Starlight: Interactive Link

M. Anderson, C. North, J. Griffin, R. Milner, J. Yesberg, K. Yiu
Information Technology Division
Defence Science & Technology Organisation
Salisbury, South Australia 5108, Australia
Ken.Yiu@dsto.defence.gov.au

Abstract

The Interactive Link forms part of a suite of products being developed as part of the Starlight research program. This research program is investigating methods for achieving military-relevant information security capabilities which are genuinely cost effective. The Interactive Link is a retrofittable device which fits to commercial off the shelf workstations and PCs which are connected to classified networks. The Link allows interactive access to low or unclassified networks, such as the Internet, in a manner which is accreditable via the authorising government agencies. The advantage of the Interactive Link over other methods, is that it allows untrusted graphical windowing applications, such as X window applications or Microsoft Windows applications, to run in a manner permitting users to have windows at differing security levels.

1. Introduction

The Interactive Link forms part of a suite of products being developed as part of the Starlight research program. This research program is investigating methods for achieving military-relevant information security capabilities which are genuinely cost effective[3][4][5][6][9][11]. Much previous research in trusted systems has not yielded the anticipated results. Typically, this research has focused on methods for achieving high assurance trusted computing bases to secure operating systems such as UNIX[1][8][15][16]. The complexity involved in reaching high assurance levels, and the associated cost, has limited the availability and state of the art of various commercial offerings.

In the light of the infosec experience of the 1980's, the Starlight research program focuses on methods for achieving security capabilities in a retrofittable, incremental manner. That is, we forsook the traditional view of “having to build security in at the beginning” for information systems such as those epitomised by workstations, and subscribed to an approach which focused on building security from a network view where any component which was complex but had a short product lifecycle (e.g. workstations) was deemed to be untrusted. In essence, we concentrated our effort in configuration methods for networks, and the construction of limited functionality, high assurance devices which could be retrofitted to untrusted components in the network to achieve the desired results. Further details on this philosophy are available elsewhere[2].

This paper focuses on how Starlight achieves one particular security capability, i.e. the Interactive Link. The term Interactive Link refers to a solution for achieving a major desire of many military commanders. That is, to be able to retrofit a cost effective device to commercial off the shelf workstations and PC's which are connected to classified networks and yet still retain interactive access to low or unclassified networks, such as the Internet, in a manner which is accreditable via the authorising government agencies. By accreditable, we refer to methods whereby subversion of any application or operating system on any machine attached to the high network will not enable misuse or leakage of information in an unauthorised manner. As such, the reader can deduce that any known method, or indeed concept, based on the firewall (smart packet filtering) paradigm to achieve this interactive link is considered insufficient and indeed insecure. However, we also wished that any solution devised could compete reasonably well on a cost basis with firewall type solutions. The current implementation of the Interactive Link is to be evaluated to an ITSEC assurance level of E5 although the design is such that it can reach E6 with surprisingly little additional effort on the part of the evaluating facility.

The following sections discuss how the service is
supplied by first describing the trusted hardware and then the untrusted application software. In addition, we discuss in more detail issues involving the user interface. Finally, several issues such as alternative interconnection topologies, authentication, and auditing are discussed.

2. Hardware

The Interactive Link is a trusted retrofittable hardware device which enables the equivalent of security level differing windows on an untrusted workstation (as shown in Figure 1). In effect, a user may undertake "secret" activities in secret windows, and unclassified activities in unclassified windows. In addition, a user may cut from an unclassified window, and paste the result in a classified window. However, a user may not cut from a classified window, and paste in an unclassified window (downgrading, or downwards cut and paste).

A typical military use of the device is to allow direct connection to a secret operational network while still retaining interactive access to the Internet to run, say, an untrusted commercially available World Wide Web browser without any fear that resident trojan horses may leak information. A prototype employing Netscape's Navigator™ browser was demonstrated to an international defence meeting during April of 1996.

The original prototype unit comprised 8 serial ports, a membrane keypad with a separate accept switch, a trusted display formed from a bank of LED light bars, two PC Card based Ethernet ports, a LCD, and an Intellikey™. Depending on the performance and cost requirements of the applications the Ethernet ports are optional.

