

Supporting Secure Services
on
Dynamic Aggregation of
Heterogeneous Networks

SUBMITTED TO
UNIVERSITY OF SOUTHERN QUEENSLAND
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF DOCTOR OF PHILOSOPHY

David Tai Wai Lai
July 2010

Certification of Dissertation

I certify that the ideas, experimental work, results, analysis, software, and conclusions reported in this dissertation are entirely my own effort, except where otherwise acknowledged. I also certify that the work is original and has not been previously submitted for any other award or degree.

Signature of Candidate

Date

Endorsement

Signature of Supervisor

Date

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

Dr. Zhongwei Zhang
(University of Southern Queensland)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

Dr. Shan Suthaharan
(University of Northern Carolina at Greensboro)

Abstract

Sharing of services over IP networks prove to be an effective approach to satisfy the demand of network users when their home network cannot offer the required services. Authentication, authorization and revocation are some of the important challenges in the service sharing services over IP networks. This research address the problem associated with the authentication because it becomes more and more complicated due to the incompatible authentication schemes used by individual autonomous networks, privacy of authentication information, and the overhead in establishing the sharing. The case gets worse when a user roams from network to network.

Many efforts have been made to address these issues in the past years. Kerberos is a solution for cross realm authentication. Unfortunately, Kerberos suffers from bottle neck and single point of failure. Ad hoc aggregation cannot make use of Kerberos. Eduroam enables sharing of wireless access to users roaming between participating institutions, but only services provided by the home network is available to a user. Mobile Host Routing can route data between mobile user. But the networks are linked together in an unscalable network by network basis.

Another authentication scheme which has gained some momentum is OpenID. However, in OpenID, authentication simply means proving the ownership of an account, and there is no binding between the account and the actual user identity.

These problems and the limitations in the existing approaches inspired us to propose Service Network Graph, a service authentication infrastructure for service sharing among heterogeneous networks aggregated dynamically via self-authenticating encrypted channels. The key feature of *SNG* is delegation of authentication authority from one network to another. A user can use the services provided by the delegatee network as well as his home network after authenticating to the delegatee network.

When an autonomous network attaches to an *SNG*, not only does the network being attached delegate its authentication authority, but all authentication authorities delegated to the network also re-delegated to the attaching network. Authentication Delegation and Re-delegation makes *SNG* scalable.

As authentication is always done by the home network, the identity of a user can be securely bound to his account. At the same time, there is no hierarchy structure for the authentication process, autonomous networks can join an *SNG* in an ad hoc fashion. No

authentication bottle neck is anticipated in *SNG*.

The information of the authentication delegation path is stored in a Service Path which can be optimized for performance . *SNG* can readily extend to include mobile users.

We also proposed Dynamic Password (*DPass*) and its associated Key Exchange Scheme to be used as one of the candidate authentication schemes for *SNG*. *DPass* provide strong passwords which are relatively easy to remember.

SNG together with *DPass* provide an infrastructure for secure service sharing on dynamic aggregation of heterogenous networks. The features and feasibility of *SNG* and *DPass* have been demonstrated on a simulated model of autonomous networks and an aggregate of networks in a laboratory. Our study has, to a certain extend, overcome the draw backs of the above mentioned approaches with efficiency and scalability.

Acknowledgements

I would like to thank my supervisors Dr. Zhongwei Zhang at University of Southern Queensland (USQ) and Dr. Shan Suthaharan at University of Northern Carolina at Greensboro (UNCG) for their guidance, advice, patience and encouragement. It is a pleasure to do research under their supervision. Without their help and support, I will not be able to finish my study.

The insight and lateral thinking of Dr. Zhongwei Zhang prompted me to look at problems from various perspectives and to focus on the major issues without losing sight of the details.

I am indebted to the Department of Mathematics and Computing, the Faculty of Sciences and the Computational Engineering and Science Research Centre (CESRC) for their financial support for attending conferences.

My thanks also go to Associate Professor Ron Addie. He fully supported my research and helped me to acquire the computers needed for the research.

Symbols and Abbreviations

Symbols

Symbol	Meaning
$\varphi \rightarrow$	Speaks for
\Rightarrow	implies

Table 1: Symbols used in this dissertation.

