Australian Academic and Research Network

Draft Policy on Network Security

Draft D

1. Introduction

While the Australian Academic and Research Network (AARN) offers great advantages to its target community, it also increases the exposure of its members to security risks.

The basic premise of the AARN is that the benefits gained are worth the risk. For this to be true, a sensible security policy is required. This policy must provide as much security protection as possible, while encouraging the sort of liberal access essential to an academic and research environment.

This requires a co-operative attitude from all AARN members. Without this co-operation, the risk of serious damage from a determined hacker attack will be greatly increased.

2. AARN security policy

The policies of the AARN are to ensure that the Network itself is as secure as reasonably possible, to encourage member institutions to protect themselves, and to ensure that security problems can be isolated and stopped as quickly as possible.

3. Security aims

The security aims should be as follows:

* The AARN and connecting institutions must offer assistance to identify and eradicate intruders (hackers) using the Network in an un-ethical fashion.

* The Network must have good protection against eavesdroppers.

* The Network must have good protection against data corruption or loss.

* The Network must have good protection against denial-of-service problems.

4. Site responsibilities

4.1 Protection against security attack via the Network

The Network itself is very secure. However, the Network of its nature provides a communications aid to the intruder, as well as legitimate users.

All AARN sites must be made aware of the security implications of connecting to the Network. Despite other parts of this policy, the AARN cannot protect a site from attack from within the AARN community.

Every connecting site must accept responsibility for protecting its own security. The increased population of potential hackers, and the more effective communications available, mean that sites will probably have to increase their attention to security, particularly in advising on security for systems not under professional supervision.

Each connecting site should consider particularly carefully the legal and other implications of connecting systems with confidential, secret, commercially valuable or financial information.

4.2 Co-operation with other sites

Connecting sites acquire an obligation to give high priority to assistance to other sites in tracking down and eradicating security attacks that appear to originate within their site, or which use their site as a conduit.

4.3 Authentication policy

It is desirable that remote login access across the Network is only made by authenticated users at member or affiliated institutions.

It is desirable that no remote login access should be allowed direct to the Network from devices such as terminal servers which do not authenticate their users. In theory this permits tracking an attack back to an authenticated user at a particular site, where action can be taken.

4.4 Internal security

It is important that sites connecting to the Network have an adequate internal computer and network security policy. Security measures to reserve system/root privileges on systems connected to the network to highly trusted staff should be treated as a high priority by connecting sites.

It is desirable that connecting sites have a computing security policy with at least the following components:

* users should be authenticated (see 4.3)

* users should not access other users data, files or passwords unless specifically authorised

* users should not access external networks unless specifically authorised

* users should not offend, harass or inconvenience others.

Inadequate attention to internal security, with evidence of security attacks exploiting this lack, could be grounds for disconnection of an institution from the Network.

5. AARN responsibilities

5.1 Co-operation with AARN sites

The AARN organisation will co-operate fully with sites experiencing security attacks, and will co-ordinate efforts with other institutions, PTTs and attached networks, to identify and eradicate the attacks.

5.2 AARN Network Attachments

Only devices approved by the AARN Management may be attached directly to the Network backbone and the associated "closed" Ethernet.

5.3 Network Data Security

The AARN should provide adequate security for data traversing the network. Data on the network should not be inspected unless absolutely essential for network operation or security reasons. AARN staff and staff at regional nodes must have a duty of confidentiality to all network data.

It is undesirable that network data should traverse other institutional networks. Where this is necessary, the intermediate institutions should acquire the same duties of confidentiality.

The AARN will not initially use encrypted data links. Connecting institutions should use end to end encryption for highly sensitive data.

5.4 Security development projects

The AARN will set aside a portion of its budget for development projects in the area of security. Such projects could include portable file encryption software, digital signature techniques, etc.

The AARN will ensure that it is kept informed of network security developments, for example in ISO or IEEE 802 standardisation processes.

The AARN will identify a person to act as Security Officer.

5.5 Additional Security Measures

AARN Management may take additional security measures within the spirit of this policy as they see fit.

Chris Rusbridge
AARN Steering Committee

17 August, 1989