

Adamantix – wzmocniona odmiana Debiana

Twardy jak diament

Nazwa projektu Adamantix wywodzi się z czasów średniowiecza od angielskiego przymiotnika *adamant* (niewzruszony). Termin ten określał niezwykle twardość kamieni szlachetnych (takich jak diament). Pomimo swych korzeni etymologicznych, projekt oparty na dystrybucji Debian Woody jest wyjątkowo nowoczesny, mimo że niekiedy wydaje się, iż na tym diamencie pojawiają się skazy.

CHRISTIAN NEY



Wszyscy główni dostawcy oprogramowania starają się jak najszybciej udostępnić poprawki usuwające usterki w swoich systemach. Jest to jednak tylko leczenie objawowe pacjenta. Prawdziwą przyczyną problemów jest przepełnienie stosu lub bufora aplikacji. Co dziwne, większość projektów nie wykazuje aktywnego podejścia do tej sprawy, mimo że odpowiednio przygotowane oprogramowanie może zmniejszyć stopień zagrożenia i podatność oprogramowania na ataki z tej strony. Projekty takie jak OpenBSD wykazują w dziedzinie zabezpieczeń oprogramowania większą odpowiedzialność. Istnieją również specjalizowane dystrybucje Linuksa – godnym uwagi przykładem jest Trustix Secure Linux [1], dystrybucja oparta na Red Hat, znana także pod nazwą Tawie Server Linux.

W niniejszym artykule zajmiemy się dystrybucją Adamantix [2], opartą na Debianie Woody. Prace nad projektem, który otrzymał nazwę Trusted Debiana, rozpoczęto pod koniec 2002 roku. Niedługo potem, lider projektu Debian Martin Michlamayr, skontaktował się z zespołem Trusted Debiana zwracając uwagę na fakt, że nazwa Debian jest zastrzeżonym znakiem towarowym. Także sło-

wo Trusted (ang. zaufany), użyte w nazwie projektu, mogłoby sugerować użytkownikom i potencjalnym klientom, że oryginalna dystrybucja Debian Linux nie jest godna zaufania. To właśnie z tych powodów Martin poprosił o zmianę nazwy.

Aby poradzić sobie z nowym problemem, zespół pracujący nad nową dystrybucją wysłał wiadomość na listę dyskusyjną projektu, prosząc ich członków o sugestie dotyczące nowej nazwy. Ostatecznie wybrano nazwę Adamantix – słowo pochodzące ze średniowiecznej angielszczyzny oznaczające diament. Obecnie nad rozwojem projektu pracuje około dziesięciu osób, każda z nich jest odpowiedzialna za określoną część i pracuje nad powierzonymi zadaniami.

Tworzeniem pakietów zajmuje się tylko jeden człowiek – Peter Busser – twórca projektu. Jest to jego ulubione zadanie, które wykonuje z pełnym profesjonalizmem. Peter zamierza rozszerzyć zakres prac na kilka osób, aby zwiększyć częstotliwość wprowadzania na rynek nowych pakietów. Oczywiście najbardziej pracochłonne jest ulepszanie dystrybucji od strony administracyjnej oraz wprowadzanie dodatkowego oprogramowania innych programistów.

Bezpieczny projekt

Adamantix, w odróżnieniu od Debiana, zawiera poprawki i programy aktywnie rozwijające bezpieczeństwo i ochronę dystrybucji. Aby zabezpieczyć produkt przed wykorzystaniem przez hackerów nie wykrytych wcześniej przepełnień stosu lub bufora, użyto dwóch metod:

- poprawka jądra Pax [3].
- Stack Smashing Protector [4] firmy IBM, poprawka dla standardowego kompilatora GNU C, używanego w Linuksie.

Ponadto, Adamantix zawiera standardowo pakiet RSBAC. Określa on zasady kontroli dostępu do zasobów systemowych, które uszczelniają dostęp. Pakiet ten łagodzi nawet skutki tzw. *root compromise* (czyli atak umożliwiający użytkownikowi uzyskanie praw roota). Najbardziej interesująca jest kombinacja pakietu RSBAC ze skanerem antywirusowym. Umożliwia to kontrolowanie w tle otwartych plików pod kątem ich niewłaściwej zawartości.

