TCKN’deki Tehlike

written by Mert SARICA | 25 August 2010

Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü’nün sayfasında yer alan bilgiye göre, T.C. Kimlik Numarası 11 basamaktan oluşan bir numaradır. Son iki rakamı doğrulama sayısıdır. Bu son iki basamak ilk dokuz basamaktan bir algoritma ile hesaplanmaktadır. Doğrulama sayısı algoritması, sadece bir numaranın tarafımızdan verilen bir T.C. Kimlik Numarası olup olmadığı hakkında bilgi vermektedir. Bu algoritma T.C. Kimlik numaralarının doğruluğunu kontrol etmeleri için diğer kamu kurum ve kuruluşları ile de paylaşılmaktadır.

Kredi kartı numarası ise en az 16 en fazla 19 haneden oluşan bir numaradır. İlk rakam kuruluşun kategorisini (banka, havayolu, vs.) , sonraki 5 rakam kredi kartı kuruluşunu (visa, mastercard vs.) ve bankayı sonraki 9 rakam ise banka tarafından müşteriye özel üretilen bir sayıdır. Son rakam ise doğrulama sayısıdır.

Doğrulama sayısı içeren her numara bir algoritmaya göre üretilmektedir. Örneğin kredi kartı numarası Hans Peter Luhn tarafından yaratılan halka açık Luhn algoritmasına göre üretilmektedir. Halka açık olması nedeniyle sizde bu algoritmaya göre geçerli bir kredi kartı numarası üretebilir veya üretilmiş bir numarayı doğrulayabilirsiniz.

Yazının ilk paragrafını okuduktan sonra TCKN doğrulama algoritması sadece kamu kurum ve kuruluşları ile paylaşıldığı için herhangi bir kişi tarafından TCKN üretilmesinin mümkün olamayacağını düşündünüz ve yanıldınız.

Google arama motoru üzerinde “TCKN algoritması” anahtar kelimesi ile arama yaptığınızda doğrulama algoritmasının bir çok web sayfasında yer aldığını görebilirsiniz. Web sayfaları üzerinde yaptığım ufak bir araştırma neticesinde TCKN doğrulama algoritmasını açıklayan en eski içerik 1 Eylül 2008 tarihinde bu sayfada oluşturulmuş. Sayfada yer alan bilgiler ışığında aynı kredi kartında olduğu gibi geçerli bir TCKN üretmek mümkündür.

