British Telecom URI Security : Project Outline

Paul Wernick

28th July 1995

1 Introduction

This document describes in outline the environment and objectives of the research which forms Work Package 5 (Security) of the BT URI Management of Multiservice Networks project.

The overall objective of the project is to provide a security architecture designed to provide the functionality and flexibility required for the telecommunications systems of the future. The main deliverable from the project will therefore be a high-level architecture [ftBTUP95] which will provide a design outline for implementers of comprehensive security mechanisms for multiservice networks. As part of the work to be performed towards this objective, some implementation work is to be performed to test the validity of the concepts involved.

Our thinking behind our work to date on the URI Security project is described in greater detail than is possible in this summary in [ftBTUP95], and the first implementation stage is examined in more detail in [Imp95].

2 The Multiservice Network Environment

The emerging public switched networking technology of ATM extends the possibility of creating new services which can make use of the bandwidth and flexibility which may soon be available. Interactive and high-bandwidth applications will become either cheaper and therefore more accessible, or feasible. These services will be capable of association with computer-based data storage and retrieval mechanisms to provide a rich consumer-oriented environment.

The capability for the provision of new types of services based on easily-accessible searchable databases has already resulted in the emergence of new categories of participants; customers/end users, service providers and network providers. As what is currently a technically-oriented niche becomes a generally-available portfolio of services, each of these is expected to increase greatly in number. Additionally, new sub-types of service providers are emerging or will arise; these might be described as wholesalers and retailers of information/services, and advisors or brokers on the obtaining of information, to specialists and the non-technical general public.

Future networks will also support different mechanisms for co-operative working. They will, for instance, provide the potential for sharing access to, and responsibility for modification of, information among several users in a session. It will be possible for two people at different locations to combine to edit a document, with a simultaneous audio-visual link being provided as part of the same service; see for example the scenario in [CM95, p.7-4].

In parallel with this, network carriage deregulation is likely to result in more than one path from a customer to a particular information or interactive service being available, and/or paths from a customer to a service passing through more than one network carrier's facilities. Mechanisms to support such multi-carrier connections will need to be transparent to the customer, but provide control over access.

3 Specific Security Issues

As the environment and functionality of the telecommunications network has changed, so the security implications of this have become more complicated.

Some of these issues are considered to be within the compass of the URI security architecture; others have been deliberately excluded. These issues relate to the provision of services, the management of the provision of services and the environment within which those services are provided, and the recording where applicable of the use made of, and actions taken concerning the use and management of services.

Those security-related issues which are to be addressed within the architecture include:

- the new actors envisaged as taking part in the multiservice networks introduce new security implications. The single point of service access which it is hoped that customers will see is in fact the nexus of a number of services provided by competing retailers through competing networks, and access to and between such services will need to be controlled;
- the complexity of future networks, requiring network management activities to cross administrative and security domains – the potential for TINA[1]-compliant systems to include customer equipment is an example of a change of thinking with wide security implications ([CM95, p.3-1]).
- the growing importance of delegation, subject to limits, as a means of providing wholesalers and retailers with a measure of control over their environments, and of allowing customers to control access within their own environments (for example limiting access to adult services)
- the greater complexity of usage and activity information needing recording for audit trail and and billing purposes. The information needed for this will be more widely diffused through the telecommunications systems, and this information will need to be secure, so that it can be trusted by all parties involved;
- many of the complexities of the new networks will require logging facilities, which must be secured [duplicate of directly above?]
- since remote network management using the same physical links as network users will become the norm as ATM is introduced, the security implications of this must be addressed and network control traffic made secure; and
- some legal issues requiring access to and control of data to be secured; such legal issues include concerns over privacy, copyright/intellectual property, contract and billing, proof of service use/provision, and the need to discharge a duty of care between parties entering into the complicated technical and legal interactions made possible by multiservice networks.

There are other issues which are related to a generally-applicable security architecture, but which we have chosen not to consider at this stage. These relate in the main to control over the provision of and access to specific types of data and data elements within services, such as licencing and censorship laws/regulations – state, national, international – and the implications of differing regulations in cross-border data transmissions. The use to be made of the facilities provided by multiservice networks will be affected by the then-current view taken by society as expressed in, for instance, currently proposed legislation such as the Exon Bill in the United States.

The decisions which we have made concerning the scope of the project are reflected in the explicit assumptions documented elsewhere in this volume [ftBTUP95].

[1] Telecommunications Information Network Architecture

4 Approaching the Problem

The URI Security project has a five-year time-span. We have taken advantage of this to take a measured approach to the security issues which it raises. This approach is also necessitated by the rapidly-changing environment which the security architecture will have to support.

The first step which we have taken in addressing these problems has been to make explicit the assumptions under which implementations of the URI security architecture will have to operate; these are presented elsewhere in this collection [ftBTUP95]. These assumptions reflect technical, managerial and social issues. To prevent the architecture from becoming obsolete, it is necessary to take such matters into account. For instance, it is assumed that technical change will continue. One of our objectives in this project is that the architecture should be capable of outlasting the life of technical implementations such as the coming ATM networks.

For the security viewpoint of the network provider, we have relied on two documents written by British Telecom staff for TINA, [Hub93] and [HRG94]. Our thinking has diverged from that of these documents referred to previously in some respects. In particular, we have placed less emphasis on supporting customer billing, regarding the logging mechanisms necessary for security as an adequate basis for calculating the necessary values. We have also emphasised the place of wider society as a stakeholder in the systems. In contrast, TINA confine their stakeholders to those directly associated with the provision, support and use of services.

Our next research activity is to be a trial implementation of security mechanisms over a number of distributed ATM management functions. This work will allow us to to test the validity and usefulness of the assumptions which have been found to date. In keeping with the guidelines for longevity, the approach to the implementation is to avoid any of the technical specifics of networks or software environments.

5 Summary

Research into the security requirements of the URI project has provided us with the opportunity to raise theoretical and general issues related to the provision and management of remote multiservice networks, and examine them in the context of an implementable architecture and a concrete trial implementation.

References

[CM95] M. Chapman and S. Montesi. Overall concepts and principles of TINA. Technical report, TINA, Feb 1995. Document Label TB_MDC.018_1.0_94.

[ftBTUP95] Assumptions Made for the British Telecom URI Project. Paul wernick. In Richard Black, editor, *ATM Document Collection 4*, chapter 9. University of Cambridge Computer Laboratory, September 1995.

[HRG94] S.D. Hubbard and M.A.Z. Rejman-Greene. TINA: Security guidelines for TINA. Technical report, British Telecom, Mar 1994. Version 1.0.

[Hub93] S.D. Hubbard. TINA: Internal team task 1 core security requirements for TINA. Technical report, British Telecom, Nov 1993. Version 1.0.

[Imp95] URI Security Architecture: Trial Implementation. Paul wernick. In Richard Black, editor, *ATM Document Collection 4*, chapter 10. University of Cambridge Computer Laboratory, September 1995.