Ozgur OZDEMIRCILI

ozgur at enderunix.org

** Federico Biancuzzi`nin "Inside NetBSD's CGD" yazisindan ceviridir. Makalenin gercegine http://www.onlamp.com/pub/a/bsd/2005/12/21/netbsd_cgd.html adresinden ulasilabilir.*

NetBSD CGD

NetBSD hepimizin bildigi gibi degisik platformlar uzerinde sorunsuz calisabilme ozelligi ile one cikan bir BSD cesidi.Bu yazida Federico Biancuzzi `nin Crypto-Graphic Disk sistemi gelistiricisi Roland Dowdeswell ile yaptigi roportaji okuyor olacaksiniz.

Gunluk hayatimizda her zaman kullandigimiz tasinabilir bilgisayarlar her ne kadar bize buyuk kolaylik saglasa da tum bilgilerimizin bir yerde saklanmasi ve tasinabilirlik ozelligi ile hem calinma hem de kaybetme sansinin cok buyuk olmasi yuzunden sorun da teskil etmektedir. Peki bu sorunu nasil cozebiliriz? Bunun en gecerli yontemlerinden birisi disk sifrelemedir.Iste bu makalede tasinabilir bilgisayarlarimizin icerdigi bilgilerin calinma ve kaybolma olasiligina karsi nasil korunacagina goz atacagiz.

CGD Nedir?

RD: CGD (PDF) siflenmis bir disk surucusudur.Diger bir disk uzerinde bulunup isletim sistemi ve uzerine yazilan bilgiler icin sifrelenmis bir disk olusturur.Her yazilan bilgi ilk once sifreli disk surucusune oradan da sifrelenip gercek diske yazilmaktadir.Yeni disk daha sonra partisyonlara ayrilarak normal diskler gibi kullanilabilmektedir. Bu yontem software RAID sirketlerince de kullanilmaktadir.

Neden CGD`yi yaratmak istediniz?

RD: Diger acik kod projeler gibi CGD`yi kendi ihtiyacimi karsilamak icin gelistirdim. O zaman BSD lisansli alternatif olarak sadece OpenBSD svnd surucusu bulunmaktaydi ki bu surucu sozluk saldirilarini durduracak onemleri barindirmamakta ve sadece tek cipher (blowfish) destegi vermekteydi.Bu yuzden kendim bir yazilim gelistirmek istedim.

Herhangi birisi gelistirme surecinde size sponsoz oldu mu?

RD: Hayir. Gelistirme icin danismanliga bir sure ara verdim.

Kullanici tarafinda yazilim nasil calisiyor?

RD: Ilk once parametreler dosyasini yapilandirmaniz gerekiyor.Bu dosya `cgdconfig` (PDF)`nin diskinizi yapilandirabilmesi icin gerekli sifreleme metodu, anahtar yaratma islemi gibi adimlari icermekte.

```
# cgdconfig -g aes-cbc 256 > /etc/cgd/wd0f
```

Varsayilan anahtar uretme methodu, bir sifre yardimi ile bunu yapan PKCS#5 PBKDF2 dir. Bunun yaninda *n*-factor kimlik denetimi veya sadece anahtari bir dosyaya kaydetmek te mumkundur.

Parametre dosyasini hazirladiktan sonra artik diski yapilandirabilirsiniz:

```
# cgdconfig -V re-enter cgd0 /dev/wd0f
        /dev/wd0f's passphrase:
        /dev/wd0f's passphrase:
```

`-V re-enter` bayragi `cgdconfig` `in sifreyi iki defa sorarak dogrulugunu kontrol etmesini soylemektedir. Genel kullanimda `cgdconfig` diskin gecerli bir disk ismi veya verilen anahtar ile gecerli bir dosya sistemi icerip icermedigini kontrol edecektir.Tabiki, ilk defa kullanimda bunlarin her ikisi de yapilmayacaktir.

Su anda , */dev/cgd0[a-h]*, diski normal bir diskin kullanilabilecegi her sekilde kullanima hazirlanmis durumdadir.

```
# cgdconfig -u cgd0
```

diskin yapilandirmasini kaldirirken

```
# cgdconfig cgd0 /dev/wd0f
```

yapilandirmayi yapacaktir.

