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
$\Rightarrow$	Speaks for
$\Rightarrow$	implies

Table 1: Symbols used in this dissertation.

Glossary

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

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

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

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

Contents

List of Tables

List of Figures