January 10, 1989

MEMORANDUM

To: Earll Murman, Dan Geer, Jeff Schiller, Ron Orcutt

From: Jerome H. Saltzer

Subject: Kerberos export plan, issues, and action items

Here is the state of the Kerberos export situation, and my recommendation for how to proceed.

1. Solving the immediate export problem for Bond University. I have obtained consensus from both the IBM lawyer, Bill Kushner, and the Digital lawyer, Tom Ehrgood, that if we produce a version of Kerberos that does not call on any encryption routines, that version can be exported as ordinary software. This step requires doing more than simply replacing the encryption routines with dummies; the actual calls must be removed from the source. The line of reasoning here is that NSA would consider a version of Kerberos with a dummy encryption package to be "ancillary encryption equipment" and even though they might approve its export they would require a specific license for every case. Ordinary software can be exported with a General Technical Data, Restricted, license, which means that the exporter need only obtain a letter from the importer saying it won't be re-exported to restricted countries.

John Kohl is in the process of preparing a version of Kerberos that meets that specification. His version has the appropriate lines of code "#IFDEF'ed" out; the actual export version should be run through a program that strips out the "#IFDEF'ed" code.

This version of Kerberos constitutes a standard protocol for a client to obtain and present credentials to a server. Because encryption is not used, the credentials are easily forged. Thus protection is effective only against users who are not knowledgeable; there is very little protection against a skilled attacker. This early export version is primarily of interest because it permits one to use all of the standard client/server software of the Athena system without having to go through and rip out all the places where Kerberos mediation is used. The value to Bond University (and to other sites) is the ability to begin using the Athena system much sooner.

Barbara Greene has not yet been apprised of this approach, but since both of our vendors' lawyers agree that it is OK, I don't know any reason why M.I.T. should not find it acceptable, too.

George Champine has raised the question of whether or not the resulting system should be given a name different from Kerberos, so that noone will be confused as to whether or not security is provided. (Does anyone know the name of a toothless Greek dog?)

Tom Ehrgood of Digital, has requested a functional description of this early-export version with the intent that he review it informally with NSA to insure against potential problems.

2. New developments. Tom Ehrgood reports that at the beginning of December, NSA announced a new policy intended to make it easier to export mass-marketed software. Although the policy is clearly intended to apply to people developing encryption packages for PC's, it may be possible to get it to Kerberos. The key requirements are that the encryption package be designed to be usable on personal computers and that it not use a "strategic" encryption algorithm. Kerberos did at one time run on PC's, and we should probably revive the PC version of Kerberos to make this part of the case consistent and solid. The main hassle is that the DES encryption algorithm is "strategic".

Barbara Greene has not yet been apprised of this development.

A memo from Tom Ehrgood is attached that outlines the new policy.

3. Jim Bitzos of RSA Security has proposed creating a non-strategic encryption algorithm that could be placed in the public domain. Although it probably would not be as secure as DES, it would certainly be adequate for most applications of Kerberos. RSA Security has a family of algorithms, including a proprietary one known as RC/2; they would develop another algorithm from that family for this purpose. Bitsos said that a contract to do this job would probably cost much less than $100,000. George Champine has inquired of the Open Software Foundation whether or not they might be interested in supporting such a project, with the intention that they also have uses for a non-strategic, exportable algorithm.

I recommend that this avenue be pursued as strongly as possible. The next step is to ask George if he can obtain the next level of commitment from OSF, and take that next level of commitment back to RSA for further discussion. (The immediate goal would be to get OSF and RSA into direct discussion and move Athena to the sidelines.)

4. Changes to Kerberos. One of the changes that should be made to the next version of Kerberos is the addition of a field to the protocol that specifies what encryption algorithm, if any, is to be used for this transaction. This change permits the early export (non-encrytpion) version, the DES version, and a non-strategic algorithm to coexist and possibly even to intercommunicate for certain situations.

5. On-line distribution. My discussion with NSA generated the remarkable conclusion that there is no objection to our making Kerberos available for anonymous FTP along with our other software, as long as there is a clear notice that export requires a license. What is really going on here is that they would like to control this path, too, but NSA fully realizes that there is no appropriate way to do so.