Glossary

Abbreviation	Term / Meaning
<i>SNG</i>	<i>Service Network Graph</i> Infrastructure which enables secure services on dynamic aggregation of heterogeneous networks.
<i>U</i>	<i>User of SNG</i> A user who is entitled to use services available within an <i>SNG</i> .
<i>SLS</i>	<i>Service Listing Server</i> Server which lists the service available to an User on an <i>SNG</i> network.
<i>S</i>	<i>Service Providing Server</i> A server which provides services within <i>SNG</i> .
<i>HNet</i>	<i>Home Network</i> <i>SNG</i> Network of which user <i>U</i> is a register user.
<i>VNet</i>	<i>Visited Network</i> Network in which the user is currently located.
<i>FNet</i>	<i>Foreign Network</i> <i>SNG</i> Network included in an <i>SPath</i> which is not a <i>HNet</i> or a <i>VNet</i> .
<i>RNet</i>	<i>Remote Network</i> <i>SNG</i> Network not included in an <i>SPath</i> .
<i>ANet</i>	<i>Alien Network</i> Network which is not part of an <i>SNG</i> .
<i>SNet</i>	<i>Service Providing Network</i> <i>SNG</i> Network which provides the requested service.

Table 2: Glossary of terms used in this dissertation - Part 1.

Abbreviation	Term / Meaning
<i>DPass</i>	<i>Dynamic Password</i> Consists of two parts: Dynamic Part and Static Part.
<i>SDPass</i>	<i>Static Part of DPass</i> First part of <i>DPass</i> with a relatively longer life span.
<i>DDPass</i>	<i>Dynamic Part of DPass</i> Second part of <i>DPass</i> with a relatively shorter life span.
<i>SPath</i>	<i>ServicePath</i> Network path that leads up to the server.
<i>AS</i>	<i>Authentication Server</i> Server which authenticates user <i>U</i> .
<i>SW</i>	<i>Switch</i> A network device.
<i>R</i>	<i>Router</i> A network device.
<i>NED</i>	<i>NEtworkDescription language</i> Language in <i>OMNeT++</i>
<i>N</i>	<i>Network</i> An autonomous Network.
<i>NPMode</i>	<i>NetworkParticipationMode</i> State of an autonomous network joining or leaving an <i>SNG</i> .
<i>USMode</i>	<i>UserServiceMode</i> State of an autonomous network providing services to a user.
<i>SPath</i>	<i>ServicePath</i> Service information including the network path from a user to a server.
<i>SAPath</i>	<i>ServiceAccessPath</i> Network path from the user to the server.
$H(X)$	<i>Hashvalue of X</i>
$\{X\}_K$	<i>Encryption of X using key K</i>

Table 3: Glossary of terms used in this dissertation - Part 2.

Contents

Abstract	v
Acknowledgements	vii
Symbols and Abbreviations	ix
1 Introduction	1
1.1 Specific Problems	1
1.1.1 The Availability of a Service	2
1.1.2 The Authentication of a User	2
1.1.3 Authorization Relay	4
1.1.4 Reluctance of Authentication for Roaming Users	4
1.1.5 Revocation of a User	5
1.1.6 Mobility of Users	5
1.2 Related Work on the Problems	6
1.3 A Practical Example of Service Sharing	9
1.3.1 Background	9
1.3.2 Authentication Information Sharing	9
1.3.3 Service Sharing	10
1.4 Research Contribution	10
1.5 Structure of the Dissertation	12
2 Service Sharing Technologies	15
2.1 Autonomous Network	15
2.2 Intranet and Internet	16
2.3 Kerberos	16
2.3.1 Cross-Realm Operation of Kerberos	19
2.3.2 Kerberos V5 Applications	22
2.3.3 Drawbacks of Kerberos	23
2.4 SESAME	23
2.5 Eduroam	24

2.5.1	Drawbacks of Eduroam	27
2.6	Mobile Host Routing	28
2.6.1	Drawbacks of Mobile Host Routing	31
2.7	OpenID	31
2.7.1	OpenID Account	31
2.7.2	OpenID Authentication	32
2.7.3	Drawbacks of OpenID	35
2.8	Chapter Summary	35
3	Service Network Graph	37
3.1	Introducing Service Network Graph	37
3.2	Autonomous Networks	38
3.3	Service Network Graph	39
3.3.1	Authentication Delegation	39
3.3.2	The Sample Service Network Graph	41
3.4	Service Path	41
3.4.1	Share Options	42
3.4.2	Service Access Path	43
3.4.3	Cost	44
3.5	Distributed Networks Service Authentication Protocol	44
3.5.1	Network Participation Mode	44
3.5.2	User Service Mode	45
3.6	Authentication Propagation	51
3.7	Changes in SNG Configuration	52
3.8	Changes in User Authorization	53
3.9	Chapter Summary	54
4	Efficiency and Scalability of Service Path	55
4.1	Overview	55
4.2	Basic Axioms and Theorems	56
4.3	Optimization of Service Path	56
4.3.1	Optimization of SPath	58
4.4	Implementing SPath Optimization	62
4.4.1	Selecting Service Paths	63
4.4.2	Service Optimization Table and Authentication Path Network Lookup Table	63
4.4.3	Authentication Re-Delegation	68
4.4.4	Revocation of Authentication Delegation	70
4.5	Chapter Summary	71

