Delegation

Example 6f

CSE 791: E-6f

Title: Delegation
SML files: none
Objective: Reasoning about Delegation

1 Introduction

Delegation is the act of sending another person or agent in one’s place. The delegate is understood to speak for or speak on behalf of the person or organization who appointed him or her. Depending on what is required, delegation can be just simple quoting with no authentication or verification of credentials to authenticated delegations and requests. The notions, notations, and development in this example primarily follow [2]. Where possible, we will make a link to [1].

The remainder of this example is organized as follows. In section 2 we look at delegation without credentials. In section 3 we look at delegation with certificates.

2 Delegation Without Certificates

Example

This form of delegation happens routinely. For example, consider the situation that happens a lot in families. Mom is in the kitchen and Dad is sitting at the dining room table in the other room with the children. Dad sends his (under-aged) son to ask Mom for a beer. The request that Mom receives is

Son says Dad says give me a beer

If Mom trusts that Dad really made the request and trusts that her son is not lying in order to drink the beer himself, she will grant the request (i.e., give access to the beer) without further checking.

Note that it is important that the son be quoting or mentioning his Dad, otherwise the request is

Son says give me a beer

which Mom would likely interpret as the beer is for her under-aged son and hopefully she would question him further.

To wrap up this example, Mom’s access control list for beer might look like
Example

Consider another example in a small restaurant where everyone knows each other. Let us say there are three principals: Alice the waitress, table 5—which Alice waits on, and Carol the cook. The way the restaurant operates is this: Alice asks the customers at the table what they want to eat (notice that it’s unimportant to identify the customers), Alice writes down the order on her order pad (as shown in Figure 1) that identifies her in some way as having placed the order, Alice puts the written order on a stack of orders for Carol who cooks the order, and when the order is cooked, Alice brings the food to the table.

<table>
<thead>
<tr>
<th>Alice’s Orders</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table: 5</td>
</tr>
<tr>
<td>Order: Steak (medium rare)</td>
</tr>
<tr>
<td>Fries</td>
</tr>
<tr>
<td>Chocolate Milk Shake</td>
</tr>
</tbody>
</table>

Figure 1: Alice’s Pad

Carol’s access control list for her kitchen includes Alice | table 5. The order slip from Alice telling Carol what to cook corresponds to

\[ Pad_{Alice} \text{ says table 5 says Steak (medium rare), Fries, Chocolate Milk Shake} \] \hspace{1cm} (3)

If Carol believes that

\[ Pad_{Alice} \Rightarrow Alice \] \hspace{1cm} (4)

then Carol can conclude that

\[ Alice | table 5 says Steak (medium rare), Fries, Chocolate Milk Shake \] \hspace{1cm} (5)

Example

Consider the case where Bob is acting on Alice’s behalf by requesting services from Carol for Alice. Alice and Bob both have keys and both keys are certified by authority S—the key distribution server. The following represents Carol’s reasoning on keys and authority.

\[ K_S \Rightarrow S \] \hspace{1cm} (6)
\[ K_S \text{ says } (K_B \Rightarrow B) \] \hspace{1cm} (7)
\[ S \text{ says } (K_B \Rightarrow B) \] \hspace{1cm} (8)
\[ S \text{ controls}(K_B \Rightarrow B) \] \hspace{1cm} (9)
\[ \text{therefore } K_B \Rightarrow B \] \hspace{1cm} (10)

When Carol receives the request

\[ K_B \text{ says } A \text{ says } r \] \hspace{1cm} (11)
Carol can conclude

\[(B \mid A) \text{ says } r\]  \hspace{1cm} (12)

and if \((B \mid A)\) is on Carol’s access control list for \(r\), Bob will gain access on Alice’s behalf.

In all the three previous examples, the principals making requests on behalf of other principals did not present any credentials backing up their claims that they were in fact delegates. In the next section we see how certificates are used to verify delegations.

3 Delegation with Certificates

Delegation using certificates of delegation as described in [2] works as follows. If Alice wishes to designate Bob as her delegate in certain matters, the following happens:

1. Alice signs a certificate stating that Bob is her delegate

2. When Bob makes requests on Alice’s behalf from Carol, Bob presents the delegation certificate to Carol along with the request \(K_B \text{ says } A \text{ says } r\)

3. Carol will check her access control list to see if the request can be honored

The logic of delegation is constructed with a (possibly imaginary) delegation server \(D\) in mind whose purpose is to verify delegations. For Alice to delegate to Bob, Alice tells the delegation server \(D\) that it should “back” Bob, i.e., if \(B \text{ says } A \text{ says } s\) then \(D\) backs \(B\), where

\[D \text{ backs } B = B \mid A \text{ says } s \supset D \mid A \text{ says } s\]  \hspace{1cm} (13)

If we use some syntactic sugar and define \(serves\) as

\[B \text{ serves } A = B \mid A \Rightarrow D \mid A\]  \hspace{1cm} (14)

then Alice can also declare

\[A \text{ says } (B \text{ serves } A)\]  \hspace{1cm} (15)

Delegation in the calculus is formally defined as

\[B \text{ for } A = (B \land D) \mid A\]  \hspace{1cm} (16)

To see the logic behind the definition, consider the definition of \(serves\) and the definition of \(\Rightarrow\).

\[B \text{ serves } A = B \mid A \Rightarrow D \mid A \text{ Definition of serves}\]  \hspace{1cm} (17)

\[= (B \mid A = B \mid A \land D \mid A) \text{ Definition of } \Rightarrow\]  \hspace{1cm} (18)

\[= (B \mid A = (B \land D) \mid A) \text{ Distributivity of } |\]  \hspace{1cm} (19)

\[= (B \mid A = B \text{ for } A) \text{ Definition of for}\]  \hspace{1cm} (20)

So, \(B \text{ serves } A\) is equivalent to saying that \(B\) quoting \(A\) is the same as \(B\) for \(A\).
The delegation works if Carol believes $A$ controls ($B$ serves $A$) and $B$ for $A$ is on Carol’s access control list. We can see Carol’s reasoning below.

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1.</td>
<td>$A$ controls ($B$ serves $A$)</td>
</tr>
<tr>
<td>A2.</td>
<td>$K_A \Rightarrow A$</td>
</tr>
<tr>
<td>A3.</td>
<td>$K_A$ says ($B$ serves $A$)</td>
</tr>
<tr>
<td>A4.</td>
<td>$A$ says ($B$ serves $A$)</td>
</tr>
<tr>
<td>A5.</td>
<td>$B$ serves $A$</td>
</tr>
<tr>
<td>A6.</td>
<td>$B \mid A = B$ for $A$</td>
</tr>
<tr>
<td>A7.</td>
<td>$B \mid A$ says $s$</td>
</tr>
<tr>
<td>A8.</td>
<td>($B$ for $A$) says $s$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Rule</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Carol recognizes Alice’s authority</td>
<td></td>
</tr>
<tr>
<td>Carol knows Alice’s key</td>
<td></td>
</tr>
<tr>
<td>Delegation certificate signed by Alice</td>
<td></td>
</tr>
<tr>
<td>A2, A3, and P8</td>
<td></td>
</tr>
<tr>
<td>A1, A4, and definition of controls</td>
<td></td>
</tr>
<tr>
<td>From A5 and (20)</td>
<td></td>
</tr>
<tr>
<td>Request from Bob quoting Alice</td>
<td></td>
</tr>
<tr>
<td>A7, A6 EQ-LR</td>
<td></td>
</tr>
</tbody>
</table>

References


CSE 774: E-6f Delegation: 4