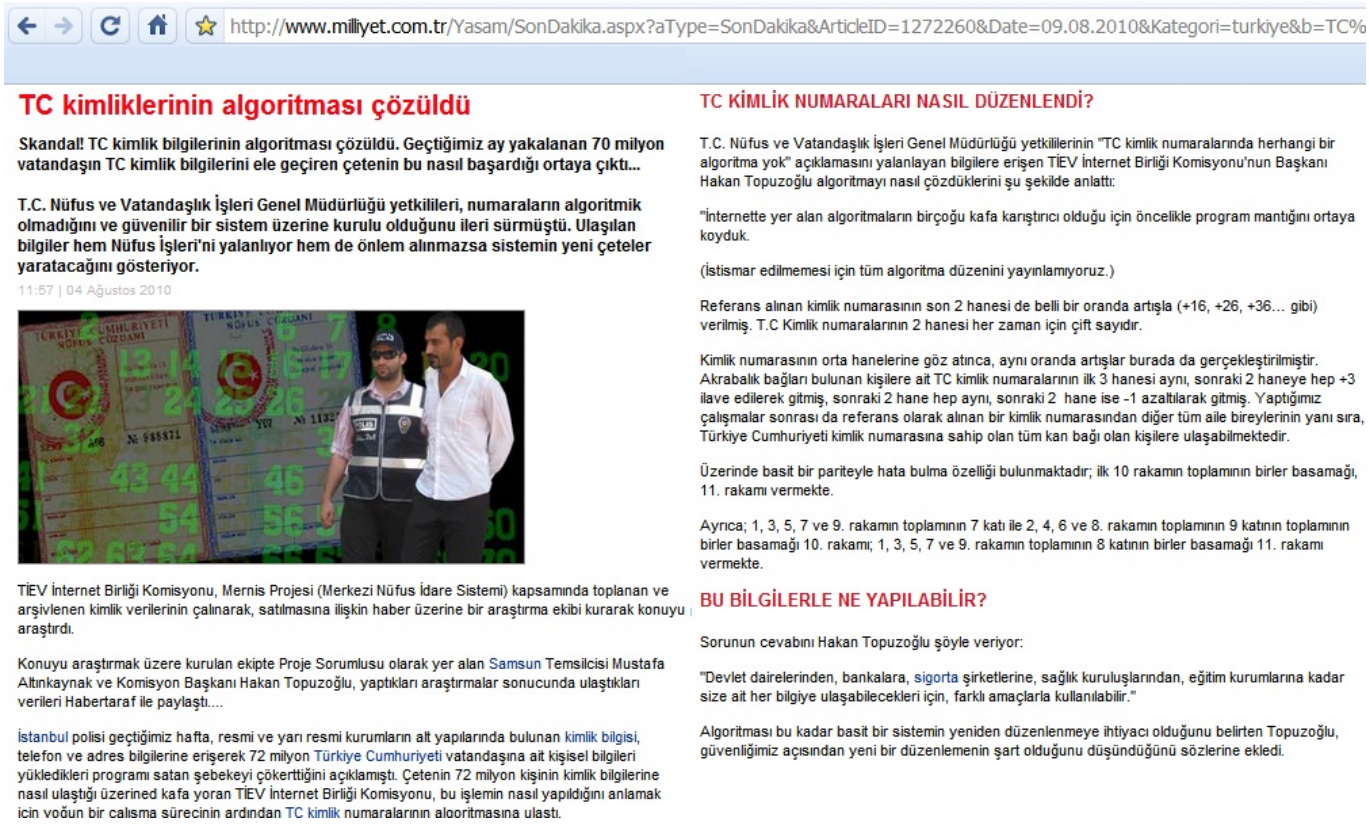
Kredi kartı numarası ile TCKN arasındaki en büyük farkların ne olduğuna gelecek olursak;

- Luhn algoritmasına göre oluşturulan bir kredi kartı numarasının size ait bir kredi kartı numarası olma ihtimali her zaman vardır fakat kredi kartı üzerinde yer alan son kullanma tarihi ve CVV2 bilgilerinin

finansal işlemlerde kontrol edilmesi sayesinde art niyetli kişiler tarafından sizin adınıza harcama yapılmasının önüne geçilmektedir.

- TCKN doğrulama algoritmasına göre oluşturulan bir TCK numarasının size ait bir numara olma ihtimali her zaman vardır fakat kredi kartı işlemlerinde kullanılan son kullanma tarihi ve CVV2 gibi ek kontrollerin aksine TCKN ile gerçekleşen işlemlerin bazılarında bu tür ek kontroller bulunmamaktadır. Bu nedenle art niyetli kişiler bu sayfalar üzerinden size ait TCK numarası ile özlük bilgilerinize (isim, soyad, yerleşim yeri) ulaşabilmektedirler!
- Kredi kartı numarasından müşterinin kişisel bilgilerine halka açık bir uygulama, web servisi üzerinden erişmeniz mümkün değildir fakat TCKN için ne yazıkki aynı şeyi söylemek mümkün değil.

Durum böyle oluncada aşağıdaki gibi haberler ile karşılaşınca insan hiç şaşırmıyor fakat aşağıdaki haberin diğerlerinden bir farkı bulunuyor.



http://www.milliyet.com.tr/Yasam/SonDakika.aspx?aType=SonDakika&ArticleID=1272260&Date=09.08.2010&Kategori=turkiye&b=TC%

TC kimliklerinin algoritması çözüldü

Skandal! TC kimlik bilgilerinin algoritması çözüldü. Geçtiğimiz ay yakalanan 70 milyon vatandaşın TC kimlik bilgilerini ele geçiren çetenin bu nasıl başardığı ortaya çıktı...

