Network Security Mechanisms and Implementations for the Next Generation Reliable Fast Data Transfer Protocol - UDT

Danilo Valeros Bernardo

A THESIS SUBMITTED AS

A PARTIAL REQUIREMENT FOR

THE DEGREE OF DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

OF

THE UNIVERSITY OF TECHNOLOGY – SYDNEY

AUSTRALIA

School of Computing and Communications

Faculty of Engineering and Information Technology

The University of Technology – Sydney

Australia

The shades of night were falling fast,

As through an Alpine Village passed

A youth, who bore, 'mid snow and ice,

A banner with the strange device,

Excelsior!

– H. Longfellow

CERTIFICATE OF AUTHORSHIP /ORIGINALITY

I certify that the work in this thesis has not previously been submitted for a degree nor has it been submitted as part of requirements for a degree except as fully acknowledged within the text.

I also certify that the thesis has been written by me. Any assistance I have received in my research work and the preparation of the thesis itself has been acknowledged. In addition, I certify that all information sources and literature used are fully indicated in the thesis.

Signature of Candidate

_____

Acknowledgements

Completing a rigorous PhD by research in half the required maximum number of years is a feat that not many can achieve, especially when there are demanding work commitments to meet outside the academia.

This milestone obviously is not possible without the support of many people.

It is therefore only audaciously appropriate to thank the members of the Faculty and i-Next and staff of the University Graduate School (UGS) for their support, and especially for the interests, advice, and assistance they provide to this project, and for their unwavering support in providing funding arrangements that resulted to a string of almost 22 peer-reviewed academic papers written and published about this work.

I wish to thank Prof. Doan B. Hoang, my thesis advisor and supervisor, who fostered good research and development of models, and helped ascertain that the focus of this work was within the specific area of research. His meticulous assessment and his honest feedback have been invaluable, leading to the improvement of this dissertation. His recognition of my strong academic and research capabilities have been instrumental, prompting the University to waive the coursework requirements which would have extended additional years of arduous challenges. His advice on the importance of the use of citations and references, which in their absence can lead to some issues for a student like me (who incidentally has a semi eidetic memory), has left me wondering if this ability of remembering information verbatim is a curse or a gift. Eventually, I obligingly consented to cite someone's work whenever necessary.

In addition, the encouragement and sheer independence I have been given in the development of this dissertation, whilst publishing 2 books and almost 18 additional research papers in other areas of interests, doubtless proved to be invaluable to my present and surely to my future research and consulting work.

Moreover, the work presented in this thesis would also not have been possible without the support, in the form of advice and research direction, of the following:

Dr. Yunhong Gu of the National Data Mining Centre at the University of Illinois, United States, now a software engineer at Google, who provided initial guidance in the implementation of UDT in a test environment, and provided invaluable insights that improved this work.

Nicolas Williams of Sun Corporation, United States, and anonymous reviewers for their constructive comments that helped improve the publications which supported and validated the overall work in the development of a few security mechanisms in this dissertation.

Prof. John Mitchell and Stephan Stiller of Security Laboratory, Stanford University, California, United States, for providing very comprehensive literature about Protocol Composite Logic technique: literature that helped improve the analysis of the proposed mechanisms for UDT.

Dr. Henry Leitner of Harvard University, for his rigorous classes in Computer Science that were instrumental in the development of the Project UDT Tool in Java.

The Australian Government for the Higher Degree Commonwealth Research Scholarship.

Friends and colleagues at NSW State Government.

Lastly and importantly, to my family for their continuing support in the countless journeys I take, including this journey, which I initially thought the longest to complete. Their support has always been the bedrock of my accomplishments.

