In this series, I've been writing about various forms of forgery. Today we'll look at the implications of packet and e-mail spoofing.

* * *

Imagine that your site has been hit by a massive denial-of-service attack and that you have lost thousands of sales in the last day. Or imagine that someone has defaced your Web site and caused great embarrassment as well as making you stay up all night as part of the emergency crew rebuilding the site.

Wouldn't you just _love_ to get even with the nasty people who caused you all this trouble? Wouldn't it be great to launch a retaliatory strike against them?

Well, it might sound like fun, but in today's Internet, any attempt to get even with the perpetrators of attacks is likely to backfire.

The practical problem is that IPv4, (Internet Protocol version 4), the current protocol in use throughout the Internet, has no provision for origin authentication as part of the packet headers. It is easy to forge the packet headers of outbound traffic or to alter the origination information of e-mail. These indicators of origin cannot be relied upon as a trustworthy pointer to the real senders of anything on the Internet.

The second problem is that criminal hackers often use hijacked systems for their nefarious deeds. Even if they don't forge their headers, the harmful traffic may be pointing to another victim rather than to the systems belonging to the criminal. For example, a criminal hacker may be using a stolen account on a university computer -- perhaps using a password stolen from an unsuspecting student or perhaps by obtaining administrative privileges and creating an account for the purpose of wreaking havoc. Attacking the university computers hardly seems like the right thing to do.

The other possibility I've been told about by several people over the years is tracking down the human beings responsible for the attacks and then Doing Bad Things to them. A couple of people have suggested baseball bats and general destruction.

I have consistently held that it is out of the question to use violence against suspected criminals. Vigilante behavior of all kinds is consistently bad: it allows the heat of the moment to overcome rational discovery of truth. Even today, people all over the planet are being hanged, burned, clubbed, and otherwise abused and killed because of suspicion, with the flimsiest of evidence and completely without benefit of a legal process to prevent injustice. Check the Amnesty International Web site for horrific details.

Finally, there's the legal aspect. As you know, I-am-not-a-lawyer-and-this-is-not-legal-advice --
for-legal-advice-consult-an-attorney-with-the-appropriate-expertise. As a lay person, I believe that premeditated revenge is not a legal justification for attacking someone else's property or person.

No, on all of these grounds, I do not think that retaliation against perceived attackers is a sound response. If you really do have credible evidence identifying your attackers, consider the pro/con arguments about whether to get involved in a criminal investigation or perhaps to lay civil charges.

But don't get involved with do-it-yourself revenge.

* * *
For further reading:


* * *

NEW! 18-month online Master of Science in Information Assurance offered by Norwich University; see <http://www3.norwich.edu/msia> for full details.


M. E. Kabay, PhD, CISSP is Associate Professor in the Department of Computer Information Systems at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2002 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.