September 16, 1988

MEMORANDUM

To: Barbara Greene, Earll Murman, Dan Geer, Jennifer Steiner, George Champine, Charles Salisbury, Jeff Schiller, Tom Ehrgood, Ron Orcutt

Subject: Kerberos export plan, issues, and action items

After many discussions with each of you the following is beginning to take shape as the most plausible approach to exporting the Kerberos authentication system outside the U.S.A. The basic issue being addressed is that Kerberos uses software encryption, and therefore falls under export controls that are potentially quite stringent. The encryption algorithm that Kerberos uses is the Data Encryption Standard (DES). At the present time, Version 1.2 of Kerberos has been in production use at M.I.T. for about 2 years, and has been in beta test at several other sites in the U.S. for about 3 months. The results of that initial use at M.I.T. and reports from the beta test will probably lead to one more round of refinement of its design before final distribution, probably with a version number of 2.0. The proposal here is intended for export of the current version, 1.2; if successful the same approach can be used for version 2.0 when it becomes available.

Summary of the proposal:

- Prepare an export version of Kerberos that omits the encryption (DES) library.

- Consider the resulting export version to be ordinary, not cryptologic, software, and export it with a General Technical Data (Restricted) (GTDR) license, only to countries to which GTDR applies. The mechanics of a GTDR license are simple: the sender checks that the importer is in an acceptable country, obtains advance assurance from the individual recipient that there will be no reexport, then simply labels the package appropriately.

- The recipient provides a DES implementation and casts that implementation into the form specified in the library definition in the manual page section DES_CRYPT(3). The laws applying to cryptography in the importing country should be reviewed to insure that this implemntation can be done legally. In some instances, the encryption library may have to be replaced with a non-DES library, in which case authentication interchange with Kerberos sites that use DES encryption will not be possible.

- Obtain, in all specific cases where it appears possible, a validated license for the export of the DES library. This license, in conjunction with the GTDR for Kerberos itself, would greatly simplify acquisition of Kerberos in those cases where it can be used.

- Arrange that all actual export and validated licenses be obtained by Digital, IBM, or other vendors, thereby avoiding the need for M.I.T. to be directly involved.

There are several issues to be resolved, and a surprising number of action items that must be completed to carry out this proposal. In some cases an action item cannot begin until some other action item is completed; these cases are indicated by a parenthesized list of prerequisites following description of the action item.

Issue 1. Would a DES-less Kerberos come under Commerce Department export supervision and the rules that allow GTDR licenses, or would it still require a specific validated license, anyway? The basic question seems to be whether or not Kerberos is cryptologic software even it the version being exported doesn't include an implementation of an encryption algorithm. This is a matter of interpretation that would probably require advice from NSA and perhaps a statement from the State Department Office of Munitions Control.

Action items:

1.1 Obtain NSA advice based on complete description of Kerberos. (Prerequisites: 2.2, 8.2, 5.1. See also 4.2, 6.1, and 7.2)
1.2 If favorable, obtain statement from State Department. (Prerequisites: 1.1)
1.3 Apply for license for DES library. (Prerequisites: 1.1)
1.4 Export, omitting DES. (Prerequisites: 1.2, 3.1)
1.5 Export, including DES. (Prerequisite: 1.3)

Issue 2. Can a good programmer implement the DES library given only our specification in the DES_CRYPT(3) man pages plus a copy of the Data Encryption Standard specification, or an already-available implementation of DES? There are three possible problems:

- accuracy/currency/completeness of our documentation of the interface.
- Kerberos defines and requires a new chaining mode, named pcbc, that is not in the DES standard.
- the string-to-key algorithm is not documented.

We won't know about accuracy/currency/completeness until someone gives it a try and attempts to run the result against a standard Kerberos server. The pcbc chaining mode appears to be adequately defined in the document; again a test is required to know for sure.
String-to-key is definitely not implementable with the information currently in the documentation; a new version of the document is in preparation; that new version is intended to define string-to-key.

Action items:

2.1 Revise the document to include description of string-to-key algorithm. (Prerequisite: 8.2)

2.2 Verify that the entire library can be implemented by having someone do it with only the documentation and a public domain implementation of DES. (Prerequisites: 2.1)

Issue 3. Can the man page DES_CRYPT(3) be exported as part of the documentation of a Kerberos that omits the DES library, or does it by itself bring the package into the category of cryptologic materials?

