Akıllı Kart ile Anahtar Güncellemeli 3-DES Algoritması Kullanarak Ön Ödemeli Sistem Uygulaması

Smart Card Based Pre-paid System Application Using Session Updated Key in 3-DES Algorithm

Musa ŞANLI, Fevzi ZENGİN, Oğuzhan URHAN

Elektronik ve Haberleşme Mühendisliği Bölümü
Veziroğlu Kampusü, Kocaeli Üniversitesi, 41040, İzmit/KOCAELİ
musanli@msn.com , f_zengin@hotmail.com , urhano@kou.edu.tr

Özetçe

Bu çalışmada simetrik anahtarlı bir şifreleme sistemi olan 3-DES (Data Encryption System) algoritması kullanılarak düşük maliyetli bir ön-ödemeli (pre-paid) sistem uygulaması geliştirilmiştir. Geliştirilen sistem, üzerinde donanımsal kod korumalı uygulama yazılımı koşan mikrodenetleyicili uçbirimler ve kullanıcılarında bulunan mikrodenetleyicili ve yine kod korumalı olan akıllı kartlardan (smart card) oluşmaktadır. Akıllı kart ile uçbirim arasında açılan her oturumda şifreli veri gönderimi için kullanılan 3-DES algoritmasının anahtarının belirli bazı bitleri, uçbirim ve akıllı kart tarafından üretilmektedir. Algoritmada kullanılan anahtarın bir kısmı ise sabittir ve hem uçbirimlere hem de akıllı kartlara önceden yüklenmiştir. Böylece her oturum için sadece o oturuma özel geçici bir anahtar üretilmiş olur. 3-DES algoritmasının tek başına kaba kuvvet atağı (brute-force attack) ile bile kırılması zayıf anahtarlar kullanılması dışında oldukça zorken, anahtarın her bir oturumda güncellenmesi ile üst seviye bir güvenlik sağlanmıştır. Geliştirilen uç birimin ve akıllı kartın donanımsal maliyetinin oldukça düşük olması sistemin en büyük avantajlarından biridir.

Abstract

A low-cost pre-paid system employing a symmetric key cryptosystem, namely 3-DES algorithm is developed in this work. The proposed system consists of terminals and smart cards that both contain code-protected microcontrollers. Certain bits of a 3-DES key are updated for each session between the smart card and the terminal. The constant part of the key is loaded to both the smart card and the terminal before utilization in the initialization stage. Thus, a unique key for each session is generated. While there is only a very small probability that the 3-DES can be broken by brute-force attack, the proposed system provides outstanding security. The low-cost of the proposed system is an important advantage.

1. Giriş

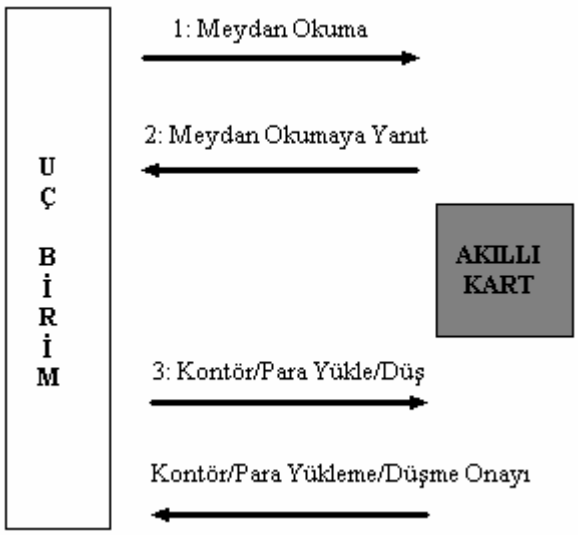
Ön ödemeli (pre-paid) sistemlerin hem kullanıcılar hem de ürün/hizmet sağlayıcılar için sağladığı kolaylıklar ile yaşamımızdaki yeri her geçen gün artmaktadır. Ön ödemeli sistemler ulaşım, telefon, doğalgaz gibi uygulamalarda yıllardır kullanılmaktadır. Türkiye'de İstanbul ve İzmir Büyükşehir belediyelerinin öncelikle ulaşım için kullandıkları AKBİL (AKıllı BİLet) ve Kent Kart sistemleri büyük bir başarı ile uygulanmaktadır. AKBİL sisteminde Dallas firması tarafından geliştirilen ve SHA-1 şifreleme sistemini kullanan iButton'lar kullanılmakta iken [1], Kent Kart sisteminde Motorola firması tarafından geliştirilen temassız (contactless) Mifare kartlar kullanılmaktadır. Bu sistem 2000 yılında "Sesame" taşımacılık ödülünü almıştır [2]. Bir ön ödemeli sistem olarak ele alınabilecek elektronik cüzdan uygulamasında ise bankalar hesap sahiplerine nakit para şeklinde kullanabilecekleri kartlar sağlamaktadırlar [3]. Bu tip ön ödemli uygulamalarda sunduğu esneklikler ve kullanım kolaylıkları ile akıllı kartların kullanımı daha yaygındır. Bir çok firma tarafından geliştirilen temaslı ve temassız akıllı kartlar mevcuttur. Temaslı akıllı kartlarda veri aktarımı için kartın kart okuyucu uçbirim ile fiziksel teması gerekmektedir. Bu durumda akıllı kart gerekli beslemeyi uçbirimden sağlamaktadır. Temassız akıllı kartlarda ise uç birime belirli uzaklıkta bulunan akıllı kart üzerindeki anten üzerinde indüklenen gerilim ile çalışmakta ve uçbirimle haberleşmektedir.

