Debian Security

An overview of features and processes

Who is this guy?

Todd Troxell

Debian Developer

“Security Enthusiast”

Logcheck maintainer

Debian Security
Todd Troxell <ttroxell@debian.org>

What is Debian?

Linux Distribution

Debian Security
Todd Troxell <ttroxell@debian.org>

Free Operating System

Debian Security
Todd Troxell <ttroxell@debian.org>

Volunteer project

Debian Security
Todd Troxell <ttroxell@debian.org>

Based on Linux Kernel

and 15,000+
free software
packages

12
Architectures

i386, m68k, sparc, alpha, powerpc, arm, mips, mipsel ,hppa, ia64, s/390, amd64

Universal

Freedom

Debian Security Team

http://www.debian.org/security

Review security problems

Upload pathced packages

Issue Advisories

Public Disclosure

Not security through obscurity

Advisories: DSAs

Available in multiple formats

debian-security-announce

http://debian.org/security

http://www.debian.org/security/dsa-long

(RSS)

Best format:

Easily installed verified patches

Updates: change as little as possible

Favor patching

Not upgrading

Secure-APT

Debian Security
Todd Troxell <ttroxell@debian.org>

Automated updating

Ideal: no security problems ever!

Not going to happen

Pro-active search for vulnerabilities

Debian Security
Todd Troxell <ttroxell@debian.org>

Debian Audit Project

http://www.debian.org/security/audit

Debian Security
Todd Troxell <ttroxell@debian.org>

Steve Kemp

Ulf Härnhammar

David A. Wheeler

White hats, pen-testers

Discovered
near 100
vulnerabilities

Audit as many packages as possible

Not a short order

15,000
Packages

20 CDs

3 DVDs

Counting only i386 binary

Priority

Packages with setuid/setgid binaries

Debian Security
Todd Troxell <ttroxell@debian.org>

Anything providing a sevice over a network

Widely-distributed packages

Anything associated with CGI/PHP

Debian Security
Todd Troxell <ttroxell@debian.org>

Automated jobs running as root

-flawfinder
-ITS4
-RATS
-pscan
(many more)

http://www.debian.org/security/audit/tools

Open code

from boot loader

to web
browser.

Not
“Trust me”
code.

possible to
audit from top
to bottom

rarely
possible in
proprietary
software

Security related packages

Intrusion Detection

Debian Security
Todd Troxell <ttroxell@debian.org>

Snort, Ntop

+ modules for My/Pg SQL logging and analysis applications: acidlab, ethereal

Integrit, AIDE, Tripwire, Fcheck

Logcheck, Logwatch, Epylog

Debian Security
Todd Troxell <ttroxell@debian.org>

debsigs, dpkg-sig

Debian Security
Todd Troxell <ttroxell@debian.org>

Encryption

GNU Privacy Guard (GPG)

Debian Security
Todd Troxell <ttroxell@debian.org>

OpenSSL/SSH

Debian Security
Todd Troxell <ttroxell@debian.org>

CFS, EncFS, loop-aes

Debian Security
Todd Troxell <ttroxell@debian.org>

Gaim-OTR

Debian Security
Todd Troxell <ttroxell@debian.org>

OpenVPN, Racoon/ipsec, stunnel, OpenSWAN

Kerberos

OpenAFS

Debian Security
Todd Troxell <ttroxell@debian.org>

Various libraries, APIs

Cryptographic algorithms already written and tested.

