Extending the NaCl Sandbox with Restricted Networking Support

Project Proposal, Operating Systems - Practical – Autumn 2011

Index terms: security, operating systems
Keywords: sandboxing, plugin, runtime environment, networking
Team size: 2

1   Project Description

Native Client (NaCl) is an open-source technology that allows building web applications that can execute native compiled code inside the browser. It relies on a sandboxing mechanism for limiting the functionality of the applications so that the running system can not be compromised. This requires filtering out all potential harmful calls to the underlying system functions. Direct access to the network and file access are forbidden, making it highly suitable for deploying CPU-intensive code into client browsers.

This project extends the NaCl sandbox with limited networking functionality, allowing NaCl applications to access the network in a restricted mode. This allows developing small networked components that can be deployed in sandboxed environments in future browsers or other application containers. A possible application for this would be integrating a BitTorrent client as a plugin inside a web browser.

2   Objectives

This project aims to develop an extension for the NaCl sandboxing solution that will meet the following requirements:

- The NaCl sandbox should be extended to allow calls to `connect`, `bind` and `accept`.

- Calls to the networking functions should be restricted to specific ports or protocols (for example: accept only outgoing connect calls to TCP port 80)

- The impact on the performance of the networking applications running in the NaCl sandbox should be evaluated.

3   Bibliography

[1] *Native Client Documentation* http://www.chromium.org/nativeclient

[2] *Native Client Project* http://code.google.com/p/nativeclient/

[3] *Native Client Ported Libraries* http://code.google.com/p/naclports/

[4] Bennet Yee, David Sehr, Gregory Dardyk, J. Bradley Chen, Robert Muth, Tavis Ormandy, Shiki Okasaka, Neha Narula, and Nicholas Fullagar. *Native Client: a sandbox for portable, untrusted x86 native code.* Commun. ACM 53, 1 (January 2010), 91-99, http://research.google.com/pubs/archive/34913.pdf

4   Prerequisites

Operating Systems Design, Security, Networking, C/C++

5   Other

For more information about this project proposal please contact:

Mircea Bardac
mircea.bardac@cs.pub.ro