Bu çalışmada içerisinde 8-bitlik RISC mimarili PIC16F877 mikrodenetleyicisi ve 64kbitlik EEPROM bulunduran bir akıllı kart (Silver Card) ve yine PIC16F877 mikrodenetleyicisi kullanılan uçbirim kullanılarak genel amaçlı bir ön ödemeli sistem uygulaması gerçekleştirilmiştir.

2. Önerilen Ön Ödemeli Sistem

Bu çalışmada, belirli yükleme noktalarından şifreli veri haberleşmesi ile akıllı karta yüklenen kontör veya para bilgisinin satış veya uygulama noktasındaki uçbirimlerde yine şifreli olarak düşülmesine olanak sağlayan genel amaçlı bir ön ödeme sistemi geliştirilmiştir.

Uçbirim ile akıllı kart arasında yapılan şifreli veri haberleşmesi için temel olarak 3-DES algoritmasının kullanılması düşünülmüştür. Basit yer değiştirme ve mantıksal işlemlerin (logical operations) kullanıldığı bu simetrik anahtarlı şifreleme yöntemi yıllardır bir çok uygulamada kullanılmış ve hala bazı zayıf anahtarların kullanımı dışında oldukça güvenlidir. Bu şifreleme algoritmasında üç adet 56-bitlik anahtar kullanılmaktadır. Geliştirilen sistemde, önerilen anahtar güncellemesi ile toplam 168-bitlik bu anahtarın 48-bitlik kısmının her oturumda değiştirilmesi ileri sürülmüştür. Şifrenin değişen kısmının 24-bitlik kısmı uçbirim tarafından üretilirken, diğer 24-bitlik kısmı akıllı kart tarafından üretilmektedir. Uçbirim ile akıllı kart arasında yapılan şifreli veri haberleşmesi Şekil-1'de gösterilmektedir.



Şekil 1 : Uçbirim ile akıllı kart arasında açılan bir oturumda veri akışı

Bir akıllı kartın uçbirimle haberleşmek istemesi durumunda oluşacak veri akışı aşağıda açıklanmıştır. Akıllı kartın uçbirime takılması durumunda, kartın sisteme dahil olup olmadığını belirlemek üzere, uç birim tarafından 256-bitlik bir veri oluşturulur. Bu 256-bitlik veri içerisinde 192-bitlik meydan okuma verisi, 24-bitlik 3-DES anahtarının uçbirim tarafından üretilen kısmı ve 40-bitlik rasgele sayı bulunmaktadır. Bu 256-bitlik veri hem uç birim hem de akıllı kart tarafından bilinen bir sıralama ile akıllı karta aktarılır.

Sisteme dahil olan bir akıllı kartın, 192-bitlik meydan okuma verisini, bu mesajda gönderilen anahtar bilgisini ve kendi ürettiği 24-bitlik anahtarı kullanarak şifrelemesi beklenir. Uç birim tarafından yapılan meydan okumaya 192-bitlik meydan okumaya yanıt, 24-bitlik 3-DES anahtarının akıllı kart tarafından üretilen kısmı ve 40-bitlik rasgele veriden oluşan 256-bitlik veri paketi ile cevap verilir. Bu veri iletimi de önceden belirlenen bir sıralama ile yapılır.

Bu aşamada, akıllı kartın sistem geri dönüş mesajını oluşturulan yeni anahtara göre 3-DES ile şifreleyip geri göndermesi için 500ms'lik süre tanınmıştır. Bu süre içerisinde akıllı karttan geçerli bir yanıt gelmemesi durumunda ilgili oturum için haberleşme sona erdirilir ve uç birim 1s için bekleme konumuna alınır, böylelikle kaba kuvvet atağının önlenmesi hedeflenmiştir.

