

Full-Disclosure: [Full-Disclosure] Sending remote procedure calls through e-mail (RPC-Mail)

## [Full-Disclosure] Sending remote procedure calls through e-mail (RPC-Mail)

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/0764.html>

---

*From:* Abe Usher ([securitylist\\_at\\_sharp-ideas.net](mailto:securitylist_at_sharp-ideas.net))

*Date:* 10/20/04

To: [full-disclosure@lists.netsys.com](mailto:full-disclosure@lists.netsys.com)

Date: Tue, 19 Oct 2004 22:26:43 -0400

Have you ever had the need to remotely send a command to a system, but you could not access it directly via ssh or telnet because the firewall is blocking all inbound connections?

The practice of portknocking <<http://www.portknocking.org/>> provides an interesting network authentication mechanism for establishing a connection to a networked computer that has no open ports (as advertised on [portknocking.org](http://www.portknocking.org)).

While I find portknocking ingenious, it is somewhat cumbersome and overly complex for most users. I propose an alternative – send remote procedure calls via e-mail. I've coded an application that fits the bill: RPC-Mail.

The premise of RPC-Mail is simple:

- (1) Construct an e-mail message that has a command that you want one of your remote PCs to execute.
- (2) Send the e-mail to a special account that is only used by RPC-Mail.
- (3) Have the remote PC set up with a scheduled task or cron job to periodically execute the application `RPC-Mail.py`.
- (4) When `RPC-Mail.py` executes, it parses all of the subject lines and message bodies of e-mail messages that it finds. If the message body contains a special passphrase, RPC-Mail executes the subject line as a command, and returns standard output as an e-mail message.

For more information check out my full write up on:

<http://www.sharp-ideas.net/>

Cheers,  
Abe Usher, CISSP

---

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>