PROCEEDINGS OF SCIENCE

IS Security in a World of Lightpaths

Robin Tasker
Science and Technology Facilities Council, Daresbury Laboratory
Warrington, Cheshire WA4 4AD, UK
E-mail: r.tasker@dl.ac.uk

IS Security is a cornerstone for the delivery of consistent and reliable services in every aspect of the business of an organisation. The traditional IP network service provided to Institutes is carefully managed and controlled to limit illegal and/or antisocial use to protect the business processes of that Institute. SuperJANET5 has the capability for additional bandwidth circuits - lightpaths - to be provided between specific endpoints across the network to meet specific need. Because these are end-to-end circuits they reach right into the heart of an organisation, typically providing a high bandwidth interconnection, and often at rates that are difficult to police. This paper explores this problem space and provides a strategy to minimise any associated risk through the development of an appropriate Security Policy that can sit alongside an Institute's overall approach in this area.

.

Lighting the Blue Touchpaper for UK e-Science - Closing Conference of ESLEA Project
The George Hotel, Edinburgh, UK
26-28 March, 2007

PoS(ESLEA)022

1. Lightpaths and IS Security - The Problem Stated

Organisations typically invest considerable resources into the provision of Information Systems (IS) Security to protect their core business operation from the many threats posed by their connection to the wider Internet. This provision will be specified in the IS Security Policy of the organisation which should provide clear instruction as to what is, and what is not, permitted with respect to any activity that make use of the IS of the organization [1]. To that end employees will almost certainly have signed their acceptance of these rules of usage as a condition of their employment. In this respect an employee's access to IS resources is conditional upon this agreement.

An IS Security Policy is normally realised through a range of technical solutions which manages the interaction between IS within the organisation and IS located remotely and beyond the jurisdiction of the organisation. The most common of such solutions is the firewall which through its associated rule-set determines what is, and is not, allowed to pass between the trusted organisational network and the untrusted generalised Internet. There are other measures that are commonly used that taken together provide layered "onion skins" of measures to protect the organisation.

The availability of lightpaths – in reality end-to-end circuits provided in addition to, and typically at rates at least equal with, the general commodity provision – challenge the IS Security *status quo*. Such provision will necessarily reach right into the heart of an organisational network with the potential to bypass any or all of the existing security measures in place.

Further, such lightpaths will be provisioned to allow collaborations across communities to develop and thrive. These virtual organisations (VO) and the individuals they represent cannot be bound by the IS Security Policy of any one single organisation. A member of a VO might expect to be bound by the IS Security policy of the VO but of course that person will physically reside within a home organisation where that organisation's IS Security Policy will have primacy [2].

It is clear that this model of operation will increasingly become the norm and there will be an expectation that the potential for conflict outlined here will be routinely handled to everyone's satisfaction.

2. Developing a Lightpath IS Security Policy

The purpose of developing a distinct IS Security Policy for a lightpath is to mitigate those risks associated with the delivery of the service associated with the lightpath. In essence the risks to service are no different from any other production network [3]. There are however two significant additions to this conventional perspective. Firstly the exceptional data rates expected over such a network means that conventional security access devices may not provide sufficient or adequate protection; and secondly, the lightpath network is designed to closely couple administratively distinct institutes to deliver the service that it carries. In setting the scene, the

IS Security Policy should address the purpose of the lightpath network, any associated assumptions that are made, and its intended audience [4].

2.1 Policy Purpose

As with any other IS Security policy it is good practice to state the purpose of the service for which the policy provides protection in terms of what it does and why that makes a difference.

2.2 Policy Assumptions

For lightpath networks the assumptions described in the lightpath IS Secuirty policy are crucial because almost certainly there will be a statement that each site that connects to the lightpath network will take its own view on what is and is not acceptable with respect to Information Security. That is to say the site IS Security policy will take precedence over the lightpath IS Security policy. Furthermore there will almost certainly be the expectation that the lightpath IS Security policy does not supersede or invalidate any local IS policies at any local site, and should the lightpath policy conflict with any local site policy then the local site policy will take precedence for that site. It is reasonable to assume that each site will assess suitability of access to the lightpath based upon the specification and implementation of its own local IS policy. The collorally to this assumption is that sites will only be allowed access to the lightpath network once they have agreed to follow the lightpath IS Security policy.

