Survivable, Real Time Network Services

Final Technical Report

Defense Advanced Research Projects Agency
Contract F30602-98-1-0225, DARPA Order G409/J175

David L. Mills
University of Delaware

1 April 2003

Abstract

This document is the Final Technical Report on Contract F30602-98-1-0225, DARPA Order G409/J175. It contains material reformatted from the web pages that are the intended final product of this project. The web pages contain an extensive network of links embedding them not only in the framework of this project, but in the framework of other related projects and reference material. The links are not available in this published document.

The text in this document is generally taken verbatim from the web pages with certain minor changes to enhance readability in paper medium. The figures are taken directly from the pages, but rendered in greyscale. The equations have been redone to conform to software publishing requirements. The reference and bibliography material has been moved to the end of the base document.

This document includes the Autokey requirements analysis, design principles and protocol specification. A detailed description of the protocol states, events and transition functions is included. A prototype of the Autokey design based on this document has been implemented, tested and documented in the NTP Version 4 (NTPv4) software distribution for Unix, Windows and VMS at http://www.ntp.org.

Keywords: network security, public-key infrastructure, digital signatures, computer time synchronization

Table of Contents

List of Figures

List of Tables