Şifreli Geridönüş Aygıtı NASIL

Cryptoloop NASIL

Yazan:
Ralf Hölzer
<cryptoloop (at) ralfhoelzer.com>

Çeviren:
İşbaran Akçayır
<isbaran (at) gmail.com>

Ekim 2005

Özet

Bu belge Cryptoloop işlevi kullanılarak nasıl şifrelenmiş dosya sistemleri oluşturulabileceğini açıklar. Cryptoloop 2.6 çekirdek serisindeki CryptoAPI'nin bir parçasıdır. Bu belge sayesinde çabucak şifreli bir disk bölümüne veya şifrelenmiş dosya sistemi içeren bir dosyaya sahip olabilirsiniz.

Ayrıca şifreleme hakkında ayrıntılı bilgi bulabileceğiniz Şifrelenmiş Kök Dosya Sistemi NASIL[B1] ve Disk Şifreleme NASIL[B2] belgelerine göz atmanızı tavsiye ederim.

Konu Başlıkları

Bu çevirinin sürüm bilgileri:

1.0	Ekim 2005	İA
İlk çeviri		

Özgün belgenin sürüm bilgileri:

1.2	2004-03-12	rh
Dm–crypt hakkında bilgi eklendi, loop–AES bilgisi güncellendi, güvenlik hakkında daha fazla bilgi eklendi.		
1.1	2004-01-24	rh
Util–linux, Loop–AES, Best Crypt yamama bilgileri güncellendi.		
1.0	2004-01-17	rh
İlk sürüm, LDP'deki TM tarafından incelendi.		
v0.9	2004-01-15	rh
Güncellendi ve DocBook XML'e çevrildi.		

Yasal Açıklamalar

1. Bu belge hakkında

Bu NASIL belgesi 2.6 çekirdek serisinde Cryptoloop döngü aygıtları şifrelemesinin nasıl yapılacağını açıklar. Cryptoloop, bir disk bölümü veya dosya sistemindeki başka bir dosya üzerinde şifrelenmiş dosya sistemi oluşturmanıza olanak sağlar. Bu şifrelenmiş dosyalar CD, DVD, USB gibi aygıtlara taşınabilirler. Cryptoloop 'loop device' (geridönüş aygıtı) kullanarak çalışır. Bu aygıt, bir dosya sistemine yapılan bütün çağrıların geçmesi gereken bir "geridönüş" sağlayan sanal–aygıttır. Bu yolla, veri şifrelenmek ve deşifre edilmek için işlenebilir. 2.6 çekirdek sürümlerinden bu yana CryptoAPI ana çekirdeğe katılmıştır ve şifrelenmiş dosya sistemi hazırlamak çok daha kolay bir hale gelmiştir. Çekirdek yamalarına gerek yoktur. Bazı kullanıcı taraflı (çekirdek/kullanıcı ilişkisindeki kullanıcı) özelliklerin güncellenmesi yeterlidir. Fakat Cryptoloop kullanımı şimdiye kadar pek iyi belgelenmemiştir. Bu NASIL belgesi herkesin standart Cryptoloop işlevi sayesinde, kolayca şifrelenmiş dosya sistemi oluşturabilmesini sağlamaya yöneliktir. Cryptoloop 2.6 Linux çekirdeğindeki CryptoAPI üzerinedir. Tamamen ayrı bir proje olan Loop–AES ile karıştırılmamalıdır. Cryptoloop, 2.4 çekirdek serisinde ayrı bir yama olan CryptoAPI ile bağdaşır. Yeni sürümüeskisiyle uyumlu değildir.

1.1. Teşekkürler / Katkıda bulunanlar

Bu NASIL belgesinin hazırlanmasında katkıları olanlara teşekkürler:

- Dennis Kaledin
- Binh Nguyen
- David Lawyer
- Tabatha Marshall
- Kian Spongsveen

1.2. Geri bildirim

Bu belge için geri bildirimlerinizi her zaman beklerim. Eklemek istediklerinizi, yorumlarınızı ve eleştirilerinizi eposta adresime gönderebilirsiniz: <cryptoloop (at) ralfhoelzer.com>.