5	Self-authenticating Channel	73
5.1	Authentication Delegation in SNG	73
5.2	Self-Authentication of Encrypted Channels	74
5.2.1	One-way Self-authentication of Encrypted Channels	75
5.2.2	Two-Way Self-authentication of Encrypted Channels	76
5.3	Chapter Summary	77
6	Authentication Protocol for SNG	79
6.1	Introduction	79
6.2	Strength of Passwords	80
6.3	Dynamic Password	82
6.3.1	Strength of Dynamic Passwords	83
6.4	Key Exchange using Dynamic Passwords	85
6.4.1	Encryption Key Exchange	85
6.4.2	Asymmetric Key Exchange	86
6.4.3	Key Exchange using Dynamic Passwords	86
6.5	Features of Proposed Key Exchange using DPass	89
6.6	Application of KEDP	90
6.6.1	Distributed Computer Networks Systems	90
6.6.2	KEDP Ported to Kerberos	91
6.7	Chapter Summary	92
7	KEDP in Service Network Graph	93
7.1	Strand Spaces and Related Notions	93
7.2	Authenticating an Encrypted Channel	96
7.3	Mapping DPS to a Strand Space	96
7.3.1	DPS Strand Spaces	98
7.4	Correctness Proof of DPS	100
7.4.1	Secrecy Guarantee	100
7.4.2	DPS Agreement Guarantee	106
7.4.3	Correctness Proof of DPS	115
7.5	Chapter Summary	116
8	Application of SNG on Simulated Networks	117
8.1	Simulation Platform Overview	117
8.1.1	Configuring OMNeT++ for the SNG Model	118
8.1.2	Specifying SNG Model for OMNeT++	119
8.1.3	Component Modules of the SNG Model	120
8.1.4	OMNeT++ Outputs	121
8.2	Service Access	121
8.2.1	Address	122

8.2.2	Server, Src, Dest	123
8.2.3	Start, Stop	123
8.2.4	Message Label	124
8.2.5	Message Kind	124
8.3	Routing Operation	125
8.3.1	User Module	126
8.3.2	Server Module and Service Listing Server Module	127
8.3.3	Switch Module	127
8.3.4	Router Module	128
8.3.5	Authentication Server Module	128
8.4	Simulation of the SNG Model	130
8.4.1	Scenario 1: User at Home Network	131
8.4.2	Scenario 2: User at Visited Network	132
8.5	Chapter Summary	133
9	Practicality of SNG on Aggregated Networks	135
9.1	The Autonomous Network Aggregate	135
9.2	<i>SNG</i> Topology and Data Files	137
9.3	Service Request Cases	138
9.4	SNG Users and Servers	141
9.4.1	SNG Authentication Server	143
9.4.2	SNG Application Servers	145
9.4.3	SNG Service Listing Servers	147
9.5	Service Path Technology	148
9.6	Dynamic Password and Encryption	149
9.7	Chapter Summary	149
10	Conclusion and Future Direction	151
10.1	Problems and Challenges in Service Sharing	151
10.2	Methodology	152
10.3	Outcomes	154
10.4	Problems for Future Studies	154
	Bibliography	157
	Appendices	165
A		165
A.1	Axiom P10	165
A.2	Theorem P8	165
A.3	Theorem P11	165