A typical interconnection topology for the Interactive Link, and indeed the one employed for the current prototypes, connects the unit between the high side workstation and the low side network. The keyboard and mouse of the high side workstation are connected directly to the Interactive Link, with a further connection from the Link to the high side workstation's mouse and keyboard ports. This configuration allows transfer of data from the keyboard and mouse input devices down to the low side network, and the transfer of display data from the low side network up to the high side network. For cost sensitive applications, these connections can be implemented using high speed serial links. For higher performance, these connections can be implemented using Ethernet or some other high speed network mechanism. With the current prototype, Ethernet is used to connect the Interactive Link to the low side network, and Ethernet is used on a direct connection to the high side workstation. Whilst a multiple (i.e. more than two) network capability expansion is possible, for the sake of clarity and simplicity the following discussion will be limited to two networks only, termed "high side" and "low side".

2.1. Data Diode and Trusted Switch

Figure 2 shows a "trust" component diagram of the Interactive Link hardware and also serves to reveal the basic operation of the device. The Interactive Link acts as a trusted switch for the keyboard between the classified and unclassified networks, and provides the equivalent of a data diode for the processor and display mechanisms of the workstation connected to the classified network. The three trusted components are the switch, data diode, and switch display. All other components are untrusted.

The basic operation of the link is simple. When the trusted switch "points" to the high side, all keyboard and mouse data is routed as normal to the workstation. When the

---

1. An advanced ("Omega") model provides this facility along with a number of other desirable capabilities [2].
2. An Intellikey is a pocket sized removable device which has a small nonvolatile memory. It can be used as a simple authentication token.

---
switch points to the low side network, keyboard and mouse data is routed to a keyboard handler routine in the low network for routing to the relevant application. Data which is to be displayed from the low network is pushed through the data diode to the high side network. This mechanism is quite simple for activities such as supporting the equivalent of one or more unclassified ASCII terminal windows but much more is needed to support real world applications such as those characterised by multindow graphics. These issues are examined in detail in the software section.

2.2. Trusted Display

The trusted display indicates to the user the current security level of the Interactive Link and hence the polarity of the switch. An example display is shown in Figure 3. The actual appearance may be customisable by a site integrator if desired, for example “Secret” and “Top Secret SCI”. The trusted display is external to the Interactive Link unit itself so that it may be positioned to provide maximum visibility to the user. Typically the trusted display will be connected to the side of the user’s monitor so that it is within the user’s peripheral vision whilst they are operating their terminal.

![Figure 3 Trusted Display Format](image)

3. Software

In this section, we look at the issues and mechanisms required to implement the Interactive Link to support graphical window sessions. To put what we mean into context, consider the user connected to a classified (high) network with an X window system or Microsoft Windows system, who desires an interactive session with the Internet in order to browse the net, say, via a World Wide Web application such as Netscape Navigator. Conceptually the software modules and mechanisms used to support the Interactive Link for both these windowing systems are very similar. However, due to the power and flexibility of the X window system there is a resulting extra complexity associated with the Interactive Link software solution. Due to this and the fact that the X window system is public domain, we will concentrate on a discussion of the X window system solution for the remainder of this section.

Figure 4 shows a snapshot from an Interactive Link session which employs applications requiring complex graphical support. The dashed display on the low side server is a representation of the low side X server session. It is included purely for ease of explanation; no physical display actually exists for the low side X server. However, it also serves to show what an intruder tapped into the low network would be able to recover. The sessions are described as follows:

1. At the start of an Interactive Link session an Interactive Link session manager tool is invoked along with default applications specified in the user’s preferences. In this example the unclassified applications are a mail tool and a drawing program. When an Interactive Link session is subsequently activated all mouse and keyboard commands are switched to the low side.

2. The user has suspended his/her Interactive Link session and resumed classified work. The trusted switch moves from the low side to the high side causing all mouse and keyboard commands to be directed to the high side server. The low side server does not see any further events. All changes to unclassified windows on the high side are not reflected on the low side. In this example we can see that the low side mail tool has been iconised and the low side graphics program has been moved whilst the user is in the high side session. These changes have not been reflected on the low side server. Changes emanating from the low side, such as the arrival of new mail in an unclassified mailbox, will still be reflected on the high side as the data diode is still active.