Penetration Testing

Debian Security
Todd Troxell <ttroxell@debian.org>

NMAP

Debian Security
Todd Troxell <ttroxell@debian.org>

Nikito, Airsnort, Aircrack

smb-nat,
tiger,
irpas

Anti-virus

Typically referring to Windows AV

ClamAV, amavis

PAM

Allows for a wide array of auth/sesssion options

libpam-chroot

Debian Security
Todd Troxell <ttroxell@debian.org>

libpam-cracklib

libpam-krb5

Debian Security
Todd Troxell <ttroxell@debian.org>

libpam-ldap

PAM Smartcard modules, SecureID

Debian Security
Todd Troxell <ttroxell@debian.org>

libpam-ccreds - Pam module to cache authentication credentials
libpam-chroot - Chroot Pluggable Authentication Module for PAM
libpam-cracklib - PAM module to enable cracklib support.
libpam-devperm - PAM module to change device ownership on login
libpam-doc - Documentation of PAM
libpam-dotfile - A PAM module which allows users to have more than one password
libpam-encfs - PAM module to automatically mount encfs filesystems on login
libpam-foreground - create lockfiles describing which users own which console
libpam-heimdal - PAM module for Heimdal Kerberos 5
libpam-http - a PAM module to authenticate via http/https
libpam-krb5 - PAM module for MIT Kerberos
libpam-ldap - Pluggable Authentication Module allowing LDAP interfaces
libpam-modules - Pluggable Authentication Modules for PAM
libpam-mount - PAM module that can mount volumes for a user session
libpam-musclecard - PAM module for MuscleCard Framework
libpam-mysql - PAM module allowing authentication from a MySQL server
libpam-ncp - PAM module allowing authentication from a NetWare server
libpam-openafs-kaserver - AFS distributed filesystem kaserver PAM module
libpam-openafs-session - PAM Module to get AFS tokens and set up PAG
libpam-opie - Use OTPs for PAM authentication
libpam-p11 - PAM module for using PKCS#11 smart cards
libpam-passwdqc - replacement for the pam_cracklib module
libpam-pgsql - PAM module to authenticate using a PostgreSQL database
libpam-poldi - PAM module allowing authentication using a OpenPGP smartcard
libpam-pwdfile - PAM module allowing authentication via an /etc/passwd-like filelibpam-pwgen - a password generator
libpam-radius-auth - The PAM RADIUS authentication module
libpam-runtime - Runtime support for the PAM library
libpam-shishi - PAM module for Shishi Kerberos v5
libpam-smbpass - pluggable authentication module for SMB/CIFS password database
libpam-ssh - enable SSO behavior for ssh and pam
libpam-tmpdir - automatic per-user temporary directories
libpam-umask - adjust users' default umask using PAM
libpam-unix2 - Blowfish-capable PAM module

Kernel Features

NetFilter

Debian Security
Todd Troxell <ttroxell@debian.org>

SELinux

Debian Security
Todd Troxell <ttroxell@debian.org>

Xen Hypervisor

Debian Security
Todd Troxell <ttroxell@debian.org>

GRSecurity
ACL patches

GR PAX Patches (address space)

Debian Security
Todd Troxell <ttroxell@debian.org>

Other GR Patches

http://www.grsecurity.net/features.php

Debian “harden” packages...

harden-clients - Avoid clients that are known to be insecure
harden-development - Development tools for creating more secure programs
harden-environment - Hardened system environment
harden-nids - Harden a system by using a network intrusion detection system
harden-remoteaudit - Audit your remote systems from this host
harden-servers - Avoid servers that are known to be insecure
harden-surveillance - Check services and/or servers automatically
harden-tools - Tools to enhance or analyze the security of the local system

Harden packages make clever use of Debian's packaging system

Debian Security
Todd Troxell <ttroxell@debian.org>

Package: **harden-servers**

Conflicts: telnetd, ftpd, lukemftpd, muddleftpd, wu-ftpd, oftpd, pyftpd, vsftpd, proftpd, bsd-ftpd, talkd, fingerd, xfingerd, ffingerd, cfingerd, efingerd, sendmail, netkit-rpc, nfs-kernel-server, nfs-user-server, rwalld, rusersd, portmap, rsh-server, uw-imapd, cyrus-imapd, rstartd, bidentd, pidentd, midentd, oidentd, gidentd, mdidentd, remstats-servers, pawserv