Prace ręczne RSBAC

System RSBAC jest nadal jedynie opcją w dystrybucji Adamantix. Użytkownicy są zmuszeni do ręcznego instalowania jądra

obsługującego RSBAC, które i tak zapewnia obecnie tylko ograniczoną funkcjonalność. RSBAC można wyłączyć nawet w czasie pracy systemu. Członkowie projektu pracujący nad RSBAC chwilowo nie zalecają stosowania tego pakietu administratorom o niewielkim doświadczeniu w zakresie bezpieczeństwa. Jak twierdzą autorzy oprogramowania, kolejna wersja jądra będzie domyślnie posiadała podstawową funkcjonalność RSBAC. Niektóre usługi nie będą zatem już wymagały uprawnień SUID użytkownika głównego (roota).

Adamantix jest jedną z niewielu dystrybucji, która zapewnia bezpieczne połączenia IP-Sec w sieci Internet. Dystrybucja zawiera gotowe do użycia pakiety FreeS/WAN. Musisz tylko dostosować do własnych potrzeb pliki konfiguracyjne (patrz Rysunek 1). Dzięki FreeS/WAN i zintegrowanemu sterownikowi AP hosta WLAN, możemy w prosty sposób przygotować komputer z dystrybucją Adamantix do pracy, jako bezpieczny punkt dostępu dla sieci przewodowych.

Niestety, z jądrem w obecnej dystrybucji (2.4.21) są pewne kłopoty. Wynika to z faktu, że jądro Debiana (na którym oparto jądro dystrybucji Adamantix), wykorzystuje łańki IPsec przeniesione (backport) ze standardowego jądra 2.5 zamiast poprawek wprowadzonych przez pakiet FreeS/WAN. Łańki te

nie współpracują do końca poprawnie z programami użytkowymi FreeS/WAN. Wkrótce powinno pojawić się rozwiązanie tego uciążliwego problemu.

Zapora i IDS

Ciekawym pomysłem jest wykorzystanie dystrybucji Adamantix jako zapory sieciowej (firewall-a) współpracującej z pakietem proxy Zorp [5]. Zorp umożliwia użycie niewidocznych proxy i radzi sobie z obsługą skomplikowanych protokołów, takich jak SSL. Jądro Adamantix-a zawiera IPTables z poprawką dla niewidocznych proxy, której brakowało w jądrze standardowym. Dzięki temu można skonfigurować firewall-e typu *application level gateway*, które nie będą wykrywane przez inne komputery. Niestety, poprawka nie współpracuje z komputerami działającymi w trybie SMP (maszyny wieloprocessorowe).

Poza możliwością pracy w trybie firewall, Adamantix nadaje się doskonale na system wykrywania intruzów (tzw. IDS – Intrusion Detection System), ponieważ zawiera on program Snort [6] w wersji 2. W przeciwieństwie do Debiana, gdzie nie ma gwarancji integralności wszystkich pakietów podczas ich instalacji, Adamantix umożliwia instalację wyłącznie pakietów podpisanych kluczem GPG z sumą kontrolną MD5 (wyjątkiem są pakiety jądra).

Prawdopodobnie upłyne jeszcze trochę czasu, zanim wszystkie zestawy pakietów Debiana zostaną przeniesione do Adamantix. Do momentu zakończenia przenoszenia okaże się, że system APT nie odnajduje wymaganych pakietów na bieżącym mirrorze. Rozwiązaniem jest tzw. *pinning* APT [10] – oznaczanie APT, które umożliwi łatwe i automatyczne pobranie pakietu niedostępnego w repozytorium Adamantixa ze źródeł Debiana. Musisz tylko dodać nazwę serwera do pliku */etc/apt/sources.list*, jak w przykładzie przedstawionym poniżej:

```
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
```