B		167
B.1	Axiom 1	167
B.2	Definition 2.1	167
B.3	Definition 2.11	167
B.4	Axiom 2	167
B.5	Proposition 2.12	167
B.6	Definition 2.2	167
B.7	Definition 2.3	167
B.8	Definition 2.4	168
B.9	Notational Convention 2.5	168
B.10	Definition 2.6	168
B.11	Lemma 2.7	168
B.12	Lemma 2.8	168
B.13	Lemma2.9	168
B.14	Definition 3.1	168
B.15	Proposition 3.3	169
B.16	Definition 3.2	169
C		171
C.1	Listing of omnetpp.ini	171
C.2	Listing of Makefile	171
C.3	Listing of dssinet.ned	173
C.4	Server Module	176
C.4.1	Listing of dssis.ned	176
C.4.2	Listing of dssis.h	176
C.4.3	Listing of dssis.cc	177
C.5	Service Listing Server Module	177
C.5.1	Listing of dssisls.ned	177
C.5.2	Listing of dssisls.h	177
C.5.3	Listing of dssisls.cc	177
C.6	Switch Module	178
C.6.1	Listing of dssisw.ned	178
C.6.2	Listing of dssisw.h	178
C.6.3	Listing of dssisw.cc	178
C.7	Router Module	178
C.7.1	Listing of dssir.ned	178
C.7.2	Listing of dssir.h	179
C.7.3	Listing of dssir.cc	179
C.8	User Module	179
C.8.1	Listing of dssiu.ned	179

C.8.2	Listing of dssiu.h	179
C.8.3	Listing of dssiu.cc for User at Home Network	179
C.8.4	Listing of dssiu.cc for User at Foreign Network	181
C.9	Authentication Server Module	182
C.9.1	Listing of dssia.ned	182
C.9.2	Listing of dssia.h	182
C.9.3	Listing of dssia.cc for user at Home Network	182
C.9.4	Listing of dssia.cc for user at Foreign Network	185
C.10	Simulation Output	188
C.10.1	Listing of Message_sent_home.txt	188
C.10.2	Listing of Module_output_home.txt	190
C.10.3	Listing of Message_sent_foreign.txt	192
C.10.4	Listing of Module_output_foreign.txt	195

D **199**

D.1	asServer.cpp	199
D.2	asClient.cpp	206
D.3	Date Server	208
D.3.1	dateGroup.cpp	208
D.3.2	dateServer.cpp	210
D.4	Echo Server	211
D.4.1	echoGroup.cpp	211
D.4.2	echoServer.cpp	213
D.5	Name Server	215
D.5.1	nameGroup.cpp	215
D.5.2	nameServer.cpp	216
D.6	Time Server	218
D.6.1	timeGroup.cpp	218
D.6.2	timeServer.cpp	220
D.7	Service Listing Server	222
D.7.1	slsSGroup.cpp	222
D.7.2	slsSServer.cpp	223
D.7.3	slsCGroup.cpp	226
D.7.4	slsCServer.cpp	227
D.8	Utility Files	230
D.8.1	GNUmakefile	230
D.8.2	security.h	233
D.8.3	security.cpp	233
D.8.4	md5ADT.h	238
D.8.5	md5ADT.cpp	239

D.8.6	bst.h	244
D.8.7	bst.cpp	245
D.8.8	sp.h	247
D.8.9	sp.cpp	247
D.8.10	path.h	248
D.8.11	path.cpp	249
D.9	Data Files	250
D.9.1	PC1Map.data	250
D.9.2	PC2Map.data	250
D.9.3	PC3Map.data	250
D.9.4	PC4Map.data	250
D.9.5	PC1SP.data	250
D.9.6	PC2SP.data	250
D.9.7	PC3SP.data	251
D.9.8	PC4SP.data	251
D.9.9	dp.data	252
D.9.10	port.data	255
D.9.11	userDP.data	255
D.9.12	userHDP.data	255
D.10	Configuration Files	255
D.10.1	Switch Configuration	255
D.10.2	Router Configuration	256
E		257
E.1	port1.data	257

List of Tables

1	Symbols used in this dissertation.	ix
2	Glossary of terms used in this dissertation - Part 1.	x
3	Glossary of terms used in this dissertation - Part 2.	xi
2.1	Components of OpenID.	32
3.1	IP addresses of authentication servers in sample SNG	41
3.2	Network paths to authentication server AS_3 in sample SNG	44
4.1	List of symbols used in this chapter	56
4.2	SPath Optimization Table for N_H	64
4.3	Authentication Path Network Lookup Table for N_H	65
4.4	SPath Optimization Table for N_H	65
4.5	Authentication Path Network Lookup Table for N_H	66
4.6	SPath Optimization Table for N_H	66
4.7	Authentication Path Network Lookup Table for N_H	67
4.8	SPath Optimization Table for N_H	67
4.9	Authentication Path Network Lookup Table for N_H	67
4.10	SPath Optimization Table for N_H	68
4.11	SPath Optimization Table for N_H	71
4.12	Authentication Path Network Lookup Table for N_H	71
6.1	Parameters for password life time calculations.	82
6.2	Typical life time of passwords.	82
6.3	Dynamic Password length using 23000-character set.	84
6.4	List of abbreviations for $KEDP$	86
6.5	List of abbreviations used in Kerberos message exchange.	91
7.1	Axioms, notational conventions and propositions from [17]	95
7.2	Definitions from [17]	96
7.3	S for $R_1, R_2, R_3, DDPass_{new}$ and $H(DDPass)$	106
7.4	Propositions for $R_1, R_2, R_3, DDPass_{new}$ and $H(DDPass)$	106

