Fırat Üniv. Müh. Bil. Dergisi
28(2), 185-188, 2016

Science and Eng. J of Fırat Univ.
28(2), 185-188, 2016

Sosyal Güvenlik Kurumu Biyometrik Kimlik Doğrulama Sisteminin Problemleri ve Olası Çözüm Önerileri

Fatih ÖZKAYNAK
Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ, Türkiye.
ozkaynak@firat.edu.tr

(Geliş/Received:23.03.2016; Kabul/Accepted:26.09.2016)

Özet

Türkiye Cumhuriyeti Sosyal Güvenlik Kurumu biyometrik kimlik doğrulama sisteminin birçok faydası olmasına rağmen çeşitli güvenlik problemleri bulunmaktadır. Bu çalışmanın amacı bu problemleri ve olası çözüm önerilerini göstermektir. Çalışmada fiziksel klonlamaz fonksiyonları temel olan bir kriptolojik anahtar üreteç algoritması önerilmiştir. Önerilen algoritmanın Android tabanlı cihazlar için uygulanabilir bir versiyonu yayınlanmıştır.

Anahtar Kelimeler: Bilgi Güvenliği, Kriptoloji, Kritik Altyapılar, Anahtar Üreteci

Problems and Possible Solutions of Social Security Institution Biometric Authentication Systems

Abstract

Although there are many benefits of biometric authentication system of Republic of Turkey Social Security Institution technique it is hosting a variety of security problems. The aim of this study is to show these security problems and possible solutions. In this study, cryptographic key generation algorithm based on physical unclonable function has been proposed. A version of the proposed algorithm has been released for devices based on Android.

Keywords: Information Security; Cryptography; Critical Infrastructure; Key Generator.

1. Giriş

Bilgi ve iletişim teknolojilerine olan bağımlılığımız elektronik çözümlerin güvenliğini ve gizliliğini zaruri hale getirmiştir [1-3]. Bu çalışmada kritik altyapı sistemleri üzerinde işlenen verinin güvenliği için geliştirilen veri işleme platformunun anahtar üreteç algoritması tanıtılmıştır. Önerilen veri işleme platformunun uygulaması Sosyal Güvenlik Kurumunun (SGK) biyometrik kimlik doğrulama sistemi üzerinde incelenmiştir.

SGK hastanelerde hizmet sunumu esnasında çeşitli istenmeyen durumlar ile karşılaşmıştır. Örneğin sosyal güvencesi olmayan kişilerin bu hakka sahip kişiler üzerinden tedavi gördüğü saptanmıştır. Bir diğer istenmeyen durum ise hastaneye dahi gitmeyen birçok kişi adına çeşitli işlemler gerçekleştirilerek bu işlem bedellerinin SGK fatura edilmesi olmuştur. Daha güvenilir ve işleyebilen bir sistem olarak SGK biyometrik kimlik doğrulama sistemine geçiş yapmıştır. SGK biyometrik kimlik doğrulama sisteminde kullanıcılar hastane polikliniklerinde kimlikleriyle beraber avuç içi verisi okutarak kimliklerini ibra etmek durumunda kalmıştır. Ancak önerilen yeni sistemin çeşitli güvenlik zafiyetleri bulunmaktadır. Kritik altyapılara yönelik gerçekleştirilecek siber saldırılar ile güvenliği kritik bilgilerin kötü amaçla kullanılma olasılığı bulunmaktadır. Bu çalışmanın temel amacı hem biyometrik hem de kişisel sağlık verilerinin kimlik doğrulama süreçlerinde kullanılması esnasında yasal düzenlemeler ile teminat altına alınan özel hayatın gizliliğine ve ticari sır niteliğindeki verilerin korunmasına ilişkin hükümler doğrultusunda güvenliği ispatlanabilir bir model geliştirmektir. Bu çalışmada geliştirilen veri işleme platformunun güvenli anahtar üreteç algoritması tanıtılmıştır.

Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde hastane polikliniklerinde hizmet sunumunda kullanılan SGK biyometrik kimlik doğrulama sisteminin

mevcut işleyişi ve problemleri tartışılmıştır. Üçüncü bölümde önerilen yöntemin detayları açıklanmıştır. Son bölümde çalışma özetlenmiştir.

2. Mevcut Sistemin İşleyişi ve Problemleri

Sağlık Bakanlığının mevcut kimlik doğrulama sisteminde vatandaşların biyometrik bilgileri SGK merkezinde bulunan sunucularda kriptolu olarak saklandığı, verilerin AES256 yöntemi ile şifrelendiği ve verilerin merkez sunucularına 128 bit SSL ile taşındığı belirtilmesine rağmen sistemin güvenliği garanti edilememektedir. Sistem üzerinde çeşitli açıklar bulunmaktadır. Veriler şifreleme işlemine tabi tutulsa bile şifreleme algoritması anahtarının kimde olduğu bilinmemektedir. Sistemin mevcut durumundaki problemini en iyi şu örnek ile açıklanabilir. Örneğin evinizin güvenliğini sağlamak için kapınızı kilitlediğinizi ama anahtarı kime emanet ettiğinizi bilmediğinizi varsayalım. Bu durumda eviniz ne kadar güvende ise mevcut sistemde biyometrik verileriniz o kadar güvendedir.

Mevcut sistemin en önemli problemlerinden bir diğeri ise bilinçsiz sistem kullanıcılarıdır. Bilgi güvenliği okuryazarlığı olmayan birçok kişi neden avuç içi verisinin alındığını bilmemekle beraber ileride karşılaşabilecekleri tehlikenin farkında değildir. Bu savı sayısal verilerle doğrulayabilmek için hastana polikliniklerine başvuran 1000 kişiyi kapsayan bir anket çalışması yapılmıştır. Farklı yaş, meslek ve statülere sahip kullanıcıların sistem hakkında ne düşündüğünü anlayabilmek için aşağıda listelenen 11 soru yöneltilmiştir:

i. Avuç içi verilerinizin neden alındığını biliyor musunuz?
ii. Cep telefonunuzu açmak için pin kodu kullanıyor musunuz?
iii. Cep telefonunuzda ekran kilidi var mı?
iv. Neden cep telefonunuzda pin kodu veya ekran kilidi var?
v. Güvenlik kelimesi size ne anlam ifade ediyor?
vi. Elektronik ortamlarda (internet gibi) bilgilerinizin güvenliğini sağlamak için ne yapıyorsunuz?
vii. Avuç içi verilerinizi muayene olmak için verirken hastanenin biyometrik verilerinizi kötü amaçla kullanabileceği ihtimalini (örneğin ilaç firmalarına satılma ihtimali gibi) hiç düşündünüz mü?
viii. Biyometrik veri ne demektir biliyor musunuz?
ix. Kötü niyetli bir kişi burada giriş için verdiğiniz avuç içi verisini kullanarak bir suç işlerse kendinizi mahkemede nasıl aklardınız?
x. Güvenliğinizi sağlamak için bir ürün geliştirilse kullanır mıydınız?
xi. Bu ürün için en çok ne kadar ödeme yapardınız?

Bu sorular aslında acı bir gerçeği ortaya çıkarmıştır. Ankete katılanların %85'inden fazlası cep telefonuna güvenli bir şekilde erişmek için kullandığı pin kodunu biyometrik verilerinin güvenliğinden daha fazla önemsediği sonucuna varılmıştır. Eğitimciler, devlet görevlileri ve akademisyenler bu ciddi problemi ivedi bir şekilde adreslemeli ülkemizde bilgi güvenliği okuryazarlığını artırmak için çalıştay, atölye çalışmaları ve konferanslar düzenlemelidirler. Bu kapsamda Elazığ Bilim Merkezi ve Kriptarium firması öncülüğünde 7-12 yaş aralığındaki 40 çocuğa "kriptoloji atölyesi" başlıklı bir eğitim verilmiştir [12]. Bu tip az sayıca sevindirici gelişme olsa da bu tip sosyal sorumluluk projelerinin sayılarının artırılması gerekmektedir.

