

# *Debian Hardened 2004*

“Improving high security for Debian”

<http://www.debian-hardened.org> & <http://wiki.debian-hardened.org>

By Lorenzo Hernández García-Hierro [lorenzo@gnu.org](mailto:lorenzo@gnu.org)  
Performance results by John Richard Moser [nigelenki@comcast.net](mailto:nigelenki@comcast.net)

# *Debian Hardened*

- ◆ Debian as a trusted, secure environment.
- ◆ Objectives(I).
- ◆ Objectives(II).
- ◆ Research & analysis for objectives fulfilling.
- ◆ Final development & implementation.
- ◆ Final result analysis.
- ◆ Advantages & Disadvantages.
- ◆ Immediate future.

# *Debian as a trusted, secure environment.*

- Implementing high security features on Debian.
- Introducing the developers to a work model that guarantees the security.
- Developing new implementations to bring those features.
- Minimal influence in the final usability & stability.
- Open, collaborative work models for cross-distribution developers.

# *Objectives (I)*

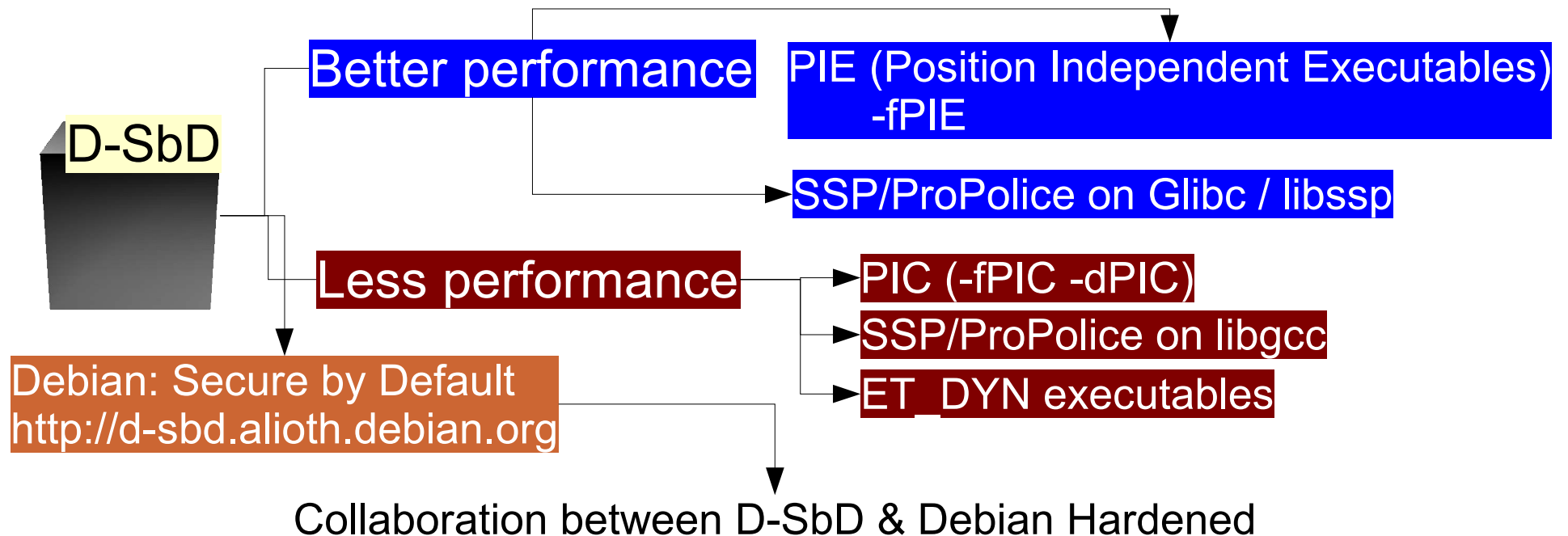
- ◆ Providing hardened kernels with the DHKP (Debian Hardened Kernel Patchset)
- ◆ Packages rebuilding for use position independent executables (PIE) and SSP/ProPolice for stack protection.
- ◆ Arbitrary patches for package security enhancements.
- ◆ Implementing a hardened GNU C library (Glibc).