2. Giriş

Şu an Cryptoloop yerine kullanılabilecek az sayıda alternatif mevcuttur. Loop–AES (http://loop-«aes.sourceforge.net) muhtemelen en çok tanınanıdır. Cryptoloop'a göre çok benzer işlevselliğe sahiptir. Aes–loop Cryptoloop'a göre daha oturaklıdır ve aynı zamanda daha hızlıdır (loop–AES in yazarına göre neredeyse iki kat daha hızlı), çünkü AES için özelleştirilmiş bir çevirici (assembler) kullanır. Bu, Cryptoloop yavaştır anlamına gelmez. Gündelik işlerde ve normal miktarlarda G/Ç olan, Cryptoloop ile şifrelenmiş bir dosya sistemi ile şifrelenmemiş bir dosya sistemi arasında kaydadeğer bir hız farkı gözlemlemedim. G/Ç performansı sizin için aşırı önemli değilse Cryptoloop işinizi görecektir diyebiliriz. Loop–AES, Cryptoloop'un çekirdekle birleşik sürümüne henüz eklenmemiş bazı ilave özelliklere sahiptir. Loop–Aes kullanıcı araçlarının değiştirilmiş hallerine ihtiyaç duyar (mount, losetup gibi) ve bu değişimler Cryptoloop ile uyumlu değildir. Yani Cryptoloop ve Loop–AES'i aynı anda kullanamayacaksınız.

Güvenlik konusunda Cryptoloop işini iyi yapıyor diyebiliriz. 'Anahtar' genellikle bir paroladan oluşturulur ve anahtarin hash' işlevinden çıkan hali AES için anahtar olarak kullanılır. Bu, salt metin saldırısı[B6] ihtimaline sebep verir. Loop–AES bu konuda çok iyidir, çünkü önce rastgele bir anahtar oluşturur ve bu anahtarı ayrı ayrı şifreler, böylece bilindik salt metin saldırısını çok daha zor bir hale getirir. Loop–AES ayrıca sektörlerin 64 ayrı AES anahtarıyla şifrelendiği çoklu–anahtar kipin destekler. Genelde eğer zayıf bir parola seçerseniz parolanıza yapılacak çok güçlü bir saldırı başarılı olacaktır. Güvenli tarafta olmak istiyorsanız parolanızı en az 20 karakter

uzunlukta seçmelisiniz. Diğer türlü, bir parola üzerine güçlü saldırı uygulamak doğrudan AES şifrelemesine saldiri uygulamaktan çok daha iyi sonuç verecektir.

Standart çekirdekteki Cryptoloop işlevi ek yamalara ihtiyaç duymadan kararlı ve temiz bir yol sunar. Henüz yeni bir uygulama olduğundan güvenlik açısından yeterince incelemeden geçmemiş olabilir. Kendiniz için uygun olanı siz seçmelisiniz.

Önemli

Cryptoloop en son 2.6 çekirdekte –tavsiye edilmez– olarak işaretlenmiştir. Bunun anlamı Cryptoloop'un çekirdekte daha fazla desteklenmeyeceğidir. Cryptoloop'un halefi olarak dm–crypt[B7] tavsiye edilmektedir. dm–crypt ana çekirdekte 2.6.4 ten beri bulunmaktadır. Cryptoloop uzunca bir süre daha çekirdekte bulunacaktır, ama ilerde disk şifrelemede seçim dm–crypt doğrultusundadır. Dm–crypt aygıt eşlemleme üzerine çalışır ve Cryptoloop ile hemen hemen aynı işlevleri gösterir. Hala çok yenidir ve kullanıcının kolayca kullanabilmesi için araçlar bulunmamaktadır. Dm–crypt'in Cryptoloop'a göre daha temiz kod içerdiği farzedilebilir, ama bazı önemli farklar bulunmaktadır. Mesela, bir dosya içinde şifrelenmiş bir dosya sistemi oluşturmak için hala bir geridönüş cihazına gidilmesi gerekir, ama bu destek hala geliştirme aşamasındadır.

