NFSv4 C. Lever
Internet-Draft Oracle
Intended status: Standards Track July 11, 2013
Expires: January 12, 2014

Federated Filesystem Security Addendum
draft-cel-fedfs-security-addendum-01

Abstract

This document addresses critical security-related items that are missing from existing FedFS proposed standards.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 12, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

Requirements for federated filesystems are described in [RFC5716]. Specification of the protocol used by administrators to configure fileservers and construct namespaces is provided in [FEDFS-ADMIN]. Specification of the protocol allowing fileservers to store namespace information is provided in [FEDFS-NSDB].

These documents are now immutable. However, some security-related concerns have arisen that should be addressed immediately rather than waiting for another version of these protocols to be ratified.

1.1. Problem Statement: GSSAPI service name for ADMIN

After IESG review, the Security Considerations chapter of [FEDFS-ADMIN] now specifically requires that implementations of this protocol support GSSAPI security mechanisms.

ADMIN protocol clients must use a service principal to establish a GSS context shared with an ADMIN server. To construct the service principal, clients need to know a priori the protocol's GSSAPI service name. The form of that service name is described in chapter 4 of [RFC2724].

According to [RFC2743], requesting an addition to the "GSSAPI/ Kerberos/SASL Service Names" registry requires a specification. Because [FEDFS-ADMIN] cannot be changed, a new specification must be provided.

1.2. Problem Statement: Compromised NSDBs

The FedFS ADMIN RPC protocol provides a mechanism for provisioning NSDBs on remote fileservers. The operations it provides are FEDFS_SET_NSDB_PARAMS, FEDFS_GET_NSDB_PARAMS, and FEDFS_GET_LIMITED_NSDB_PARAMS.

FEDFS_SET_NSDB_PARAMS specifies the name of an NSDB and the security mode to use when connecting to this NSDB. The fileserver connects to an NSDB in order to resolve a FedFS junction. The ADMIN protocol specification further says:

> On success, this operation returns FEDFS_OK. When the operation returns, the new connection parameters SHOULD be used for all subsequent LDAP connections to the given NSDB. Existing connections MAY be terminated and re-established using the new connection parameters. The connection parameters SHOULD be durable across fileserver reboots.

There are two security modes defined in the protocol specification: FEDFS_SEC_NONE, which does not authenticate the LDAP server; and FEDFS_SEC_TLS, which uses START_TLS (RFC 4513) to authenticate the LDAP server.

When FEDFS_SEC_TLS is specified with the FEDFS_SET_NSDB_PARAMS operation, an x.509v3 certificate chain is also provided to the fileserver. The fileserver uses the provided certificate to authenticate subsequent connections to this NSDB. The FEDFS_SET_NSDB_PARAMS operation can change the connection security used by a fileserver to connect to a particular NSDB from NONE to TLS or TLS to NONE.

Over time, domain administrators add NSDB connection parameters to each of their fileservers to enable FedFS junction resolution. The specified NSDB may be the domain's own, or it might be an NSDB in a foreign domain.

Many junctions on multiple fileservers can be created that use a particular NSDB. There is no way to find such junctions without an exhaustive search. Since filesystem namespace topology can evolve arbitrarily over time, a recorded pathname of any junction is almost guaranteed to become stale.

Now suppose we have two FedFS domains: example.net and university.edu. Suppose university.edu fileservers have a number of junctions that refer to locations maintained by example.net, and thus university.net's fileservers are configured to resolve junctions on example.net's NSDB.

One day Mallory compromises example.net's NSDB, but the domain administrator there is on a long vacation. The administrator at university.net discovers the compromise immediately, but has no control over the foreign NSDB and cannot create a fresh x.509 certificate or verify that the contents of the NSDB are unmolested. The only choice is to find and remove every junction in the university.edu domain that contains the compromised NSDB.

If university.edu is using a good implementation of FedFS, the administrative tools it provides might allow an administrator to simply visit each of its fileservers and mark the example.net NSDB as compromised. Any junction resolution that attempts to use that NSDB would fail, but all junctions remain in place. When example.net's administrator gets back from holiday and cleans up the mess, the university.edu administrator can then update each of her fileservers with fresh connection parameters for that NSDB.