NetBSD`nin rc sistemi CGD disklerini boot zamninda yapilandirmaya izin vermektedir. Bunun icin yapilandirmayi */etc/cgd/cgd.conf* dosyasina eklemeniz yeterli oalcaktir.

Eger baska bir sistem yoneticisi icin sifre belirlemek istiyorsaniz, ilk dosyadan ikinci bir dosya yaratip ayri bir sifre belirleyebilirsiniz:

```
# cgdconfig -G old_params > new_params
```

Bu method eger *old_params* guvenli sekilde silinirse, sifreyi degistirmek icin kullanilabilir.

Eger su anda kullandigim disk uzerinde bilgilerim var ise bu bilgileri sifreleyebilir miyim?Yeni bir bolum yaratip tum bilgileri oraya mi tasimaliyim?

RD: Evet. Hali hazirda bulunan bilgileri sifrelemek icin yeni bir bolum yaratmali ve bu bilgileri yeni bolume tasimalisiniz.

Sifreleme ne kadar yer kaplamakta? Eklenen bilgiler ile buyuyen mi yoksa belli bir buyuklugu olan mi bir yapisi bulunmakta?

RD: CGD tarafindan kullanilan sifrelem methodlari sifrelenen bilginin buyuklugunu degistirmemkte. Yapilandirma dosyasi disinda, ki bu birkac yuz byte`tan ibaret olmakta, yer kaplamamaktadir.

Sifreleme sirasinda CDG hangi adimlari izlemekte?

RD: `cgdconfig` ilk olarak parametre dosyasini okuyarak algortima, anahtar uretim methodu, anahtar uzunlugu ve Vektor uretim methodu gibi bilgileri edinecektir.

Varsayilan anahtar uretim methodu sifre kullanan, PKCS#5 PBKDF2, salted itarated hash olarak gecmektedir. Salt ozelligi sozluk saldirilarini onler. Boylece parametre dosyasina ulasmadan sozluk saldirisi duzenleyemezsiniz. Iterating ise sozlukteki her kelime icin yapilan denemeyi daha uzun zamana yayr. Varsayilan zaman su anda 2 saniye olarak ayarlanmistir.

Su anda desteklenen sifreleme algoritmalari AES (128-, 192-, and 256-bit anahtar), blowfish (40-448-bit anahtar), ve 3DES (192-bit anahtar)`dir.Birden cok cipher kullanimi kullaniciya guvenlik ve performans arasinda secim yapma sansini sunmaktadir. Bir cipher`da kesfedilen zayiflik durumunda kullanici diger cipher`a isletim sistemini guncellemeden gecebilmektedir.

Her sektor ayri ayri sifrelenmektedir. Bir sektoru sifrelemek icin:

1. Baslangic Vektor`u (Initialization Vector) yapilandirilmis IV methodu ile uretilmekte.

2. 1. Sektor ise 1. bolumde IV ile uretilen sifreleme algoritmasi ile sifrelenmektedir.

Desifreleme ise ayni sekilde calismaktadir.

Sifrelenmis kesiti yapilandirdiktan sonra, cipher`i degistirebilir veya cgd`yi devre disi birakabilir miyim?

RD: Hali hazirda bulunan bolumdeki sifreleme cesidini degistirmenin su anda icin hicbir yolu bulunmamakta. Bunu yapmanin yolu yeni bir bolum olusturulmasi ve tum bilgilerin bu bolume tasinmasidir. Su anda bunu otomatik olarak yapabilecek bir yazilim uzerinde calismaktayim.

Herhangi bir sekilde yazilim veya donanim RAID`leri ile etkilesimde bulunuyor mu?

RD: Hayir.

Rastgele numara ureticileri veya hizladiricilardan yararlaniyor mu?

RD: Su anda degil fakat bunu planliyorum.

Herhangi bir hafiza/ islemci gereksinimi bulunmakta mi?

RD: Yazilimin calismasi icin gerekli herhangi bir en az islemci veya hafiza degeri bulunmamakta. Fakat yavas islemcilerin kullanimi performansi etkileyecektir.

I/O performansini ne kadar sinirlamakta?

RD: Islemci ve disk gucune gore degismekte.Burada iki ana nokta bulunmakta. En yuksek cikis islemci gucu ile sinirlanabildigi gibi, sifreleme diske yazilmadan once, de sifreleme ise diske yazildiktan sonra gerceklesecegi nden, CGD her disk isleminde biraz gecikme ekleyecektir.

