A GRAPHICAL DELEGATION SOLUTION FOR X.509 ATTRIBUTE CERTIFICATES

Isaac Agudo, Javier Lopez, Jose A. Montenegro
Computer Science Department, University of Malaga, Spain

Delegation is becoming a major topic for distributed authorization. Several approaches have been proposed in order to provide delegation in distributed environments. However, none of these matches all the requirements of a flexible delegation method. Based on work from the project PRIVILEGE[1], a flexible solution based on the use of graph theory is proposed.

Delegation is a major goal when a real scalable distributed authorization system is needed. However, the uncontrolled use of delegation statements can become an important security threat; for instance, any user could improperly obtain over a resource the same privileges as the owner of that resource. Therefore, delegation solutions should include a mechanism to control the delegation of privileges as well as making use of suitable authorization statements.

One of the first tasks in the project PRIVILEGE, developed in the Computer Science Department at the University of Malaga, has been to study and put into perspective the delegation implications of standard schemes that have been proposed in the literature as solutions for distributed authorization problems. As such, we have realized that in *PolicyMaker* and *Keynote* schemes, the delegation statement does not exist; that is, any authorization statement can be delegated once and then again without any control. On the other hand, *SDSI* considers three different possibilities for controlling delegation, although *SPKI* reduced it to a Boolean condition. Such a Boolean parameter is only a modest mechanism to control the depth of delegation.

There are more theoretical solutions that use logic programming for the representation of authorization and delegation statements. In logic programming, those statements are represented as predicates, and decisions are based on formulae verification. Although logic programming offers a powerful mechanism to represent authorization and access control decisions, it has important drawbacks: it is difficult to understand and has obscure transcription. Moreover, no logic solution has been integrated in any standard authorization framework.

Additionally, there are graphical solutions that are thought to be less powerful but more expressive and easily understood. A graphical solution may be based on the use of directed graphs to model authorization and delegation processes. Basically, this maps each credential in the system to a directed edge in a graph. Edges go from the issuer of the authorization or delegation statement to the subject who is authorized or granted privileges. Usually, the root of the tree is the owner of the resource under consideration. It is therefore possible to study the relations between entities in the system in a graphical way.

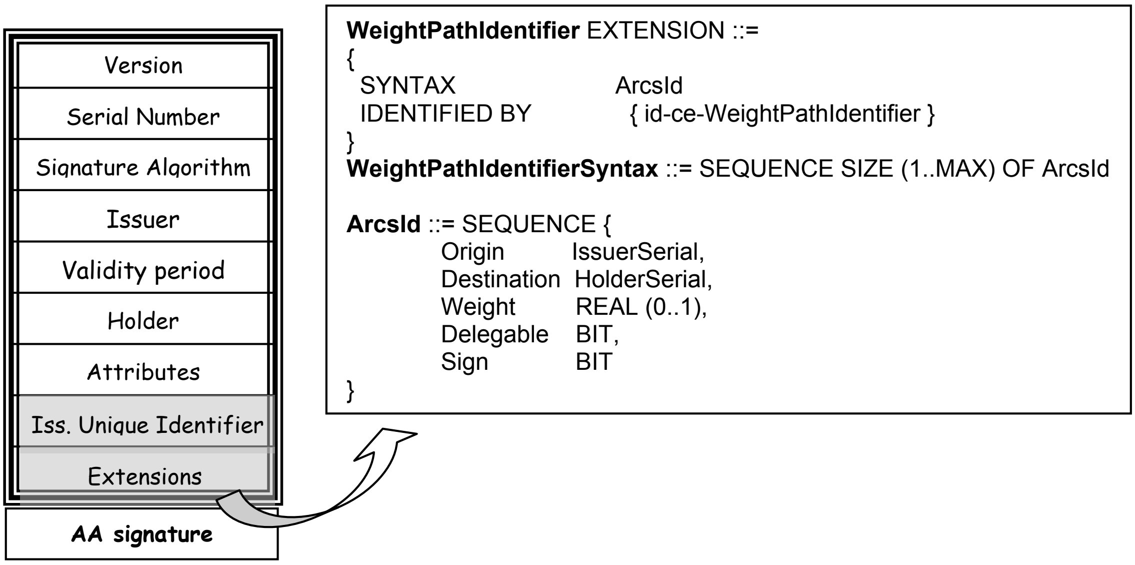
[1] The Research Project PRIVILEGE (TIC2003-8184-C02) has been funded by the Spanish Ministry of Science and Technology.

The project PRIVILEGE focuses on the use of X509 Attribute Certificates. Therefore, it includes a practical implementation of a *Privilege Management Infrastructure (PMI).* As part of our work, we have developed a mechanism to perform a controlled delegation that uses the extension fields of the attribute certificates. Our proposal is based on graphical solutions, attaching extra information to every edge in the graph. In particular, we include an index, a real number in the interval [0,1], that measures the level of confidence of the issuer on the issued certificate. Moreover, we distinguish between positive and negative statements. Positive ones grant the right encoded in the certificate and negative ones deny it. In order to encode it, we use the variable *sign* (see Figure 1). We also add another Boolean variable, *delegation,* to define whether the certificate can be chained, ie delegated.