2.3 Policy Scope

Of crucial importance is a clear detail of the scope of the lightpath IS Security policy with respect to the set of rules which govern the right to transmit or receive data across the lightpath network. Certainly the better the specification of the data flows across the lightpath network, the more precise can be the specification of those rules.

The Scope should also provide a statement that each site ensures that any traffic for which it is responsible is generated in accordance with the lightpath IS Security policy. Further the list of sites - the members - that are authorised to make use of the lightpath network must be clearly specified.

Where a site does not agree to implement the lightpath IS Security policy, all other sites connected to that network and that have agreed to the policy may reject all transmissions from the site and in that manner protect themselves from some undefined or unspecified risk. Where a site attempts to use the lightpath network in a manner beyond its declared and agreed purpose any traffic resulting from such usage may be discarded by any member site without warning or notification.

2.4 Governance - Roles and Responsibilities

It is important that for each member site, a security contact is nominated and advertised and it is that person's responsibility to engage with the local site IS Security officer in all matters relating to the use of the lightpath network at that site. Furthermore it is to be expected that the local site IS Security officer at each site will be satisfied with the mitigation of any

information security risk associated with that site's connection to the specified lightpath network. This mitigation is achieved through the implementation of the lightpath IS Security policy and the nominated representatives will be responsible for all necessary on-site liaisons with the local site to obtain a formal record from the local site's IS Security officer of acceptance and implementation of this policy.

Changes to the lightpath IS Security policy must be discussed and agreed by the nominated representatives with any resulting operational changes taking place only at specified advertised times once agreement has been reached.

2.5 Governance - Legislation and Compliance

It is reasonable to expect that each site will act in accordance with any national or international legislation applicable in that country to the operation of a data network. Further the nominated representatives should be expected to ensure that the member sites are aware of any such matter that bears upon the operation of the network..

The nominated representatives might be expected to work with the local site IS Security officer to demonstrate compliance with the lightpath IS Security policy with the output from such a review being shared with the other nominated representatives to ensure broad dissemination.

2.6 Technical Considerations

An IS Security policy will contain very specific technical detail which provides the guidance on how the policy is to be delivered. The detail is clearly beyond the scope of this paper and will most certainly vary from one policy to another but may include statements with regard to, for example, IP routing, IP protocol usage and access control.

2.7 Procedural Matters – Incident Handling and Reporting

Security incidents are never planned and take no account of convenience. It is therefore vital that an IS Security policy states clearly and concisely the action to be taken should such an incident arise. An IS Security policy for a lightpath network is no different except that it will require the engagement of the nominated representatives together with the IS Security offices for each member site so that the composite risk might properly be assessed and accommodated.

3. Conclusions

At the time of writing and within the UK academic network there are already in excess of a dozen lightpath networks in use, and with the advent of SuperJANET5 this trend will accelerate. In so doing the complexity of the inter-connections between sites will grow as a consequence the associated risks will increase. It is not clear yet whether issues of lightpath network security are taken seriously. Certainly there remains a tension between the site network service providers and users of these lightpath networks who are concerned that precious performance may be impacted by the requirements for security. There is a case to be made on both side of this debate, however it is clear that a site's IS Security policy will be dictated by the business needs of the organisation and its ability to manage risk. To do so account must be

taken of any component that increases the risk to an organisation, and an *ad hoc* lightpath network most certainly increases that risk.

This paper describes a proactive approach which seeks to balance the needs of the service provider with those of a user of a lightpath network. An open and transparent approach serves both sides best and to achieve that end clear lines of communication need to be established and exercised through the lifetime of a lightpath network.

References

[1] UCISA, Information Security Toolkit, Edition 2.0 (2005), ISBN 978-0-9550973-0-4

[2] Kelsey (ed.), Grid Security Policy, https://edms.cern.ch/428008/4

[3] UCISA, Exploiting and protecting the network, Edition 3.0 (2006), ISBN 978-0-9550973-1-2

[4] LHC Optical Private Network Information Security Policy, https://edms.cern.ch/file/708248/LAST_RELEASED