Speed Step ozelligine sahip laptoplar icin ise CGD performansi degisken olacaktir.

Sanirim her laptop sahibi tum bilgilernin calinma dusuncesi ile buyuk rahatsizlik duymaktadir. Eger boyle bir durum ortaya cikar ise, CGD diske fiziksel olarak ulasimi olan saldirganlara karsi ne gibi koruma saglamakta?

RD: Eger laptop kapali ise saldirgan, sifrelemeyi ya sozluk saldirisi veya brute force ile kirmak zorunda kalacaktir.

Sozluk saldirisi diski sifreleyen sifreyi bulmaya calisacaktir. Kullanicilar cogu zaman modern sifrelerdeki kadar guvenli sifreler secmedikleri icin bu saldiri ilk akla gelen saldiri cesidi olacaktir.CGD PKCS#5 PBKDF2 (an iterated salted hash) ile brute force saldirilarini yavaslatmaktadir. Basit olarak yaptigi her sozcugu hesaplamak icin gerekli olan bilgi islem gucunu arttirmaktir.CGD ayrica 2-faktor kimlik denetimi ile size ikinci anahtarin bir usb uzerinde saklanabilmesine olanak saglamaktadir.

Brute force saldirisi sifreleme icin gerekli olan anahtari hedef alir. CGD tarafindan desteklenen sifreleme yontemleri AES 128, AES 192, AES 256, 3DES, ve Blowfish`in 100 bit uzerinde anahtarlari oldugu dusunulurse, bunlarin bulunmasi 2^ 100 tahmin gerektirecektir.

Eger laptop hala acik veya askiya alinmis sekilde calinir ise saldirgan anahtari hafizadan alabilir.

"CGD ayrica 2-faktor kimlik denetimi ile size ikinci anahtarin bir usb uzerinde saklanabilmesine olanak saglamaktadir." demistiniz. Bu nasil calismakta?

RD: CGD aygitini yapilandirirken, bildiginiz gibi bir sifreleme teknigi, anahtar uzunluklari ve anahtar uretim yontemlerini iceren bir yapilandirma dosyasi olusturuyoruz. Normalde kisi PKCS#5 PBKDF2 kullanarak bir anahtar uretecektir. Fakat yapilandirma dosyasinda birden cok anahtar uretim methodu belirtilirse her ikisi de gercek anahtari uretmek icin birlestirilecektir. Oyle ise 2-faktor kimlik denetiminin kullanimasi icin kisinin, birisi PKCS#5 PBKDF2 gibi bir sifre kelimesi methodu digeri ise yapilandirma dosyasinda bulunacak basit anahtar olan iki anahtar uretim methodu belirtmesi gerekecektir..

Anahtarimi kaybedersem veya unutursam ne olacak?

RD: Eger anahtarinizi kaybeder veya sifrenizi nutursaniz bilgilerinizi kaybettiniz demektir. Bu sizi laptopunuzu calan kisi ile ayni duruma koyacaktir. Eger bu konuda endiseleriniz var ise bilgilerinizi yedeklemelisiniz.

`cgdconfig` sifre dogrulama icin birkac yontem sunmakta. Gecerli bir disk ismini veya FFS dosya sistemini tarayabilmekte. Acaba gecersiz bir sifrenin gecerli bir disk ismi veya dosya sistemi olusturmasi olasiligi nedir?

RD: Yanlis bir sifrenin dogru sekilde kimlik denetiminden gecmesi ihtimali oldukca ufak. SU anda 4 seyi kontrol ediyoruz: 32-bit numara, ki bu iki kere tekrarlaniyor; 32-bit saglama toplami (checksum); ve bolum numaralari.Bolum numaralari mimariye gore degismesine ragmen maksimum 22 bit ile sinirli, 16-bit degisken uzerinde tutulmakta ki bu da diger 11 bit`in 0 oldugu anlamina gelmekte. Oyle ise su degerleri kontrol ediyoruz: 32 + 32 + 32 + 11 = 107 bits.

Eger yanlis sifrenin yazilmasinin gercekten rastgele bir bloga denk gelecegini dusunursek disk isminin artima (sanity) testini gecme ihtimali 1/2^107 olacaktir.Bu da yaklasik olarak `0.00000000000000000000000000000000000616`a denk gelmektedir.

