Surveillance and Protection in IBC Management
The Applicability of Two RACE Security Projects - SecureNet II and SESAME

Dimitris Androutsopoulos (Expertnet), Per Kaijser (Siemens Nixdorf);
Socratis Katsikas (Univ. of Aegean), Kåre Presttun (Alcatel), Don Salmon (ICL),
Paul Spirakis (Univ. of Patras)

1. Introduction and Scope

This brief note considers the potential usefulness of security technology being
developed under the RACE programme to the management of very high-
performance telecommunications services.

Realization of the full potential of the very high performance communications
technologies will depend on the availability and effectiveness of supporting
intelligent control and management of the environment and infrastructure, allowing
the delivery of end user services offering significant benefits in areas such as
mobility, dependability, security, usability, as well as plain basic bits-per-second-
per-ECU. The raw performance and facility levels will be of little benefit without
the means to deploy the capacity in line with a wide spectrum of demands spanning
- bulk commitments for, say, delivery of cable-tv and on-demand video,
- high instantly available bandwidth for virtual private networks,
- absolute priority needs of emergency services,
- and so on down to the humble phone conversation or public electronic mail
  service.

To achieve simultaneously the quality needs of this set of clients, the management
and administration of the networks and services must have at its disposal two sets
of tools:
- to control the configuration and operation of the users and resources to the
  necessary degree of fineness;
- to have the relevant information about the status - dynamic and static - of the
  resources and users.

To exploit the full flexibility and potential of the new technology, the management
and administration of the networks and services must be partitioned and distributed.
The realization of Open Network Provision, operation of Virtual Private Networks,
flexible trading of bandwidth etc. depend on the ability to hand-over with confi-
dence aspects of network control to sub-operators, service providers or clients.

But having been sub-divided, the management processes must be no less well
protected; on the contrary, they need additional and stronger protection than when
they could be concealed behind locked doors. The distributed components require
control over who or what may use them, and what they may do to other network
components; rights and privileges must be precisely delineated, and responsibilities
allocated; access controls and accountabilities need to be provided; relationships
between the distributed management components, and between them and their man-
aged resources must be controlled and protected. The protection provided must in turn operate within a fragmented, distributed environment, and itself be subject to distributed management.

The management information process, as well as collecting the normal MIB information through specified management interfaces and processes [1], must also maintain a view of the status of the system and sub-systems from observation of other aspects of behaviour. It must then collate, interpret, infer, recognize, and present status and warnings of attack to the relevant control processes for action.

2. Security Requirements in IBC Networks

All the recitals of threats in the standards literature [2], [3] apply to the network and the services, but the major threats to the integrity, availability and continuity of services arise from the ability to maintain management control over the operations in the face of malicious or accidental human instigated actions, technical malfunction, or natural mishap. The concern here is to provide for the secure distributability of management processes, secure intercommunication, the accurate recognition of actual or threatened problems, and the ability to prevent or to recover from such problems by management actions.

Probably the single biggest threat to the network is still the penetration of the management and control processes, whether by accident, mindless vandalism or malicious attack. Current methods of two-key operations in locked rooms are no longer appropriate to the scenario described above requiring de-centralization and dispersion of controls. A further major threat is iatrogenic: the intelligence in the network getting it wrong by mis-diagnosing a problem, and doing all the wrong things to try to fix it - the downward spiral of misguided re-routing attempts, say. Hence the emphasis here on the need for sound surveillance - the counter-insurgency forces can only be as good as their intelligence gathering.

3. Areas covered by RACE projects

The principal RACE projects addressing this area are:

SecureNet II (R2113): threat recognition and identification;
SESAME: (R2051): security services and protocols.
Samson (R2058): development of a framework for the management of security [4];
Prism (R2041): Reference configurations for TMN

SecureNet II and SESAME are the subjects of this note.

3.1 The Role of SecureNet

However carefully one designs the security mechanisms of a network, certain vulnerabilities are likely to exist, as a result of either design decisions related to criteria such as cost or simply poor design. Therefore, no set of security