1999 CERT Tech Tip: Spoofed/Forged Email

Original publication date: April 26, 1999

This document provides a general overview of email spoofing and the problems that can result from it. It includes information that will help you respond to such activity.

I. Description

Email spoofing may occur in different forms, but all have a similar result: a user receives email that appears to have originated from one source when it actually was sent from another source. Email spoofing is often an attempt to trick the user into making a damaging statement or releasing sensitive information (such as passwords).

Examples of spoofed email that could affect the security of your site include:

- email claiming to be from a system administrator requesting users to change their passwords to a specified string and threatening to suspend their account if they do not do this
- email claiming to be from a person in authority requesting users to send them a copy of a password file or other sensitive information

If, after investigating the activity, you find that there is more to the incident than spoofed email (such as a compromise at your site or another site), please refer to Section IV below.

II. Technical Issues

- If you provide email services to your user community, your users are vulnerable to spoofed or forged email.
- It is easy to spoof email because SMTP (Simple Mail Transfer Protocol) lacks authentication. If a site has configured the mail server to allow connections to the SMTP port, anyone can connect to the SMTP port of a site and (in accordance with that protocol) issue commands that will send email that appears to be from the address of the individual's choice; this can be a valid email address or a fictitious address that is correctly formatted.
- In addition to connecting to the SMTP port of a site, a user can send spoofed email via other protocols (for instance, by modifying their web browser interface).

III. What You Can Do

1. Reaction
    a. You may be alerted to spoofed email attempts by reports from your users or by investigating bounced email error messages.
    b. Following relevant policies and procedures of your organization, review all information (such as mail headers and system log files) related to the spoofed email.
    Examine tcp_wrapper, ident, and sendmail logs to obtain information on the origin of the spoofed email.

    The header of the email message often contains a complete history of the "hops" the message has taken to reach its destination. Information in the headers (such as the "Received:" and "Message-ID" information), in conjunction with your mail delivery logs, should help you to determine how the email reached your system.

    If your mail reader does not allow you to review these headers, check the ASCII file that contains the original message.

    NOTE: Some of the header information may be spoofed; and if the abuser connected directly to the SMTP port on your system, it may not be possible for you to identify the source of the activity.
    c. Follow up with other sites involved in this activity, if you can identify the sites. Contact them to alert them to the activity and help them determine the source of the original email.
    We would appreciate a cc to "cert@cert.org" on your messages; this facilitates our work on incidents and helps us relate ongoing intruder activities.

    If you have a CERT# reference for this incident, please include it in the subject line of all messages related to this incident. (NOTE: This reference number will be assigned by the CERT/CC, so if you do not have a reference number, one will be assigned once we receive the incident report.)

    To find site contact information, please refer to

    http://www.cert.org/tech_tips/finding_site_contacts.html

    You may also want to contact the postmaster at sites that may be involved. Send email to

postmaster@[host.]site.domain (for example, postmaster@cert.org)

Please include a copy of this document in your message to sites.

d. To provide as much information as possible to help trace this type of activity, you can increase the level of logging for your mailer delivery daemon.
e. Realize that in some cases, you may not be able to identify the origin of the spoofed email.

1. Prevention (Deterrence)
   a. Use cryptographic signatures (e.g., PGP "Pretty Good Privacy" or other encryption technologies) to exchange authenticated email messages. Authenticated email provides a mechanism for ensuring that messages are from whom they appear to be, as well as ensuring that the message has not been altered in transit. Similarly, sites may wish to consider enabling SSL/TLS in their mail transfer software. Using certificates in this manner increases the amount of authentication performed when sending mail.
   b. Configure your mail delivery daemon to prevent someone from directly connecting to your SMTP port to send spoofed email to other sites.
   c. Ensure that your mail delivery daemon allows logging and is configured to provide sufficient logging to assist you in tracking the origin of spoofed email.
   d. Consider a single point of entry for email to your site. You can implement this by configuring your firewall so that SMTP connections from outside your firewall must go through a central mail hub. This will provide you with centralized logging, which may assist in detecting the origin of mail spoofing attempts to your site.
   e. Educate your users about your site's policies and procedures in order to prevent them from being "social engineered," or tricked, into disclosing sensitive information (such as passwords). Have your users report any such activities to the appropriate system administrator (s) as soon as possible. See also CERT advisory CA-1991-04, available from

      http://www.cert.org/advisories/CA-1991-04.social.engineering.html

IV. Additional Security Measures That You Can Take

1. If you have questions concerning legal issues, we encourage you to work with your legal counsel.
   U.S. sites interested in an investigation of this activity can contact the Federal Bureau of Investigation (FBI). Information about how the FBI investigates computer crimes can be found here

   http://www.cert.org/tech_tips/FBI_investigates_crime.html

   For information on finding and contacting your local FBI field office, see

   http://www.fbi.gov/contact/fo/fo.htm

   Non-U.S. sites may want to discuss the activity with their local law enforcement agency to determine the appropriate steps for pursuing an investigation.
2. For general security information, please see

   http://www.cert.org/

Revision History	
Apr 26, 1999	Converted to new web format
Mar 20, 2000	Updated links
Sep 04, 2002	Minor updates