Daha kesinlik kazanmak icin diskisminde daha cok bit denetimi yapabiliriz. Ornegin sektor buyuklugu, her guzergahta (track) bulunan sektor sayisi, bolum yerlesimleri vs. Disk isminde bircok bilinen bilgi oldugu dusunulurse, yanlis bir sifrenin dogru disk ismini olusturmasi sansi cok dusuk olacaktir.

Buna benzer bir analiz FFS superblogu icin uygulanabilir.

Kod diger isletim sistemlerinde calisabilir durumda mi?

RD: CGD`nin cogu kodu yapilandirma programi oldugu icin diger sistemlerde calistirilmasi kolay oalcaktir. Kernel`lar API ve davranislarda daha buyuk farkliliklar tasidiklari icin kernel kodunun aktarilmasi biraz daha zor oalcaktir. CGD Ted Unangst tarafindan OpenBSD 3.2`ye aktarilsa da ana OpenBSD agacina eklenmedi.

CGD`ye alternatif veya CGD`de bulunmayan ozellikleri barindiran baska bir yazilim biliyor musunuz?

RD: CGD ve OpenBSD svnd, FreeBSD GBDE, veya Linux Loop-AES sozde (pseudo) diskleri belli bir modele gore dizayn edilmislerdir. Sifrelenmis dosya sistemleri baska bir modele cevap verebilir veya farkli ozellikler icerebilir.Bazi durumlarda CFS veya nCryptfs daha uygun bir cozum olarak alinabilir. Tabiki bu durumda dikkat edilmesi gereken hangi noktalarin avantaj hangi noktalarin dezavantaj saglayacaginin onceden dusunulmesidir. CFS ve nCryptfs ile degisik kullanicilara degisik anahtar verme avantajina ulasirken dosya sistemi bilgilerini gereginden fazla dagitmis olmaktasiniz.NFS uzerinden her kisi icin sifreleme onemli olsa da bu bir laptop icin gereksiz olacaktir.Bir sunucuda bile root kullanicisinin tum kullanici anahtarlarini hafizadan okuyabilecegini dusunmeli. Oyle ise sifrelenmis dosya sistemi root kullanicisina karsi sizi koruyamayacaktir, en azindan sistemde siz calisirken.

OpenBSD CGD Ted Unangst tarafindan port edilmesine ragmen port agacina eklemedi. OpenBSD`nin `svnd` `si sizce ayni ozellikleri barindiriyor olabilir mi?

RD: Bu durumda OpenBSD'nin `svnd` yazilimi CGD ile bazi ortak ozellikleri tasiyor olabilir. CGD`yi gelistirmeden once `svnd` yazilimini inceleyip bazi sorunlari barindirdigini farketmistim.

`svnd` `nin en buyuk sorunlarindan birisi genel kullanimda guvenlikten eksin olmasidir. Herhangi bir sozluk saldirisina aciktir. Yani, diske sahip olmasaniz bile 0(1) olarak

girilebilen sifreler ve disk uzerindeki bilinen sifre bloklari icin bir veritabani olusturabilirsiniz. Daha kotusu ise bu veritabaninin herhangi bir `svnd` diski uzerinde de calisabilmesidir. Muhtemelen NSA gibi kuruluslar su anda boyle bir veritabanini olusturmus ve 1 saniyeden az bir surede herhangi bir `svnd` disk sifresini kirabilir durumdadirlar.Cevirim disi (offline) sozluk saldirilarinin onlenmesi sifre ile mantiksal carpima sahip bir salt kullanilmasi olacaktir.CGD`yi yazarken ben de bu ozelligi PKCS#5 PBKDF2 kullanarak gerceklestirdim. 70`lilerden beri bilinan cevirim disi sozluk saldirilari soncunda 30 yildan beri sifrenin salt hale donusturulmesi bir standart olmustur.

