

# Securing the testing distribution

Joey Hess

DebConf5



# The Debian testing distribution: insecure by design

- ▶ dependency hell
- ▶ unrelated release critical bugs can block security fixes
- ▶ built in "testing" delays
- ▶ autobuilder lag
- ▶ based on unstable, which has no security team



# How Debian developers can help

- ▶ include CVE ids in changeogs and bug reports
- ▶ get CVE ids assigned for security holes that lack ids
- ▶ don't hide security fixes
- ▶ respond quickly to security bugs (or be NMUed)
- ▶ communicate with the team



# A rough comparison of stable and testing

112 DSAs issued between January and May 2005

- ▶ 56 (50%) fixed in stable first
- ▶ 37 (33%) fixed in testing first
- ▶ 19 (17%) did not affect testing
- ▶ XXX (XX%) affected stable with DSA
- ▶ XXX (XX%) did not affect stable



# Links

- ▶ Testing Security Team:  
<http://secure-testing.alioth.debian.org/>
- ▶ Tracking page:  
<http://newraff.debian.org/~joeyh/testing-security.html>