Dedicated to DAB†, Linda, Beverly, Jojo, and Bee Bee

Abstract

TCP protocol variants (such as FAST, BiC, XCP, Scalable and High Speed) have demonstrated improved performance in simulation and in several limited network experiments. However, practical use of these protocols is still very limited because of implementation and installation difficulties. Users who require to transfer bulk data (e.g., in Cloud/GRID computing) usually turn to application level solutions where these variants do not fair well. Among protocols considered in the application level are User Datagram Protocol (UDP)-based protocols, such as UDT (UDP-based Data Transport Protocol). UDT is one of the most recently developed new transport protocols with congestion control algorithms. It was developed to support next generation high-speed networks, including wide area optical networks. It is considered a state-of-the-art protocol, addressing infrastructure requirements for transmitting data in high-speed networks. Its development, however, creates new vulnerabilities because like many other protocols, it relies solely on the existing security mechanisms for current protocols such as the Transmission Control Protocol (TCP) and UDP. Certainly, both UDT and the decades-old TCP/UDP lack a well-thought-out security architecture that addresses problems in today's networks. In this dissertation, we focus on investigating UDT security issues and offer important contributions to the field of network security. The choice of UDT is significant for several reasons: UDT as a newly designed next generation protocol is considered one of the most promising and fastest protocols ever created that operates on top of the UDP protocol. It is a reliable UDP-based application-level data-transport protocol intended for distributing data intensive applications over wide area high-speed networks. It can transfer data in a highly configurable framework and can accommodate various congestion control algorithms. Its proven success at transferring terabytes of data gathered from outer space across long distances is a testament to its significant commercial promise. In this work, our objective is to examine a range of security methods used on existing mature protocols such as TCP and UDP and evaluate their viability for UDT. We highlight the security limitations of UDT and determine the threshold of feasible security schemes within the constraints under which UDT was designed and developed. Subsequently, we provide ways of securing applications and traffic using UDT protocol, and offer recommendations for securing UDT. We create security mechanisms tailored for UDT and propose a new security architecture that can assist network designers, security investigators, and users who want to incorporate security when implementing UDT across wide area networks.

We then conduct practical experiments on UDT using our security mechanisms and explore the use of other existing security mechanisms used on TCP/UDP for UDT. To analyse the security mechanisms, we carry out a formal proof of correctness to assist us in determining their applicability by using Protocol Composition Logic (PCL). This approach is modular, comprising a separate proof of each protocol section and providing insight into the network environment in which each section can be reliably employed. Moreover, the proof holds for a variety of failure recovery strategies and other implementation and configuration options. We derive our technique from the PCL on TLS and Kerberos in the literature. We maintain, however, the novelty of our work for UDT particularly our newly developed mechanisms such as UDT-AO, UDT-DTLS, UDT-Kerberos (GSS-API) specifically for UDT, which all now form our proposed UDT security architecture.

We further analyse this architecture using rewrite systems and automata. We outline and use symbolic analysis approach to effectively verify our proposed architecture. This approach allows dataflow replication in the implementation of selected mechanisms that are integrated into the proposed architecture. We consider this approach effective by utilising the properties of the rewrite systems to represent specific flows within the architecture to present a theoretical and reliable method to perform the analysis. We introduce abstract representations of the components that compose the architecture and conduct our investigation, through structural, semantics and query analyses.

The result of this work, which is first in the literature, is a more robust theoretical and practical representation of a security architecture of UDT, viable to work with other high speed network protocols.

Publications

Most of the chapters that are presented in this dissertation have been accepted, published or have been submitted for publication in refereed /peer reviewed research journals and conference proceedings (IEEE, Elsevier, Springer Verlag – LNCS and IETF).

Research Accomplishments:

Served as Technical Session Chair at the Information Security Assurance Conference in Japan, sponsored by Springer –Verlag Berlin Heidelberg in 2010.

Served as research and technical reviewer for the following international journals:

- Computer & Security –Elsevier 2011, 2012
- International Journal of Earth Science Informatics - Springer Verlag 2012
- Management of Information Systems -MIS Review (MISR) 2012
- Open Access Journals – Network Protocols and Algorithms, sponsored by Polytechnic University of Valencia 2010-2012
- International Journal of Network and Information Security 2009

This research work was supported by UTS FEIT, i-NEXT and Vice Chancellor Travel Grants. This was also partly supported by industry Global Science and Technology Initiatives Grant sponsored by Db2Powerhouse Social Enterprise.

