UNIVERSITA' DEGLI STUDI DI PISA

FACOLTA' DI INGEGNERIA

Corso di Laurea Specialistica in
INGEGNERIA INFORMATICA

TESI DI LAUREA SPECIALISTICA

Studio e implementazione di un Profilo SAML per Trait-based Identity Management System nel Session Initiation Protocol

Candidato :
Francesco la Torre

Relatori :
Prof. Gianluca Dini
Dott. Ing. Giovanni Stea
Dott. Fabio Martinelli

Anno Accademico 2007/2008

A mia madre

Indice

1. Introduzione 1

2. Il protocollo Sip e l'Identity Management 7
2.1 Il protocollo SIP 7
2.1.1 Introduzione 8
2.1.2 Obiettivi 8
2.1.3 Protocollo di trasporto 10
2.1.4 Risorse SIP 12
2.1.5 Address of Record 12
2.1.6 Architettura del protocollo 13
2.1.7 Entità 14
User Agent 14
Proxy Server 16
Redirect 17
Registar 17
2.1.8 Messaggi SIP 18
2.1.9 Header 19
2.1.10 Messaggi di richiesta 21
Register 22
Invite, ACK, BYE 23
Estensioni delle richieste 24
2.1.11 Messaggi di risposta 28
2.1.12 Sip Transaction e Dialog 34
Transaction 34
Dialog 35
2.1.13 Routing dei messaggi 37
2.1.14 Modalità di connessione 38
2.1.15 Record Re-Routing 39
2.1.16 Sip e Voip 40
2.1.17 Negoziazione di una sessione 40
2.2 Identity Management in SIP 42
2.2.1 Introduzione 42
2.2.2 SIP Digest authentication 44
2.2.2.1 Overview della Digest Authentication 44

2.2.2.2 Digest Authentication in SIP 47
2.2.2.2.1 Autenticazione user-to-user 48
2.2.2.2.2 Authenticazione proxy-to-user 50
2.2.2.2.3 Calcolo del Digest 51
2.2.2.2.4 Esempio 51
2.2.3 Secure/Multipurpose Internet Mail Extensions 58
2.2.3.1 Certificat S/MIME 59
2.2.4 Transport Security Layer 60
2.2.5 SIP Uniform Resource Identifier 61
2.2.6 Limitazioni 62
2.2.7 Enhancement for Authenticated Identity Management in SIP 64
2.2.7.1 Introduzione 64
2.2.7.2 Authentication Service 64
2.2.7.3 Verifier 65
2.2.7.4 Impiego 66
2.2.7.5 Test ed Esempi 66
2.2.7.6 Considerazioni 69
2.2.7.6.1 Virtual hosting e Subordination 71
2.2.7.6.2 Conclusioni 72

3 Trait-Based Identity Management System 74
3.1 Descrizione del sistema 75
3.1.1 Introduzione 75
3.1.2 Framework per il sistema Trait-Based 79
3.1.3 Esempi di casi d'uso 83
3.1.3.1 Servizi a pagamento 83
3.1.3.2 Permessi su risorse limitate 85
3.1.3.3 Gestione delle priorità 86
3.2 Security Assertion Markup Language 88
3.2.1 Concetti generali 88
3.2.2 Componenti di SAML 90
3.2.3 SAML : dalla teoria alla pratica 95
3.2.3.1 Relazioni fra i componenti SAML 95
3.2.3.2 Struttura degli attribute statement 98
3.2.3.3 Struttura dei messaggi e il Binding SOAP 100
3.2.3.4 Privacy in SAML 103
3.2.3.5 Sicurezza in SAML 103
3.2.3.6 SAML e la firma digitale in XML 104
3.3 Profilo SAML per il Protocollo SIP 109
3.3.1 Introduzione 109
3.3.2 Integrazione del framework SAML in SIP 110

3.3.3 Le assertion e il protocollo operativo 111
3.3.4 Creazione e verifica delle assertion 115
3.3.5 Considerazioni sulla sicurezza 121

4 Implementazione 123
4.1 Introduzione 124
4.2 Sip Express Router 124
4.2.1 File di configurazione 126
4.2.2 Gestione dei messaggi SIP 126
4.2.3 Analisi e struttura di un modulo 128
4.3 Il modulo auth_saml 131
4.3.1 Strutture dati rilevanti 135
4.3.2 Invio richiesta per inizio sessione 137
4.3.3 Ricezione richiesta per inizio sessione 139
4.3.4 Ricerca dei tratti 143
4.4 Trait Management System 143
4.5 Configurazione del SER per la gestione dei tratti 147
4.6 Analisi delle prestazioni 149
4.6.1 Configurazione senza supporto ai tratti 149
4.6.2 Configurazione con supporto ai tratti 151

5 Conclusioni e sviluppi futuri 153
5.1 Conclusioni 154
5.2 Sviluppi futuri 157

Appendici 159
Appendice A – Firma digitale in XML 160
Appendice B – Setup architetturale 166

Bibliografia 188

Elenco delle figure.

