Purple Penelope: Extending the Security of Windows NT

DRA/CIS3/WN/SRW/97/1.4
Simon Wiseman
24th February 1997

1 Introduction

As part of the UK MOD's Applied Research Programme, a demonstration secure system, informally known as "Purple Penelope", is being produced by the Defence Research Agency. The aim of this work is to show that the security functionality of Windows NT can be extended to provide labelling, and other security mechanisms, which support users who must handle sensitive information. This is despite the fact that NT does not provide any direct support for labelling functionality.

The scope of the work is the production of a proof-of-concept demonstration system. The functionality provided by the demonstration is intended for use within domains that work in System High or Compartmented mode – it is not thought to be adequate in Multi-Level mode.

The assured discretionary labelling functionality prevents those users with inadequate clearance from observing some data directly, but users with adequate clearance may use their discretion to relabel data, typically by copying it and giving the copy a lower label than the original.

Tighter controls are imposed on the exchange of data between domains. In particular, assured controls prevent data being exported from a domain without this being sanctioned by one of the domain's members using a Trusted Path. Accounting and audit functionality is used to monitor what data is exported in order to detect, at a later date, inappropriate behaviour amongst users. Firewalls are deployed to prevent, in a proactive way, any inter-domain communication that is not required.

The current implementation of Purple Penelope provides the discretionary labelling functionality and export sanction controls. Work is continuing to extend NT further in the areas of easy-to-use role based access controls, accounting and audit functionality.

2 Overview of solution

The Windows NT operating system, and the Microsoft applications that run on it, contain many open extensible interfaces which allow them to be customised with third party value-added services. The "Purple Penelope" demonstration has exploited these interfaces to extend NT's security functionality.

The additional security functionality provided by Purple Penelope:

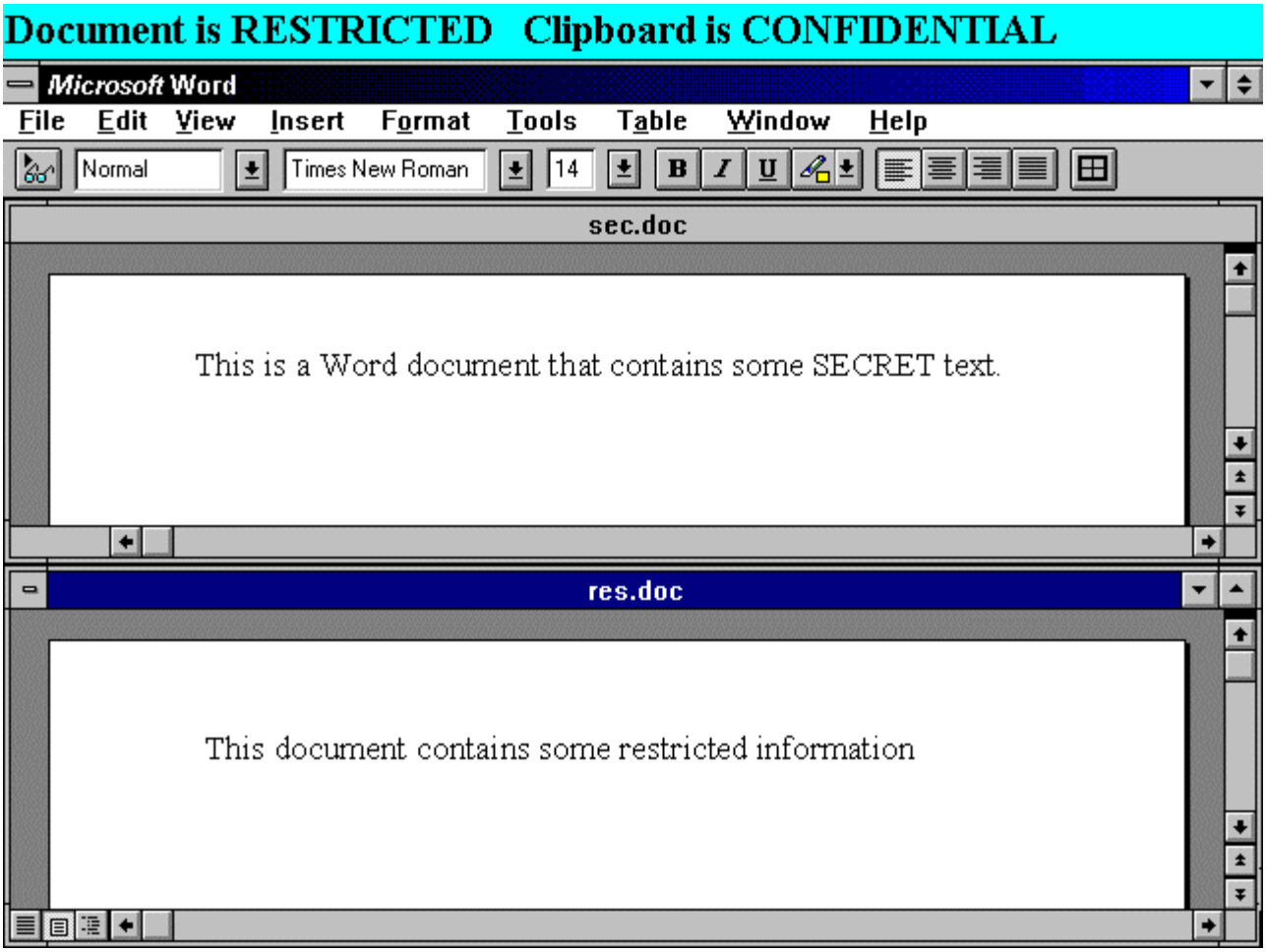
a. is generally applicable to a wide range of systems within Government and commerce, including those handling the most sensitive information;
b. works in systems with a heterogeneous mixture of NT and Unix servers, including Secure Unix servers such as CMWs;
c. has been implemented as a fully functional prototype, but not to product-quality software engineering standards (the prototype is being licensed to companies who wish to produce evaluated products);

d. is implemented in a way which minimises the effort that would be required to obtain an ITSEC security evaluation, though such an evaluation could not be conducted until product-quality software is available;
e. did not require Microsoft to divulge any proprietary information about their products – in particular neither the source code of Windows NT nor any that of any Microsoft application is required;
f. is implemented with a modest amount of software.