Şifrelenmiş bir dosya sistemi yapmanızı sağlayacak başka araçlar vardır. BestCrypt Jetico firmasından çıkan ticari bir üründür. Şifrelenmiş taşıyıcılar oluşturmanızı sağlar ve geniş bir şifreleyici seçimi sunar. Ayrıca 'gizli taşıyıcılar' gibi bazı çekici özellikler de sunar. Hem windows hem Linux altında çalışır, böylece şifrelenmiş taşıyıcıları windows ve Linux arasında kolayca değiştirebilmenizi sağlar. BestCrypt şu an 2.6 çekirdeklerle de derlenebilir. Cryptoloop da aşağıda bahsedeceğimiz gibi bir dosya içerisinde şifreli dosya sistemi oluşturarak taşınabilir şifrelenmiş taşıyıcılar yapabilir. Ama Cryptoloop ile şifrelenmiş bir dosyaya diğer işletim sistemlerinden nasıl erişileceğini bilmiyorum. Böyle bir durumda BestCrypt tek seçeneğiniz olabilir.

PGP disk gibi başka ticari disk şifreleme araçları da bulunmaktadır, ama bildiğim kadarıyla Linux destekleri bulunmuyor.

3. Çekirdeğin Yapılandırılması

Cryptoloop'u kullanmak için bazı çekirdek seçeneklerini etkin hale getirmelisiniz. Bu seçenekleri doğrudan çekirdek içine derleyebilir veya ayrıca modül olarak da derleyebilirsiniz. Aşağıda bu seçenekleri modül olarak derledik. Eğer bir 2.6 çekirdeği nasıl derleyeceğiniz hakkında pek bilginiz yoksa Linux Kernel HOWTO[B8] belgesine bakmalısınız. Bahsedeceğimiz komutlar sadece en kısa adımları içeriyor.

1. Çekirdek kaynak kodunu barındıran dizine gidin (genellikle `/usr/src/linux/`) ve yapılandırmayı başlatın:

   ```
   make menuconfig
   ```

2. Genel geridönüş aygıtı desteğini etkinleştirin.

   ```
   Device Drivers -> Block Devices -> Loopback device support
   ```

   seçimleriyle "Loopback device support" bölümüne girin.

3. Bu bölümdeki "Cryptoloop support" seçeneğini etkinleştirin. Seçenek "general loopback support" kısmını işaretlediğinizde otomatik olarak açılacaktır.

4. Ana menüden "Cryptographic options" kısmına giderek cryptographic API'yi etkin hale getirin. Burada bulunan çoğu algoritmayı güvenle seçebilirsiniz. Ben aşağıdakileri seçmenizi öneririm:

```
-- Cryptographic API
  <*>   HMAC support
  < >   Null algorithms
  <*>   MD4 digest algorithm
  <*>   MD5 digest algorithm
  <*>   SHA1 digest algorithm
  <*>   SHA256 digest algorithm
  <*>   SHA384 and SHA512 digest algorithms
  <*>   DES and Triple DES EDE cipher algorithms
  <*>   Blowfish cipher algorithm
  <*>   Twofish cipher algorithm
  <*>   Serpent cipher algorithm
  <*>   AES cipher algorithms
  <*>   CAST5 (CAST-128) cipher algorithm
  <*>   CAST6 (CAST-256) cipher algorithm
  <*>   Deflate compression algorithm
  < >   Testing module
```

Eğer bunları modül olarak derlemeye karar verirseniz gerekli modülleri (cryptoloop, aes, vs.) sistem açılışında yüklemeyi unutmayın.

5. Çekirdek ve modüllerinizi derleyin ve gerekli modülleri yükleyin. Mesela x86 makinede önyükleyici olarak lilo kullanıyorsanız, şöyle yapabilirsiniz:

```
make
make modules_install
make install
```

6. Gereken modülleri sistem açılışında yükleyin. Bu değişik dağıtımlarda değişik yollarla ele alınır. Mesela, Gentoo'da bu dosyalar `/etc/modules.autoload/kernel-2.6` dosyasına eklenebilirler. Eğer Cryptoloop'u modül olarak derlediyseniz ilk olarak onun yüklenmesi gerekir. Otomatik olarak temel geridönüş aygıtı modülünü de yükleyecektir. Modülü elle şu şekilde yükleyebilirsiniz:

```
modprobe cryptoloop
```

