Security in Debian

Food for thought and for discussion
http://people.debian.org/~jfs/debconf/security/

Javier Fernández-Sanguino Peña

jfs@debian.org
Main Goal: spark some discussion of the Debian GNU/Linux status from a security point of view.

Secondary Goals:
- share some personal views on where are we heading.
- prompt for action in some areas

Personal Goals:
- CC certification (EAL4?)
- Easy setup (Knoppix-like) of security-related servers (NIDS, VA..)
Security in Debian: Avoiding issues

http://tira.escomposlinux.org/ecol-79-e.png
The Security Team is doing an excellent work at keeping stable free of security bugs.

- Mean time for the team to upload a new package fixing a security vulnerability published on Bugtraq is 7 days.

- Security vulnerabilities are fixed for all our (11) supported architectures at the same time (well, most of the time..)
Debian provides much more security-related tools than any other operating system.

- Some *white-hat* (protection) tools: intrusion detection systems, integrity checkers, forensics tools, firewall wrappers, log analysis, encryption...

- Some *grey-hat* (attack) tools: vulnerability assessment, network scanners, sniffers

- Security-related work can be done with Debian, from disaster recovery to pen-testing.
Security in Debian: The Good Things

Debian takes part in security standards and bodies:

- Linux vendors security mailing list
- CERT
- Mitre:
  - CVE (not in the Board, but an approved "product")
  - and OVAL (in the Board soon)
- NSA’s Selinux (thanks Russell!)
You can do a very minimal installation of Debian GNU/Linux.

The default setup of most daemons / network services / viewers is usually secure.

Most Debian maintainers are security-conscious.
  - If you are not, please start by reading the Developers Reference: http://www.debian.org/doc/manuals/developers-reference/ch-pkgs.en.html#s-bug-security
  - Maybe follow up with http://www.dwheeler.com/secure-programs/
Security in Debian: The Bad Things

- Average time to fix a security issue and number of DSAs increases every year. From (median) time of 3.5 days (1999) to 63 days (this year, kernel issues...)

- Number of DSAs issues is also increasing every year. 17 in 1997, 124 last year and with the current trend expect 233 this year.

- Our Security Team is behind other Security Teams with security fixes. To fix the same vulnerability issue:
  - RedHat, median is 8 days later (average 16)
  - Mandrake, median is 3 days later (average 18)

- But faster than others (Conectiva 10 days -median-faster)
Security in Debian: The Bad Things

Full data at http://people.debian.org/~jfs/debconf/security/
Security in Debian: The Bad Things

Full data at http://people.debian.org/~jfs/debconf/security/
Possible reasons:

- The size of the distribution is increasing (a similar trend can be seen for CERT advisories, Bugtraq reports...)
- Complexity is too.
- The Security Team does not have enough resources.
- After all this is done in a volunteer basis.
Consequences for this Bad Thing

- User Awareness is low (take the kernel ptrace vuln, lots of questions on that one)
  - Need to issue DSA or include "work in progress" in DSAs
  - Need to publish security information in security.debian.org (Tags: security as well as pending DSAs)

- With the current trend (1 DSA a day?) people will make it difficult to keep up.
  - So machines will have to do it for us.
Security in Debian: More Bad Things

- No fully secure downloads prevents full automation.
  - Single point of failure: security.debian.org
  - No encrypted/authenticated connection to download site (vulnerable to spoofing and MITM attacks)
  - Checks for downloaded packages not automated (signed releases but there’s not support in apt)
  - No user-friendly front-end to secure updates (a single button)
  - No easy way to check system update w/o net access (coupled with too many DSAs)
Security tools turn old due to release process

- Render security tools useless (see #173254 -snort- and #183524 -nessus)

- False sense of security to stable users (chkrootkit does not detect newer rookits, rule-based IDS cannot detect new attacks, antivirus...)

- Could be fixed providing a backport to stable of some of these tools if possible.
Security in Debian: Some improvements

No formal audit yet conducted

- Need to do this for upstream?
- Start with base system, network servers and popular packages
- Several efforts: Steve Kemp (http://www.steve.org.uk/Debian/), and Drew Daniels (https://sourceforge.net/projects/debraudit/)

Move this to Alioth? Official backup? Coordinate with Sardonix.org?
Full daemon compartmentalization (sp?) and privilege separation

- Chroots (or other separation, maybe user-mode linux) for network services.
- Both OpenBSD and HP-UX are starting to do this automatically
- Difficult to handle by the package management system
- Some DDs do not consider it top priority (sample: bind see #50013,#94760, #157245, #169124)
How easy is to make a hardened version of Debian?

- No task-secure-server
- Standard is bloated? (includes telnetd!) See #81118
- No way to replace software with reduced functionality counterparts (IF the user wants a dns-server don’t give him bind...)

- No pre-configuration of Firewall or HIDS in the system (checksecurity is *not* an HIDS: #163813)
- Some network services open to the network (exim, rpc)

(It’s a pity the Adamantix guy turned away...)
No easy way to recompile every package (libsafe?)

No easy way to say: "do not start any network services even if I install the packages."

Abandoned port to OpenBSD, but it just might be interesting considering the improvements in 3.3:

- Propolice stack protection (stack canary)
- W xor X (execute-bit support in MMUs which support it)
- pf (packet filtering)

More info: http://www.openbsd.org/33.html
But:

- We have Bastille
- We have harden-XYZ
- We have a lot of secure patches for the Linux kernel (grsecurity...)
- Packages are shipping secure configurations per default (sample: X –nolisten-tcp)

Why not provide a way for the user to set the non-default things up properly on installation?
Final remarks (summary)

- Raise User Awareness: Uses DSAs to alert users of pending issues, provide a tracking database with a public interface.
- Security Audit Team (or Task Force)
- Hardened distro: fully integration on installation
- Secure Update Button
- Investigate automatic compartimentalization of services
- Service to receive personalised DSAs (based on user profile), similar to RHN.
- Probably many more (but let’s focus on some :-)

Debconf3 - Oslo - 19th July 2003 – p.20/20