OpenBSD`nin cozumu sadece Blowfish`i desteklerken CGD`nin bir gurup sifrelemeyi destekleyebilmesini istedim. Bu birkac neden yuzunden onemli olsa da, gnel olarak kullanicilarimizefiyata karsi risk konusunda secim yapabilmeleri sansini vermis oluyoruz. Blowfish hizli olsa da AES`ten daha guvensizdir. Bazi durumlarda kullanicilar hizliligin guvenlikten daha onemli oldugu kararina varabilirler. Bazi durumlarda ise tam tersi kararlar alinabilir. Ayrica, eger bir sifreleme yonteminde zayiflik kesfedilirse kullanicilar CGD`lerini diger sifreleme yontemini kullanmalari icin yapilandirabilir ve bunu islerim sistemini yenilemeden gerceklestirebilirler.Blowfish in ayrica 64 bit blok buyuklugu oldugu hesaba katilirsa, buyuk diskler icin yapisal analiz`e izin verecek kadar kucuk oldugu gorulebilir.

CGD Linux`un Loop-AES i ile karsilastirilabilir mi?

RD: Ilk olarak OpenBSD'snin `svnd` sisteminde bulunan tum sorunlari ve daha fazlasini iceren Linux cryptoloop`a baktim. Loop-AES bu tur sorunlara CGD`den farkli bir sekilde cozum bulmaya calismakta.

CGS ve FreeBSD GBDE arasinda ne gibi farkliliklar bulunmakta?

RD: Her ne kadar ne ben ne de GBDE`nin gelistiricisi birbirimizden haberdar olmasak da, FreeBSD GBDE ve CGD hemen hemen ayni zamanda gelistirildi.Tek farklilik benim CGD`yi iki hafta kadar once yayimlamamdi.Hemen hemen ayni islemi yapsalarda gelistirme sirasinda izlenen yollar birbirinden farkli idi. GBDE`nin diski desifrelemek icin farkli sifrelere izin vermesi ozelligini sevdim ve bunu CGD`ye ekledim.

GBDE eger 2-faktor kimlik denetimi mekanizmasi kullanilmiyor ise ve ikinci faktor herhangi bir sekilde ele gecirilirse cevrimici sozluk saldirilarina aciktir.Fakat bu saldiri hicbir zaman OpenBSD's `svnd` deki kadar tehlikeli degildir.Cevrimici sozluk saldirisi GBDE ile sifrelenmis olan her disk icin ayri ayri gerceklestirilmek zorundadir.2-faktorun FreeBSD kullanicilari tarafindan guvenligi daha saglam tutmak adina kullanilmamasinin daha buyuk bir saldiri tehlikesine yol acmasi acikca buyuk bir dezavantaj olarak alinabilir. OpenBSD's `svnd` sisteminde bu cozulmus bir sorun olsa da. GBDE`nin gelistiricisine aylar once bu sorunu bildirsem de hala acik kapatilmamis durumdadir.

GBDE de bulunan diger bir sorun dosya sistemlerinin diskler hakkinda olan varsayimlarini bozmasidir. Diske bir sektor yazdiginizda GBDE, disk iki ayri yazma islemi gerceklestirir ki bu yazma islemi sirasinda diskler onarilamaz halde olacaktir. Yazma sirasinda eger elektrik kesilir ise sektor kaybolacak ve bir daha buradaki bilgilere ulasilamayacaktir, en azindan AES sifrelemesini kirmadan. GBDE`nin bu tur kesilmelerde uyari vermemesi durumu ise gercek hayat kullanimlarinda buyuk sorun

teskil etmektedir.

FreeBSD GELI adinda yeni bir program yayimladi. Cok fazla detayli bakamasam bile GBDE`den cok daha iyi gorunuyor. Kolay yapilandirilma size sistemin isleyisi hakkinda daha kolay anlayis sagliyor. Ayrica daha once bahsettigim aciklarin hepsine birden cozum bulmus gibi gorunmekte.

Yaziliminiza yakin gelecekte hangi yenilikleri eklemeyi dusunuyorsunuz?

RD: Bir suredir CGD`ye donanim sifrele destegi eklemek istiyorum. Moduler bir yapida oldugu ve hali hazirda bir tane temel bulundugu icin ayri bir IV methodu eklemek istiyorum. Steven Bellovin dogruluk saglamasini cok fazla bilgi islem gucune gerek kalmadan yapabilmenin birkac yolunu onerdi. Fakat gunluk dosyasini hesaba katinca bunun yazma suresini etkilememesi imkansiz gibi gorunuyor. Diger bir yenilik ise yukleme dosyasina CGD`leri olusturma icin bir bolum eklemek olacak.