SensorNet Security Implementation

Because of this problem, we decided to replace user IDs and passwords with X.509 public Key Infrastructure (PKI) certificates.

SensorNet has decided to implement a Public/Private

To aid users in using and managing their certificates, SensorNet has developed extensive online help for users (Things that encourage the collaboratory aspects of SensorNet should be encouraged.

Infrastructure (PKI) has several advantages:

contains the encryption tools and information necessary to provide protection from most of these threats. SensorNet has decided to implement a Public/Private

We believe that this implementation meets the security requirements of SensorNet. Specifically

information is always required during the certificate issuance process to assure the true identity of a person, and to be sure that the correct person obtained the

SensorNet when their personnel change. When new organizations join SensorNet, Owners may have to redefine their policies for data access. Out-of-band

creates a list of allowed owners and functional labels, and returns it with an allowed status to the WFS server. The WFS server merges the request functional

3) The accessible owners list is passed to the database query

Currently there are no distinctions between owner read and write permissions. We believe that the different entity types and separate read/write functional labels

event, its location, and scope. The SPS will use this alert to (for example) add additional roles to First Responders near the event.

Done

field in the certificate for that entity type. The fields are populated from the LDAP which contains the information for all issued certificates. The fields in the

There is a different policy for each entity type (people, nodes, applications, servers). These policies are managed by the entity assigned by the owner of the data,

O=="Ft Bragg" && OU=="SSC" && !(T=="Test" || T=="Guest")

(name is SSgt Doe)

for Oracle, but an external function implemented in C is faster for PostgreSQL.

Consider the process flow for a wfs:GetFeature request (a query against the data).

1) The request includes a list of functional labels for data requested (and client certificate). in this example, the request specifies

model.dispersion.hysplit, model.

1) The request includes a list of functional labels for data requested (and client certificate). in this example, the request specifies

model.*, sensor.noaa.dcnet

model.effects.*, sensor.chem.*

Features Services (WFS) and Web applications use Secure HyperText Transport Protocol (HTTPS). HTTPS uses Transport Layer Security/Secure Sockets Layer

All SensorNet communications are encrypted to prevent eavesdropping and to assure data integrity (via the secure hashes used by the encryption protocols). Web

Energy (DOE) orders. However, these labels are not currently used for access control. Instead, SensorNet used separate but complementary mechanisms for type-

Alternatively, the WFS returns a list of possible functional labels, and the client has to reissue the request with the selected functional labels.

Role assignment for entities.

The Owner List interface as seen by an organization's manager.