Mevcut sistemin bir diğer problemi de sisteme yapılabilecek aktif saldırılardır. Teknolojik gelişmeler sadece hayatımızı kolaylaştırmamış saldırganların da yeteneklerini geliştirmiştir. Son zamanlarda popüler olan yan kanal saldırıları ve benzeri saldırı teknikleri kullanılarak aktif dinleme araçları ile biyometrik veriler alınıp daha sisteme girilmeden başka kaynaklara gönderilebilir. Mevcut sistemde bu probleminde adreslenmediği gözlemlenmiştir.

Sistem üzerinde gözlemlenen bir diğer problem ise kötü niyetli sistem kullanıcılarıdır. Bu durumu daha yaygın bir diğer vaka üzerinden söyle açıklanabilir. Birçok kişinin kredi kart bilgileri bankada çalışan kötü niyetli kişiler tarafından üçüncü şahıslarla paylaşılmakta ve bu bilgilerle çeşitli suçlar işlenmektedir. Kötü niyetli kişiler her zaman her yerde olabileceği için bu tip bir saldırı senaryosu için de önlem alınmalıdır

3. Önerilen Yöntem

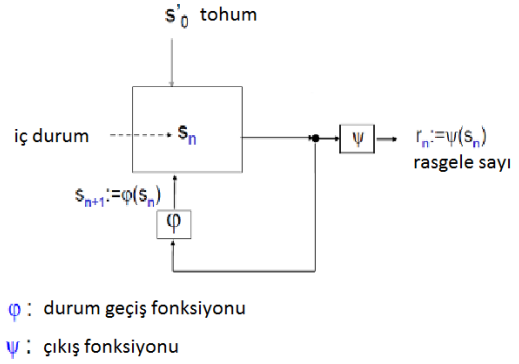
SGK biyometrik kimlik doğrulama sistemi aslında vergisini ödeyen yasaları önemseyen her

vatandaş için adil hizmet sunumu hedeflediği için önem teşkil etmektedir. Bu yüzden önerilen yöntemin mevcut sisteme uygulandığında kullanıcı verilerinin gizliliği ve güvenliğinin sağlandığı ispatlanabilir bir model ile garanti edilebilmelidir. Dolayısıyla kullanıcı ve hizmet verenler herhangi bir şüphe duymadan sistemi gönül rahatlığı ile kullanabileceklerdir.

Bu çalışmayı benzerlerinden ayıran yönü önerilen yöntemin kanıtlanabilir güvenlik yaklaşımını temel almasıdır. Bu özellik ile sistem kullanıcıları hiçbir şüphe duymadan sistemi kullanabileceklerdir [4].

Önerilen sistemin temel çalışma prensibi şifreli verinin sahibinin şifreleme algoritmasının anahtarına sahip olması prensibine ve biyometrik verilerin şifreli veri uzayında işlenmesi prensibine dayanmaktadır.Modern kriptolojide anahtar üretimi zorlu bir görevdir [5]. Çünkü Kerckhoff prensibine göre saldırganın şifreleme sistemi hakkında anahtar haricinde her şeye ulaşabildiği varsayımı altında sistemin ne kadar güvenli olduğu değerlendirilmektedir. Çalışmada ilk olarak güvenli bir anahtar üreteç algoritması geliştirilmiştir. Geliştirilen anahtar üreteci hibrit bir tasarım mimarisine sahiptir. Hibrit mimari gerekirci ve gerçek rasgele sayı üreteçlerini (RSÜ) birleştirmiştir [6-8]. Böyle bir tercih yapılmasının sebebi hem gerekirci RSÜ hem de gerçek RSÜ çeşitli problemler içermesidir. Bu problemleri gidermek için çeşitli hibrit tasarım mimarileri kullanılmaktadır. En yaygın biçimde kabul görmüş hibrit tasarım mimarilerinden biri Şekil 1'de gösterilen gerekirci RSÜ'nün her bir yeni rasgele sayı üretilirken bir gerçek RSÜ aracılığı ile tohum güncellemesi işleminin yapılmasıdır. Bu tasarım mimarisinin detayları için Kaynak [6] incelenebilir.