3. The user needs to alter a diagram in the low side graphics program and has resumed the Interactive Link session. The trusted switch moves to the low

---

3. For extreme threat environments, a deployment of the Interactive Link could include a special buffer-free & resettable keyboard to eliminate keystroke & key state storage.
1. Connection setup
Low side session

2. High side session

3. Low side session
Synchronisation

High side X server
Low side ("Dummy") X server

Figure 4 Interactive Link Session

side directing all keyboard/mouse commands to the low side. In addition, a signal is sent to the low side server requesting an update of all low side application windows. This causes the low side mailtool to be deiconised and the low side graphics program window to be relocated/resized to the same position/size as when the Interactive Link session was last suspended. In addition, the unclassified windows are popped to the front of the high side display to ensure that synchronisation is retained. The low side application windows are now synchronised on both servers. The user is now able to modify the diagram with the low side graphics program.

To move between high side and low side windows, a user depresses a switch/actuator which is directly connected to the trusted switch in the Link. The trusted display of the Link provides feedback on the success of the change to the desired security level. It is expected that the production versions may incorporate a deployable switch which can be connected to the mouse for ease of use.

3.1. X Window Support

To achieve the Interactive Link utilising the X window system on the high side workstation, the applications which supply unclassified data from the unclassified (low) network, or receive input from the user, must run as X clients on the unclassified network. Hence, these clients are informed that the high side X server is the remote display onto which they must pass their display data. The passage of display data from these unclassified remote X clients is easily achieved since the data diode in the Interactive Link
will allow the passage of data into the classified network where the X server display resides. All would be well and nothing much more required as long as the client does not require any acknowledgement from the X server. Unfortunately, this is not typically the case. For example, in connecting to the relevant X server, the client receives an acknowledgement packet containing the display’s geometry and characteristics (such as colour support). Depending on the application which runs as a client, callback and event packets may also be needed. Figure 5 illustrates this problem by showing a snapshot of an X application session with bi-directional communication.[14].

In order to solve the aforementioned acknowledgement problem we need to find a mechanism to supply the low side client with the relevant data. To allow event and callback packets from the high X server would imply that the server is trusted; an unpalatable and difficult undertaking. Previous work by TRW is testimony as to how difficult it is to achieve a high level of trust in an X server [12]. What is needed is some mechanism which avoids the need to trust the high side X server by removing the low side X client’s requirement for acknowledgements from this particular server.

The basic approach to the problem is to provide an unclassified or low “dummy connection” for the X client which mimics the high side server. To effect this dummy connection a low side proxy X server is run on the unclassified network. The low side proxy X server’s task is to provide all the acknowledgment and replies that the high side server would usually provide if there were not a data diode in the way blocking traffic to the low side. When the low side client application starts up, it in effect connects to both the low side server and the high side server. All display data and X protocol requests emanating from the client application are transmitted to both low side and high side X servers by an untrusted software module dubbed the “T Junction”. Naturally, the high side X server will attempt to respond to connect requests, events, etc., but they will be blocked from travelling to the low or unclassified network. In place of these the client application will receive all such responses from the low side proxy or dummy server. Figure 6 shows the software modules and architecture required to support an X session over the Interactive Link. The requirement for the high side “dummy” X client will be described later in this section.

4. The terminal (telnet) implementation is easier to implement since the terminal window appears effectively as a write only terminal interface, and all its input comes from the trusted switch connected to a keyboard. Thus no acknowledgements are necessary to the window.
position so that the low side and high side X servers synchronise their notions of the actual mouse position. In addition to resynchronising the mouse, all the low side client's windows must be redisplayed. This is to ensure that any modifications to these low side client windows, such as iconisation and resizing/repositioning, performed in a classified session are reset to the same state as they are in the unclassified session. The resynchronisation is handled by an Interactive Link management process on the low side network. Whenever the Interactive Link changes security state and the trusted switch moves to the low side a resynchronisation request is sent from the Interactive Link to the Interactive Link management process which handles the mouse repositioning and the updates of all the low side application windows.

In addition to the synchronisation problems described above, the data diode causes a referential integrity problem between the high side X server and the low side X client. As shown in Figure 5, the X server passes back information in replies to an X client. As an example, consider the launch of a new X client. Upon the successful request of a new X connection from an X client, the X server responds to the X client with a connection accepted packet. As well as containing information on the display geometry (bits per pixel, screen size, motion buffer size etc.) the packet contains specific connection set-up information which the client will need to create and reference resources. This information includes the resource-id-base and resource-id-mask for the client. These two values specify how the client constructs resource identifiers for its windows and graphics contexts etc. Resource identifiers constructed using these values are uniquely identifiable by the X server as belonging to this X client. These resource identifiers are then used by the client to reference its windows, graphics contexts, drawables etc. The security policy and data diode disallow this information to flow to the low side. The low side X server can respond with this information but the resource-ids will be different to those that the high side X server issues. Hence the resource IDs used on the low side do not correlate with the high side IDs. This leads to what we have termed a referential integrity problem.