Aby wskazać menedżerowi pakietów, z których źródeł powinien korzystać w pierwszej kolejności, użytkownik root powinien utworzyć plik */etc/apt/preferences* o podobnej wartości jak pokazano poniżej:

```
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
```

Dzięki temu program APT będzie preferował pakiety Adamantixa – ich numer wersji jest po prostu bardziej aktualny. W naszym przykładzie pakiety ze źródła *security.adamantix.org* będą miały wyższy priorytet nad innymi pakietami. Jeżeli APT nie odnajdzie tamżądanego pakietu, rozpocznie przeszukiwanie kolejnego z listy pakietów serwera lustrzanego Adamantixa. W naszym przykładzie serwerem tym jest *ftp.szczepanek.de*. Jeżeli i ta próba będzie nieudana, APT wraca do repozytorium Debiana znajdującego się pod adresem *ftp.debian.org*.

Wszystko za darmo i dla wszystkich

Kolejną zaletą Adamantixa jest to, że jest dystrybucją darmową. Projekt jest ogólnodostępny, co oznacza, że możemy skompilować

Instalacja

Instalację Adamantixa najlepiej rozpocząć od minimalnej wersji dystrybucji Debian Woody, bez instalowania aktualizacji Taskselect i Security. Aby uruchomić instalację Adamantixa, wybierz serwer [7] i pobierz aktualizację Debiana poleceniem *apt-get update*. Uwaga! Do poprawnego działania powłoki Bash, niezbędna jest biblioteka *libncurses5*. Zatem w pierwszej kolejności powinniśmy zainstalować bibliotekę *libncurses5* poleceniem *apt-get install libncurses5*. Następnie, w celu instalacji pakietów Adamantixa, należy wykonać *apt-get dist-upgrade*.

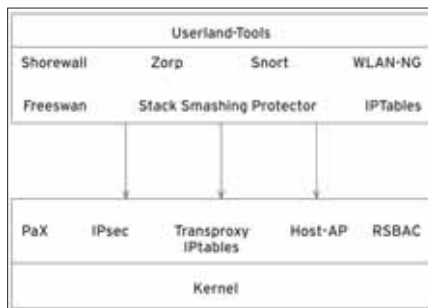
W podobny sposób możesz wykonać zamiast istniejącego już systemu opartego na Debiana Woody na system Adamantix. W zależności od konfiguracji, niezbędne mogą okazać się pewne czynności, które trzeba wykonać ręcznie. Pamiętaj, że nie zawsze znajdziesz odpowiednik każdego z pakietów Debiana w wersji dla Adamantix-a. Repozytorium zawiera do chwili obecnej 952 pakiety. Przegląd pakietów znajdziesz pod adresem [8]. Repozytorium Adamantix-a dostarcza także pewne programy z gałęzi *testing* i *unstable* Debiana, takie jak skaner antywi-

rusowy Clam AV (oprogramowanie Open Source). W Adamantix możemy także instalować pakiety Debiana, ale nie będą one chronione przez Stack Smashing Protector.

Ostatnim krokiem, jak na Debiana przystało, jest ręczna instalacja jądra. Dystrybucja obecnie korzysta ze zmodyfikowanej wersji rozwojowej jądra 2.4.21 Debiana. Do wyboru są trzy jądra:

- Jądro standardowe z poprawką Pax, lecz bez funkcjonalności RSBAC.
- Jądro z przyrostkiem *-soft*, zawierające podstawową konfigurację RSBAC, którą można wyłączyć podczas pracy.
- Jądro z przyrostkiem *-sec*, z poprawioną obsługą RSBAC.

Należy szczególnie uważać przy instalacji trzeciego jądra, gdyż użytkownik root może w prosty sposób zablokować dostęp dla samego siebie. Jeżeli chcesz korzystać z RSBAC, powinieneś w pierwszej kolejności dobrze zapoznać się z nim. Niektórzy próbują nawet instalacji Adamantixa na istniejącym Debianie Sarge (status *testing*) czy Debianie Sid (status *unstable*), ale to się raczej nie uda...