T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü yetkilileri, numaraların algoritmik olmadığını ve güvenilir bir sistem üzerine kurulu olduğunu ileri sürmüştü. Ulaşılan bilgiler hem Nüfus İşleri'ni yalanlıyor hem de önlem alınmazsa sistemin yeni çeteler yaratacağını gösteriyor.

11:57 | 04 Ağustos 2010

TİEV İnternet Birliği Komisyonu, Mernis Projesi (Merkezi Nüfus İdare Sistemi) kapsamında toplanan ve arşivlenen kimlik verilerinin çalınarak, satılmasına ilişkin haber üzerine bir araştırma ekibi kurarak konuyu araştırdı.

Konuyu araştırmak üzere kurulan ekipte Proje Sorumlusu olarak yer alan Samsun Temsilcisi Mustafa Altınkaynak ve Komisyon Başkanı Hakan Topuzoğlu, yaptıkları araştırmalar sonucunda ulaştıkları verileri Habertaraf ile paylaştı....

İstanbul polisi geçtiğimiz hafta, resmi ve yarı resmi kurumların alt yapılarında bulunan kimlik bilgisi, telefon ve adres bilgilerine erişerek 72 milyon Türkiye Cumhuriyeti vatandaşına ait kişisel bilgileri yükledikleri programı satan şebekeyi çökerttiğini açıklamıştı. Çetenin 72 milyon kişinin kimlik bilgilerine nasıl ulaştığı üzerined kafa yoran TİEV İnternet Birliği Komisyonu, bu işlemin nasıl yapıldığını anlamak için yoğun bir calısma sürecinin ardından TC kimlik numaralarının algoritmasına ulastı.

TC KİMLİK NUMARALARI NASIL DÜZENLENDİ?

T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü yetkililerinin "TC kimlik numaralarında herhangi bir algoritma yok" açıklamasını yalanlayan bilgilere erişen TİEV İnternet Birliği Komisyonu'nun Başkanı Hakan Topuzoğlu algoritmayı nasıl çözdüklerini şu şekilde anlattı:

"İnternette yer alan algoritmaların birçoğu kafa karıştırıcı olduğu için öncelikle program mantığını ortaya koyduk.

(İstismar edilmemesi için tüm algoritma düzenini yayınlamıyoruz.)

Referans alınan kimlik numarasının son 2 hanesi de belli bir oranda artışla (+16, +26, +36... gibi) verilmiş. T.C Kimlik numaralarının 2 hanesi her zaman için çift sayıdır.

Kimlik numarasının orta hanelerine göz atınca, aynı oranda artışlar burada da gerçekleştirilmiştir. Akrabalık bağları bulunan kişilere ait TC kimlik numaralarının ilk 3 hanesi aynı, sonraki 2 haneye hep +3 ilave edilerek gitmiş, sonraki 2 hane hep aynı, sonraki 2 hane ise -1 azaltılarak gitmiş. Yaptığımız çalışmalar sonrası da referans olarak alınan bir kimlik numarasından diğer tüm aile bireylerinin yanı sıra, Türkiye Cumhuriyeti kimlik numarasına sahip olan tüm kan bağı olan kişilere ulaşabilmektedir.

Üzerinde basit bir pariteyle hata bulma özelliği bulunmaktadır; ilk 10 rakamın toplamının birler basamağı, 11. rakamı vermekte.

Ayrıca; 1, 3, 5, 7 ve 9. rakamın toplamının 7 katı ile 2, 4, 6 ve 8. rakamın toplamının 9 katının toplamının birler basamağı 10. rakamı; 1, 3, 5, 7 ve 9. rakamın toplamının 8 katının birler basamağı 11. rakamı vermekte.

BU BİLGİLERLE NE YAPILABİLİR?