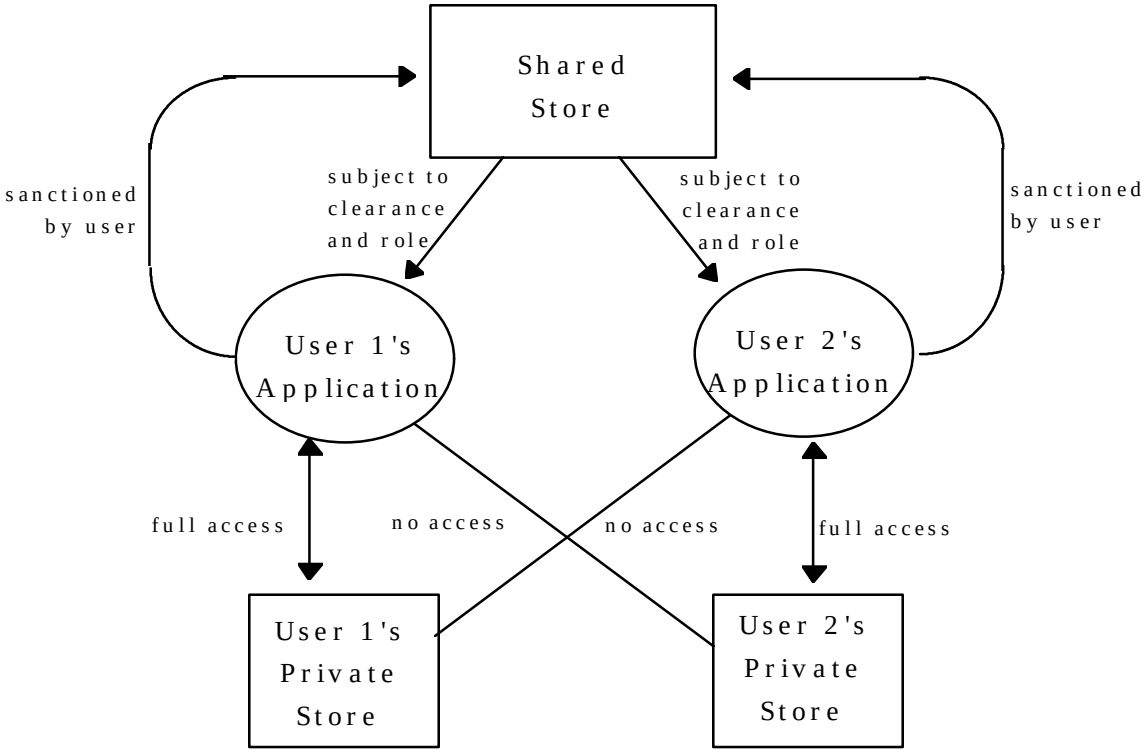
Windows NT already provides assured security functionality, but this only allows access to data to be controlled according to user identity rather than by security label. It has, however, proved possible to use the native security functionality as the basis for an implementation of discretionary labelling whose assurance is largely derived from that of the base product.

The visible manifestation of the additional security is the appearance of a stripe across the top of the screen. This displays the security marking of the application or data with focus. Depending upon the application, the marking may be associated with an entire application, an individual document or a database field. The screen stripe also displays the marking associated with the data in the clipboard. The marking of other data which is visible on the screen, but which does not have focus, is not displayed in the stripe, though some applications may display markings in their window alongside their data.

The screen shot below shows Microsoft Word with two documents open – one marked Secret and the other Restricted. The Restricted document is current (has input focus) and so its marking is displayed in the screen stripe. Alongside is an indication that the clipboard contains Confidential data. The Secret document is visible on the screen, but its marking is only fortuitously visible in its header.



Each user has a private filestore and access to a shared filestore. Applications are free to read and write files in the user's private filestore, but they cannot access the private filestore of any other user. Applications can read files in the shared filestore if the user has sufficient clearance and role-based access rights, but applications cannot modify any shared files. Applications may export files to the shared filestore by copying them, remove files from the shared store, or relabel shared files, however these are accountable actions which must be sanctioned by the user and are subject to role-based controls. The software which solicits the user's approval establishes a Trusted Path and cannot be bypassed by the applications. The diagram below illustrates the access restrictions:



The marking applied to selected data may be changed using a dialogue box activated by clicking on the screen stripe. For data which is private to the user the action is not accounted for, even if a lower marking is applied. For shared files, however, the action is subject to role based controls and is noted so the users can later be held to account for their actions.

Users can exchange messages, which may have attached files. Independent labels are applied to the message body and any attachments. Checks are made to ensure messages cannot be sent to users with inadequate clearances.

Users may access services hosted on Unix servers. Two services have been included in the first phase of Purple Penelope: a database containing labelled data and an unlabelled track management system.

