Adamantix, the hardened Debian derivative

As hard as diamond

The Adamantix project derives its name from the Middle English word adamant, which was used to describe stones (such as diamonds) of impenetrable hardness. Despite the etymological background, the design of this Debian Woody-based distribution is extremely modern, although the implementation does leave the impression of a diamond with rough edges. BY CHRISTIAN NEY

The major distributors all attempt to patch vulnerabilities as soon as they are disclosed. But this is symptomatic treatment for known issues. Heap and buffer overflows are the most common attack vectors. Strangely, most distributors have failed to take a proactive approach, although software could mitigate the effect of attacks. Projects such as OpenBSD have a more responsible security posture. Specialized distributions can easily hold their own, when there is a need to cater to special interests, one notable example being Trustix Secure Linux [1], a Red Hat-based product which you may know as Tawie Server Linux.

This article describes the Adamantix [2] distribution, which is based on Debian Woody. When it was founded at the end of 2002, the free project was known as Trusted Debian. However, Debian project leader, Martin Michlmayr, sent a message to the Adamantix team pointing out that "Debian" was a registered trademark. Also, the word "Trusted" in the name chosen for the project implied that the original Debian Linux was not to be trusted. This led Martin to ask them to change the name.

To tackle this issue, they posted a message on the project's mailing list, asking people to suggest a new name. The project finally opted for "Adamantix", the Middle English word for diamond. At present, about ten people are actively involved in development, and tasks have been assigned among them.

At the moment Peter Busser, the founder of the project, is the only one who puts new packages into the distribution, but he is looking to spread the load over several people to up the release frequency of new packages. Behind the scenes, a lot of work is going into generally streamlining the administrative side of the distro, and to introducing additional developer software.

Security by Design

In contrast to Debian, Adamantix contains patches and programs that proactively enhance the distribution's security. Two techniques help to prevent malevolent hackers from exploiting previously undiscovered buffer or heap overflows:

- A Pax kernel patch (see [3]).
- IBM's Stack Smashing Protector [4], a patch for the GNU C compiler. This was used to compile a major part of the distribution.

Also, Adamantix includes the RSBAC package by default. RSBAC defines mandatory access control rules that can tighten up access to the system, if required. This even mitigates the effect of a root compromise. The combination of RSBAC and an antivirus scanner is

interesting. This allows the system to investigate open files for malevolent content in the background.

Manual Labor – RSBAC

RSBAC is (still) optional on Adamantix. Users need to manually install a RSBAC-capable kernel, which provides only reduced functionality at present. If required, RSBAC can even be disabled at runtime. The project members working on RSBAC advise admins with little experience of security to leave this out for the time being. According to the developers, the next generation kernel will have basic RSBAC functionality by default. This will remove the need for SUID privileges, and the root privileges required by certain services.

Adamantix is one of only a few distributions that can provide secure IPsec connections across the Internet out of the box. The distribution comes with ready-to-run FreeS/WAN packages. You only need to modify the configuration files (see Figure 1). Thanks to FreeS/WAN and the integrated WLAN host AP driver, you can easily set up an Adamantix computer as a hardened access point for wireless networks.

Unfortunately, there are one or two issues with the distribution's current kernel (2.4.22). This is due to the fact that the Debian kernel on which the Adamantix kernel is based uses a backport of IPsec from the standard 2.5 kernel, rather than the FreeS/WAN patches. This backport does not cooperate gracefully with userland programs. A solution to this critical issue should be available shortly.

Firewall and IDS

Using Adamantix as a firewall with the Zorp [5] proxy suite is another interesting prospect. Zorp is capable of transparent proxying and can handle complex protocols like SSL. The kernel includes IPTables with the patch for transparent proxies, which is missing from the vanilla kernel. It can set up an application level gateway which is invisible to other machines. Unfortunately, the patch will not run on SMP machines at present.

Besides its firewall capabilities, Adamantix makes a perfect Intrusion Detection System (IDS). It includes the signature based Snort [6] tool in the current version 2. In contrast to Debian, which cannot guarantee the integrity of all packages during package installation, Adamantix provides only GPG signed packages with MD5 checksums (with the exception of the kernel packages).