4. Kullanıcı araçları

Cryptoloop sürücüsü şifrelenmiş dosya sistemini oluşturmak ve bağlamak için güncellenmiş kullanıcı araçlarına ihtiyaç duyar. Güncellenmiş bir util–linux paketi gereklidir ve http://ftp.cwi.nl/aeb/util-«linux/util-«linux-«2.12.tar.gz adresinden bu paket edinilebilir. Yeni bir sürüm her an çıkabilir ve önemli değişiklikler içerebilir, bu yüzden bu NASIL belgesine devam etmeden önce yeni sürümleri ve bu belgenin yeni sürümlerini kontrol etmelisiniz. Şanssızlık eseri util–linux için çok sayıda yama bulunmaktadır. Şifrelenmiş bölümlerin oluşturulma şeklinde ve bunların bağlanmasında değişiklikler söz konusudur. Bir 2.6 çekirdek ile util–linux 2.12 kullanacaksanız en azından şu iki yamayı uygulamalısınız:

1. Birleşik losetup yaması[B10]
2. Util–linux 2.6 yaması[B11]

util–linux paketini ve yukarıdaki iki yamayı bilgisayarınıza indirin. Önce util–linux paketini aç ın ve iki yamayı uygulayın:

```
tar xvfz util-linux-2.12.tar.gz

cd util-linux-2.12

patch -p1 </path_to_patchfile/losetup-combined.patch
```

```
patch -p1 < /path_to_patchfile/util-linux-2.12-kernel-2.6.patch
```

Yamaları uyguladıktan sonra util–linux paketini INSTALL dosyasındaki yönergeleri izleyerek derleyin ve kurun.

Ben Gentoo Linux[B12]'u tercih ediyorum, gentoo linux util–linux paketini kurarken bu yamaları da otomatik olarak uyguluyor. Diğer dağıtımların da bu yamaların uygulanmış olduğu util–linux'un başka sürümleri olabilir.

5. Geridönüş aygıtının (loop device) ayarlanması

Cryptoloop bir dosya üzerine veya bütün bir dosya sistemi üzerine uygulanabilir. Aşağıda belirli bir bölüme nasıl uygulanabileceğini görebilirsiniz. Bu bölüm istediğiniz herhangibir bölüm olabilir; örnekte `/dev/sda1` kullanılıyor. Şifreleyici olarak AES'i seçtim, ama siz çekirdekte seçtiğiniz diğer şifreleyicileri de seçebilirsiniz. Şu an çalıştığınız çekirdeğinizin desteklediği algoritmaları `/proc/crypto` altına bakarak görebilirsiniz. Bruce Schneier'in 'Applied Cryptography' ve 'Practical Cryptography' isimli kitapları değişik kriptografik algoritmaları tartışan mükemmel kaynaklardır. AES ve Serpent mantıklı birer seçimdir. AES uzun süredir analiz edilmiştir ve şimdiye dek ciddi zayıflıkları bulunmamıştır. Serpent fazla test edilmemesine rağmen AES ten biraz daha güçlü olduğu düşünülür. Fakat Serpent aynı zamanda AES'ten biraz daha yavaştır. DES'ten uzak durun, hem yavaş hem de zayıftır. Üçlü–DES (triple–des) bir çözüm olabilir, ama AES büyük ihtimalle hem daha güvenli hem daha hızlıdır, yani aslında Üçlü–DES'i kullanmanın artık pek mantığı yok.

1. Bir bölümde şifreli dosya sistemi kurmadan önce o bölümü biçimlemeniz ve rastgele veriyle doldurmanız tavsiye edilir. Bu, bir saldırganın şifrelenmiş diskiniz üzerinde anlamlı dizgelere/kalıplara rastlamasını zorlaştıracaktır.

   

   Uyarı

   Bölümünüz için burada ne yazdığınıza dikkat edin. Bir hata yaparsanız, yanlış bölümü rasgele veriyle doldurabilirsiniz!

   Bir disk bölümünü şu şekilde rasgele veriyle doldurabilirsiniz:

   ```
   dd if=/dev/urandom of=/dev/sda1 bs=1M
   ```

   Aygıtın dolduğunu bildiren bir hata iletisi alabilirsiniz. Bunu önemsemeyin.

2. Bir şifreleyici ve anahtar boyu seçin. çekirdeğiniz tarafından desteklenen şifreleyicileri `/proc/crypto` dosyasından öğrenebilirsiniz. Ben 256 bitlik anahtar ile AES kullanmanızı tavsiye ediyorum.