Best Paper Award

Bernardo, D.V., Hoang, D.B., (2010), 'Security Analysis of Proposed Practical Security Mechanisms for High Speed Data Transfer Protocol' 4th Information Security Assurance 2010, Japan, LNCS Springer –Verlag Berlin Heidelberg, June 23-25, 2010 (Book Chapter).

Outstanding Research Presentation

Bernardo, D.V., (2012),' Enciphering the Thoughts: Towards Achieving Ultimate Information Security', 3rd International Arts and Sciences, Harvard University Boston, USA, May 27-31, 2012 ,ISSN 1943-6114 (Conference).

Innovation Patents

Innovation in Encryption systems Patent 2012100172
Innovation in e-information systems Patent 2006100469

Portions of this work are published in the following publications:

Other/Books

Bernardo, D.V., (2008) i-Think 1st Edition: Selected Works in Business , Technology, Research and Innovation, March 2008, book paperback, Sydney, Singapore, UK and USA, ISBN 978-0-646-486- 543. http://nla.gov.au/anbd.biban42560289

Bernardo, D.V., Hoang, D.B., (2009) Security Requirements for UDT, IETF[3] (working paper), RFC Request for Comments, Internet and Engineering Task Force.

Bernardo, D.V., (2009) i-Think 2nd Edition: Selected Works in Business , Technology, Research and Innovation, March 2008, book paperback, Sydney, Singapore, UK and USA, ISBN 978-0-646-486- 543. http://nla.gov.au/anbd.biban42560289

International Journals

Bernardo, D.V., Hoang, D.B., (2011) 'Multi-layer Security Analysis and Experimentation of High Speed Protocol Data Transfer for GRID', *Int. Journal of Grid and Utility Computing (IJGUC)*, SN 1741-8488, ISSN 1741-847X. (by invitation)

Bernardo, D.V., Hoang, D.B., (2010), 'A Pragmatic Approach: Achieving Acceptable Security Mechanisms for High Speed Data Transfer Protocol – UDT', SERSC, *International Journal of Security and its Applications* Vol. 4, no. 3, ISSN 1738-9976.(by invitation)

Bernardo, D.V., Hoang, D.B., (2010),'Securing Data Transfer in the Cloud through Introducing Identification Packet, and UDT Authentication Option Field: A Characterization', *International Journal of Network Security and its Applications* ISSN 0974- 9330 and 0975-2307. (by invitation)

Bernardo, D.V., Hoang, D.B., (2009), 'Network Security Considerations for a New Generation Protocol UDT' *JCSIA- Journal of Computer Security and Information Assurance*, Volume 4 –Issue 4, 2009 , Dynamic Publishing, USA, ISSN 1554- 1010 (by invitation)

Book Chapters

Bernardo, D.V., Hoang, D.B.,(2011), Security Technology 2011," Formalization and Information-Theoretic Soundness in the Development of Security Architecture for Next Generation Protocol – UDT" Jeju Island Korea, LNCS Springer–Verlag Berlin Heidelberg, December 8-10, 2011 (Book Chapter)

Bernardo, D.V., Hoang, D.B.,(2010), International Conference on Future Generation Communication and Networking 2010, "End-to-End Security Methods for UDT Data Transmissions" Jeju Island Korea, LNCS Springer–Verlag Berlin Heidelberg, December 13-15, 2010 (Book Chapter)

Bernardo, D.V., Hoang, D.B.,(2010), 4th Information Security Assurance 2010, "Security Analysis of Proposed Practical Security Mechanisms for High Speed Data Transfer Protocol", Japan, LNCS Springer–Verlag Berlin Heidelberg, June 23-25, 2010 (Book Chapter)

International Conferences Publications and Proceedings

Bernardo, D.V., Hoang, D.B.,(2012), "Securing the Cloud, Dispelling Fears: An initiative" 16th IEEE Network Based-Information Systems (NBIS) Trustworthy Computing (TwC-2012) Workshop, Melbourne, September 26-28, 2012

Bernardo, D.V., Hoang, D.B.,(2012), "Symbolic Analysis of UDT Security Architecture " 26th IEEE Advanced International Network Information and Application -Workshop , AINA Fukuoka Japan, March 26-29, 2012