To overcome this problem, a process is needed that maps the resource-ids issued by the low side X server to the resource-ids issued by the high side X server. The high side dummy X client shown in Figure 6 performs this role. It sits on the high side network between the high side X server and the low side network. When the high side X server issues resource-ids these are captured by the high side dummy client. As the low side X server receives duplicate X protocol requests it will also issue resource-ids which will be used by the low side X client. The replies from the low side X server are copied to the high side network. These replies are captured by the high side dummy client, which stores them in a mapping table. Hence, whenever the low side X client later uses the resource-ids issued by the low side X server these are mapped into the appropriate resource-ids for the high side X server by the high side dummy client. This mechanism extends to other X resources provided by the high side X server such as colour resource management and allocation, font information, and atom management.

Note that some products, such as Xmx, are able to provide the resource-id translation required for remote display applications. However, the Interactive Link solution provides full X Server mirroring capability, true acknowledgment decoupling, and greater support for the X protocols.

4. Discussion

The Interactive Link enforces confidentiality between the networks using the data diode. The only way security sensitive information can be passed to the low network is via the keyboard and mouse which are under user control. We assume that the user of a classified network is trusted not to retype classified information into an unclassified window. The user has access to a trusted display which indicates which network is receiving keyboard data.

4.1. Auditing

Accreditable auditing mechanisms for the Interactive Link can be incorporated as shown in Figure 7. In this setup, network based auditing is being implemented with the audit machine acting as a gateway to the unclassified network. For the Interactive Link to communicate to the low side proxy X server it must pass all its communications through the dedicated audit machine. Thus, the audit machine can not only log all keyboard and mouse events on a per user basis, but also, if necessary, log all display commands communicated back from the low side proxy server. This allows an auditor to determine and visually inspect an Interactive Link session. As long as the low side connection cable is physically secure (as indeed it typically is in military installations employing system high networks), the audit path can be considered trusted, as only the interactive links (trusted) and the audit machine, are on the audit data path.

60
Covert Channels

The implementation of the data diode is via trusted software in the prototype Interactive Link. The basic algorithm makes use of the traditional producer consumer paradigm applied to model concurrency. Essentially, packets are transferred from a producer queue in which packets from the low network are placed, and deposited in a consumer queue from which the packets are then transmitted to the high network.

When a packet is received from the low network, the Interactive Link may acknowledge its receipt. The critical security condition which must be satisfied by the Link in order to prevent the emergence of a potential covert channel is to ensure that packets can only be placed in the consumer queue at a set rate. This rate is determined by implementing a predetermined set of time slots for transference from the producer queue to the consumer queue. As long as the opportunities for transference between the queues occur at a set rate, and there is no acknowledgement of the transfer, the producer queue itself can send acknowledgements, even queue full messages back down to the low network. We call this mechanism a low side choke. That is, the low side of the system deliberately throttles the movement of data.

The advantage of this approach is that while overflow and packet loss can occur, it is much reduced as corrupt packets are retransmitted, and the low side can detect a full producer queue. The disadvantage is that the full network capacity cannot be utilised due to fixed time slots for data transfer, and for a reliable connection, this must be less than the maximum permitted data bandwidth. In this case, packet loss due to a full consumer queue will become more apparent. Note however, even with packet loss, the situation is not that disastrous since this can and does happen with any X window system. For display data, the ubiquitous "refresh" command can be initiated.

A potential covert channel exists by manipulating the display commands to force the user into a predetermined course of action by which information can flow from the high side to the low side. As a simple example, take the case of a user wishing to save their document within their unclassified word processor. If the document is new and untitled the "Save" command will be disabled. The malicious high side server could intercept the display commands for the pull down menu and change the ordering of the "Save" and "Save As" options (see Figure 8). The change in mouse positioning acts as a covert transmitter to the low side. There are a number of pitfalls and limitations with this method. The obvious one is that the user complains to the system administrator on the annoying and frequent menu order changes. It can be shown (using Nyquist's theorem) that the bandwidth of this channel is approximately:

\[ H \log_2 N \]

Where H is the average rate of mouse clicks per second, and N is the number of reorderable menu items.