It will probably take a while to port the whole collection of Debian packages to Adamantix. Until the port has been completed, you may discover that Apt fails to find required packages on the current mirror. In this case, Apt pinning [10] is the answer. This allows you to download a package that is not available from the Adamantix repository easily and automatically from the Debian sources.

To make this work, add the server to the */etc/apt/sources.list* file, as in the following entry:

```
deb http://ftp.szczepanek.de/ stable main contrib
deb http://security.adamantix.org/ stable-security main contrib
deb ftp://ftp.de.debian.org/debian/ stable main contrib
```

To tell the package manager which sources it should prefer, the root user should create a */etc/apt/preferences* file with something like the following content:

```
01 Package: *
02 Pin: origin security.adamantix.org
03 Pin-Priority: 700
04
05 Package: *
06 Pin: origin ftp.szczepanek.de
07 Pin-Priority: 690
08
09 Package: *
10 Pin: origin ftp.debian.org
11 Pin-Priority: 610
```

This tells Apt to prefer Adamantix packages – their version number is more recent anyway. In our example, packages from the *security.adamantix.org* source, are preferred to any others. If Apt does not find the required package there, it searches the next Adamantix mirror server in the list for the package. In our example, this server is *ftp.szczepanek.de*. If all fails, Apt reverts to the original Debian repository at *ftp.debian.org*.

All for Free, Free for All

Adamantix also has the advantage of being free. The project is publicly available, and that means you can easily compile any packages you need, using special options – that is, you can specify Stack Smashing Protector switches. A useful Howto is available from [11]. If a

Installation

When installing Adamantix, the best approach is to start off with a minimal Woody. Leave out the Taskselect and Security updates. To launch the Adamantix part of the install, specify a mirror [7], and then issue a typical Debian *apt-get update*. You need the libncurses5 library to make the Bash installation work, this means that *apt-get install libncurses5* should be one of your first moves. Root can then issue *apt-get dist-upgrade* to install the Adamantix packages.

The same approach can be used to replace an existing Woody system with Adamantix. This may involve some manual steps depending on your original configuration. Note that there will not always be a counterpart for every Debian package. The repository includes 952 packages to date. An overview is available at [8]. The Adamantix repository also provides some software from Debian *testing* or *unstable*, such as the Open Source virus scanner Clam AV [9]. Although original Debian packages can be installed on Adamantix, they will not be protected by the Stack Smashing Protector.

In typical Debian style, you will need to install the kernel manually as the last step. The distribution currently uses a modified kernel 2.4.22 from Debian unstable:

- The normal kernel with Pax patch but without RSBAC functionality.
- The kernel with the *-soft* suffix including a basic RSBAC configuration, which can be disabled at runtime.
- The kernel with the *-sec* suffix, with fixed RSBAC support.

Be careful when using the third kernel, as the root user can easily lock herself out using RSBAC. If you are considering using RSBAC, you should take time to acquaint yourself with RSBAC first. More adventurous types thinking of installing Adamantix on an existing Debian Sarge (*testing*), or even Debian Sid (*unstable*) are in for a disappointment. This is doomed to failure by the version numbers alone, not to mention a whole bunch of other issues.

package refuses to cooperate, you can put on your thinking cap, or turn to the Developers mailing list for help.

Hybrid Systems and Pax Issues

As Adamantix is a stable version (the current version is 1.0.2), it is increasingly found on production machines – typically in areas where security is a major concern. As Adamantix is based on a Debian stable, instability or even crashes are a rare exception. In those cases where problems have occurred, history shows that inappropriate mixtures of Adamantix and Debian packages have been to blame. The user mailing list at [12] provides an extremely useful and quick source of help. Unfortunately, the list archives are only available to registered users, although this is due to change some time in the future.

Additional workarounds are needed for packages and programs that will not work with Pax. The kernel patch immediately dumps any software with this problem that you launch into a black hole. The more notable examples include any Java VM and the Kaspersky AVP virus scanner.

Irritatingly, seemingly sure signs of incompatibility prove not to be generic. The affected programs have a problem with the way Pax separates the code and stack segments in memory. This prompted the developers of the Pax patch to produce a fix. They wrote the *chpax* tool which disables specific Pax functions for individual binaries.