3 Users' view

3.1 The Screen Stripe

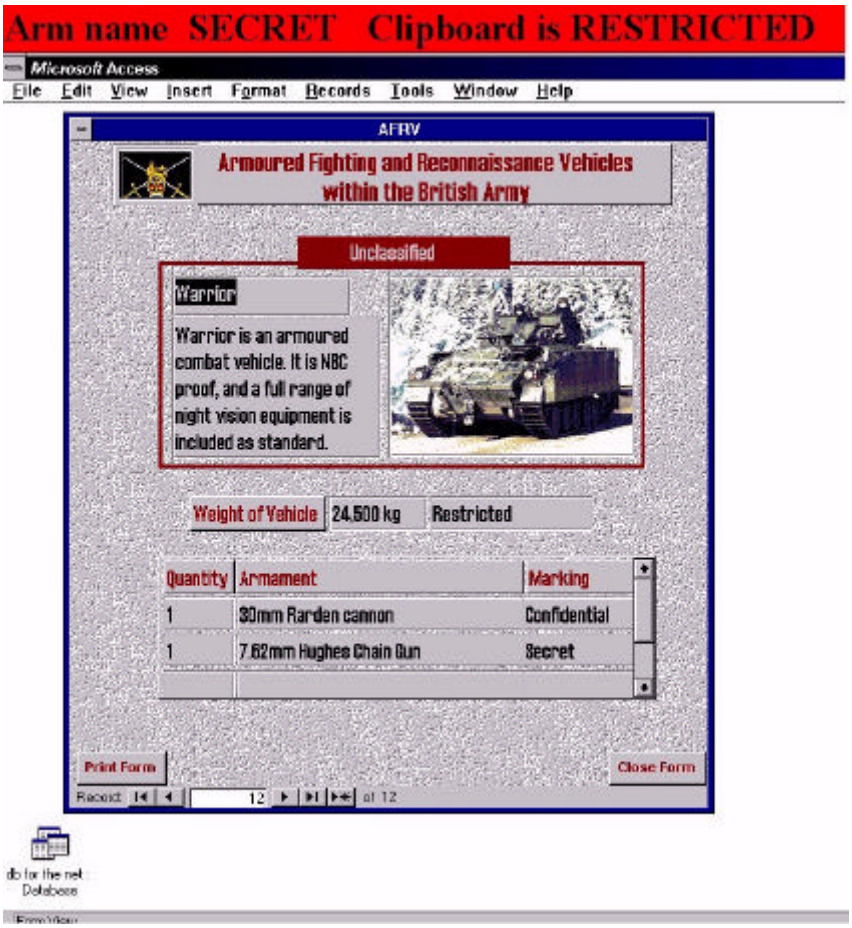
The users' view of a Purple Penelope system is that of a standard Windows NT 3.51 interface, except that a stripe across the top of the screen is reserved for the display of security markings. The screen stripe displays the security marking of the data that the user is currently working with, and the marking associated with the data in the clipboard.

The background colour of the screen stripe changes to reflect the label of the current data.

The granularity of data to which the displayed marking applies depends upon the nature of the current application. For simple applications, such as Notepad, the marking applies to all the documents and data handled by the application. With more sophisticated applications the marking may apply to the current document or field, as appropriate. An indication of what the marking applies to is shown in the stripe.

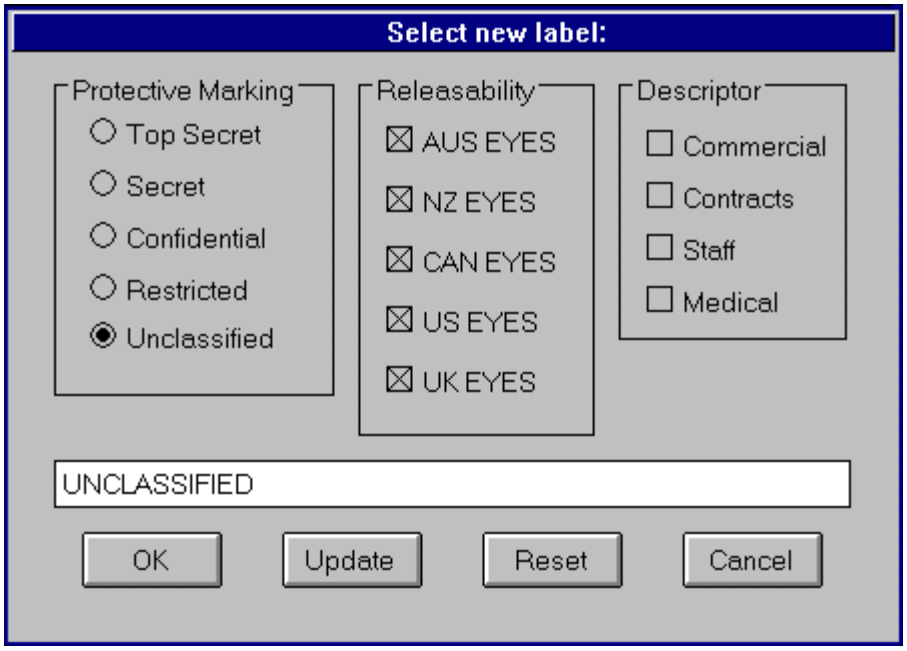
The screen shot below shows an example Microsoft Access form which is being used to access data stored in a labelled relational database managed by Trusted Oracle 7. The data fields enclosed in the

red box at the top of the form, showing name and description, share a common label of Unclassified. The weight of the vehicle is also displayed, but is not enclosed in the red box as it always has a higher label than the name and description. A subform is displayed showing armaments carried on board the vehicle. The "Quantity" and "Armament" fields carry the same label which is displayed alongside for each armament. The label of the field currently in focus and a legend for the field is displayed in the screen stripe. The cursor is currently within the "Armament" field labelled Secret.



