From: Kenneth J Hendrickson
To: Microsoft ATR
Date: 1/27/02 7:39pm
Subject: Microsoft Settlement

[Text body exceeds maximum size of message body (8192 bytes). It has been converted to attachment.]

Date: 27 January 2002

To: microsoft.atr@USDoJ.gov
Subject: Microsoft Settlement

To:
Renata B. Hesse
Antitrust Division
U.S. Department of Justice
601 D Street NW, Suite 1200
Washington, DC 20530-0001

From:
Kenneth J. Hendrickson
2747 W. Anklam Rd., Apt E.
Tucson, AZ 85745-3705

Dear Renata,

Executive Summary:

I strongly urge the Department of Justice (DoJ) and the Court to modify the Proposed Final Judgment (PFJ) in order to achieve an effective remedy against a continuing Microsoft monopoly, and the harm to consumers that will inevitably continue to result.

The modifications I recommend are:

1 Microsoft must be required to publish COMPLETE and ACCURATE documentation for all Application Programming Interfaces (APIs), protocols, and file formats, for *ALL* Microsoft products. This should include a requirement to publish full and complete source code. However, as the source is likely to be very difficult to understand, Microsoft must also be required to fund an independent documentation effort to study the source code and completely and accurately document it. Such documentation and source code must be made available AT NO CHARGE to anybody who wants it, via an Internet download. In addition, Microsoft must NOT be allowed to require a Non-Disclosure Agreement (NDA) in order to obtain this important information.

2 Security considerations must NOT be an excuse for continuing the harmful practice of closed, hidden, and/or undocumented APIs, protocols, and file formats. All algorithms, APIs, protocols, and file formats, must be COMPLETELY and ACCURATELY documented, *ESPECIALLY* when those algorithms, APIs, protocols, and file formats are needed for security and authentication. Sections III.J1 and III.J2 should be entirely stricken from the PFJ.

3 Microsoft must not be allowed to use its patents offensively. A patent is a government granted monopoly. As Microsoft already has a monopoly (even without government granted patents), and has been convicted of illegally ABUSING that monopoly, the government should not be in the business of granting Microsoft more monopoly power with which to abuse its competitors. The PFJ should be amended to forbid Microsoft from using its patents offensively.

Before preparing my comments, I read the following documents in their entirety:

1 Original Complaint
http://www.USDoJ.gov/atr/cases/f1700/1763.htm

2 Findings of Fact
http://www.USDoJ.gov/atr/cases/f3800/msjudgex.htm

3 Stipulation and Revised Proposed Final Judgment
http://www.USDoJ.gov/atr/cases/f9400/9495.htm

4 State's Proposed Final Judgment
http://www.NAAG.org/features/microsoft/ms-remedy_filing.pdf

5 Competitive Impact Statement
http://www.USDoJ.gov/atr/cases/f9500/9549.htm

Justification for my Recommended Modifications:

Full Disclosure of Algorithms, APIs, Protocols, and File Formats:

I was very heartened to note that the PFJ would require that Microsoft must publish details of its APIs (section III.D. and others). However, as published, this provision will be largely ineffective, because it does not include Free Software and Open Software development efforts.

Microsoft's own lawyers indicated in 1999 that Microsoft views Linux and the GNU GPL license as its greatest threat.

http://www.OReillyNet.com/pub/a/mediakit/linux.html

Microsoft produced a white paper on the GNU GPL license, in an effort to dissuade companies from trying and/or using Linux.

http://www.Microsoft.com/business/downloads/licensing/Gpl_faq.doc

Although Linux and the Free Software movement are not yet a true competitor to Microsoft (as stated in the Findings of Fact), Linux offers the best hope for a future competitor to Microsoft. In light of this, the DoJ and the Court should tailor the PFJ such that it does not lock out Free Software and Open Software developers from the fruits of the PFJ.

Free Software and Open Software developers must be granted access to COMPLETE and ACCURATE documentation on *ALL* algorithms, APIs, protocols, and file formats for *ALL* Microsoft products, without any cost, and without any non-disclosure agreement (NDA) requirements.

The most complete and accurate documentation is the actual source code, and so that should be made available. The source code, however, is not enough. It is likely that the source code will be very difficult to understand; therefore Microsoft must also be required to fund an independent documentation effort to study the source code and completely and accurately document it. Such documentation and source code must be made available at no charge to anybody who wants it, via an Internet download, without any requirement for an NDA.