Sorunun cevabını Hakan Topuzoğlu şöyle veriyor:

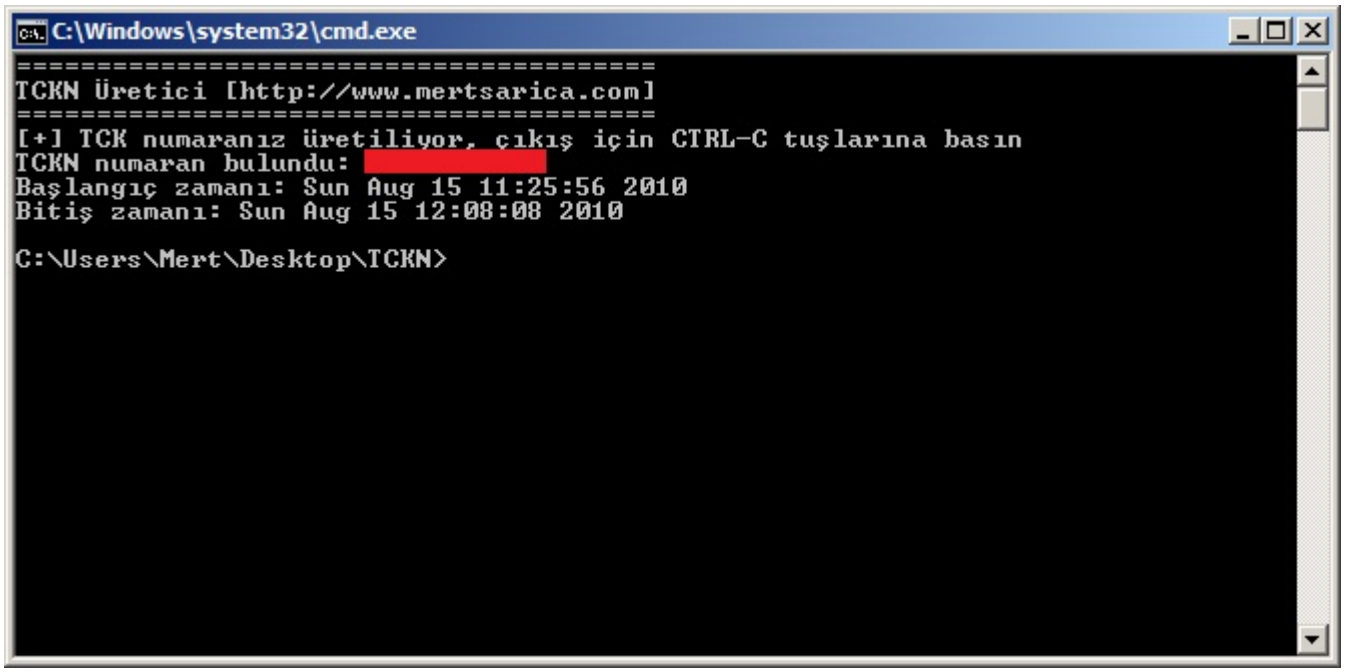
"Devlet dairelerinden, bankalara, sigorta şirketlerine, sağlık kuruluşlarından, eğitim kurumlarına kadar size ait her bilgiye ulaşabilecekleri için, farklı amaçlarla kullanılabilir."

Algoritması bu kadar basit bir sistemin yeniden düzenlenmeye ihtiyacı olduğunu belirten Topuzoğlu, güvenliğimiz açısından yeni bir düzenlemenin şart olduğunu düşündüğünü sözlerine ekledi.