3. Geridönüş aygıtını ayarlayın. Bu, util–linux paketi ile gelen **`losetup`** komutu kullanılarak yapılır. Aşağıdaki komut `/dev/sda1` üzerinde `loop device 0` kullanarak 256 bitlik anahtar ve AES ile şifrelenmiş bir dosya sistemi oluşturur:

   ```
   losetup -e aes-256 /dev/loop0 /dev/sda1
   ```

   Komut bir parola sorar. Güçlü bir parola seçin ve parolayı bir yere yazmadan aklınızda tutmaya çalışın. Cryptoloop ile ilgili büyük bir soruna geldik. Şifreleme anahtarı oluşturulurken parola hash' landığından parolayı ileride değiştirmek pek kolay değildir. Bunun en kolay yolu şifrelenmiş yeni bir bölüm oluşturup bütün veriyi oraya taşımaktır. Bu yüzden başlangıçta güçlü bir parola seçtiğinizden emin olun. AES güçlü bir algoritmadır, ama siz kötü bir parola seçerseniz güvenliği çöpe atmış olursunuz.

   Eğer **`losetup`** bir yanlış argüman (INVALID ARGUMENT) şeklinde hata iletisi verirse util–linux paketinizde bir sorun var demektir. Yukarıda bahsettiğimiz yamalı sürümü yüklemede bir hata yapıp yapmadığınızı kontrol edin. Eski veya yamasız sürümler bu hataya sebep olabilir.

4. Bir dosya sistemi oluşturun. İstediğiniz türden dosya sistemi oluşturabilirsiniz. Aşağıda geridönüş aygıtı kullanılarak ext3 dosya sistemi oluşturulmuştur:

```
mkfs.ext3 /dev/loop0
```

5. Şifrelenmiş dosya sistemini bağlayın. Önce bir bağlama noktası oluşturmalısınız, mesela `/mnt/crypto`:

```
mkdir /mnt/crypto
```

Sonra dosya sistemini bağlamalısınız. Bu aşamada bağlayıcıya tam olarak hangi geridönüş aygıtını kullanacağını söylemelisiniz:

```
mount -t ext3 /dev/loop0 /mnt/crypto
```

6. Şimdi sıkılana kadar şifrelenmiş dosya sisteminizle oynayabilirsiniz. :)

7. İşiniz bittiğinde dosya sistemini ayırın:

```
umount /mnt/crypto
```

8. Geridönüş aygıtını çıkarın. Geridönüş aygıtı hala sizin bölümünüze bağlanmış durumdadır. Şu şekilde çıkarın:

```
losetup -d /dev/loop0
```

6. Şifrelenmiş dosya sisteminin bağlanması

Cryptoloop aygıtı üzerindeki tüm işlemler için gerekli modüllerin yüklü olması önemlidir. En azından Cryptoloop modülü ve her şifreleyici için gereken modülü **modprobe** ile yüklemelisiniz. Eğer bu özellikleri doğrudan çekirdekle derlediyseniz bu işleme gerek yoktur.

Yukarıda bahsettiğimiz şifrelenmiş dosya sistemini bağlamak için util–linux paketindeki standart **mount** komutunu kullanabilirsiniz:

```
mount -t ext3 /dev/sda1 /mnt/crypto/ -oencryption=aes-256
```

Bu aşamada size parola sorulacak ve sonrasında herhangibir dosya sistemi gibi örneğimizde `/mnt/crypto` altına bağlanacaktır. Komutta `encryption` seçeneği bulunduğundan bunun bir Cryptoloop dosya sistemi olduğu anlaşılıp uygun bir geridönüş aygıtına bağlanacaktır.

İşiniz bittiğinde dosya sistemini ayırmayı unutmayın:

```
umount /mnt/crypto
```

Aşağıdaki satırı `/etc/fstab` içine ekleyebilirsiniz:

```
/dev/sda1               /mnt/crypto     ext3            noauto,encryption=aes-256
```

Şimdi aygıtı basitçe aşağıdaki gibi bağlayabilirsiniz:

```
mount /mnt/crypto
```

Hepsi bu kadar. İyi eğlenceler :)

7. Bir bölüm yerine bir dosyanın kullanılması

Başka bir dosya sistemindeki bir dosyada şifrelenmiş dosya sistemi kurmak da bu kadar kolay. Bu durum eğer dosyayı DVD vs. gibi aygıtlarda yedeklemek isterseniz işinize yarayacaktır. Böylece dosyayı kolayca başka bir makineye taşıyabilirsiniz.