...too many packages to mention

```
checksecurity - basic system security checks
libapache2-mod-security - Tighten web applications security for Apache 2.x
libnasl-dev - Nessus Attack Scripting Language, static library and headers
libnasl2 - Nessus Attack Scripting Language, shared library
libnessus-dev - Nessus static libraries and headers
libnessus2 - Nessus shared libraries
libpcap0.7 - System interface for user-level packet capture
libpcap0.7-dev - Development library and header files for libpcap 0.7
libpcap0.8 - System interface for user-level packet capture
libpcap0.8-dev - Development library and header files for libpcap 0.8
libsasl2 - Authentication abstraction library
libselinux1 - SELinux shared libraries
libselinux1-dev - SELinux development headers
libsepol1 - Security Enhanced Linux policy library for changing policy binaries
libsepol1-dev - Security Enhanced Linux policy library and development files
libwrap0 - Wietse Venema's TCP wrappers library
libwrap0-dev - Wietse Venema's TCP wrappers library, development files
libxmlsec1 - XML security library
libxmlsec1-dev - Development files for the XML security library
libxmlsec1-nss - Nss engine for the XML security library
libxmlsec1-openssl - Openssl engine for the XML security library
logcheck - mails anomalies in the system logfiles to the administrator
mod-security-common - Tighten web applications security - common files
nessus - Remote network security auditor, the client
nessus-dev - Nessus development header files
nessus-plugins - Nessus plugins
nessusd - Remote network security auditor, the server
nmap - The Network Mapper
tcpd - Wietse Venema's TCP wrapper utilities
unattended-upgrades - Install security upgrades automatically
vsftpd - The Very Secure FTP Daemon
apticron - cron-script to mail impending apt updates
bastille - Security hardening tool
bfbtester - Brute Force Binary Tester
ccrypt - secure encryption and decryption of files and streams
cfs - Cryptographic Filesystem
checkpolicy - SELinux policy compiler
```

```
chiark-really - really - a tool for gaining privilege (simple, realistic sudo)
chpax - user-space utility to control PaX flags
clamassassin - simple virus filter wrapper for ClamAV
cron-apt - automatic update of packages using apt-get
cvsd - chroot wrapper to run `cvs pserver' more securely
dcfldd - enhanced version of dd for forensics and security
debsecan - Debian Security Analyzer
elfsh - The ELF shell
flawfinder - examines source code and looks for security weaknesses
gnunet - Secure, trust-based peer-to-peer framework
gradm - Administration program for the GrSecurity ACL system
gradm2 - Administration program for the grsecurity2 RBAC based ACL system
gsasl - GNU SASL commandline utility
guarddog - firewall configuration utility for KDE
harden - Makes your system hardened
harden-development - Development tools for creating more secure programs
harden-tools - Tools to enhance or analyze the security of the local system
ipkungfu - iptables-based Linux firewall
isakmpd - The Internet Key Exchange protocol openbsd implementation
kernel-patch-skas - Separate Kernel Address Space patch
kernel-patch-vserver - context switching virtual private servers - kernel patch
knocker - a simple and easy to use TCP security port scanner
lcap - Removes 'capabilities' in the kernel, making the system more secure
libapache-mod-ssl - Strong cryptography (HTTPS support) for Apache
libapache-mod-ssl-doc - Documentation for Apache module mod_ssl
libcrypt-ecb-perl - Perl library to encrypt data using ECB mode
libcryptokit-ocaml - cryptographic algorithm library for OCaml - runtime
libcryptokit-ocaml-dev - cryptographic algorithm library for OCaml - development
libdigest-md2-perl - MD2 Message Digest for Perl
libdigest-md4-perl - MD4 Message Digest for Perl
libelfsh0 - The ELF shell library
libelfsh0-dev - The ELF shell library
libetoken - PC/SC Driver for Aladdin's eToken usb plug
libgsasl7 - GNU SASL library
libgsasl7-dev - Development files for the GNU SASL library
libopensc2 - SmartCard library with support for PKCS#15 compatible smart cards
```


```
libpam-tmpdir - automatic per-user temporary directories
libroxen-ntuserauth - WinNT/SMB user authentication module for the Roxen Challenger web server
libroxen-referrerdeny - File deny module for the Roxen Challenger web server
libsemanage1 - shared libraries used by SELinux policy manipulation tools
libsemanage1-dev - Header files and libraries for SELinux policy manipulation tools
libxmlsec1-gnutls - Gnutls engine for the XML security library
makepasswd - Generate and encrypt passwords
maradns - Simple security-aware Domain Name Service server
mew - mail reader supporting PGP/MIME for Emacs
mew-beta - mail reader supporting PGP/MIME for Emacs (development version)
nikto - web server security scanner
opensc - SmartCard utilities with support for PKCS#15 compatible cards
openswan - IPSEC utilities for Openswan
openvpn - Virtual Private Network daemon
otp - Generator for One Time Passwords
paxctl - user-space utility to control PaX flags - new major upstream version
paxtest - Test suite for the PaX kernel patch
popa3d - A tiny POP3 daemon, designed with security as the primary goal
pscan - Format string security checker for C files.
python2.4-selinux - Python2.4 bindings to SELinux shared libraries
python2.4-semanage - Python2.4 bindings  for SELinux policy manipulation tools
raccess - Security Tool to audit remote systems
rats - Rough Auditing Tool for Security
realtime-lsm - Scripts for handling the realtime Linux security module
realtime-lsm-source - Source for the realtime Linux security module
rssh - Restricted shell allowing only scp, sftp, cvs, rsync and/or rdist
sanitizer - The Anomy Mail Sanitizer - an email virus scanner
schroot - Execute commands in a chroot environment
secpolicy - KDE PAM security policy configuration tool
selinux-doc - documentation for Security-Enhanced Linux
selinux-policy-default - Policy config files and management for NSA Security Enhanced Linux
```

```
selinux-utils - SELinux utility programs
sepol-utils - Security Enhanced Linux policy utility programs
slat - Tools for information flow analysis of SELinux policies
smb-nat - Netbios Auditing Tool
smtp-refuser - Simple spam-block with refusal message
spikeproxy - Web application security testing proxy
splint - A tool for statically checking C programs for bugs
splint-doc - Documentation for splint: a tool for statically checking C programs
for bugs
systraq - monitor your system and warn when system files change
tcpspy - Incoming and Outgoing TCP/IP connections logger
tiger - Report system security vulnerabilities
tiger-otheros - Scripts to run Tiger in other operating systems
xmlsec1 - XML security command line processor
xprobe - Remote OS identification
xsu - Allow users to run commands as root, after prompting for password.
irpas - Internetwork Routing Protocol Attack Suite
uae-suid - The Ubiquitous Amiga Emulator: Suid root binaries
libgnutls-dev - the GNU TLS library - development files
libgnutls12 - the GNU TLS library - runtime library
libnss-dev - Network Security Service Libraries - development
libnss3 - Network Security Service Libraries - runtime
gnutls-bin - the GNU TLS library - commandline utilities
libgnutls11 - GNU TLS library - runtime library
libgnutls11-dbg - GNU TLS library - debugger symbols
libgnutls11-dev - GNU TLS library - development files
libgnutls12-dbg - GNU TLS library - debugger symbols
```