Rysunek 1. Adamantix, pochodna Debiana zawiera poprawki i składniki bezpiecznego Linuksa

sobie potrzebne pakiety stosując specjalne opcje (stosując przełącznik ochrony stosu – *Stack Smashing Protector*). Cenne wskazówki w tym zakresie znajdziesz na stronie [11]. Jeżeli jakiś pakiet nie będzie działał prawidłowo, zawsze można poddać problem do dyskusji lub zwrócić się o pomoc na liście dyskusyjnej projektu.

Systemy hybrydowe i problemy z PAX

Obecnie coraz częściej wykorzystuje się stabilną wersję dystrybucji Adamantix (obecna wersja 1.0.2) na serwerach produkcyjnych, szczególnie tam, gdzie konieczne jest zapewnienie wysokiego poziomu bezpieczeństwa. Jako że Adamantix jest oparty na Debianie, niestabilność czy zawieszanie się systemu jest rzadkim zjawiskiem. Jak pokazuje doświadczenie, problemy powstają, gdy dochodzi do pomieszania pakietów Adamantixa i Debiana. Lista dyskusyjna znajdująca się pod adresem [12], jest w tym względzie wy-

jątkowo pomocnym i szybkim źródłem informacji. Niestety, archiwum jest dostępne tylko dla zarejestrowanych użytkowników, chociaż sytuacja ta ma się niedługo zmienić.

Obecnie niezbędne są dodatkowe prace nad pakietami i programami nie współpracującymi z Pax. Pax wykonuje natychmiast zrzut pamięci przy próbie uruchomienia jakiegokolwiek oprogramowania nie obsługującego Pax. Najbardziej znanymi przykładami jest tutaj wirtualna maszyna Java i skaner antywirusowy Kaspersky AVP.

Ponadto niektóre oznaki niestabilności aplikacji mają wyjątkowo subtelne i trudne do wychwycenia przyczyny. Wynika to stąd, że niektóre programy nie radzą sobie z separacją kodu i segmentów stosu w pamięci narzucaną przez Pax. Popchnęło to twórców oprogramowania Pax do stworzenia poprawki usuwającej tę usterkę. Stworzyli oni program *chpax*, umożliwiający wyłączenie pewnych funkcji Pax dla określonych plików binarnych.

Jeżeli na przykład demon Kasperky AVP (który ma charakter stale aktywnego procesu sięgającego do funkcji systemowych) odmawia uruchomienia, musisz zainstalować pakiet *chpax*, a następnie wykonać następujące polecenie:

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

Umożliwi to wyłączenie funkcji Pax dla demona programu Kaspersky AVP. Strona podręcznika *man* wyjaśnia znaczenia poszczególnych opcji. Aby jednak administratorzy systemów poradzili sobie z tym problemem, muszą koniecznie zagłębić się w lite-

raturę dotyczącą Pax.

Nadal do rozwiązania pozostają jeden czy dwa problemy związane z określonymi pakietami, np. z FreeS/WAN, o którym mówiliśmy już wcześniej. Kolejnym poleceniem, które nie działa poprawnie (z powodu poprawek bezpieczeństwa), jest *smbpasswd* – zwykle wykorzystywane podczas dodawania nowych użytkowników do bazy serwera Samba. Poza tymi dwoma wyjątkami, reszta problemów została zażegnana. Aby uniknąć problemów z IPsec, możesz użyć starszej wersji jądra 2.4.20, która umożliwia Adamantix pracę jako brama VPN (wirtualnej sieci prywatnej). Jeżeli koniecznie potrzebujesz polecenia *smbpasswd*, nie ma innego wyjścia jak wrócić do oryginalnej wersji Debiana – Woody.

Satysfakcja gwarantowana, mimo braków

Do czasu, gdy twórców Adamantixa będzie mniej niż błędów do poprawienia, użytkownicy mogą spodziewać się problemów podobnych do opisanych powyżej. Tak czy inaczej administratorzy serwerów produkcyjnych muszą kontrolować rozwój Adamantix-a i sprawdzać wszelkie aktualizacje systemu na systemach testowych. Tak naprawdę, zasadę tę powinno się stosować do każdej dystrybucji, z którą mamy zamiar pracować. ■

Bardziej podobny do OpenBSD niż do Linuksa?