Bernardo, D.V., Hoang, D.B.,(2012), "Compositional Logic for Proof of Correctness of Proposed UDT Security Mechanisms " 26th IEEE Advanced International Network Information and Application AINA Fukuoka Japan, March 26-29, 2012

Bernardo, D.V., Hoang, D.B.,(2011), "Empirical Survey: Experimentation and Implementations of High Speed Protocol Data Transfer for GRID " 26th IEEE Advance International Network Information and Application –AINA and 8th FINA Frontiers Information Network and Application, Workshop Singapore, March 22-25, 2011

Bernardo, D.V., Hoang, D.B.,(2010), "A Conceptual Approach against Next Generation Security Threats: Securing High Speed Network Protocols " 2nd IEEE International Conference of Future Networks ICFN 2010 proceedings Sanya, China January 22-24, 2010

Bernardo, D.V., (2010), "UDT –AO Approach" 6th IEEE International Assurance and Security, sponsored by IEEE Intelligent Transportation Systems Society, Atlanta, USA August 23-25, 2010

Bernardo, D.V., Hoang, D.B.,(2009), 2nd IEEE ICCSIT 2009 proceedings re Network Security Considerations for a New Generation Protocol UDT, Volume 3, IEEE ISBN 978-1-4244-4519-6, Beijing China, August 8-11, 2009

Bernardo, D.V., Hoang, D.B.,(2009), 8th IEEE ICISM 2009 proceedings re Quantitative Security Risk Assessment (SRA) Method: An empirical case study , Coimbatore India, December 9 -11, 2009.

Bernardo, D.V., Hoang, D.B.,(2010), 4th IEEE International Conference on Emerging Security Information, Systems and Technologies SECURWARE 2010 re "Protecting Next Generation High Speed Protecting–UDT through Generic Security Service Application Program Interface GSS-API" Venice/Mestre, Italy , July 18-25, 2010.

The research work presented in this thesis has been performed jointly with

Prof. Doan B. Hoang

Head of School

Director, iNext, School of Computing and Communications

Faculty of Engineering and Information Technology

The University of Technology, Sydney

NSW, 2000

Australia.

Abbreviations	Description
ACK2	Acknowledge of ACK
AES	Advanced Encrypt Standard
AH	Authentication Header
AIMD	Additive Increase/Multiplicative Decrease Algorithm
AIP	Accountable Internet Protocol
AO	Authentication Option
BDP	Bandwidth-Delay Product
BiC	Binary Increase Congestion Control
CCC	Configurable Congestion Control
CGA	Cryptographically Generated Addresses
CRS	Constrained Rewrite Systems
CTCP	TCP Congestion Control Algorithm
DCCP	Datagram Congestion Control Protocol
DTLS	Data Transport Layer Security
EMIST	Evaluation Methods for Internet Security Technology Tool
FAST	FAST TCP Avoidance Algorithm for Long Distance
GRS	Growing Rewrite Systems
GSS-API	Generic Security Service - Application Program Interface
HI /HIT	Host Identifier
HIP	Host Identity Protocol
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IPv4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
KDF	Key Derivation Functions
MAC	Message Authentication Code
MD5	Message-Digest algorithm 5
MSS	Maximum Segmentation/Segment Size
MTU	Maximum Transmission Unit
NAK	Negative Acknowledgement
NBN	Network Broadband Network
NS2	Network Simulation 2
PCL	Protocol Composite Logic

P2P	Peer to Peer
POP3	Post Office Protocol 3
PSK	Private Shared Keys
RFC	Request For Comments
RSA	Rivest, Shamir and Adleman Algorithm
RTT	Round-Trip Time
SASL	Simple Authentication and Security Layer
SDSS	Sloan Digital Sky Survey
SHA-1,2,256	Secure Hash Algorithm
SMTP	Simple Mail Transport Protocol
STCP	Stream Transport Protocol
SYN	Synchronisation/Synchronise
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UDT	UDP-based Data Transfer
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
WOAN	Wide Optical Area Network
XCP	Xplicit Congestion Protocol

Table of Contents

In Deo confidimus