Protocols

Steven Allen

April 11, 2013

1 Variables and Notation

R Number of resources

G Number of groups per person

F Number of friends per person

S Number of services

A Average number of groups per resource

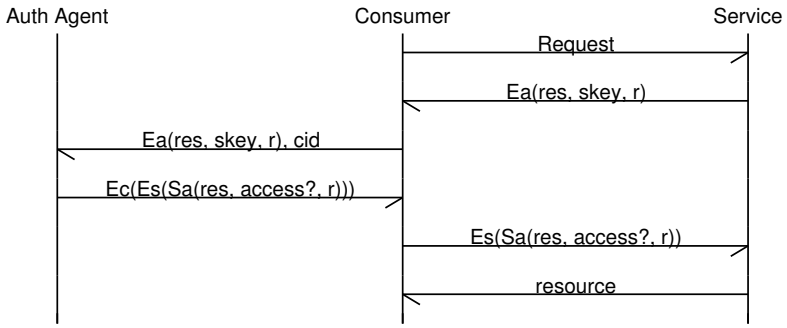
c Request rate

g Group change rate

g Group change rate

2 Obvious PK

2.1 Protocol



2.2 Costs

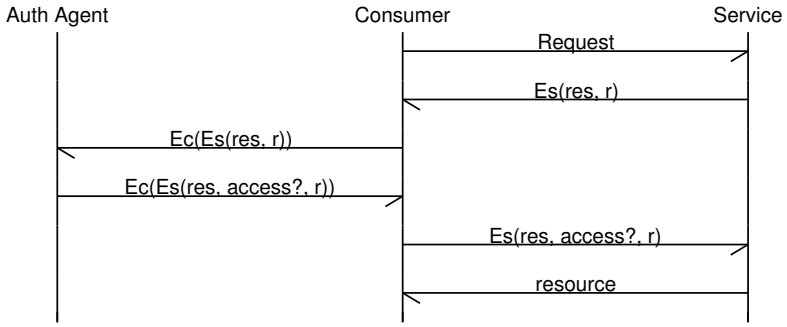
Op	Auth Agent	Consumer	Service
Encryption	$\Theta(c)$	$\Theta(c)$	$\Theta(c)$
Storage	$\Theta(RG + RS)$	$\Theta(1)$	$\Theta(R)$
Transfer	$\Theta(c)$	$\Theta(c)$	$\Theta(c)$

2.3 Analysis

Perfect privacy.

3 Obvious Shared Secret

3.1 Protocol



3.2 Costs

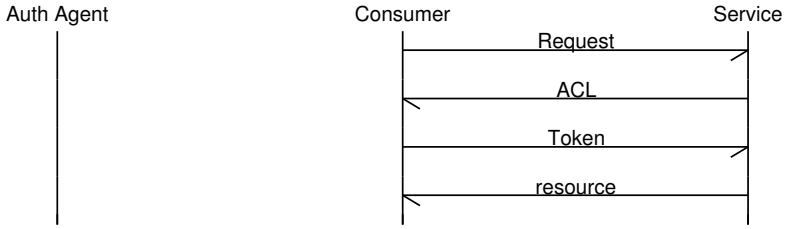
Op	Auth Agent	Consumer	Service
Encryption	$\Theta(c)$	$\Theta(c)$	$\Theta(c)$
Storage	$\Theta(RG + RS)$	$\Theta(F)$	$\Theta(R)$
Transfer	$\Theta(c)$	$\Theta(c)$	$\Theta(c)$

3.3 Analysis

Perfect privacy.

4 Public Key ACL (Basic)

4.1 Protocol



4.2 Costs

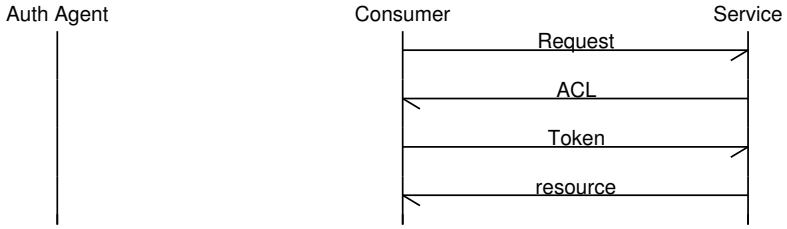
Op	Auth Agent	Consumer	Service
Encryption	$\Theta(g)$	$\Theta(rA)$	0
Storage	$\Theta(GA)$	$\Theta(1)$	$\Theta(RA)$
Transfer	$\Theta(g)$	$\Theta(rA)$	$\Theta(rA)$

4.3 Analysis

The ACL is of the form: $\{E_{c_1}(t), E_{c_2}(t), ...\}$. Consumers are able to determine the size of the ACL group.

5 Public Key ACL (Per Group)

5.1 Protocol



5.2 Costs

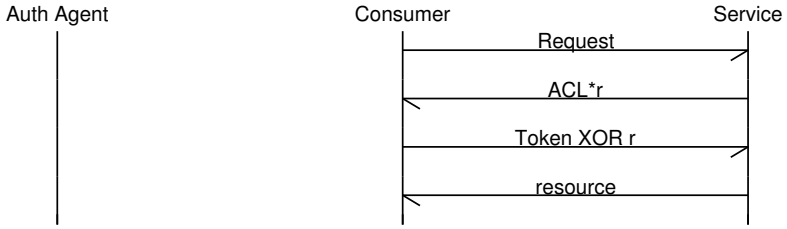
Op	Auth Agent	Consumer	Service
Encryption	$\Theta(g)$	$\Theta(rA)$	0
Storage	$\Theta(GA)$	$\Theta(1)$	$\Theta(GA)$
Transfer	$\Theta(g)$	$\Theta(rA)$	$\Theta(rA)$

5.3 Analysis

Both the consumers and the services are able to group content.

6 Public Key ACL (per group, enhanced)

6.1 Protocol



6.2 Costs

Op	Auth Agent	Consumer	Service
Encryption	$\Theta(g)$	$\Theta(rA)$	0
Storage	$\Theta(GA)$	$\Theta(1)$	$\Theta(GA)$
Transfer	$\Theta(g)$	$\Theta(rA)$	$\Theta(rA)$

6.3 Analysis

Using Goldwasser-Micali for pk encryption, compute $r * \text{ACL} = \{E_{c_1}(t \oplus r), E_{c_2}(t \oplus r), ...\}$. This allows us to hide the group from the consumer.

With this encryption scheme, the consumers can't group content but the server still can.