SubjectAltNames in X.509 Certificates

Overview

X.509 certificates bind a public key to the contents of the Subject field, the SubjectAltName extension, or both. The SubjectAltName extension has become the preferred location for Email addresses (S/MIME), and is recommended for use in the host identification phase of TLS. SubjectAltName supports a variety of data types. Do current revisions of well-known web browsers support this method of verifying a server connection? We conducted a few experiments with the development version of the DOEGrids CA certificates to see if we can issue host certificates with this feature. [[Also could test openssl – based client; ldap; also could test S/MIME; need to decide on scope for final draft]]. Motivation, method, and the results of these tests are described in detail

Table of Contents

Introduction

X.509 certificates are used in a wide variety of applications, providing a means to assure identity, secure communications, encrypt data, sign data (such as other certificates), and deliver authorization information based on these capabilities [ref1]. The DOEGrids Certificate Authority issues certificates that are used by to identify subscribers in Grid applications; on an experimental basis, they are used in S/MIME based email to sign and/or encrypt data. They may also be used to encrypt data [ref2]. We discuss techniques used to

name the entity that owns the X.509 certificate. The X.509 section will describe the naming techniques available in the X.509 certificate. The standards bodies responsible for X.509 and for the various protocols and services that use X.509 certificates have been specifying how and why to use different naming techniques. But do the protocols and applications use these naming techniques? And why bother? The motivation section will discuss why we are interested in this problem. We have performed several experiments using our own custom certificates used in popular browsers [[and??]] to see how naming techniques are supported and how they interact. The tests section describes our methods and catalogues the results. Results show poor support in browsers for some naming choices [[and?]] [[and s/mime?]. Conclusions sums up these results and discusses changes to our service.

X.509 Certificates

X.509 certificates are defined by the ITU in a slowly-changing ITU-T Recommendation document as part of its Directory (X.500) series [ref]. DOEGrids certificates are used in web-based and Grid contexts, and these particular domains are further refined by the IETF PKIX working group's Certificate Profile documents [refs] and the IETF TLS specifications [refs]. TLS itself is only partly implemented in most environments and so the SSLv3 specification is more cogent [ref].

X.509 certificates bind the name of an entity in the real world, such as human being named "Barbara Jennings", to a public key. The name is referred to as the "Subject", and both subject field and public key are part of the certificate contents. This binding is usually done by a third party, and many other things may be added to the certificate, but we are only concerned with the subject name here. The subject name is in the form of an X.500 or LDAP directory name and is often identical to the entity's directory name. Because of that close association the X.509 certificate subject name is often called the distinguished name, which really has meaning only in the directory.

There is an alternate representation of the subject name available in X.509v3 and later certificates, in the form of an X.509 extension called "SubjectAltName". This extension is defined fully in the X.509 document. It is a structure supporting several different identified name types as well as multiple entries. [[insert representation from X.509 8.3.2.1]].

[[We are interested here in which types: dnsname, rfc822name, ipaddress; what is happening in ipv6?]]

X.509 certificates contain a large number of fields and extensions, many optionally. We are only concerned here with the interaction between the subject field and the subjectaltname extension.

Motivation

SSLv3 and TLS

TLS does not specify a particular naming convention or rule for X.509 certificate subjects [ref]. However, certain protocols which employ TLS to support security services have adopted a hostname check as part of the identification phase of the protocol. This is the standard practice in web servers. A web server using SSL will present a certificate to the client, and this certificate will contain a fully qualified domain name in the CN component of the subject field. [[Discuss the way sslv3 describes this and the informational rfc for TLS]].

An internet draft for LDAPv3 requires the same behavior for an LDAP server using TLS. Note that this is currently a standards-track draft [ref].
The Common Name (CN) of the Subject DN can be a descriptive server name or fully qualified domain name, if the entity is server or service. In addition to that the 'SubjectAltName' extension may contain additional Domain Names, rfc822names,or ipAddresses.
It became customary for clients, such as browsers, to do an additional check on the certificate it receives from the server. This test checks a hostname in the certificate subject against the hostname it determines through some means. [[Describe web host name check, ldap hostname check, and globus hostname check; web based is, "Does the cert contain a name that matches the URL I use to connect?" The Globus hostname check is more like tcpwrappers [ref], which is (connecton-ip->name = cert-hostname ? good : bad) … I think. Must check details]]
It is often desireable for one server to support multiple names. An ISP might offer a virtual hosting service. Services might consolidate onto a single server, or a single service might be deployed on multiple platforms. There are many scenarios where a certificate containing multiple identities would improve the efficiency of the operation without any loss of assurance.
The obvious solution would be to add multiple names to the certificate subject. This does not work in a directory based PKI, because the resulting subject name does not describe a sensible directory entry. Besides the architectural objection, in practice it simply does not work [[should we also include this case in experiments]].
Ipaddresses, DNS names, and email addresses also represent structured naming systems that are outside the control of the directory, and objections have been raised to having such information in directory relative distinguished names [ref: Steve Kent correspondence]. SubjectAltName extension was developed and added to the X.509 standard to provide a way to deal with these problems. New IETF RFC's promote the use of this extension as a container for one or more server host names, client email addresses &c [refs]. The acceptance of these standards or recommendations by IETF security working groups suggests these uses should be deployed in the DOEGrids CA's if possible. The use and impact on Globus software is unclear; however, Globus makes use of openssl software to support GSI [refs]. [[If openssl clients do something good , bad, or indifferent with SubjectAltName we can expect Globus might act accordingly. We may also be able to help Globus developers with this.]]
.