The current marking may be changed with a left-mouse click on the screen stripe in the area where the marking is displayed. The user is then presented with a dialogue box which allows them to choose a new marking. In a similar fashion the user may change the label of the clipboard data.

The screen shot below shows the dialogue box which is used to select a new marking (the module which provides this dialogue is pluggable and so can be customised to meet the requirements of any particular marking scheme). The marking may be changed by clicking the buttons or by editing the text of the marking.



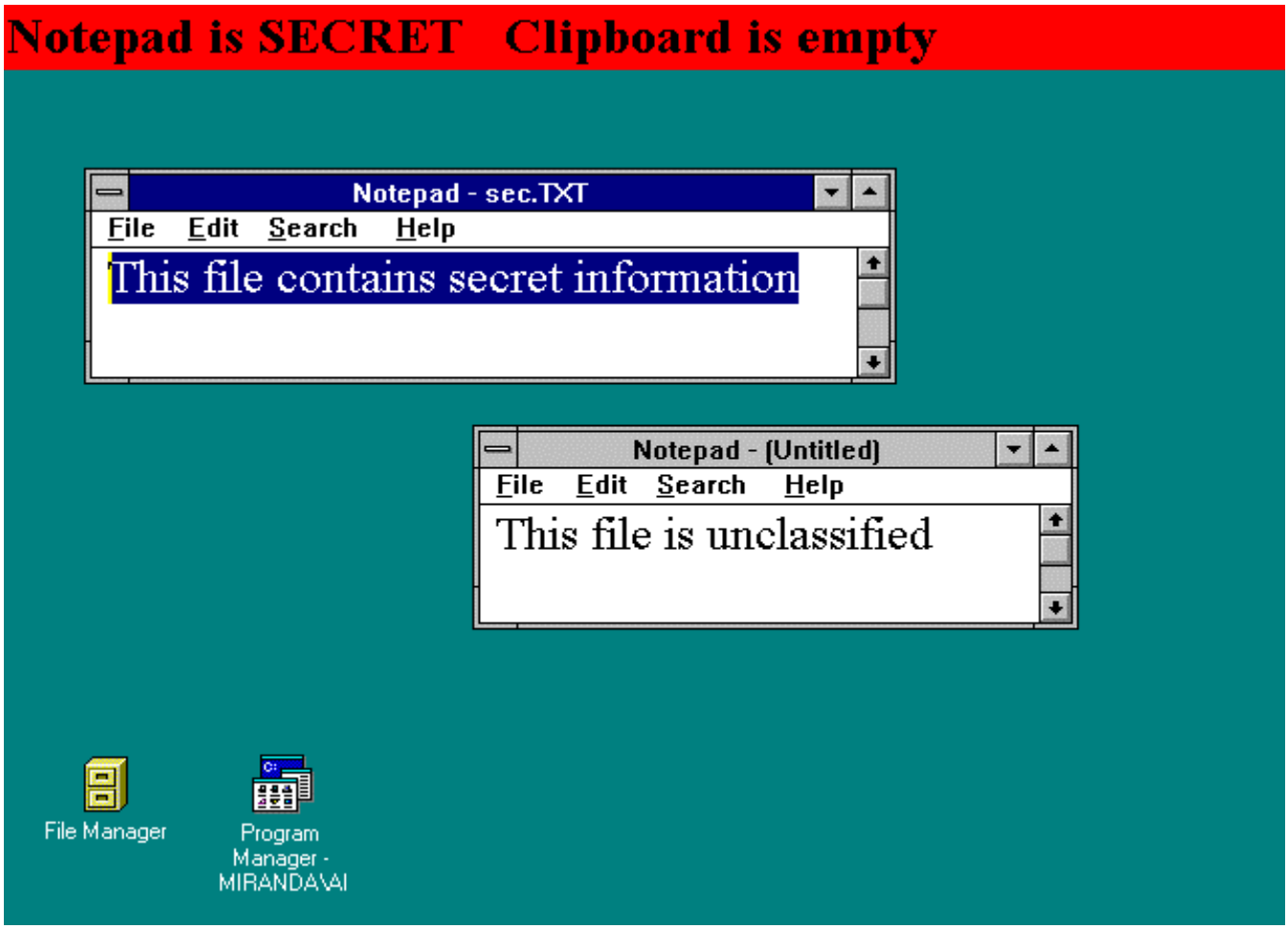
A right-mouse click on the screen stripe allows the user to configure the appearance of the screen stripe. In the current version of Purple Penelope, the user may select the font size of the markings and the background colours that are associated with the markings. In the future it is planned to allow the user to alter the position of the stripe.