## *Objectives (II)*

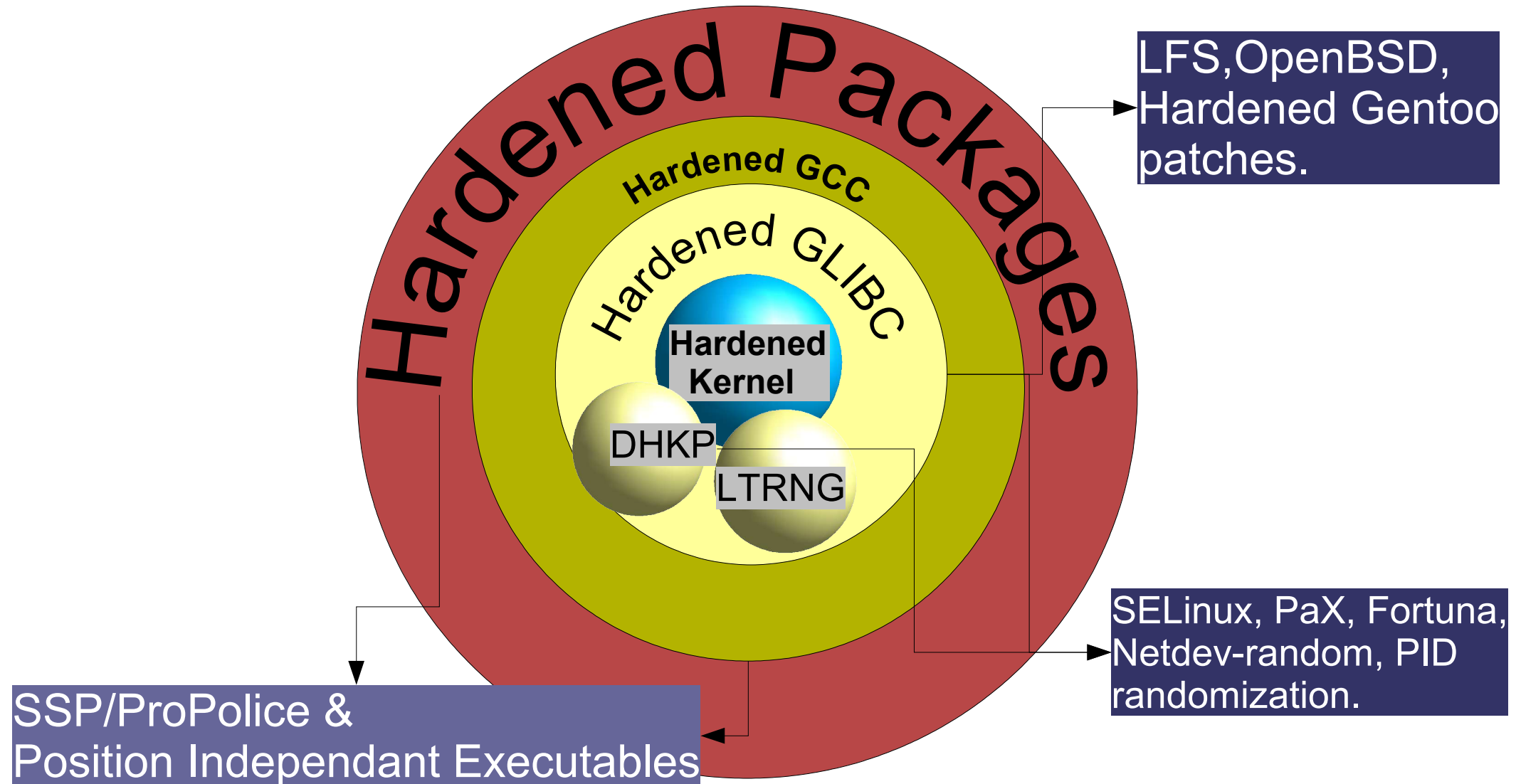
- ◆ Implement SSP/ProPolice & PIE in the GNU C Compiler Library (libgcc).
- ◆ Provide documentation for developers changing into the new work model.
- ◆ Open documentation for all of the implementations.
- ◆ Collaboration between developers from different projects: Hardened Gentoo, Adamantix, OpenBSD...etc.

# Research & analysis for objectives fulfilling.

- ◆ Possibilities & alternatives study.
- ◆ Influence analysis (performance, etc).