6. Summary of recommendations:

   - complete the early export (encryption-free) version of Kerberos
   - prepare a functional description of the early export version and give it to Tom Ehrgood to review with NSA
   - continue to use DES for domestic Kerberos applications
   - Get OSF to fund creation of a public domain non-strategic algorithm
   - Create a late export (public domain encryption) version of Kerberos
   - Let all actual export be done by DEC, IBM, Apollo, etc.
   - Get Barbara Greene to run this plan by her legal consultants

7. Other loose ends.

   - Apollo (Bill Sommerfeld) has requested permission to redistribute the M.I.T. implementation of string_to_key. Since we have agreed that it will be released anyway, I see no reason not to grant that permission.

   - I will turn over the complete paper file to Ron Orcutt for safekeeping.

8. Contacts

Digital Equipment Corporation export legal specialist:

Tom Ehrgood (202) 383-5698
DEC
1331 Pennsylvania Avenue NW
Suite 650
Washington, D.C. 20004

IBM Corporation program manager, export control:

Bill Kushner (202) 778-5519
IBM Corp.
1801 K Street
Washington, D.C.

Defense Department specialist who can offer advise as to what NSA will and won't approve. (At NSA; contact should be made by Kushner and Ehrgood rather than directly.):

Dale Peterson (301) 688-7834

President of RSA Security, Inc. (N.B., further contact info may be obtained from Prof. Ron Rivest at M.I.T. X 3-5880, mail address <rivest@Theory.lcs.mit.edu>:

James Bitzos (415) 595-8782

Date: Tue, 27 Dec 88 09:57:38 PST
Message-Id: <8812271757.AA28182@decwrl.dec.com>
From: ehrgood%wnpv01.DEC@decwrl.dec.com (TOM EHRGOOD, CORP. LAW, 427-5698)
To: Saltzer@ATHENA.MIT.EDU, EHRGOOD%wnpv01.DEC@decwrl.dec.com
Subject: Kerberos - Possibility Of Commerce Jurisdiction

> I guess that leaves the following question: Can ANY encryption
> algorithm, no matter how light-weight, ever end up in your category
> 4, if it permits message encryption? Jim Bitzos (president of RSA)
> seemed to believe that he could build one that would qualify, based
> on his experience dealing with NSA. You sound skeptical, based on
> your experience.

Jerry,

I have today discovered a freshly-minted policy being applied by NSA and the State Department. Under this policy, State will issue commodity jurisdiction determinations placing under Commerce jurisdiction file encryption products meeting the following criteria:

1. The product is micro-computer based software.

   Comment: Purpose of this criterion is to exlude mainframe applications. The NSA official who explained the policy indicated that there is some "flexibility" here. Applications that run on both workstations and micro-computers would meet this criterion.

2. The algorithm is "non-strategic."

   Comment: DES will never meet this criterion. RC2 would almost certainly meet this criterion, assuming that criteria 3 and 4 are met. (RSA's MailSafe does not meet #3.)

3. The file encryption application is a subset of a larger SW package. If the whole application is a security application (e.g., MailSafe), the criterion would not be met.

   Comment: My sense is that Kerberos, as one piece of the overall Athena SW package, would meet this criterion.

4. The file encryption application meets Commerce's "mass-market software" definition.

   Comment: Commerce has published a proposed new section 15 C.F.R. section 779.5(c)(4), which would establish a new category of sofware - "mass market software" - qualifying for a new General License GTDU (essentially, the old GTDR but w/o need for written assurance). Software falling into this category would be software that is available from a "retail source" and that meets the following five criteria:

- the software is not specially designed or modified for use by a specific individual or party;

- the software is designed for installation by the user;

- the software is specially designed for use on computers exceeding Note 9 parameters;

  Comment: Computers having PDRs in excess of 43 and virtual memory exceeding 512 exceed Note 9 parameters. Some workstations using Athena applications will exceed Note 9. Others will not.

- the software is designed and produced for civil applications; and

- the software is not designed or modified for computers designed and produced within a restricted country.

Commerce has not figured out what a "retail source" is. It may be that any method of distributing an application in small numbers or singly - to users - will qualify.

Bottomline on "mass-market software": Athena applications MIGHT meet the definition.

Based on first impression, a "non-strategic algorithm"-based Kerberos might fall into my Category 4. My caution this time is that it may not be as simple for Athena to do this with Kerberos as it would be for RSA to do this if certain SW application developers built RSA's RC2 algorithm into their products.

I look forward to your sense of whether this might work.

Regards,
Tom