If the AVP daemon refuses to run, you can install the chpax package, and then enter the following

```
chpax -XMRspe `which avpd`
```

to disable the troublesome function. The manpage explains the meanings of the individual options. But to get to grips with the issue, admins have no alternative but to do some serious reading on the subject of Pax.

There are still one or two home-grown problems with specific packages, such as the flawed Free-S/WAN support referred to earlier. Another command that fails to deliver (due to security patches), is the *smbpasswd* command, which normally facilitates creating new Samba users. This said, workarounds are available for most issues. To avoid the IPsec issue, you can use the older kernel 2.4.20, which allows Adamantix to run as a production VPN gateway. If you really need *smbpasswd*, you have no alternative but to use the original Debian Woody binary.

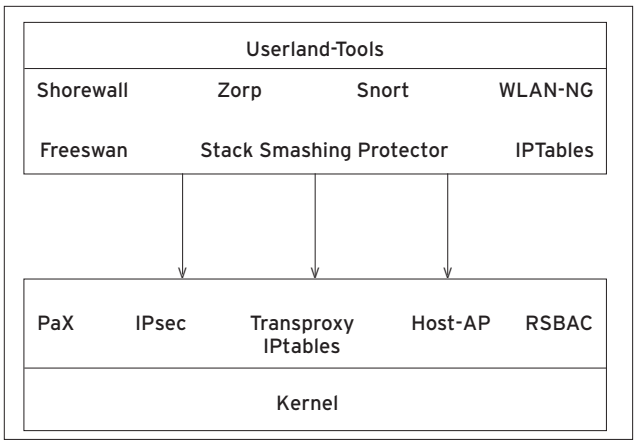

Figure 1: Adamantix, a Debian derivative includes patches and components for a secure Linux

Satisfaction Despite the Deficits

Users can expect problems like the ones just discussed to persist, as long as there are fewer Adamantix developers than issues to fix. Until then, admins of production servers are well advised to check new installs and updates in the lab first. In fact, this is a recommendation that applies universally, no matter which distribution you intend to deploy.

If you keep to this rule, Adamantix should provide you with untroubled, secure computing and a lot of fun reviewing logfiles full of failed attempts to hack your machines. ■

More like OpenBSD than a Linux Distribution?

The Adamantix release announcement gave rise to comparisons with OpenBSD. The response from the OpenBSD camp was almost immediate [13]. An unbiased comparison reveals major differences between the two systems:

- In contrast to Linux (and thus to Adamantix), OpenBSD, or any other BSD for that matter, is an extremely homogenous product. That makes it easy to audit the source code for security issues from top to toe. Linux distributions make a generic check of this kind difficult, due to the disparate nature of the sources.
- Adamantix' biggest advantage is RSBAC, which provides a selection of hardening methods to reflect your security needs. It even takes some of root's privileges away, and thus mitigates the effect of a root compromise.

Having said this, Adamantix and OpenBSD have similar goals, and sometimes use the same means to achieve them:

- Just like "W^X" on OpenBSD, Pax restricts code and stack segment conflicts, and thus avoids stack overflow vulnerabilities.
- OpenBSD also uses the Stack Smashing Protector for the GCC – although it calls the protector "Pro Police".
- OpenBSD was one of the first operating systems to incorporate an IPsec implementation.
- Version 3.0 and higher of OpenBSD can be used as a WLAN access point, again using an IPsec protected variant.

INFO

[1] Trustix: *http://www.trustix.org*
[2] Adamantix: *http://www.adamantix.org*
[3] Pax: *http://pageexec.virtualave.net*
[4] Stack Smashing Protector: *http://www.trl.ibm.com/projects/security/ssp/*
[5] Zorp: *http://www.balabit.com/products/zorp/*
[6] Snort: *http://www.snort.org*
[7] Adamantix, mirrors: *http://www.adamantix.org/mirrors.html*
[8] Adamantix package overview: *http://www.adamantix.org/packages*
[9] Clam AV: *http://clamav.elektrapro.com*
[10] Apt pinning: *http://www.debian.org/doc/manuals/apt-howto/ch-apt-get.en.html#s-pin*
[11] Porting packages: *http://www.adamantix.org/development.html*
[12] Users mailing list: *http://mail.adamantix.org/cgi-bin/mailman/private/users-l/*
[13] OpenBSD reacts: *http://www.deadly.org/article.php3?sid=20030322004413*