3.2 Cut and Paste

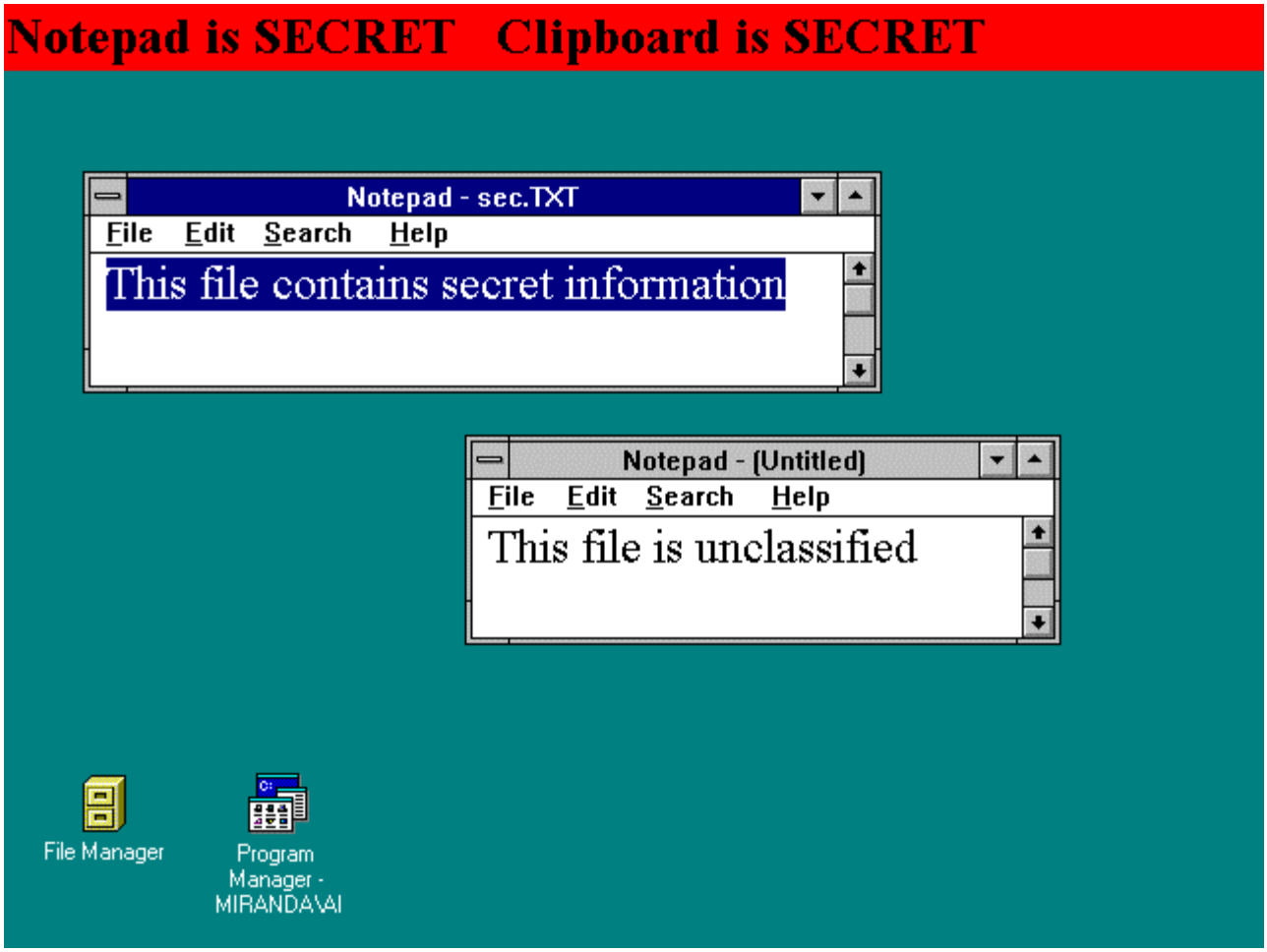
A marking is associated with the data in the clipboard. Whenever the user cuts or copies data to the clipboard, the clipboard's marking is set to that of the data's source. Whenever the user pastes data from the clipboard, the marking of the destination is set to the highest of its existing value and that of the clipboard.

The sequence of screen shots shown below illustrate how markings are tracked when cut-and-paste is used to move data from one application to another.

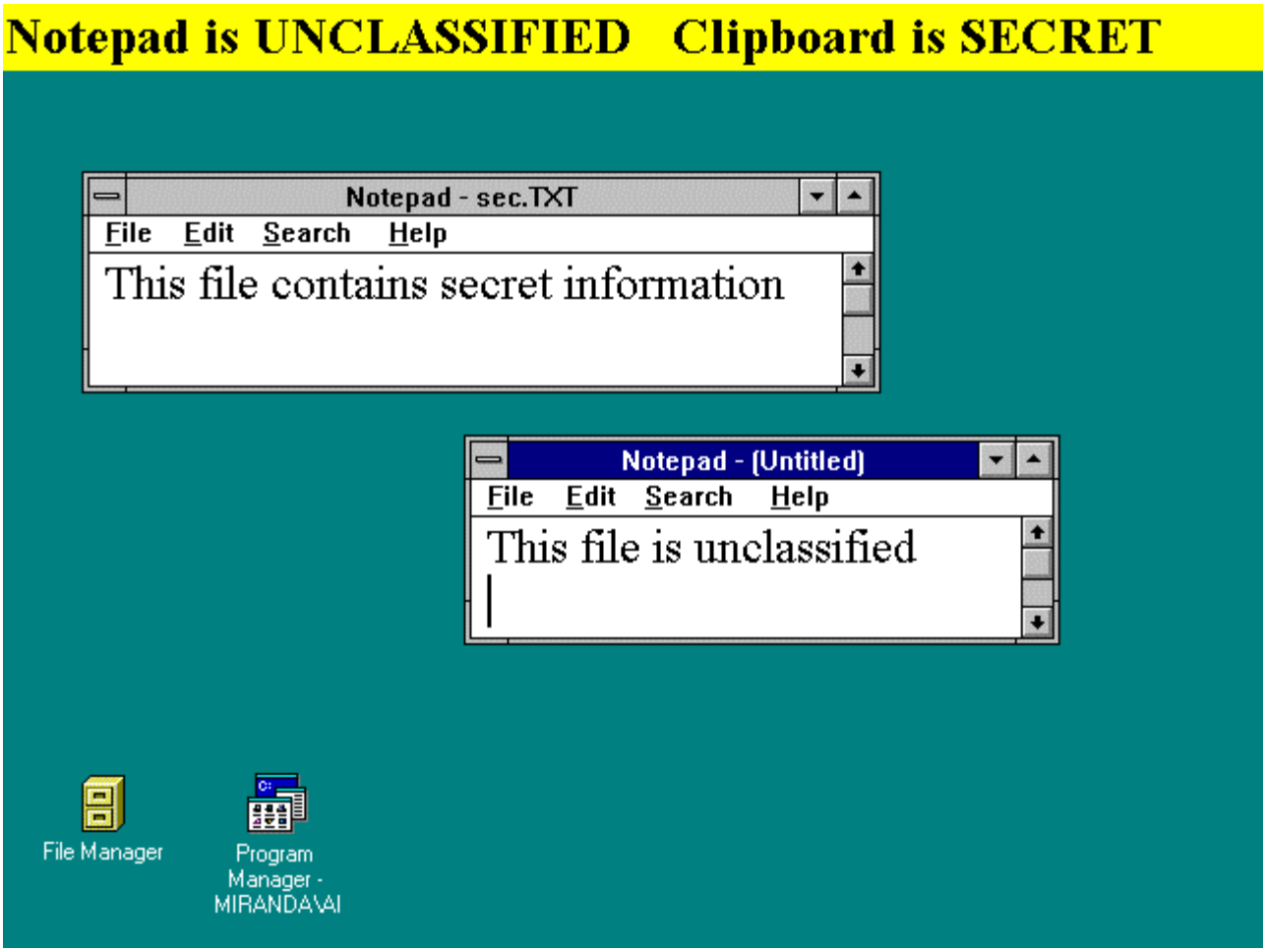
a. ***The first shot shows some Secret data selected in a Notepad document. At this point the clipboard is empty.***