Secure Development of Debian

Debian Security
Todd Troxell <ttroxell@debian.org>

“If it's volunteer project, what stops someone from uploading a trojan?”

Cryptographic Web of trust

Debian Security
Todd Troxell <ttroxell@debian.org>

Verify identies, Exchange GPG key signatures

Debian Security
Todd Troxell <ttroxell@debian.org>

“Key signing parties”

A DD must have a key in debian keyring to upload.

Uploads are also hand screened by ftpmasters

Voting in Debian: GPG signed email

Debian Security
Todd Troxell <ttroxell@debian.org>

Same type of keys are used to sign:

Pacakges

Releases

Advisories

No (known) trojans uploaded to date.

Debian Policy enhances security

http://www.debian.org/doc/debian-policy/

Debian Security
Todd Troxell <ttroxell@debian.org>

Clearly defined rules for how things should work

Section 3.1: “Every package must have a unique name”

Section 10.9:

“Files should be owned by root.root, and made writable only by the owner and universally readable (and executable, if appropriate), that is mode 644 or 755.”

Breaking policy is considered a very serious bug.

Debian stable release cycle

Debian Security
Todd Troxell <ttroxell@debian.org>

“Relaxed”

“Laid Back”

By which I mean

Notoriously slow

While software is a bit older,

Debian packages are time-tested

Debian Security
Todd Troxell <ttroxell@debian.org>

Fewer security vulnerabilities

-Stable
-Testing
-Unstable

Testing: rigorous peer overview

Debian Security
Todd Troxell <ttroxell@debian.org>

If you want newer code: run testing!

Testing even has a security team.

Debian Developers and Community

Debian Security
Todd Troxell <ttroxell@debian.org>

Schneier:
“Security is a process.”

Our users and developers include many enthusiasts

--folks interested
in the technology

Security nerds rabidly tracking down vulnerabilities

Debian Security
Todd Troxell <ttroxell@debian.org>

Google: don't force anyone to work on anything

Huge user-base means vulnerabilities matter

open code ==
secure code

“Given enough eyeballs, all bugs are shallow”

"Commercial software typically has 20 to 30 bugs for every 1,000 lines of code, according to Carnegie Mellon University's CyLab Sustainable Computing Consortium. This would be equivalent to 114,000 to 171,000 bugs in 5.7 million lines of code. The study identified 0.17 bugs per 1,000 lines of code in the Linux kernel."

-Wired

“15,000 packages! How can that possibly be secure?”

A tiny subset form
a solid base
install.

Thanks!