There are a number of variations on this theme that provide higher bandwidths and are less susceptible to detection. Some of the possibilities for implementing a covert channel are:

1. Change the complete ordering of a menu list. This method works well when an application has disabled all but one item in a menu list. Given that there are n items in the menu the covert channel is equal to \( \log_2 n \) bits. For 10 menu items this would equate to approximately 3 bits of information per mouse click.

2. Vary the placement of sub-menus. This is similar to changing the ordering of common menu items, however it works by changing the position of pop-up sub menus to the left or right of the main menu (see Figure 8). This covert channel is limited to one bit of information per menu selection.
selections are prone to detection.

4.3. Related Work

The Interactive Link is significantly different from previous attempts to connect workstations to classified and unclassified networks. These attempts included a simple mechanical switch connected to the network I/O port of the workstation. However, all suffered from a potential vulnerability if trojan horses were resident on the untrusted workstation. That is, a trojan horse could easily store data for transfer to and from the classified network after a switch. Previous work [18] proposed the addition of a “purge” function, i.e. a workstation had to return to a known state before a switch from a classified to an unclassified network took place. However, implementing such a purge, e.g. rebooting the machine, in a trusted fashion is a nontrivial exercise and can cause significant delays in user operations. In addition, it is not at all clear how such purge functions can be implemented in a trusted fashion on an untrusted workstation. The Interactive Link provides a solution which does not suffer from this problem.

Other work in this area [10] has used encryption devices to provide a trusted pathway. This approach relies on encryption devices placed between the keyboard, the workstation's display unit, and the untrusted workstation. Data transferred from the input/output devices is intercepted, encrypted and passed on to the untrusted workstation. The data is then relayed, typically via an untrusted network, to a trusted secure host computer. The trusted host computer decrypts the user's commands, and then sends back encrypted display packets. These packets are relayed by the untrusted workstation to the decryption unit before being displayed. The Interactive Link differs significantly from this approach, by allowing unclassified sessions on classified untrusted workstations without the need for encryption.

Several extant systems such as the Ops/Intel Interface (OII) [7] are based on the Compartmented Mode Workstation (CMW)[17] concept, which provides multi-level security via a hardware and software Trusted Computing Base (TCB). These systems can be handicapped by the continuing need to re-evaluate systems as the hardware, software and network environment change. We claim that the Interactive Link, being a retrofittable hardware product which does not change with workstation upgrades, places the minimal possible trust in software and no trust in the host operating system thereby minimising the impact of these delays and costs. In addition, since the basic configurations of the networks into which the Link is to be inserted assume no trust in components other than the Link, reaccreditation of the network is simplified when hardware and software upgrades are performed. Indeed, the main
accreditation issues are focused on the security boundaries and communication link topologies which are part of any isolated system high network.

The Ops/Intel Interface itself appears to be a variant of the “man in the middle” system, requiring dedicated human review to manage information flow between networks. As with the Interactive Link, the OII user is trusted to handle data correctly at the correct classification; unlike the Interactive Link, specific users are required to manage all cross-network data flow. However, the OII has a data downgrade path; the base-level Interactive Link does not allow this functionality - high to low data downgrade is not supported by the basic model. Trusted downgrading, i.e. cutting from a high window and pasting into a low window, requires the use of an additional Starlight module which can be fitted to the Link to enhance its capability[4].

5. Conclusion

The Interactive Link enables a high assurance method of achieving multi-level network connections without sacrificing interactive connectivity.

Since the only trusted components to enable the Interactive Link capability are a diode, switch, and associated display (the most simple trusted components to implement), the trusted implementation of the Interactive Link is markedly simplified and high assurance levels are achievable without exponential evaluation cost curves due to implementation complexity.

Many accredited system high networks can be retrofitted with Links in a manner which enables the assurance of the Link to cover the entire network, thereby enabling these networks to be interconnected with others at a much lower classification level.

The Interactive Link concept is the subject of international patent action and the technology is now being transferred to Australian defence industry for development and subsequent fielding in the Australian Defence Force as part of a major command and control capability project.

6. References