Without this extremely important provision, the most important potential competitor to Microsoft's monopoly will not be able to compete. In addition, without this important provision, Microsoft will be able to *CONTINUE* using closed and secret APIs, Protocols, and File Formats to extend, enhance, and broaden their existing monopoly. It is absolutely necessary that the PFJ be amended to require that Microsoft COMPLETELY and ACCURATELY document *ALL* of their algorithms, APIs, protocols, and file formats, and provide this information at no charge and without NDA requirements to everybody, via a free Internet download.

Security:

The security technique espoused in the PFJ is "security through obscurity". The idea is that if nobody knows how authentication or encryption is accomplished, they will not be able to bypass the authentication routines or break the encryption. There is a significant problem with this idea (and thus with the PFJ): IT IS FALSE! It is widely known and accepted within the security community that "security through obscurity" is no security at all.

SECURITY THROUGH OBSCURITY IS NO SECURITY AT ALL.

The following papers detail why "security through obscurity" is no security at all:

http://Slashdot.org/features/980720/0819202.shtml
http://www.VnuNet.com/Analysis/1126488
http://www.WideOpen.com/print/101.html
http://www.NightfallSecurity.com/whitepapers/obscurityeu.html
http://www.Albion.com/security/intro-8.html
http://www.eCommerceTimes.com/perl/printer/11060/
http://Adjacency.org/essays/securitythroughobscurity.html
http://www.Treachery.net/~jdyson/toorcon2001/

Many more examples exist; they can be found with a Google search.

http://www.Google.com/search?hl=en&q
=%22security+through+obscurity%22&btnG=Google+Search

This is perhaps the most important comment I am making, so I will repeat this important point:

SECURITY THROUGH OBSCURITY IS NO SECURITY AT ALL.

Bruce Schneier and Adam Shostack, two of the world's foremost experts in the area of computer and network security, have given a list of recommendations for Microsoft to follow in order to achieve more secure products, after the recent announcement by Bill Gates that Microsoft will henceforth be concentrating on security.

http://www.SecurityFocus.com/news/315

IT WILL BE NOTED THAT NOWHERE IN THIS LIST OF RECOMMENDATIONS IS THERE ANY NOTION THAT ANYTHING SHOULD BE KEPT SECRET. Instead, the recommendations from Messrs Schneier and Shostack encourage complete openness, full and accurate documentation, and a waiting period before Microsoft's proposed protocols and encryption methods are implemented. This is in order that the security community may examine Microsoft's proposed protocols and encryption methods and algorithms in order to find weaknesses, and repair those weaknesses, *before* they are implemented and insecure systems are built and fielded.

Messrs Schneier and Shostack also encourage Microsoft to publish its entire source code, even though they have no hope that Microsoft will do this. The source code should be published so that the security community can examine Microsoft's *implementations* for flaws and weaknesses, and suggest remedies for those flaws and weaknesses. The most well designed security protocols and encryption algorithms can be made worthless by poor implementation. The only way to check the implementation is to have access to the source code.

It is in the best interests of all those who must use Microsoft products, and all those who use computers on networks that include Microsoft products (which includes the entire Internet), that Messrs Schneier's and Shostack's recommendations are

adopted by Microsoft. Paradoxically, it is also in Microsoft's best interests to adopt *ALL* of Messrs Schneier's and Shostack's recommendations!!

If Microsoft is forced to COMPLETELY and ACCURATELY document *ALL* algorithms, APIs, protocols, and file formats -- without restriction -- and make the documentation and source code available to everybody without charge, and without any NDA requirement, bugs will be found in Microsoft's code and fixes will be suggested, just as they are for other open source OSes such as Linux, FreeBSD, NetBSD, and OpenBSD. Microsoft's products will improve as a result of this process. Microsoft will receive the benefit that all Open Source software receives: bug fixes, increased security, and increased stability, all at no cost to Microsoft.