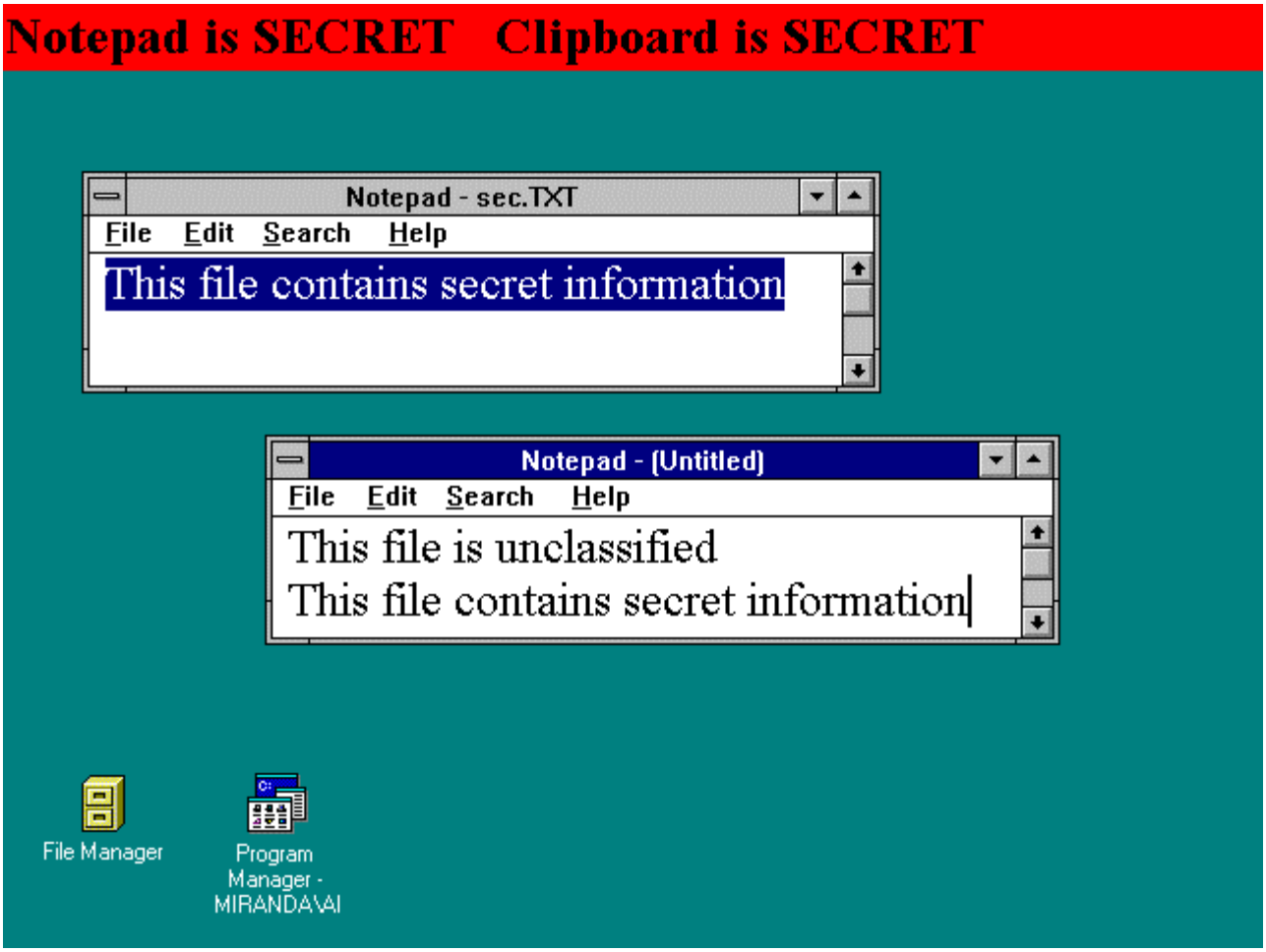
b. ***The second shot shows the screen after the user cuts the data. The clipboard now contains Secret data.***



c. After the user moves the cursor to the second Notepad document, the screen appears as follows.



d. Finally, once the user pastes the clipboard data into the second document, the document's marking floats up to Secret.



