Security in BOINC crowd computing

Alyssa Milburn

Leiden University

Crowd Computing 2014

The IDGF-SP project is supported by the FP7 Capacities Programme under grant agreement nr RI-312297.

Trust

Crowd computing depends on trust.

Trust

Organised groups of users can falsify results.

Trust

Users allow projects to run arbitrary code on their machines!

Cat and mouse

Sandboxing?

Local privilege escalation

Windows: CVE-2014-0318, CVE-2014-1814, CVE-2014-1819, ...

Linux: CVE-2014-0038, CVE-2014-0196, ...

Cat and mouse

Containers, virtual machines?

VM/container escapes

VirtualBox (on a Windows host): CVE-2014-0983, CVE-2013-2487, CVE-2014-4261, ...

Docker: CVE-2014-3499, CVE-2014-5206, ...

Cat and mouse

No native code?

Java?

July 2014: Critical Patch Update contains 20 new security fixes

April 2014: Critical Patch Update contains 37 new security fixes

January 2014: Critical Patch Update contains 36 new security fixes

October 2013: Critical Patch Update contains 51 new security fixes

June 2013: Critical Patch Update contains 40 new security fixes

April 2013: Critical Patch Update contains 42 new security fixes

Trust

We have to assume that projects can be trusted.

Well-meant attacks

"Optimising" code, "fixing" bugs.

Trying to game the BOINC credit system.

Result validation

- Validation
- Replication (run tasks N times)

  (Adaptive replication, Homogeneous replication)
- Custom validation

Hostile attackers

The usual problems: XSS, e-mail addresses, passwords.

(Especially when projects are e.g., mining bitcoin.)

But also: Crowd computing provides convenient botnets!

Prevent sniffing

Free/cheap SSL certificates.

Code signing

Volunteers should be safe if your web server is compromised.

Keep the key *offline*! Replace it if necessary.

Data signing

Signing the data is usually unnecessary.

(Beware: encryption for confidential payloads dosn't work!)

Upload certificates help avoid DoSes.

Vulnerabilities

Various security issues in BOINC server and client.

(SQL injections, stack overflows, heap overflows)

Vulnerabilities

Also in the web server, OS, database . . .

Server security

Keeping the OS and web server up-to-date is (hopefully) easy.

Updating/patching BOINC server components can be difficult for projects.

Mitigation strategies:

- Firewalls/IDS
- Separate machines
- Logs
- Hardening flags

Trust

A successful attack could discredit all BOINC-based projects, and volunteer computing in general.

`http://boinc.berkeley.edu/trac/wiki/SecurityIssues`

Summary

Crowd computing depends on trust.

But complete security is (near-) impossible to achieve.

Ask for help if you need it!

Questions?