8.1	OMNeT++ configuration files.	119
8.2	Module files for the <i>SNG</i> used in OMNeT++.	120
8.3	OMNet++ output files.	121
8.4	Addresses of devices used in the Simulation.	122
8.5	Addresses of devices used in the Simulation.	122
8.6	Destination addresses of a message in the simulation.	123
8.7	Example of message variable values from S_4 to U	124
8.8	List of message labels.	125
8.9	List of message kinds and color.	125
8.10	List of messages generated by user module U_1	126
8.11	Code used by routing messages in server and service listing server modules.	127
8.12	List Network linkage for the simulation cases.	129
8.13	List of <i>SNG</i> routes.	130
9.1	IP addresses of PCs used in the <i>SNG</i>	136
9.2	Summary of network and <i>VLAN</i> data.	137
9.3	Data files used in the implementation.	137
9.4	Types of Service Request.	139
9.5	Listings of <i>ServiceGroup servers</i> and <i>Service servers</i>	146
9.6	Data files used in the implementation.	147
9.7	Functions used by Dynamic Password.	149

List of Figures

2.1	An autonomous network.	15
2.2	The Kerberos logo.	16
2.3	A Kerberos realm.	17
2.4	Steps 1 and 2 of Kerberos in action.	18
2.5	Steps 3 and 4 of Kerberos in action.	18
2.6	Steps 5 and 6 of Kerberos in action.	19
2.7	Steps 1 to 4 of multiple realm Kerberos in action.	20
2.8	Extra steps, steps 5 and 6 of multiple realm Kerberos in action.	20
2.9	Steps 1 to 4 of multiple realm Kerberos in action.	21
2.10	Extra steps, steps 5 and 6 of multiple realm Kerberos in action.	21
2.11	Hierarchical arrangement of Realms for cross-realm authentication	22
2.12	The Eduroam logo.	24
2.13	Action of Eduroam for a user in home network	25
2.14	Action of Eduroam for a user in a visited network	26
2.15	Tunneling of Eduroam for a user in a visited network	27
2.16	Authentication for a mobile user.	28
2.17	Mobile user calling a home network user.	29
2.18	Home network user calling mobile user.	29
2.19	Mobile user calling another mobile user.	30
2.20	Authentication Process for OpenID	33
3.1	A typical autonomous network.	38
3.2	A Service Network Graph	40
3.3	Attaching one network to another network	45
3.4	User requesting a local service	46
3.5	User requesting a shared service	47
3.6	User requesting a shared service	48
3.7	Mobile user requesting a shared service	49
3.8	Changes in user authorization is pushed to server	54
4.1	Sharing of key before SPath optimization	63

4.2	Sharing of key before SPath optimization	69
4.3	SPath optimization in general	70
7.1	<i>DPS</i> events for a principal	97
7.2	Causal links between <i>DPS</i> events for principal A and B	98
7.3	A <i>DPS</i> Bundle	98
8.1	OMNeT++ configuration files for <i>SNG</i> simulation.	118
8.2	OMNeT++ <i>SNG</i> network model for user at home network.	119
8.3	Routing logic for the simulation.	131
8.4	Simulation Topology for user at home network.	132
8.5	Simulation Topology for user at a visited network.	133
9.1	<i>SNG</i> topology used	136
9.2	Logical topology of <i>SNG</i> showing the authentication delegations.	138
9.3	User accessing Home Network services at Home Network.	139
9.4	User accessing Foreign Network services at Home Network.	140
9.5	User accessing Network services at a Foreign Network.	140
9.6	User accessing Network services at a Remote Network.	141
9.7	Logic diagram of the client program.	142
9.8	Diagram of algorithm used by the asServer program.	144
9.9	Diagram of algorithm used by an appGroup program.	145
9.10	Diagram of algorithm used by an application program.	146