The user may change the clipboard's marking by clicking on the screen stripe in the area where the clipboard marking is displayed.

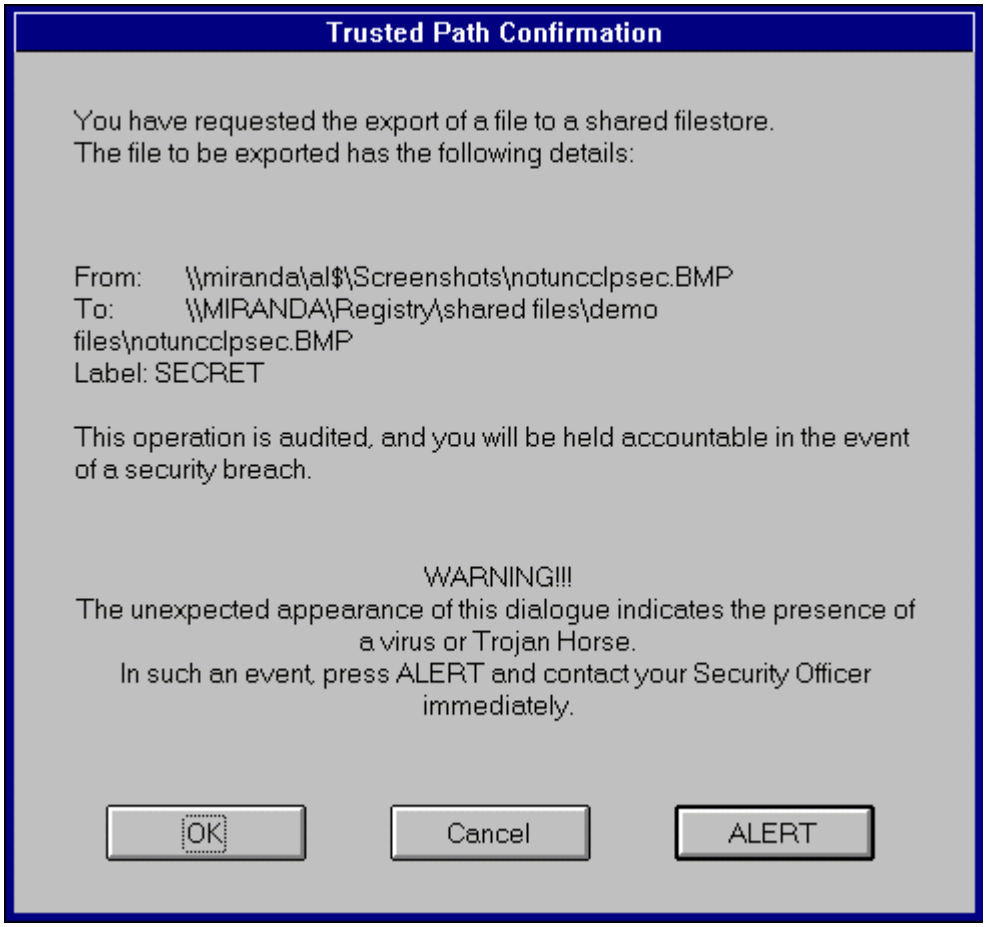
If the clipboard is empty, no marking is displayed. The clipboard is empty when the user logs in, and subsequently the user may empty it explicitly by right-mouse clicking the screen stripe and selecting the 'empty clipboard' option from the configuration dialogue.

3.3 File Manager

When files are selected within File Manager (customisation of NT4's Explorer Shell is in progress), the screen stripe displays their marking. If files with different markings are selected, the lowest and the highest markings are both displayed.

File Manager can be used to copy files to the shared filestore, remove files from the shared filestore and to change the marking of shared files. However, to avoid attacks by Trojan Horse software, these actions must be sanctioned by the user. To ensure that this is so, each action causes a dialogue to appear requesting confirmation (this occurs with any application that copies files to the shared store, not just File Manager). The OK button of this dialogue can only be pressed by the user physically clicking the mouse (or by the standard keyboard equivalent). The action cannot be simulated by Trojan Horse software because a protected NT Desktop is used to display the window (this is why the screen stripe and other application windows are not displayed while the confirmation dialogue is showing).

The screen shot below shows the dialogue box used. The example shown appears in response to an application attempting to export a file called “notuncclpsec.bmp” with a marking of “Secret”. Similar dialogues are used to confirm other modifications of the shared store and floppy discs.



3.4 Microsoft Word

When a Word document has focus, the screen stripe displays the marking of the document. If Word has more than one document open, each may have a different marking but only that of the document with focus is displayed in the screen stripe.

Security Marking ‘objects’ may be placed in a Word document by using the new ‘Insert/Marking’ menu item. These objects display the current marking of the document, and are automatically updated if the label of the document is changed. Standard templates may be provided which already include marking objects in the appropriate place, for example in the headers and footers of the document.

The marking of a document may change when data is pasted into the document or at the explicit request of the user. The user may change a marking by clicking on the screen stripe or by double-clicking on a marking object within the document. Whichever method is used to change the marking, both the screen stripe and all marking objects within the document are updated.