Microsoft will be opposed to this requirement, arguing that their business will be destroyed by forcing their code open. This is not true! COPYRIGHT LAW AND CONTRACT LAW PROVIDE ALL THE LEGAL PROTECTION THAT MICROSOFT REQUIRES TO MAINTAIN THE VALUE IN THEIR SOURCE CODE. In the end, however, it does not matter if Microsoft benefits from the PFJ. What does matter is that Microsoft's monopoly abusing powers are restricted, and that the DoJ and the Court create the possibility for competitors to Microsoft to arise in the marketplace.

Microsoft has been found guilty of abusing their monopoly. One of the ways that Microsoft has abused their monopoly is by using closed and proprietary algorithms, APIs, protocols, and file formats, and by changing them from time to time in order to create incompatibilities with non-Microsoft products, and with older Microsoft products that Microsoft wishes to make obsolete. Microsoft's *secret* algorithms, APIs, protocols, and file formats are part of the problem that the DoJ and the Court must remedy. Such secrecy cannot be part of the solution, even when it comes to "anti-piracy, anti-virus, software licensing, digital rights management, encryption or authentication systems, including without limitation, keys, authorization tokens or enforcement criteria". Furthermore, in light of the fact that SECURITY THROUGH OBSCURITY IS NO SECURITY AT ALL, there is never any justification for any "governmental agency of competent jurisdiction" to "direct Microsoft not to" COMPLETELY and ACCURATELY document *ALL* algorithms, APIs, protocols, and file formats -- without restriction -- and make the documentation and source code available to everybody without charge. Therefore, section III.J1 and III.J2 must be entirely stricken from the PFJ.

As it is necessary to require Microsoft to COMPLETELY and ACCURATELY document *ALL* algorithms, APIs, protocols, and file formats -- without restriction -- and make the documentation and source code available to everybody without charge, and without any NDA requirement, it is not reasonable to require "any of the Plaintiffs to keep secret any information or documents obtained from Microsoft" as detailed in section IV.A.3 of the PFJ. This section should also be stricken from the PFJ.

Patents

Patents are a government granted monopoly. Microsoft has been judged to have a monopoly, and further, to have illegally abused that monopoly. For this reason, Microsoft should be forbidden from using its patents offensively. The government should not continue to grant a preferential monopoly to a convicted monopoly abuser.

This is especially true in the case of Open Software and Free Software. Those who develop Free and Open Software and give it away to the world for no charge are greatly enhancing the wealth of the entire world. These people CANNOT afford to participate in the patent system. In addition, those who develop Free and Open Software are often philosophically opposed to the patent system, and would not participate even if they could. These people who are greatly increasing the world's wealth, should not have the patent system used against them by a convicted monopoly abuser.

Microsoft has already threatened to use patents as an offensive weapon against Linux, the Free Software Foundation, the GNU Project, and other Free and Open Software producers. Full details can be found in the 2nd Halloween document.

http://www.OpenSource.org/halloween/

In order to protect the Free and Open Software movement from future monopoly abuse, Microsoft must be forbidden from using their patent portfolio offensively. This prohibition should *never* expire. A clause to this effect must be added to the PFJ in order to achieve an effective remedy.

Enforcement

A *very* strong enforcement mechanism needs to be put in place by the DoJ and by the Court. We have arrived at this juncture today because Microsoft failed to abide by previous consent decrees (1994) of the Court. Microsoft has proven themselves to be obstinate and belligerent. They cannot be trusted to obey this PFJ without strong and effective oversight.

If by some unfortunate circumstance, the DoJ and the Court decide not to require Microsoft to disclose all source code, then an especially vigorous enforcement mechanism must be put in place to ensure COMPLETE and ACCURATE documentation of *ALL* algorithms, APIs, protocols, and file formats. I would suggest that the PFJ should include a clause stipulating that if anybody finds any errors or discrepancies in Microsoft's documentation, then at that point the Technical Enforcement Committee shall have the authority to immediately force the disclosure of all relevant source code, in order to force compliance with the COMPLETE and ACCURATE documentation requirement.

Dan Kegel's Comments

I would like to add that I am a co-signer to Dan Kegel's comments.

http://www.Kegel.com/remedy/letter.html

I fully agree with Mr. Kegel's entire letter, including all links therein, and strongly urge that each of the problems noted therein must be remedied in the PFJ before the PFJ is adopted by the DoJ and by the Court.

Thank you,
Kenneth J. Hendrickson

* All web references were current on 26-27 January 2002, during the writing of these comments.