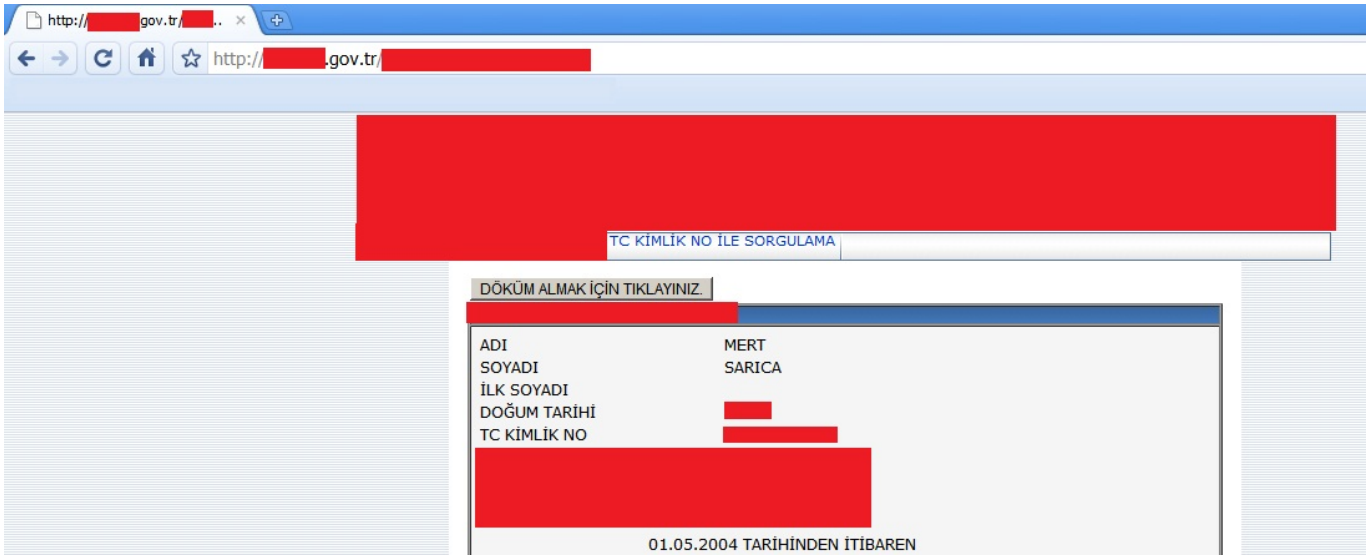
Haberde TC kimliklerinin algoritmasının çözüldüğüne, algoritma ile ilgili olarak internet sitelerinde yer alan bilgilerin aynısına ve T.C. Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü yetkililerinin yaptığı “TC kimlik numaralarında herhangi bir algoritma yok” açıklamasına yer verilmiş. Yukarda anlattıklarım ışığında haberi okuyacak olursanız neyin doğru neyin yanlış olduğunu ayırt edebileceğinizi varsayarak haber üzerine yorum yapma gereği duymuyor, art niyetli kişilerin TCKN üreterek kişisel bilgilerine nasıl

ulaşılabileceğini teknik detay vermeden gözler önüne sermek ve bu sayede kredi kartı numarasından daha değerli olan TCK numarası ve kişisel bilgileri çetelerin eline geçmiş olan bir vatandaş olarak ilgilileri daha güvenli bir sistem oluşturmaları adına göreve çağırmak istiyorum.

Öncelikle internet sitelerinde yer alan algoritmaya göre rastgele TCKN üreten bir program hazırladım ve bu programın kendi TCK numaramı ne kadar süre içinde üretebildiğine baktım ve yaklaşık 40 dakika sonunda ürettiğini gördüm.



Daha sonra üretilen TCK numaramdan kişisel bilgilerime erişmenin yolunu ararken çok geçmeden bir devlet kurumu üzerinde yer alan TCKN sorgulama uygulaması ile isim ve soyad bilgilerime ulaşabildim.



Bunun dışında sorgulama sayfalarında keşfettiğim bazı eksikliklerin ve hatalı tasarımların art niyetli kişilerin işlerini daha da kolaylaştırabileceğini

düşünüyorum bu nedenle konu ile ilgili olarak yetkililer benimle iletişime geçerlerse kendileri ile bu eksiklikleri paylaşabilirim.

T.C vatandaşı olarak kişisel bilgilerime erişilmesine imkan tanıdığı için hassas bilgi sınıfına giren TCK numaramın devletin tüm organlarında aynı hassasiyet ile saklanması ve Luhn algoritması gibi halka açık bir algoritma ile kontrol edilebilmesi sebebiyle sadece benim bildiğim ve sahip olduğum ek bilgiler ile kontrol edilerek (kredi kartı işlemlerindeki son kullanma tarihi ve CVV2 kontrolleri gibi) ilgili sistemler/sorgular üzerinde yer alan işlemlerimin gerçekleştirilebilmesini temenni ederim. Aksi durumda benzer haberler okumaya devam edeceğimizden hiç şüphem yok.

Bir sonraki yazıda görüşmek dileğiyle şimdiden herkesin 30 Ağustos Zafer Bayram’ını kutlarım.