[[S/Mime]]

Tests

[[Need to list plan, other tests, decide what we will and won't do &c. See above for note on checking multi-cn case.]]

DNS Host name as identifying name - Test Server

- Server with Multiple hostname (beryl.es.net, ldap.doegrids.org & ldap.doesciencegrid.org)
- Each hostname corresponds to different IPaddress

- Running iPlanet Web Server, Enterprise Edition 6.0

Test Data

Certificate X: Subject: CN=beryl.es.net,OU=Services,O=doegrids.org

Certificate A:
Subject: CN=beryl.es.net, OU=services, O=doegrids.org.
SubjectAltName: ldap.doegrids.org
ldap.doesciencegrid.org

Certificate B:
Subject: CN=test web server, OU=services, O=doegrids.org.
SubjectAltName: beryl.es.net
ldap.doesciencegrid.org
ldap.doegrids.org

Certificate C:
Subject: OU=services, O=doesciencegrid.org.
SubjectAltName: beryl.es.net
ldap.doesciencegrid.org
ldap.doegrids.org

Test Cases

- Install Certificate A with iPlanet Web Server
- Access the secured web site https://beryl.es.net using Internet Explorer 6.0
- Access the secured web site https://ldap.doegrids.org using Internet Explorer 6.0
- Access the secured web site https://ldap.doesciencegrid.org using Insternet Explorer 5.0
- Record the results
- Continue the same test using Opera 6.02, Netscape 4.79, Mozilla 1.0 and Netscape 6.2 browsers

-Repeat the test with Certificate B installed with iPlanet Web Server
-Repeat the test with Certificate C installed with iPlanet Web Server

Test Results

Browsers	Cert A	Cert B	Cert C
Internet Explorer 6.0			
beryl.es.net	SA	Works Fine	Works Fine
ldap.doegrids.org	Works Fine	Works Fine	Works Fine
ldap.doesciencegrid.org	Works Fine	Works Fine	Works Fine
Netscape 4.79			
beryl.es.net	Works Fine	CNC	ERR
ladp.doegrids.org	CNC	CNC	ERR

ldap.doesciencegrid.org	CNC	CNC	ERR
Mozilla 1.0			
beryl.es.net	Works Fine	DNM	NULL
ldap.doegrids.org	DNM	DNM	NULL
ldap.doesciencegrid.org	DNM	DNM	NULL
Netscape 6.2			
beryl.es.net	Works Fine	DNM	NULL
ldap.doegrids.org	DNM	DNM	NULL
ldap.doesciencegrid.org	DNM	DNM	NULL
Opera 6.02			
beryl.es.net	Works Fine	WCN	WCN
ldap.doegrids.org	WCN	WCN	WCN
ldap.doesciencegrid.org	WCN	WCN	WCN

CNC – Certificate Name Check warning
DNM – Domain Name Mismatch Security Warning/Error
WCN – Wrong Certificate Name warning
SA – Security Alert (does not match the name of the site)
ERR – out of memory error
NULL – identity problem “null”

Conclusion

Hostname as identifier

Only Internet Explorer 6.0 behaved in a useful fashion. Opera and the various Netscape browsers are only capable of using CN of the subject as the basis for an SSL hostname check. IE 6.0 will use either the DNS contents of SubjectAltName, or Subject's CN= AVA, but not both. [[is this acceptable to the various stds docs?]]
[[openldap or other clients; openssl based clients; java sec clients]]

[[S/MIME?]]

Impact on PKI

Issuing certificates for S/MIME with email address in the SubjectAltName has proved very useful and without any undesirable side effects. [[what about multiplei id's]]
Issuing host certificates for use in SSLv3 servers with the host's fully qualified domain name or names in SubjectAltName may cause problems due to the lack of support for this use of the extension in most browsers. Only a Subject field that contains a CN=fully qualified domain name (such as CN=foo.es.net) can be expected to be managed well by clients. Clients will receive warning messages that they do not understand in interactive applications, and automated processes (such as scripted web clients) will behave unpredictably, when they attempt to use servers with complex certificates supporting multiple name choices.

Impact on CA

[[SMIME]]

Host and Service certificates

Harmless to issue certificates with fully qualified domain name in SubjectAltName, but must contain the FQDN in subject also.
Do not issue multiple subjectaltname entry certificates. [?]

References

[RFC2459] – Section 4.2.1.7 Subject Alternative Name
[RFC3280] - Section 4.2.1.7 Subject Alternative Name
[Need to insert end notes, tons of references not filled out above]