Key words: Data Security, Security Architecture, Data Communication, Open Systems, OSI, FTAM

Abstract

An architecture for building secure open systems communicating via untrusted global data networks is presented. The work is based on the ISO OSI reference model and its security architecture addendum but the results are directly applicable to virtually any layered communications architecture such as the DoD Internet architecture (TCP/IP). Also, several extensions and modifications to the OSI model are suggested.

A semiformal model for the security of communications between peer entities within an OSI layer and between entire application instances is presented. This model, along with some new concepts introduced, is successfully used to analyze the security functions of open systems. This work brings a whole new research area at the boundary between formal protocol research and cryptology within the reach of formal study. Complete formalization of and further elaboration on the model are beyond the scope of this work and left for further study.

The degree of freedom offered by the OSI Security Architecture in placing the security services and mechanisms defined in the OSI reference model into its layers is restricted in such a way as to not affect the security of the over-all communication service and well-founded placements for various services and mechanisms are proposed.

In order to demonstrate the implementability of the solutions proposed here, actual low-level security mechanisms are chosen to fill in the missing parts. Finally, a communications profile for secure FTAM is drawn up and a subset of it is implemented based on existing OSI implementations.

 © Arto Karila, 1991

Foreword

This paper is a cosmetically updated version of my Doctoral Dissertation completed in late 1990 and defended in March 1991 at Helsinki University of Technology.

This work is based on the experience of several years of protocol implementation work with the Technical Research Centre of Finland and my more recent experience in the development of value added services for our customers at Telecom Finland. The approach is rather pragmatic (for a dissertation) and the problems are taken from real life. I hope this paper will serve a purpose in raising the general level of consciousness of the security risks of open systems and stimulating discussion and research in the area of developing secure open systems.

I hope my possible American readers will not be scared off by the seeming OSI-orientation of this work. I am by no means an OSI pedantic and most of the results obtained here are directly applicable to other layered communications architectures such as the DoD Internet (TCP/IP) architecture.

I wish to thank my reviewers Dr. Kaisa Nyberg of the Finnish Army and Dr. Olli Martikainen of the Technical Research Centre of Finland for their constructive criticism and many comments on the draft versions of this paper. I also thank professor Jarmo Harju of Lappeenranta University of Technology for the many discussions on this topic at the early stage of this work. I thank my opponent professor David Farber of University of Pennsylvania, who urged me make these minor changes to my work and make it publicly available through the internet, for his careful examination of my thesis and the stimulating conversations with him in March 1991.

Comments, suggestions, corrections and critique are welcome.

Helsinki, Finland, May 31, 1991

Arto T. Karila

 © Arto Karila, 1991