Internet-Draft IAB and IESG

draft-iab-raven-00.txt

Target Category: Informational January 2000

Expires: July 2000

IETF Policy on Wiretapping

Status of this Memo

The following text is food for the I-D machinery.

> The file name of this memo is draft-ietf-iab-raven-00.txt
>
> This document is an internet-draft and is in full conformance with all provisions of Section 10 of RFC2026.
>
> Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.
>
> 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."
>
> The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt
>
> The list of internet-draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

The intended place to discuss this memo is the RAVEN mailing list <raven@ietf.org>.

Abstract

The IETF has been asked to take a position on the inclusion into IETF standards-track documents of functionality designed to facilitate wiretapping.

This memo explains what the IETF thinks the question means, why its answer is "no", and what that answer means.

1. Summary position

The IETF has decided not to consider requirements for wiretapping as part of the process for creating and maintaining IETF standards.

It takes this position for the following basic reasons:

- The IETF, an international standards body, believes itself to be the wrong forum for designing protocol or equipment features that address needs perceived by national law, which vary widely across the areas that IETF standards are deployed in.
  Bodies that are constrained to a single regime of jurisdiction are more appropriate for this task.

- The IETF, being a standards body for communications that pass across networks that may be owned, operated and maintained by people from numerous jurisdictions with numerous requirements for privacy, believes that the operation of the Internet and the needs of its users are best served by making sure the security properties of connections across the Internet are as well known as possible.
  At the present stage of our ignorance this means making them as free from security loopholes as possible.

- Adding a requirement for wiretapping will make the designs considerably more complex, thereby jeopardizing the security of communications even when it is not being tapped by any legal means; there are also obvious risks raised by having to protect the access to the wiretap. This is in conflict with the goal above.

- The IETF believes that in the case of traffic that is today going across the Internet without being protected by the end systems, the use of existing network features, if deployed intelligently, will be adequate for the wiretapping needs seen at present. The IETF does not see an engineering solution that allows such wiretapping when the end systems take adequate measures to protect their communications.

- The IETF restates its strongly held belief, stated at greater length in [RFC 1984], that both commercial development of the Internet and adequate privacy for its users against illegal intrusion requires the wide availability of strong cryptographic technology.

- On the other hand, the IETF believes that mechanisms for wiretapping

should be openly described, so as to ensure the maximum review of the mechanisms and ensure that they adhere as closely as possible to their design constraints. The IETF believes that the publication of such mechanisms, and the publication of known weaknesses in such mechanisms, is a Good Thing.

2. The Raven process

The issue of the IETF doing work on legal intercept technologies came up as a byproduct of the extensive work that the IETF is now doing in the area if IP-based telephony.

In the telephony world, there has been a tradition that companies that build telephone equipment add wiretapping features to their telephony-related equipment, and some traditional telephony standards organizations have supported this by adding intercept features to their telephony-related standards.

Since the future of the telephone seems to be intertwined with the Internet it is inevitable that the primary Internet standards organization would be faced with the issue sooner or later.

In this case some of the participants of one of the IETF working groups working on a new standard for communication between components of a distributed phone switch brought up the issue. Since adding features of this type would be something the IETF had never done before, the IETF management decided to have a public discussion before deciding if the working group should go ahead. A new mailing list was created (the Raven mailing list, see http://www.ietf.org/mailman/listinfo/raven) for this discussion. Close to 500 people subscribed to the list and about 10% of those sent at least one message to the list. The discussion on this list was a precursor to a discussion held during the IETF plenary in Washington.

Twenty nine people spoke during the plenary session. Opinions ranged from libertarian: 'governments have no right to wiretap' - to pragmatic: 'it will be done somewhere, best have it done where the technology was developed'. At the end of the discussion there was a show of hands to indicate opinions: should the IETF add special features, not do this or abstain. Very few people spoke out strongly in support for adding the intercept features, but a sizable portion of the audience refused to state an opinion (raised their hands when asked for "abstain" in the show of hands).

This is the background on the basis of which the IESG and the IAB was asked to formulate a policy.

3. A definition of wiretapping

The various legal statutes defining wiretapping do not give adequate definitions to distinguish between wiretapping and various other activities at the technical level. For the purposes of this memo, the

following definition of wiretapping is used:

Wiretapping is what occurs when information passed across the Internet from one party to one or more other parties is delivered to a third party:

1. Without the sending party knowing about the third party

2. Without any of the recipient parties knowing about the delivery to the third party

3. When the normal expectation of the sender is that his information will only be seen by the recipient parties or parties obliged to keep the information in confidence

4. When the third party acts deliberately to target the transmission of the first party, either because he is of interest, or because the second party's reception is of interest.

Of course, many wiretaps will be bidirectional, monitoring traffic sent by two or more parties.

Thus, for instance, monitoring public newsgroups is not wiretapping (condition 3 violated), random monitoring is not wiretapping (condition **4 violated), a recipient passing on private email is not wiretapping** (condition 2 violated).

Telephone call tracing by means of accounting logs (sometimes called "pen registers") is also wiretapping by this definition, since the normal expectation of the sender is that the telephone company will keep this information in confidence.