3.5 Microsoft Access

If labels are to be used to mediate access to data within the database, Access can only be used as a user interface front end to labelled data managed by a DBMS which supports labels (the

demonstration system uses Trusted Oracle on a Sun CMW server). Access can be used to store the data, with labels held as string (or integer) data, if mediation is not required.

The way in which labels returned from the database are displayed depends entirely upon the way the forms have been designed. In the databases constructed for the Purple Penelope demonstration, attribute level labelling is provided so labels are associated with individual fields within forms. The demonstration provides an example of the most general case, where some form fields display data and others display the markings of that data, and the fields on one form may contain data with different markings. With this approach, the integrity problems normally associated with the use of labelled databases do not arise.

When one of the form's data fields gets focus, i.e. the cursor appears within it or text within it is selected, the screen stripe displays the field's name and the marking associated with its data.

If the form allows markings to be changed, the user may select a new marking by clicking on the screen stripe, by clicking an application specific button or by double clicking on the associated marking displayed in the form.

3.6 Eudora

Eudora is a popular Internet mail package which allows messages with attachments to be created and received. Eudora has been incorporated into Purple Penelope, but because its user interface could not be customised it was not possible to display the labels of message bodies in the screen stripe. Work is now underway to include Microsoft Exchange, whose user interface is customisable, into Purple Penelope.

3.7 Printing

When applications which cannot be customised print documents, the documents' marking (which is that of the application) is placed at the top and bottom of every page. Customised applications which have already formatted the page in an appropriate way can disable this feature. With Word, the intention is that each template will have a flag that indicates whether or not markings should be added to pages.

4 Terminology

A system is said to operate in **Multi-level** mode if any of its potential users have insufficient clearance to permit them routine access to some of the information which may be legitimately processed by the system.

In contrast, if all users have adequate clearance for all the information, but formal restrictions apply which mean not all users are authorised to access all of the information, the system operates in **Compartmented** mode. The restrictions may be in terms of the users' nationality or the use of codewords.

A system in which all users have adequate clearance and no formal restrictions apply, is said to operate in **System High** mode (a special case known as **Dedicated** mode is sometimes defined when referring to systems that are dedicated to a few individuals).

Note that, while there has traditionally been a one-to-one relationship between a system's security operating mode and the security functionality required in its implementation, this is not the case with

modern networked systems. In particular, a system may need labelling functionality regardless of its mode.

A **Security Label** is applied to a container of data to convey how the contents should be protected and distributed, and how access should be mediated with respect to people's clearances. When used in the Infosec context, "label" is taken to mean "security label". A label may be represented in a number of different ways, even within a single system. The form which is intended to be readable by humans is particularly important and is referred to as a **Security Marking**.

A security label may comprise a number of components. In the UK the **Protective Marking** component is perhaps the most important (elsewhere this is called the Classification). The protective marking or classification is that component of a label which gives an indication of the damage that would be caused if the information content of the container is compromised (meaning inappropriate disclosure or inappropriate modification).

The functionality relating to security labels in a system may provide **Mandatory Labelling**. This means that the originator of some information is able to mandate its security marking, as represented in the computer by a security label. This marking cannot subsequently be changed by other users, regardless of how the information is used or represented within the computer. [More usually the term Mandatory Access Control is used, but this has yet to be defined in a definitive or universally accepted way. If MAC is interpreted as a requirement oriented statement, rather than as a mechanistic one, then it has roughly the same meaning as mandatory labelling].

Labelling may also be supported in a discretionary form, termed **Discretionary Labelling**. This is where users obtaining some information may, at their discretion, change its marking. Typically, the change is made as data conveying the information is copied.

A **domain** is a required boundary, in a model of the business constructed from the viewpoint of security, that restricts what data can be accessed by which people. The people who are allowed into a domain are its **members**, while those members who are in a domain at any one time are its **occupants**. A **user** is someone who uses a computer to achieve some business objective, rather than someone who procures the computer or manages its operation.

A **document** is some textual, graphical or other data constructed by a user, which is viewed by that user as an electronic form of paper (or celluloid) document. A **file** is an artefact of an operating system which can be used to store a document, or part thereof, or any other data. A document can be placed in persistent storage, that is stored on disk as a file or files, or may be in the transient storage of an application while the user is creating or modifying it.

A **Trusted Path** is an interface which allows a user to interact with a security critical function in a way that allows one party to be assured of the identity of the other party. That is, either the user can be sure they are communicating with the critical function, or the critical function can be sure they are communicating with the user. Often the requirement is for mutual assurance of identity, but this need not be so. A Trusted Path is often used during login to ensure passwords are not compromised.

A **firewall** or **guard** is a communications device that exerts control over the usage of communications services. Some practitioners make a distinction between firewalls and guards, but such distinctions are often somewhat artificial and none are universally accepted. This report adopts the term firewall, on the basis that this is more prevalent because it is current in industry, even though the term guard is more current within defence.

A **Compartmented Mode Workstation** (CMW) is a Unix workstation which provides mandatory labelling using a special system of dual-labels. Every container of data has two labels, a Sensitivity

Label (SL) and an Information Label (IL). The SLs are fixed labels, meeting the labelling requirements of ITSEC functionality class F-B1, which can be used to mediate access. The ILs are floating labels which cannot be used to mediate access, though they do support mandatory labelling (unless privileges are assigned) suitable for use in System High mode systems.

Role based controls are a form of discretionary control that provide the means of restricting the activity of users based upon the business role they fulfil in the system. In Purple Penelope, users are generally able to fulfil all their roles concurrently, though some applications run with restricted rights, and users select a ‘current role’ to act as a default role in many operations.