Possible resolution: It has been proposed that to ensure that the document DES_CRYPT(3) is exportable, we should get it into the public domain by having it published. That can be done as soon as it is revised in accordance to other requirements of this plan.

Action item:

3.1 Arrange for publication of the revised man page. (Prerequisites: 2.2, 5.1, 7.1)

Issue 4. There is a library, known as DES_NOOP, that replaces the encryption algorithm with a program that returns as the output cipher block the original cleartext block. The export version of Kerberos should include this library as a replacement for DES_CRYPT, so that the importer can immediately determine that all of Kerberos except for the encryption library is actually workable. Two problems are involved:

a. The DES_NOOP library replaces only the basic encryption algorithm; it does not replace the implementations of cipher chaining, etc. Those subroutines, if included, may require a validated license.

b. DES_NOOP has been used only to verify that clients not using encryption properly fail to communicate with clients that are using encryption. To my knowledge, noone has assembled a complete working version of Kerberos and verified that it is self consistent when used with DES_NOOP rather than with DES_CRYPT.

Action items:

4.1 Construct a complete working version of Kerberos that uses the NOOP encryption library. (Prerequisites: 8.2)

4.2 Prepare and include documentation of NOOP library in the inquiry to NSA and in the request for clearance from State department. (Prerequisite: 5.3)

Issue 5. The library named DES_CRYPT, the library named DES_NOOP, and the interface specification named des.h all unnecessarily invoke the name of the Data Encryption Standard. This invocation is quite misleading. Nothing about the library is specific to the DES algorithm and the libraries define an interface between Kerberos and any desired block encryption algorithm. To avoid confusion among people making export and import decisions these three items should be renamed KRB_CRYPT, KRB_NOOP, and krb_crypt.h, respectively, and three subroutines of DES_CRYPT should be renamed to avoid the unnecessary invocation of the name of DES.

Action items:

5.1 Revise documentation of DES_CRYPT to eliminate references to DES. (Prerequisites: 8.2)
5.2 Revise Kerberos to use non-DES subroutine call names. (Prerequisite: 8.2)
5.3 Revise DES_NOOP to eliminate references to DES. (Prerequisite: 8.2)

Issue 6. There are two programs named "test" and "verify" that are used to debug the DES implementation and to verify that it conforms with the standard by applying test cases that have known results. Does including the "test" and "verify" programs bring the package into the category of cryptologic materials?

If we avoid this issue by omitting test and verify from the export version of Kerberos, recipients will find that they are faced with a much more difficult debugging job, and a significant risk of constructing an encryption library that is self-consistent but that does not exactly implement the standard; such an implementation may have unevaluatable security risks and it would not allow interchange of authentication with other implementations.

Action item:

6.1 Document the programs named test and verify, and include that documentation in requests to NSA and State, with plan to pull them out if they interfere with approval to use GTDR. (Prerequisite: 8.2)

Issue 7. There is an interface specification written in the C language, known as "des.h". Does including the file des.h bring the package into the category of cryptologic materials? This file currently contains two kinds of specifications; some are used for communication between different parts of the encryption library implementation, while others are used for communication between the library and its client.

Resolution: Move from des.h to krb_crypt.h those things required for clients of the encryption library, leaving things needed for communication within the DES library in a separate des.h file that then becomes part of the DES version of the KRB_CRYPT library. Then review the result against issue number 1, above, to see if it changes the conclusion.

Action items:

7.1 Create krb_crypt.h, Revise des.h and rebuild entire Kerberos system to verify that all parts still work. (Prerequisite: 8.2)

7.2 Include revised krb_crypt.h in published specification of Kerberos and in the representations to NSA and State. (Prerequisite: 7.1)

Issue 8. It is in everyone's interest to insure that M.I.T.'s policies and requirements with respect to Kerberos export are

coordinated both with Digital Equipment Corporation and with IBM.

Action items:

8.1 Review this proposal with M.I.T. legal staff.

8.2 Review this proposal with Digital legal staff.

8.3 Review this proposal with IBM legal staff.

Issue 8. A substantial amount of currently unscheduled and unbudgeted system development programming and documentation is required to do all the things described above. The priority of this work required for export should be evaluated against the priority of other Project Athena activities to determine how soon it can be done.

Action items:

8.1 Evaluate effort required.

8.2 Decide whether, when, or where resources can be reallocated to do it. (Prerequisite: 8.1)