However, none of this can be done remotely using the FedFS ADMIN protocol. It does not have a mechanism for removing NSDB connection parameters or for fencing a compromised NSDB.

1.3. Scope Of This Document

This document specifies additional requirements for the FedFS ADMIN protocol specified in [FEDFS-ADMIN], which is a standards track specification.

2. GSSAPI Service Name for the FedFS ADMIN protocol

Section 6 of [FEDFS-ADMIN] requires a FedFS ADMIN server to support the RPCSEC_GSS framework [RFC2203]. The present document specifies the GSSAPI service name, as described in Section 4.1 of [RFC2743], to be used for the FedFS ADMIN protocol.

Regardless of what security mechanism under RPCSEC_GSS is in use, a FedFS ADMIN server MUST identify itself in GSSAPI via a GSS_C_NT_HOSTBASED_SERVICE name type. GSS_C_NT_HOSTBASED_SERVICE names are of the form:

```
service@hostname
```

For the ADMIN protocol, the "service" element is

```
fedfs-admin
```

Implementations of security mechanisms will convert fedfs-admin@hostname to various different forms. For Kerberos V5, the following form is RECOMMENDED:

```
fedfs-admin/hostname
```

This service name SHOULD NOT be used to authenticate other GSSAPI services.

3. Fencing Compromised NSDBs

An NSDB is considered "foreign" relative to a particular FedFS domain if that domain's administrator has no administrative access to that NSDB.

When a FedFS domain administrator is faced with a foreign NSDB that is compromised or otherwise unusable, and in the absense of an implementation-provided mechanism for fencing an NSDB, the administrator can fence that NSDB using the following technique.

1. The administrator locally generates a new certificate for the compromised foreign NSDB. The certificate can be self-signed, or signed by the administrator's local certificate authority.

2. The administrator distributes this certificate to all of her domain's fileservers using the FedFS ADMIN protocol or some other secure means. The connection security for the foreign NSDB is set to FEDFS_SEC_TLS on each of the local domain's fileservers.

3. The administrator requests fresh certificate material from the administrator of the foreign NSDB.

4. When the threat has passed and the foreign NSDB is safe to use again, the administrator can distribute the new valid certificate material to her domain's fileservers.

No change to the ADMIN protocol as specified in [FEDFS-ADMIN] is required to fence a compromised NSDB. Step 2 guarantees that, on fileservers in the administrator's local FedFS domain, resolving a junction that references the compromised foreign NSDB will fail until updated certificate material is provided.

4. Security Considerations

There are no additional security considerations.

5. IANA Considerations

In accordance with Section 4.1 of [RFC2743], the service name "fedfs-admin" will be registered in the GSSAPI Service Name registry at http://www.iana.org/assignments/gssapi-service-names/ gssapi-service-names.xml

The new entry should reference the present document as the specification.

6. Acknowledgements

The author of this document gratefully acknowledges the contributions of Nico Williams, Spencer Shepler, Tom Haynes, and David Noveck.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2203] Eisler, M., Chiu, A., and L. Ling, "RPCSEC_GSS Protocol Specification", RFC 2203, September 1997.

[RFC2743] Linn, J., "Generic Security Service Application Program Interface Version 2, Update 1", RFC 2743, January 2000.

7.2. Informative References

[FEDFS-ADMIN] Lentini, J., Everhart, C., Ellard, D., Tewari, R., and M. Naik, "Administration Protocol for Federated Filesystems", draft-ietf-nfsv4-federated-fs-admin (Work In Progress), 2010.

[FEDFS-NSDB] Lentini, J., Everhart, C., Ellard, D., Tewari, R., and M. Naik, "NSDB Protocol for Federated Filesystems", draft-ietf-nfsv4-federated-fs-protocol (Work In Progress), 2010.

[RFC2724] Handelman, S., Stibler, S., Brownlee, N., and G. Ruth, "RTFM: New Attributes for Traffic Flow Measurement", RFC 2724, October 1999.

[RFC5716] Lentini, J., Everhart, C., Ellard, D., Tewari, R., and M. Naik, "Requirements for Federated File Systems", RFC 5716, January 2010.

Author's Address

Charles Lever
Oracle Corporation
1015 Granger Avenue
Ann Arbor, MI 48104
US

Phone: +1 734 274 2396
Email: chuck.lever@oracle.com