Security

System Protection

Contribute.com's servers are configured to prevent intrusions and protect from abuse in day to day use by a combination of features.

- **Software and OS**
  Our production systems use Solaris 2.6, fully patched, with patch updates run weekly.

  Monitoring of binaries and critical configuration files is performed daily using tripwire, the industry standard file integrity checker, which is installed on every machine before the machine is brought live on the network. Should an intruder somehow gain access, any change to the critical binaries would be immediately noted in the daily tripwire output and responded to.

  All sensitive connections to our servers are done over SSH (RSA-encrypted secure shell) for fully encrypted communications when dealing with sensitive system issues.

- **Restricted Access**
  Our network is configured in a manner that greatly restricts access even by authorized accounts from any machines other than those within our direct control.

  All access other than mail, web, DNS and ftp access to our machines is limited to machines within our internal network (physically located in our offices, and behind our firewall), and specified external machines. Connections from external machines are restricted to specific accounts on specific IP addresses, on machines audited by our own staff, and all connection attempts (authorized or otherwise) are logged in multiple locations to defeat cleanup software used by hackers. This restriction is achieved using a redundant combination of router packet filtering, firewalling and tcp wrapper implementation.

  Any services not absolutely necessary to our business are disabled, and the binaries removed, before any machine goes live on our network.

- **Secure System Layout**
  In case of intrusion, to contain an intruder long enough for our monitoring to notice the intrusion, the network is laid out so that on any given host, during normal operations, no passwords pass through the console or network interface to that server. Each server can only host connections, so you can only connect from a client to a host, not from a host to a host. Any machine that holds client programs has all daemon and other host capable binaries deleted before going live on the network.

  Console on our servers is maintained as root, and any root access required is obtained at the console, so after the machine is brought up, the root password is never entered, defeating session monitoring and packet sniffing attempts to obtain passwords.

  Su is only executable by root, preventing other users from switching accounts on that machine, which would require entering a password.

  Any accounts capable of making shell connections to the host can only do so using SSH. Any services that use plaintext passwords that could theoretically be sniffed are either removed (binaries deleted) such as telnetd, or are denied shell logins by ssh to that machine

- **Password Discipline**
  Passwords are required to be crack-resistant (no dictionary words, combination of upper-case, lower-case, numbers and punctuation), with no duplication of passwords on different hosts. Passwords expire after 3 months, and must be renewed.