100MB boyutunda rasgele bilgi içeren bir dosya oluşturmak için aşağıdaki komutu kullanın:

```
dd if=/dev/urandom of=/mystuff.aes bs=1k count=100000
```

Eğer dosyanın boyutunu değiştirmek isterseniz *count* değişkeninin değerini değiştirin. Yukarıdaki komut her biri 1k boyutlu 100000 blok oluşturur, ama siz istediğiniz gibi değiştirebilirsiniz. Sadece boyutun seçtiğiniz dosya sistemini taşıyamayacak kadar küçük olmamasına dikkat etmelisiniz. Elbette `/dosya_ismi.aes` yerine istediğiniz yolu ve dosya adını seçebilirsiniz.

Yukarda yaptığımıza benzer şekilde bu dosya içerisine şifrelenmiş dosya sistemini şu şekilde oluşturabilirsiniz:

```
losetup -e aes-256 /dev/loop0 /mystuff.aes
```

Şimdi dosya sistemini oluşturabilirsiniz:

```
mkfs.ext3 /dev/loop0
```

ve bağlayalım:

```
mount -t ext3 /dev/loop0 /mnt/crypto
```

Son olarak dosya sistemini ayırın ve geridönüş aygıtını çıkarın:

```
umount /mnt/crypto
losetup -d /dev/loop0
```

İhtiyacınız olduğunda dosya sistemini tekrar bağlayabilirsiniz:

```
mount /mystuff.aes /mnt/crypto -oencryption=aes-256
```

Eğer dosyayı taşımak veya CD/DVD ye yazmak isterseniz önce **unmount** komutuyla dosya sistemini ayırdığınızdan emin olun.

GNU Free Documentation License

Version 1.2, November 2002

```
Copyright © 2000,2001,2002 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA  02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
```

1. PREAMBLE

   The purpose of this License is to make a manual, textbook, or other functional and useful document *free* in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or noncommercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

   This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

   We have designed this License in order to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work,

regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

2. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world–wide, royalty–free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front–matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front–Cover Texts or Back–Cover Texts, in the notice that says that the Document is released under this License. A Front–Cover Text may be at most 5 words, and a Back–Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine–readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ascii without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard–conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine–generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

3. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or noncommercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

4. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front–Cover Texts on the front cover, and Back–Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine–readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer–network location from which the general network–using public has access to download using public–standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

5. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front–matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties—-for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front–Cover Text, and a passage of up to 25 words as a Back–Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front–Cover Text and one of Back–Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements."

7. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

8. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

9. TRANSLATION

   Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

   If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

10. TERMINATION

    You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

11. FUTURE REVISIONS OF THIS LICENSE

    The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See http://www.gnu.org/copyleft/.

    Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

```
  Copyright (C)  year  your name.
  Permission is granted to copy, distribute and/or modify this document
  under the terms of the GNU Free Documentation License, Version 1.2
  or any later version published by the Free Software Foundation;
  with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
  A copy of the license is included in the section entitled "GNU
  Free Documentation License".
```

If you have Invariant Sections, Front–Cover Texts and Back–Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being list their titles, with
the Front-Cover Texts being list, and with the Back-Cover Texts
being list.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.

Notlar

Belge içinde dipnotlar ve dış bağlantılar varsa, bunlarla ilgili bilgiler bulundukları sayfanın sonunda dipnot olarak verilmeyip, hepsi toplu olarak burada listelenmiş olacaktır.

(*B1*) `../howto/encrypted-«rootfs-«howto.pdf`

(*B2*) `../howto/disk_sifreleme.pdf`

(*B6*) `http://lwn.net/Articles/67216/`

(*B7*) `http://www.saout.de/misc/dm-«crypt/`

(*B8*) `http://www.linuxdocs.org/HOWTOs/Kernel-«HOWTO.html`

(*B10*) `http://www.stwing.org/~sluskyb/util-«linux/losetup-«combined.patch`

(*B11*) `http://www.ece.cmu.edu/~rholzer/cryptoloop/util-«linux-«2.12-«kernel-«2.6.patch`

(*B12*) `http://gentoo.org`

Bu dosya (cryptoloop–howto.pdf), belgenin XML biçiminin TEXLive ve belgeler-xsl paketlerindeki araçlar kullanılarak PDF biçimine dönüştürülmesiyle elde edilmiştir.

23 Ocak 2007