INTERNET-DRAFT Steven M. Bellovin
draft-ymbk-obscurity-00.txt Randy Bush
2002.02.28 AT&T Research

Security Through Obscurity Considered Dangerous

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.

0. Abstract

   Hiding security vulnerabilities in algorithms, software, and/or
   hardware decreases the likelihood they will be repaired and increases
   the likelihood that they can and will be exploited by evil-doers.
   Discouraging or outlawing discussion of weaknesses and
   vulnerabilities is extremely dangerous and deleterious to the
   security of computer systems, the network, and its citizens.

1. Open Discussion Encourages Better Security

   The long history of cryptography and cryptoanalysis has shown time
   and time again that open discussion and analysis of algorithms
   exposes weaknesses not thought of by the original authors, and
   thereby leads to better and more secure algorithms. As Kerckhoff
   noted about cipher systems in 1883 [Kerc83], "Il faut qu'il n'exige
   pas le secret, et qu'il puisse sans inconv'enient tomer entre les
   mains de l'ennemi." (Roughly, "the system must not require secrecy
   and can be stolen by the enemy without causing trouble.")

   It is also against the ethos and laws of a number of countries to
   disallow open discussion of science and technology.

Within the IETF, frank discussion of the flaws of proposed and actual protocols has led to improvement versions. Hence, the IETF does not discourage open discussion and analysis of cryptographic or security methods, and enthusiastically encourages open and frank technical discussion thereof in its research, working groups, mailing lists, and all other discussion venues.

2. Revealing Vulnerabilities is Useful

Revealing and discussing vulnerabilities in hardware and software products allows the users to protect themselves, and encourages general protection and repair strategies.

On the other hand, there is a well-established culture of giving the manufacturer of the vulnerable product a short but reasonable early warning of discovered vulnerabilities so that they have an opportunity to repair them and or prepare to distribute patches or work-arounds. Furthermore, it is better if developers have time to test their patches; much of the current mess comes from inadequate software testing.

The IETF supports and encourages the open but prudent discussion of vulnerabilities in hardware and software in all appropriate IETF venues.

3. The Culture of Sharing

In parts of the hacker subculture, information is currency. That is, by disclosing vulnerabilities or by providing exploit code, the purveyor gains status. As a consequence, knowledge of security holes tends to spread rapidly.

By contrast, when security professionals withhold such information from the community, the broader community does not have an opportunity to find solutions. In extreme cases, such as that described in [Bell95], the result can be that the bad guys know about the problem long before most defenders do. That, in turn, likely delayed the development of cryptographic security mechanisms for the DNS [RFC2065].

3. Security Considerations

This document is about security, and specifically warns about increased vulnerability if weakness in algorithms and products are

not able to be openly discussed.

4. Acknowledgments

I dunno

5. References

[Bell95]
S..M. Bellovin, "Using the Domain Name System for System Break-
Ins", Proc. Fifth Usenix Security Symposium, 1995.

[Kerc83]
A. Kerckhoffs. "La Cryptographie Militaire". 1883.
<http://www.cl.cam.ac.uk/~fapp2/kerckhoffs/>

[RFC2065]
D. Eastlake and C. Kaufman. "Domain Name System Security Exten-
sions". RFC 2065, 1997.

6. Authors' Addresses

Steven M Bellovin
AT&T Labs Research
Shannon Laboratory
180 Park Avenue
Florham Park, NJ 07932
Phone: +1 973-360-8656
email: bellovin@acm.org

Randy Bush
5147 Crystal Springs
Bainbridge Island, WA US-98110
+1 206 780 0431
randy@psg.com

7. Full Copyright Statement