

World Community Grid Security Overview

Security is a top concern for World Community Grid to ensure the trust of our members. Therefore, security is something we address seriously, and we remain vigilant in this regard.

The following describes our security measures and how security is achieved in the operation of the grid software and hardware.

THE AGENT AND ITS OPERATION

- **Installation**

Starting from software download/install, the user is able to check the downloaded agent install file using the md5sum value. This assures that the install file has not been corrupted. Next, the Verisign certificate, used to sign the code, clearly states that this is a World Community Grid-provided program. All of the files are stored in one install directory except for the ud.scr screensaver file and Start-menu entries. All of the agent's use of disk storage also is confined to this install directory.

- **Registration**

After installing the agent program, a registration process records the member's machine in the server database and establishes a unique identification key for identifying this device during future communications. If someone were to install cloned copies of the agent onto different machines, a key increment procedure causes these cloned agent registrations to become invalid, requiring a new registration. In this way, the grid servers have unique records for each device. This aids in assuring that results returned to the server are valid and correspond to the correct input data. The server sends out work redundantly and votes on the returned results so that errant computations or those which have been tampered with, are discarded.

- **Contact with World Community Grid's Server**

The agent -- rather than the server -- always initiates any contact. As an added security measure, the member's software firewall can be set so that the agent only can make outgoing connections via port 443, the same port used for https web browsing, and only to World Community Grid's server site at server.worldcommunitygrid.org. Because the agent does not accept incoming

World Community Grid Security Overview

connections, incoming attacks would be very difficult. Furthermore, the agent must be known to World Community Grid's server per the above registration process, otherwise its communication is rejected until it is properly registered.

Communications from the agent occur only at registration and when processing on a unit of work is finished. When a unit of work is finished, the agent returns the results to the server and downloads new work to process. If for some reason the server is not accessible (e.g., due to a maintenance period or some network outage), the agent automatically waits for an extended amount of time before attempting to communicate again. This prevents needless and fruitless rapid retries and avoids network congestion. These communications average about once per ten hours of agent CPU processing, but vary from just a few hours to weeks depending on the speed of the particular machine, on the difficulty of the work unit being processed, and on how much time the agent is free to process the work.

The agent's communications to the server are encrypted and the files the agent uses are encrypted when stored on the machine. A packet modified in transit will be rejected. If the agent finds that any of the stored files are damaged by possible disk failure or tampered with in any way, for example by a virus, then the agent discards these files and downloads fresh copies from the server.

World Community Grid sends out the same work units to multiple machines and compares results to eliminate those coming from machines with faulty hardware or any kind of possible tampering. The agent checkpoints intermediate state every several minutes so that if the machine is powered off or shut down, it does not lose significant processing time.

- **Trace Route Probes**

Users might see incoming trace route probes from other IBM domains after communicating with our server site. These are used for optimizing data transmission by choosing from among several Internet providers. These can be blocked if the user prefers. More information about this can be found at <http://www.routescience.com>.

EXECUTABLES

Occasionally, the agent software may be updated. This will happen when the agent next contacts the server and such an update is available. The agent uses a public-private key authentication scheme to assure that the updated executable code, received by the agent, can only have originated from World Community Grid. Otherwise, it will reject the update. This makes it impossible for hackers to set up a

World Community Grid

Security Overview

false server site pretending to be the server at World Community Grid. The private key used for this authentication is closely guarded and is not even stored on the servers at World Community Grid. Furthermore, the executables for the agent and research processing are audited for any vulnerabilities, viruses and Trojan horses before being accepted for use in World Community Grid.

Announcements about any such updates are available on the web site at World Community Grid. If a user configured his firewall to permit a specific program -- i.e. the World Community Grid agent -- to contact the server, rather than using a blanket rule for the outgoing connection discussed, the user will be prompted by the firewall software to authorize the new version of the agent to communicate back to the server.

SERVER SITE

The servers are hosted at a high-security IBM hosting site located in Boulder, Colorado used for = critical business applications. Extensive IBM-established corporate security procedures are followed for all aspects of security. Physical access to the servers is controlled via biometric access controls. Several layers of firewalls are used to permit only the particular communication types required outside and among the machines involved. Furthermore, multiple authentication layers are required to gain access to the servers. All of the servers are continually monitored for any anomalies, all of which are carefully investigated.

SECURITY AUDITS

World Community Grid performs security audits led by IBM security experts to prevent security breaches and expose any attempted attacks. Security exposures discovered during the audits will be immediately repaired. The Security Audit focus areas include: the physical security of the Boulder, Colorado hosting site; all United Devices software; World Community Grid's grid and web servers and their software; the research application software, the Human Proteome Rosetta Software used in the first project. Periodically, ethical hackers are used to examine the software and attempt to find security vulnerabilities.

When World Community Grid makes code changes, an audit team rechecks for vulnerabilities, viruses and Trojan horses. New research code is examined via a walk-through and modified to conform to the requirements of the grid infrastructure. The code is also tested on a beta grid server environment before deployment on the primary grid.

We encourage others to examine the client, and communicate any vulnerabilities as soon as possible. The grid infrastructure and agent we use has not been successfully

World Community Grid **Security Overview**

compromised in over five years of use. While we've taken measures to ensure the safety and security of our clients, we remain open to suggestions on how we could make this architecture even more secure.

REGARDING COMPETITION FOR RESOURCE CAPACITY

The agent does not compete with any work that needs to be done by the user's PC. The agent runs its work at the lowest CPU priority so that it yields to anything else in the system. Normally this permits the agent to use all of the free time available on the machine without any performance interference. However, if the machine has a relatively small amount of real memory, some paging delays can occur. For such situations, World Community Grid gives the user the option to make the agent run only as a screen saver and the option to specify time windows during the week when the agent is allowed to run and to communicate with the server. In addition, there is a snooze option, which lets the user right click on the tray icon for World Community Grid (when minimized) to have it stop processing for a specified number of minutes. World Community Grid also is working on a way to throttle the agent's work so that it sleeps an average of NN% of the time to better permit other lowest priority work in the machine to run effectively at higher priority than World Community Grid and to reduce CPU temperatures in especially hot machines. Thus CPU utilization should not be a problem.

World Community Grid allocates about 200MB of virtual memory currently, but the working set size is about 25MB. World Community Grid is working on reducing this footprint. On machines with limited real memory, there can be brief paging delays due to this. But again, the user has the option to run the agent at times when it will not interfere.

Disk usage is minimal. The Human Proteome Folding (HPF) project, the first project on World Community Grid, uses less than 30MB of disk space. The user is given the option to allow the agent to use more, potentially for later projects that might need the extra space. The space is used to store the executables, the input and output data. This state information is encrypted as are the other files.

Network usage is also relatively low. For HPF, the original install and registration requires about 5MB of download. However after that, each unit of work needs about 1MB of input data to process. After an average of 10 to 20 hours of CPU processing (which typically takes a day to a week or more depending on usage patterns and machine speed), the agent sends back about 1 MB output data and gets another work unit of input data.

World Community Grid
Security Overview