shared filestore
  - planned for diskette and printing

- Sub Sessions
  - to constrain applications
  - underway

- Exploitation
  - 2 licences
  - DERA continues to develop and support
Conclusions

- UK MOD’s new strategy for Infosec
- Focus not on any one of:
  - Implementation Techniques
  - Security Policy
  - Presentation of Security Policy
  - Business needs of end user
- Considered all these aspects together