We add this information directly in the certificate, by using the *extensions* field. This field allows us to include additional information into the attribute certificate. Although the X.509 standard provides several predefined extension categories, we focus on the delegation extension category, which defines different extension fields. Among them, the ITU-T recommendation includes:

> *Authority attribute identifier:* In privilege delegation, an AA that delegates privileges shall itself have at least the same privilege and the authority to delegate that privilege. An AA that is delegating privilege to another AA or to an end-entity may place this extension in the AA or end-entity certificate that it issues. The extension is a back pointer to the certificate in which the issuer of the certificate containing the extension was assigned its corresponding privilege. The extension can be used by a privilege verifier to ensure that the issuing AA had sufficient privilege to be able to delegate to the holder of the certificate containing this extension.

That extension is suitable for our purposes. However, it does not define the weight associated to the arc between the issuer and the holder of the certificate. Therefore, we define our own extension, in ASN.1 (Figure 1), based on the *authority attribute identifier*.



```
WeightPathIdentifier EXTENSION ::=
{
  SYNTAX                 ArcsId
  IDENTIFIED BY          { id-ce-WeightPathIdentifier }
}
WeightPathIdentifierSyntax ::= SEQUENCE SIZE (1..MAX) OF ArcsId

ArcsId ::= SEQUENCE {
          Origin        IssuerSerial,
          Destination   HolderSerial,
          Weight        REAL (0..1),
          Delegable     BIT,
          Sign          BIT
}
```

Figure 1: Attribute certificate and weight path identifier extension.

This new extension determines a sequence between the source of authority (SOA) and the holder. Each sequence includes another sequence, *ArcsId,* in which is included the information of the arcs in the graph, weight of the arc, origin node, and Boolean information about statements, delegation and sign. The destination node must match the serial number of the attribute certificate.

As the reader can infer, the design of authorization and delegation statements in a graphical mode can be converted automatically into X509 attribute certificate chains. The example included in Figure 2 shows the graphical design of delegation statements (normal line) and authorization statements (dotted line) and its equivalent representation using attribute certificates. Every attribute certificate stores, in the extensions field, the graphical information.

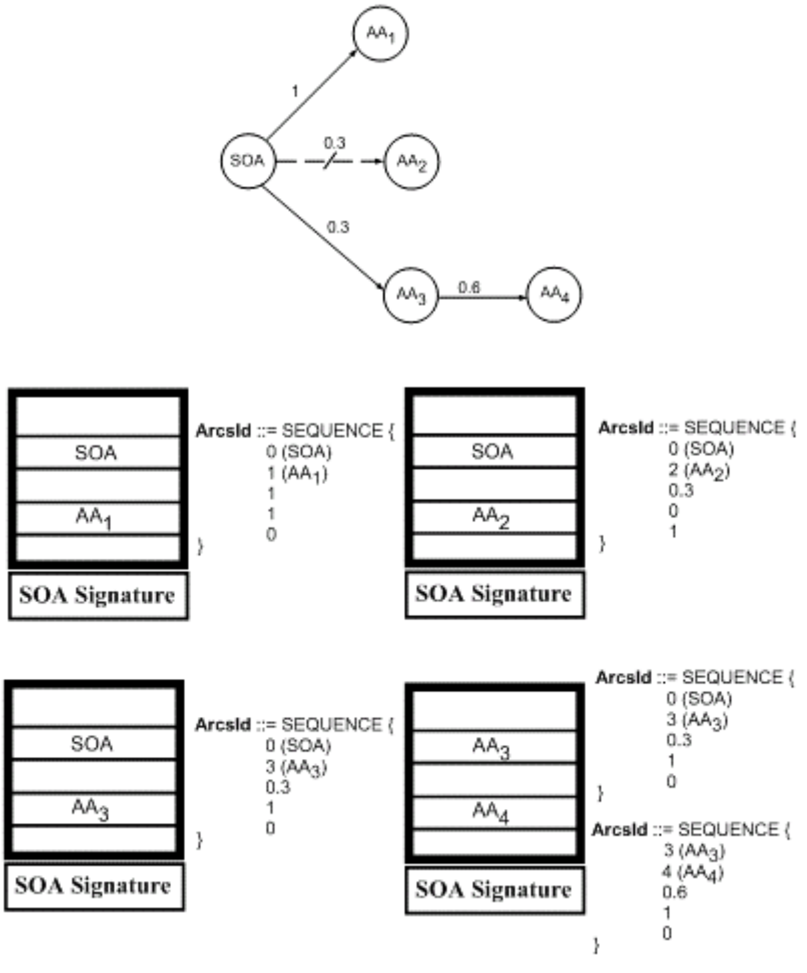


Figure 2: Design of statements and corresponding certificate chains.

PRIVILEGE will finish at the end of 2006, and is scheduled to have a complete practical implementation of the delegation solution, further elaborating on the complexity of management of delegation chains in fully distributed authorization systems.

Please contact:
Javier Lopez
Computer Science Department, University of Malaga, Spain
Tel: +34 952 131327
E-mail: jlm@lcc.uma.es