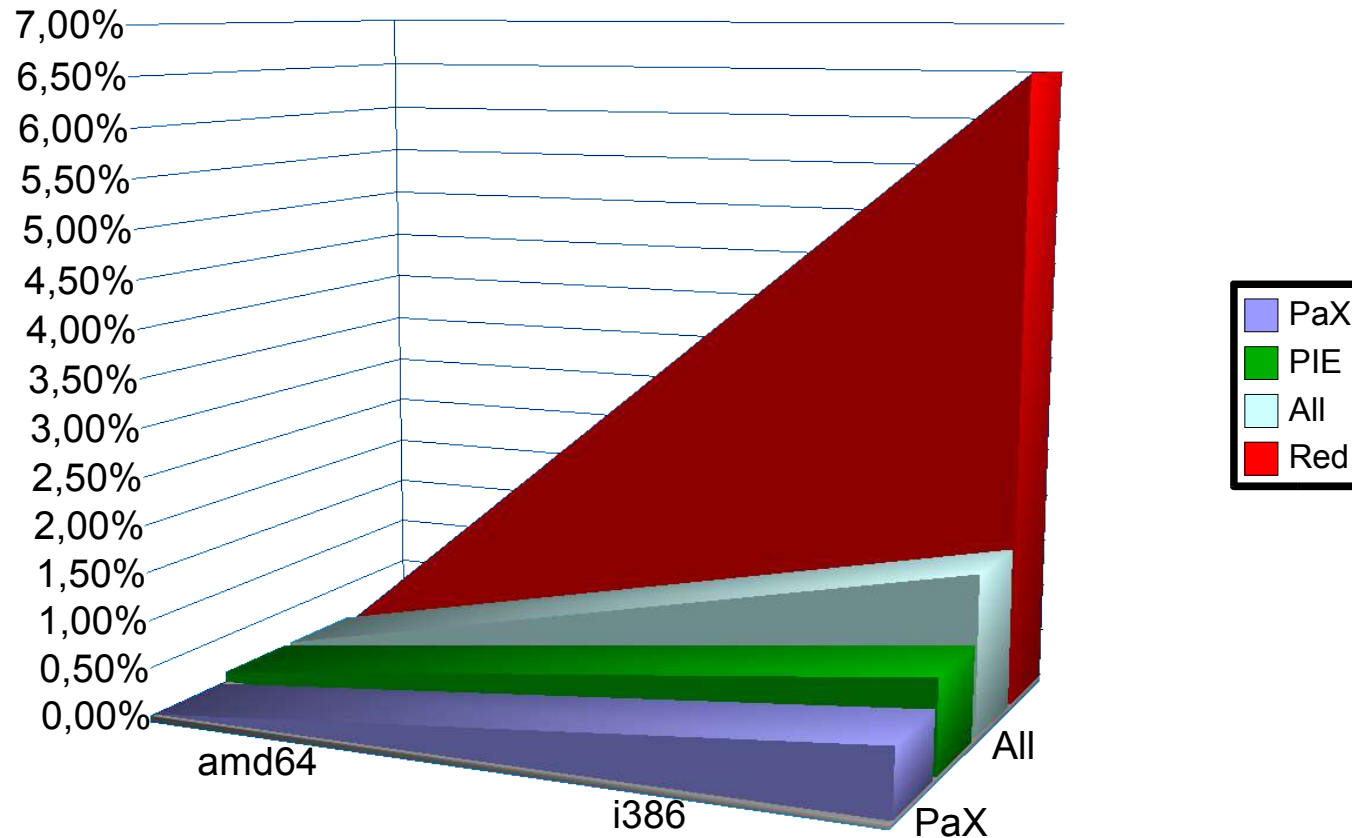


# *Final development & implementation.*



# Final result analisys.

## PaX & PIE Performance Impacts



The red total accounts for the inability of `-fomit-frame-pointer` to increase the performance of an executable in the presence of PIC; however, because most of the system is PIC anyway (every shared object, library, and plug-in is PIC), the overhead from PIE is in reality lower (possibly much lower).

The testing was made with BYTEmark\* Native Mode Benchmark ver. 2, on a PaX enabled kernel.

# *Advantages & Disadvantages.*

- ◆ Easy way for getting in the rid of Debian-based systems hardening.
- ◆ Free Software: free as in freedom, open development.
- ◆ Non-agressive implementations but it may cause unexpected errors that will be known during long time of testing.
- ◆ Tested, proved performance, but may consume more disk space and processing cycles.
- ◆ Making software security updates a lower priority, but it doesn't protects everything.
- ◆ It can be difficult to be understood by normal user, but not for sysadmins.

## *Inmediate future.*

- ◆ Progressive inclusion into the Debian project.
- ◆ 2.6.9 hardened kernel development.
- ◆ DHKP 1.0 release for 2.6 & 2.4 kernel brands.
- ◆ Adamantix's SSP/ProPolice implementation by Peter Busser.
- ◆ Automated debian package builder (autobuilder) for automatic packages hardening.
- ◆ Porting to sparc, sparc64, ppc, alpha, hppa archs.