Ogłoszenie o wydaniu Adamantixa wywołało porównania z projektem OpenBSD. Odpowiedź z obozu OpenBSD była prawie natychmiastowa [13]. Obiektywne porównanie tych dwóch systemów ujawnia główne różnice:

- W przeciwieństwie do Linuksa (a więc także do Adamantixa), OpenBSD i każdy inny BSD w tym względzie, jest produktem typowo homogenicznym. Możemy w łatwy sposób sprawdzić kod źródłowy pod kątem zabezpieczeń. W dystrybucjach Linuksa taka kompleksowa kontrola jest bardzo utrudniona z powodu odmiennej natury źródeł.
- Największą zaletą dystrybucji Adamantix jest RSBAC, który zapewnia wiele odpowiadających różnym potrzebom zabezpieczeń. Ponadto RSBAC usuwa niektóre z przywilejów użytkownika root, dzięki cze-

mu łagodzi wpływ tzw. *root compromise*.

Adamantix i OpenBSD mają również podobne cele i czasem korzystają z tych samych środków do ich osiągnięcia:

- Podobnie jak W^X w systemie OpenBSD, tak samo Pax ogranicza konflikty kodu i stosu, zmniejszając w ten sposób podatność na przepełnienie stosu.
- OpenBSD także korzysta ze Stack Smashing Protector dla GCC, określanego jednak tutaj nazwą Pro Police.
- OpenBSD był jednym z pierwszych systemów operacyjnych zawierających obsługę IPsec.
- OpenBSD w wersjach 3.0 i wyższych można wykorzystać jako bezpieczny punkt dostępu WLAN (dzięki zabezpieczonej wersji IPsec).

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.tri.ibm.com/projects/security/ssp/>
- [5] Zorp: <http://www.balabit.com/products/zorp/>
- [6] Snort: <http://www.snort.org>
- [7] Adamantix, mirrory: <http://www.adamantix.org/mirrors.html>
- [8] Adamantix, przegląd pakietów: <http://www.adamantix.org/packages>
- [9] Clam AV: <http://clamav.elektropro.com>
- [10] Opcja oznaczania pakietów w Apt: <http://www.debian.org/doc/manuals/apt-howto/ch-apt-get.en.html#s-pin>
- [11] Przenoszenie pakietów: <http://www.adamantix.org/development.html>
- [12] Listy mailingowe: <http://mail.adamantix.org/cgi-bin/mailman/private/users-1/>
- [13] Reakcje OpenBSD: <http://www.deadly.org/article.php3?sid=20030322004413>



Linux Magazine w Internecie:

WIADOMOŚCI

Na stronach WWW Linux Magazine znajdziesz najnowsze wiadomości ze świata Linuksa.

OBSŁUGA PRENUMERATY

Wszystkie sprawy związane z prenumeratą możesz załatwić sam na naszych stronach WWW. Można tutaj uaktualnić dane adresowe, przedłużyć prenumeratę lub zmienić jej parametry.

POMOC DLA CZYTELNIKÓW

Chcemy pomagać naszym Czytelnikom w poznawaniu Linuksa. Na naszych stronach WWW znajdziesz kompetentne informacje. Zaprawszamy również do korzystania z naszej listy mailingowej.

CO W NASTĘPNYM NUMERZE?

Dowiedz się pierwszy, co będzie w następnym numerze Linux Magazine. Każdego miesiąca publikujemy pełny spis treści oraz kilka wybranych artykułów z numeru Linux Magazine wchodzącego właśnie do sprzedaży.

ARCHIWUM ONLINE

Pełna zawartość numerów archiwalnych dostępna bezpłatnie (dla osób prywatnych) w postaci plików PDF. Funkcja pełnotekstowego wyszukiwania pozwoli łatwo znaleźć potrzebne informacje.