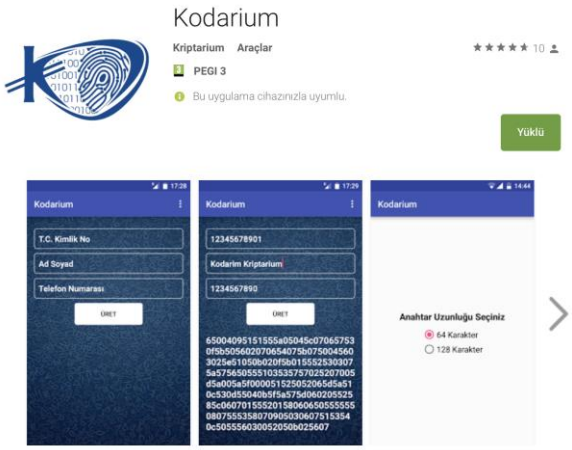
Bu çalışmayı diğerlerinden ayıran özellik ise gerçek RSÜ tasarımında fiziksel klonlanamaz fonksiyon (Physical Unclonable Function - PUF) teknolojisi kullanılmasıdır. PUF aygıta özgü bilgi veren, elde edilmesi basit olan fakat aygıt olmadan elde edilebilmesi pratik olarak imkânsız olan fiziksel rastgele fonksiyonlardır. Bu tanıma göre PUF'ın en önemli iki özelliği elde edilmesinin basit olması ancak aygıt olmadan elde edilmesinin çok zor olmasıdır [9, 10].



Şekil 1. Gerekirci RSÜ'nün genel tasarım mimarisi

PUF yapılarının oluşturulmasında mobil cihaz teknolojisinden yararlanılmıştır. PUF mantığını daha iyi anlayabilmek için aynı marka ve model iki akıllı cihazı göz önüne alalım. Bu iki cihaz ekran, kamera, hoparlör, mikrofon, flash hafıza gibi bire bir aynı bileşenlere sahiptir. Ancak bu bileşenler bire bir aynı olsa bile üretimden kaynaklanan çeşitli farklılıklar barındırmaktadır [9, 10]. Bu farklılıklara üretim değişkenliği (manufacturing variability) denilmektedir. Örneğin, kamera sensör matrisi karesel bir şekilde organize edilmiş ışığa duyarlı birkaç milyon fotosel sensörden oluşmaktadır. Her bir fotoselin ışık şiddeti ve rengine duyarlılığı farklılıklar gösterir ve bu da bir sensör matrisini diğerinden dolayısıyla bir kamerayı diğerinden ayırır. Çalışmada akıllı telefonların RAM verisi içerisinde bulunan anlık veriler kullanılarak ek girdi sağlanmaktadır. Burada elde edilecek eşdeğeri olmayan (unique) bir sayı gerekirci RSÜ kısmın yeniden tohumlanması sürecinde kullanılmaktadır. Teorisi yukarıda açıklanan mimari Android işletim sistemine sahip akıllı cihazlar için geliştirilmiş ve Android Market üzerinden kullanıma sunulmuştur [13]. Geliştirilen programa ilişkin ekran görüntüleri Şekil 2'de gösterilmiştir.

Programda her defa üret düğmesine basıldığında farklı farklı sayılar üretilecektir. Bu sayıların tahmin edilme olasılığı teorik olarak yoktur ve bu özelliği matematiksel olarak ispatlanabilmektedir. Önerilen yöntemin kanıtlanabilir güvenli olduğuna ilişkin detaylar için ayrıntılı olarak Kaynak [6] ve [11] incelenebilir.



