Network Working Group
Request for Comments: 3751
Category: Informational

S. Bradner
Harvard U.

1 April 2004

Omniscience Protocol Requirements

Status of this Memo

Copyright Notice

Abstract

There have been a number of legislative initiatives in the U.S. and elsewhere over the past few years to use the Internet to actively interfere with allegedly illegal activities of Internet users. This memo proposes a number of requirements for a new protocol, the Omniscience Protocol, that could be used to enable such efforts.

1. Introduction

In a June 17, 2003 U.S. Senate Judiciary Committee hearing, entitled "The Dark Side of a Bright Idea: Could Personal and National Security Risks Compromise the Potential of Peer-to-Peer File-Sharing Networks?," U.S. Senator Orrin Hatch (R-Utah), the chair of the committee, said he was interested in the ability to destroy the computers of people who illegally download copyrighted material. He said this "may be the only way you can teach somebody about copyrights." "If we can find some way to do this without destroying their machines, we'd be interested in hearing about that," Mr Hatch was quoted as saying during a Senate hearing. He went on to say "If that's the only way, then I'm all for destroying their machines." [Guardian]

Mr. Hatch was not the first U.S. elected official to propose something along this line. A year earlier, representatives, Howard Berman (D-Calif.) and Howard Coble (R-N.C.), introduced a bill that would have immunized groups such as the Motion Picture Association of America (MPAA) and the Recording Industry Association of America (RIAA) from all state and federal laws if they disable, block, or otherwise impair a "publicly accessible peer-to-peer file-trading network."

The attitude of some of the copyright holders may be that it's OK for a few honest people to have their computers or networks executed as long as the machines and networks of the dishonest are killed. But it is not likely that any measurable error rate would be acceptable to the public. Clearly, anyone implementing laws of this type need some way to reduce the error rate and be sure that they are dealing with a real bad guy and not an innocent bystander.

Part of determining if someone is a "bad guy" is determining his or her intent. Historically, western jurisprudence has required that prosecutors show that a person intended to commit a crime before that person could be convicted of committing that crime. [Holdsworth, Restatement, Prosser, United States v. Wise, Garratt v. Dailey] Because it can be quite difficult to establish a person's intent lawmakers have, in some cases, reduced the requirement for prosecutors to establish intent and mere possession is now proof enough of intent.

This memo proposes a set of requirements for a new protocol to be used by prosecutors to determine a person's intent, thus reducing the need to dilute the historical legal requirement to show intent and by groups such as the MPAA and RIAA to be sure they are dealing with lawbreakers and not 60 year old non computer users.

2. Omniscience Protocol Requirements

For the purpose of these requirements, I will assume that the OP is implemented using a client-server model, where the OP client is installed on the user's computer and the server is installed on a computer run by a law or copyright enforcement organization. OP Clients would register with all OP Servers that pertain to the legal jurisdiction in which the client is located each time the computer is started. OP Servers would then, on whatever schedule they have been configured to use, send OP Queries to OP Clients to find out if the computer operator has engaged in an illegal act of interest to the operator of the OP Server. Future versions of the OP might operate using a peer-to-peer model if the copyright enforcement people can ever get over their visceral disgust at the very concept of peer-to-peer networks.

For the purpose of this memo, I will use copyright infringement as an example of an illegal act that the OP protocol could be used to expose. The OP has numerous possible applications beyond ferreting out copyright infringement. For example, the OP would be of great assistance to instructors trying to determine if their students are producing original work or engaging in plagiarism. The same function would be invaluable to newspaper editors checking up on reporter's dispatches.

Also for the purpose of this memo, I assume that an evil-doer (also referred to as a miscreant) is in full control of a computer and that OP Servers will generally be operated by "Good guys." (See Functional Requirements FR5-7 for requirements to ensure that the latter is the case.) In the context of this memo, "evil-doer" and "miscreant" are defined as individuals or groups of individuals who perform acts that the operator of an OP Server has a legally recognized right to prevent. In the context of this memo, "good guys" refers to individuals or groups of individuals who have a legally recognized right to prevent certain acts that computer users may attempt to do with their computers. The use of this term is not meant to convey any value judgment of the morality, forward thinking nature, public spiritedness, or the monetary worth relative to most of humanity of such individuals or groups of individuals.