This definition deliberately does not include considerations of:

- Whether the wiretap is legal or not, since that is a legal, not a technical matter

- Whether the wiretap occurs in real time, or can be performed after the fact by looking at information recorded for other purposes (such as the accounting example given above)

- What the medium targeted by the wiretap is - whether it is email, IP telephony, Web browsing or EDI transfers

These questions are believed to be irrelevant to the policy outlined in this memo.

Wiretap is also sometimes called "interception", but that term is also used in a sense that is considerably wider than the monitoring of data crossing networks, and is therefore not used here.

Wiretapping may logically be thought of as 3 distinct steps:

- Capture - getting information off the wire that contains the information wanted

- Filtering - selecting the information wanted from information gathered by accident

- Delivery - transmitting the information wanted to the ones who want it.

In all these stages, the possibility of using or abusing mechanisms defined for this purpose for other purposes exists.

4. Why the IETF does not take a moral position

Much of the debate about wiretapping has centered around the question of whether wiretapping is morally evil, no matter who does it, necessary in any civilized society, or an effective tool for catching criminals that has been abused in the past and will be abused again.

The IETF has decided not to take a position in this matter, since:

- There is no clear consensus around a single position in the IETF

- There is no means of detecting the morality of an act "on the wire". Since the IETF deals with protocol standardization, not protocol deployment, it is not in a position to dictate that its product is only used in moral or legal ways.

However, a few observations can be made:

- Experience shows that tools which are effective for a purpose tend to be used for that purpose.

- Experience shows that tools designed for one purpose that are effective for another tend to be used for that other purpose too, no matter what its designers intended.

- Experience shows that if a vulnerability exists in a security system, it is likely that someone will take advantage of it sooner or later.

- Experience shows that human factors, not technology per se, is the biggest single source of such vulnerabilities.

What this boils down to is that if effective tools for wiretapping exist, it is likely that they will be used as designed, for purposes legal in their jurisdiction, and also in ways they were not intended for, in ways that are not legal in that jurisdiction. When weighing the development or deployment of such tools, this should be borne in mind.

5. Utility considerations

When designing any communications function, it is a relevant question to ask if such functions perform the task they are designed for in an efficient manner, or whether the work spent in developing them is worth the benefit gained.

Given that there are no proposals on the table, it is not possible to weigh proposals for wiretapping directly in this manner.

However, as above, a few general observations can be made:

- Wiretapping by copying the bytes passed between two users of the Internet with known, static points of attachment is not hard. Standard functions designed for diagnostic purposes can accomplish this.

- Identifying users' points of attachment to the Internet can be significantly harder, but not impossible, if the user uses standard means of identification. However, this means linking into multiple

Internet subsystems used for address assignment, name resolution and so on; this is not trivial.

- An adversary has several simple countermeasures available to him in order to defeat wiretapping attempts, even without resorting to encryption. This includes Internet cafes and anonymous dialups, anonymous remailers, multi-hop login sessions and use of obscure communications media; these are well known tools in the cracker community.

- Of course, communications where the content is protected by strong encryption can be easily recorded, but the content is still not available to the wiretapper, defeating all information gathering apart from traffic analysis.
  Since Internet data is already in digital form, encrypting it is very simple for the end-user.

These things taken together mean that while wiretapping is an efficient tool for use in situations where the target of a wiretap is either ignorant or believes himself innocent of wrongdoing, Internet-based wiretapping is a less useful tool than might be imagined against an alerted and technically competent adversary.

6. Security considerations

Wiretapping, by definition (see above), releases information that the information sender did not expect to be released.

This means that a system that allows wiretapping has to contain a function that can be exercised without alerting the information sender to the fact that his desires for privacy are not being met.

This, in turn, means that one has to design the system in such a way that it cannot guarantee any level of privacy; at the maximum, it can only guarantee it as long as the function for wiretapping is not exercised.

For instance, encrypted telephone conferences have to be designed in such a way that the participants cannot know to whom any shared keying material is being revealed.

This means:

- The system is less secure than it could be had this function not been present.

- The system is more complex than it could be had this function not been present.

- Being more complex, the risk of unintended security flaws in the system is larger.

Wiretapping, even when it is not being exercised, therefore lowers the security of the system.

7. Acknowledgements

This memo is endorsed by the IAB and the IESG.

Their membership is:

IAB:

Harald Alvestrand
Randall Atkinson
Rob Austein
Brian Carpenter
Steve Bellovin
Jon Crowcroft
Steve Deering
Ned Freed
Tony Hain
Tim Howes
Geoff Huston
John Klensin

IESG:

Fred Baker
Keith Moore
Patrik Falstrom
Erik Nordmark
Thomas Narten
Randy Bush
Bert Wijnen
Rob Coltun
Dave Oran
Jeff Schiller
Marcus Leech
Scott Bradner
Vern Paxson
April Marine

The contributors to the discussion are too numerous to list.

8. Author's Address

This memo is authored by the IAB and the IESG.

The chairs are:

Fred Baker, IETF Chair
519 Lado Drive
Santa Barbara California 93111
Phone: +1-408-526-4257
fred@cisco.com

Brian E. Carpenter (IAB Chair)
IBM
c/o iCAIR
Suite 150
1890 Maple Avenue
Evanston IL 60201
USA
email: brian@icair.org

9. References

[RFC 1984]

IAB and IESG Statement on Cryptographic Technology and the Internet. IAB & IESG. August 1996.