Şekil 2. Geliştirilen algoritmanın ekran görüntüleri

4. Sonuç ve Öneriler

Bu çalışmada SGK biyometrik kimlik doğrulama projesinin barındırdığı problemlere dikkat çekilmiştir. Bu problemlerin adreslenmesi hem kişisel veri güvenliğinin sağlanması hem de kritik altyapılara yapılabilecek siber saldırıların önlenmesi açısından önem teşkil etmektedir. Bu kapsamda çalışmada iki temel çözüm önerisinde bulunulmuştur.

- Sistemin paydaşlarının bilinçlendirilerek bilgi güvenliği okuryazarlığının artırılması
- Doğrudan biyometrik veriler ile kimlik doğrulama yapmak yerine şifreli veri uzayında işlemlerin gerçekleştirilmesidir.

Şifreli veri uzayında güvenli kimlik doğrulama yapabilmek için güvenli bir anahtar üretecine gereksinim duyulmaktadır. Çalışmada güvenli anahtar üreteci olarak hibrit bir tasarım önerilmiştir. Önerilen hibrit tasarım ile hem gerekirci hem de gerçek rasgele sayı üreteçlerinin sahip olduğu çeşitli problemlerin önüne geçilmiştir. Çalışmada gerçek rasgele sayı üreteçlerinin gereksinim duyduğu entropi kaynağı olarak akıllı cihazların fiziksel klonlanamaz özellikleri kullanılmıştır.

5. Teşekkür

Bu çalışma Bilim Sanayi ve Teknoloji Bakanlığı, Teknogirişim Sermaye Desteği Programı 0167.TGSD.2015-2 numaralı proje kapsamında desteklenmiştir.

6. Kaynaklar

1. Veugen, T., Blom, F., Hoogh, S., Erkin, Z., (2015) Secure comparison protocols in the semi-honest model. IEEE J. Sel. Top. Signal Process.**9(7),** 1217–1228.
2. Beye, M., Erkin, Z., Lagendijk, L., (2011) in Proc. in IEEE Workshop on Information Forensics and Security (WIFS'11). Efficient privacy preserving k-means clustering in a three-party setting, pp. 1–6.
3. Erkin, Z., Veugen, T., Toft, T., Lagendijk, L., (2012) Generating private recommendations efficiently using homomorphic encryption and data packing. IEEE Trans. Inf. Forensics **Sec.7(3),** 1053–1066.
4. Katz, J., Lindell, Y., (2006) Introduction to modern cryptography : principles and protocols, Chapman & Hall.
5. Paar C., Pelzl J., (2010) Understanding Cryptography A Textbook for Student and Practitioners, Springer.
6. Ozkaynak, F., (2015), Kriptolojik Rasgele Sayı Üreteçleri, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, Cilt 8, **Sayı 2**, sayfa 37-44.
7. Schindler, W., Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators. www.bsi.bund.de/zertifiz/zert/interpr/ais20e.pdf
8. Márton, K., Suciu, A., Săcărea, C. and Creţ, O., (2012) Generation and testing of random numbers for cryptographic applications, Proceedings Of The Romanian Academy, Series A, Volume 13, Number **4/2012**, 368–377.
9. Suh, G., Devadas, S., (2007) Physical unclonable functions for device authentication and secret key generation, In Proceed- ings of the 44th annual Design Automation Conference , DAC '07, 9–14, New York, NY, USA
10. Guajardo, J., Kumar, S., Schrijen, G.-J. and Tuyls, P., (2007) Physical unclonable functions and public-key crypto for fpga ip protection, In Field Programmable Logic and Applications, International Conference on,189 –195.
11. Özkaynak F., (2014) Cryptographically secure random number generator with chaotic additional input, Nonlinear Dynamics (2014) **78** pp. 2015–2020.
12. http://www.kriptarium.com/galeri.html
13. https://play.google.com/store/apps/details?id=com.kriptarium.kodarium