2.1. Operational Requirements

OR1: The OP client must be able to install itself into all types of computers over the objections of the computer user.

Discussion: The OP client would be installed by legal mandate in all new computers, but since there are hundreds of millions of existing computers, the OP client must be able to install itself in all of these existing computers in order to afford universal coverage of all possible miscreants. This installation must be accomplished even if the user, many of whom have full administrative control over their computers, tries to prevent it.

OR2: True OP clients must not be findable by the computer user by any means, including commercial virus detectors, but all hackers' programs that mimic OP clients must be easily findable by commercial virus detectors.

Discussion: Since anyone whose intent was to violate the law would not want the OP client to be watching their action, they would try to disable the OP client. Thus the OP Client, once installed, should be invisible to all methods a user might employ to discover it. Users must be able to find and remove any virus or worm that tries to masquerade as an OP client to escape detection.

OR3: The OP must be able to communicate through uncooperative firewalls, NATs, and when the computer is disconnected from the Internet.

Discussion: Since the evil-doer may have control of a local firewall or NAT, the OP must be able to communicate with the OP server, even when the firewall or NAT has been configured to block all unused ports. Also, since the evil-doer might try to hide his or her evil-doing by disconnecting the computer from the network, the OP must be able to continue to communicate, even under these circumstances. Meeting this requirement may require that the OP client be able to reconfigure the user's machine into a cell phone or to implement GMPLS-WH [GMPLS-WH].

OR4: Neither the operation of the OP client or the OP server must be able to be spoofed.

Discussion: The user must not be able to create their own version of an OP client that can fool the OP server. Nor can it be possible for someone to create their own OP server that can be used to query OP clients.

Discussion: Because of the potential for a user to hide their illicit activities by mimicking the operation of the OP client on their machine, it must not be possible to do so. In the same vein, because of the potential for violating the user's privacy, it must not be possible for a non-authorized OP server to be seen as authorized by OP clients. Since there will be an arbitrary, and changing, number of OP servers, at least one for each type of protected material, OP authentication and authorization must be able to be accomplished with no prior knowledge of a particular OP server by the OP client.

OR5: The OP client must be able to be installed on any portable device that can be used to play protected material or execute protected software.

Discussion: Since small, portable devices, such as MP3 players, are becoming the preferred method of playing back prerecorded music and videos, they must all include OP clients. OP clients must be able to be automatically installed on all such existing devices.

2.2. Functional Requirements

FR1: The OP client must be able to determine the user's intent.

Discussion: Just knowing that the user has a copy of a protected work on their system does not, by itself, mean that the copy is illegal. It could easily be a copy that the user purchased. The OP must be able to tell if a copy is an illegal copy with complete reliability. The OP must be able to differentiate between an original, and legal, copy and a bit-for-bit illegal reproduction. The OP client must be able to differentiate between copies that were created for the purpose of backup, and are thus generally legal, and those copies created for the purpose of illegal distribution. In the case of some types of software, the OP client must be able to determine the intent of the user for the software. An example of this need is related to the U.S. Digital Millennium Copyright Act (DMCA) and similar laws around the world. These laws outlaw the possession of circumvention technology, such as crypto analysis software, in most cases. Some exemption is made for legitimate researchers, but without an OP it is quite hard to determine if the circumvention technology is to be used for research or to break copyright protections for the purpose of making illegal copies of protected material. With the OP, the DMCA, and laws like it, can be rewritten so that circumvention technology is legal and developers can find out if their security protocols are any good, something which may be illegal under current law.

FR2: The OP client must be able to remotely differentiate between illegal material and other material with the same file name.