Figura 2.1. Interazione fra UA. 15
Figura 2.2. Interazione di Proxy server. 16
Figura 2.3. Redirect server. 17
Figura 2.4 . Registar. 18
Figura 2.5. Subscribe/Notify. 26
Figura 2.6. Transaction. 34
Figura 2.7. Dialog. 36
Figura 2.8. Trapezoide SIP. 38
Figura 2.9. Meccanismi di sicurezza in SIP. 43
Figura 2.10. Flusso di messaggi. 52
Figura 2.11. Identity Encoding. 67
Figura 2.12. Identity Decoding. 68
Figura 3.1. (A) Identità classica. (B) Identità con tratti. 76
Figura 3.2. Trust Relationship. 79
Figura 3.3. Modello per la gestione delle assertion. 81
Figura 3.4. Scenario Accounting. 84
Figura 3.5. Scenario con risorse limitate. 85
Figura 3.6. Scenario con gestione delle priorità. 86
Figura 3.7. Struttura del framework SAML. 89
Figura 3.8. Relazione fra i componenti di SAML. 95
Figura 3.9. Esempio di assertion. 96
Figura 3.10. Attribute Statement. 99
Figura 3.11. SOAP Over HTTP. 100
Figura 3.12. Attribute Query in un SOAP Envelop. 101
Figura 3.13. Messaggio di response in un SOAP Envelop. 102
Figura 3.14. Esempio di messaggio con assertion. 108
Figura 3.15. Binding SAML per SIP. 112
Figura 3.16. SIP-SAML Asserted Identity. 113
Figura 3.17. Esempio di asserition non firmata. 118
Figura 3.18. Esempio di assertion firmata. 120
Figura 4.1. Struttura logica del Sip Express Router. 125
Figura 4.2. Confronto fra proxy stateful e stateless. 127
Figura 4.3. Elaborazione di un messaggio SIP di richiesta. 127
Figura 4.4. Elaborazione di un messaggio SIP di risposta. 128

Figura 4.5. Struttura dati ass_attribute. 136
Figura 4.6. Struttura dati saml_attribute. 136
Figura 4.7. Flusso di chiamate della funzione add_identity(). 137
Figura 4.8. Flusso di chiamate della funzione get_Assertion() 137
Figura 4.9. Flusso di chiamate della funzione query_user_attr(). 138
Figura 4.10. Flusso di chiamate della funzione CreateXmlAssertion(). 138
Figura 4.11. Flusso di chiamate della funzione rsa_sign_digest(). 139
Figura 4.12. Flusso di chiamate della funzione VerifyAssertion(). 139
Figura 4.13. Flusso di chiamate della funzione verify_file(). 140
Figura 4.14. Flusso di chiamate della funzione parseAssertionFile(). 140
Figura 4.15. Flusso di chiamate della funzione getvalue(). 141
Figura 4.16. Flusso di chiamate della funzione get_certificate(). 141
Figura 4.17. Flusso di chiamate della funzione check_certificate(). 142
Figura 4.18. Flusso di chiamate della funzione check_validity. 142
Figura 4.19. Flusso di chiamate della funzione lookup_attribute_incoming(). 143
Figura 4.20. Flusso chiamate della funzione lookup_attribute_outcoming(). .. 143
Figura 4.21. Piattaforma TMS. 144
Figura 4.22. Architettura del TMS. 144
Figura 4.23. Architettura del database per la gestione dei tratti. 145
Figura 4.24. Performance del SER senza il supporto ai tratti. 150
Figura 4.25. Performance del SER con il supporto ai tratti. 151

Elenco delle tabelle.

Tabella 2.1. Intestazioni SIP. 20
Tabella 2.2. Metodi SIP. 22
Tabella 2.3. Tipi di Response. 28
Tabella 2.4. Messaggi di risposta dopo verifica del campo Identity. 69
Tabella 4.1. Principali funzioni esportate. 132
Tabella 4.2. Principali parametri del modulo auth_saml. 134

Elenco dei listati.

Listato 4.1. Struttura dati param_export. 129
Listato 4.2. Struttura dati param_export_t. 129
Listato 4.3. Struttura dati cmd_export_. 130
Listato 4.4. Esempio esportazione funzione. 131
Listato 4.5. Struttura dati per esportazione delle funzioni. 133
Listato 4.6. Interfaccia del modulo auth_saml. 135
Listato 4.7. Struttura dati per la gestione delle assertion. 135
Listato 4.8. Script di configurazione per la gestione dei tratti in entrata. 148
Listato 4.9. Script di configurazione per la gestione dei tratti in uscita. 148