Discussion: A user might create a file that has the same filename as that of a protected work. The OP must not be fooled into thinking that the user's file is a protected one.

FR3: The OP client must be able to find illegal copies, even if the filename has been changed.

Discussion: The user must not be able to disguise a protected work by just changing its name.

FR4: The OP client must be able to find illegal copies, even if the user has modified the work in some way.

Discussion: The user must not be able to disguise a protected work by modifying the work, for example, by prepending, appending, or inserting extra material, or by changing some of the protected work. The OP must be able to make a legal

determination that a modified work is no longer legally the same as the original if the amount and type of modification exceed a subjective threshold.

FR5: The OP client must not be able to be run by a hacker, and the OP interface into a user's computer must not be able to be exploited by a hacker.

Discussion: OP clients will be attractive targets for hackers since they will have full access within a user's computer. The interface between the OP client and server must be secure against all possible hacking attacks.

FR6: The OP client must be able to discern the motives of the operator of the OP server and not run if those motives are not pure.

Discussion: Since it cannot be assumed that the operators of the OP server will always have the best motives, the OP client must be able to reject requests from the OP server if the operator of the server has an evil (or illegal) intent. For example, the OP client must block any operation that might stem from a vendetta that the OP server operator might have against the user.

FR7: The OP client must not be able to be used to extract information from a user's computer that is unrelated to illegal copies.

In order to minimize the threat to the privacy of the user, the OP client must not be able to be used to extract information from the user's computer that is not germane to determining if the user has illegal copies of works or intends to use protected works in illegal ways.

FR8: The OP client must be able to differentiate between protected material that was placed on the user's computer by the user and any material placed by others.

Discussion: It must not be possible for a third party to put protected material on a user's computer for the purpose of incriminating the user. The OP client must be able to know, with certainty, who placed material on each computer, even in the cases where a third party has physical access to an unprotected computer or when the third party knows the user's logname and password.

FR9: The OP client must only implement the laws that apply to the specific computer that it is running on.

Discussion: Since the Internet crosses many legal boundaries, an OP client will have to know just where, in geo-political space, the computer it is running in is currently located in order to know what set of laws to apply when it is scanning the user's computer. The OP client must also be able to be automatically updated if the laws change or the computer is moved to a location where the laws are different. Note that this requirement also implies that the OP client knows where its OP server is located to know if the client and server are both in the same legal jurisdiction. The OP client must know what to do, or not do, when they are not in the same legal jurisdiction. The OP client must also include a mechanism to automatically retrieve any applicable new laws or court decisions and properly interpret them.

3. Security Considerations

The OP requires strong authentication of the clients and servers to ensure that they cannot be spoofed. It also requires the use of strong integrity technology to ensure that the messages between the client and server cannot be modified in flight. It also requires strong encryption to be sure that the communication between the client and the server cannot be observed. All of this is required in an environment where many of the users are in full control of their computers and will be actively hostile to the reliable operation of the protocol. Good luck.

4. Informative References

[Garratt v. Dailey] Supreme Court of Washington, 6 Wash. 2d 197; 279 P.2d 1091 (1955)

[GMPLS-WH] Generalized Multi-Protocol Label Switching (GMPLS) for Worm Holes, work to be in process

[Guardian] "Senator proposes destruction of file-swapping computers." The Guardian, June 19, 2003. (http://www.guardian.co.uk/usa/story/0,12271,980890,00.html)

[Holdsworth] Holdsworth, W., History of English Law 680-683 (1938)

[Processer] Prosser, W., et al., "Prosser and Keeton on Torts," Hornbook Series, 5th ed., 1984

[Restatement] 1. Restatement of the Law: sec 13 Torts (American Law Institute) (1934)

[United States v. Wise] 550 F.2d 1180, 1194 (9th Cir.)

5. Authors Address

Scott Bradner
Harvard University
29 Oxford St.
Cambridge MA, 02138

EMail: sob@harvard.edu
Phone: +1 617 495 3864

6. Full Copyright Statement

Intellectual Property

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.