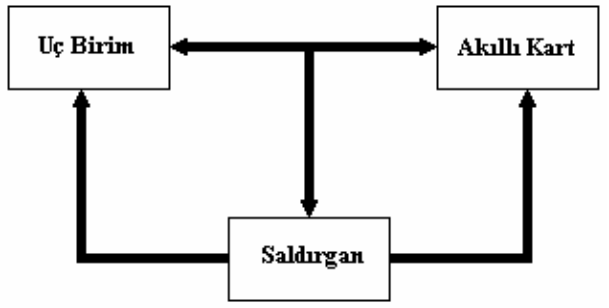
Uç birim, akıllı kart tarafından gönderilen meydan okumaya yanıtı aldığında öncelikle 3-DES anahtarının kart tarafından üretilen 24-bitlik kısmını çekerek 3-DES anahtarını oluşturur. Sonrasında bu anahtarı kullanarak meydan okuma verisine yanıtın şifresi çözerek gönderdiği veri ile aynı olup olmadığını kontrol eder. Verinin aynı olması durumunda kartın sistemde dahil olduğu kararına vararak komut/veri gönderme işlemlerine geçer. Aksi taktirde kartın sisteme dahil olmadığı kararına varılıp, oturum sonlandırılır ve uç birim yine 1s boyunca bekleme konumuna alınır.

Meydan okuma aşamasından sonra uçbirim tarafından, yüklenecek veya düşülecek kontör/para miktarı ve yükleme ve düşme bilgisi, yukarıda anlatılan şekilde oluşturulan 3-DES oturum anahtarı ile şifrelenerek oluşturulur. 192-bitlik bu verinin yanına 64-bitlik rasgele bir veri eklenerek oluşturulan 256-bitlik veri paketi akıllı karta yollanır.

Akıllı kart aldığı bu veriden 192-bitlik işlem bilgisini çekerek bu veriyi 3-DES kullanarak çözer. İşlem bilgisinde belirtilen kontör/para yükleme veya düşme işlemi yapıldıktan sonra bir sabit bir onay kodu oturum anahtarı kullanılarak 3-DES ile şifrelenir. Şifreli onay koduna 64-bitlik rasgele veri de eklenerek oluşturulan 256-bitlik veri uçbirime iletilir. Uç birim tarafından onay kodunun doğrulanması ile oturum başarı ile sonlandırılır.

2.1. Sistemin Güvenlik Değerlendirmesi

Bu çalışmada önerilen ön ödemeli sisteme yapılabilecek saldırılar uçbirim veya akıllı kartın çalışmasını taklit etmek şeklinde olabilir. Hem uç birimde hem de akıllı kartta kullanılan mikrodenetleyiciler program kodu koruma özelliğine donanımsal olarak sahip oldukları için program koduna ve dolayısıyla verileri şifreleme için kullanılan 3-DES anahtarının sabit kısmına erişim olanaksızdır. Aynı şekilde oluşturulan veri paketlerinde hangi bitlerin anahtarın değişen kısmını, hangi bitlerin 3-DES ile şifrelenmiş bilgiyi oluşturduğu ve hangi bitlerin 256-bitlik veriyi tamamlamak için rasgele üretildiği program kodları incelenmeden bilenemeyeceğinden ve bu program kodlar donanımsal olarak korunduğundan böyle bir olasılık da söz konusu değildir.



Şekil 2: Sisteme yapılabilecek saldırılar

Bu durumda sistemi yapılabilecek saldırılar kaba kuvvet saldırısı (brute force attack) ve seçilen veya bilinen açık metin saldırısı (chosen or known plaintext attack) olarak ele alınabilir. Saldırganın veri iletimi sırasında hattı dinleyerek bu şifreli verilere ulaşabildiği durum Şekil-2'de gösterilmektedir.

DES algoritmasının yeteri güvenliği olmadığı ve kaba kuvvet, bilinen veya seçilmiş açık metin gibi çeşitli saldırılara açık olduğu [4-5]'de bildirilmiştir. DES algoritması 1998 yılında EFF (Electronic Frontier Foundation) tarafından 220.000$'lık bir donanım ile kaba kuvvet atağı ile kırılmıştır. Bu noktada 3-DES'in de kırabileceği ileri sürülse de açık literatürde böyle bir çalışma bulunmamaktadır. B. Schneier tarafından 3-DES algoritmasının kırılmasının zorluğu "Bu galaksede 3-DES'i kaba kuvvet atağı ile kırabilecek kadar silikon veya güneş yok olmadan önce kırabilecek kadar zaman yok" ifadesi ile vurgulanmıştır [6]. DES algoritmasını 1 sn içerisinde kırabilen bir donanımın veya yazılımın 3-DES'i kırmasının 2 milyar yıldan fazla süreceği göz önüne alındığında 3-DES'in güvenliği açıkça ortaya çıkar [7].

Kaba kuvvet, seçilen ve bilinen açık metin saldırısı açısından önerilen anahtar güncellemeli sistemin güvenliği aşağıda incelenmiştir. 3-DES algoritmasında kullanılacak anahtarın bazı bitleri her oturumda değiştirildiğinden ve meydan okumaya karşılık 500ms içerisinde bir yanıt verilmesi gerektiğinden, donanımsal veya yazılımsal olarak akıllı kart taklit edilerek uçbirime yapılacak bir kaba kuvvet saldırısı

mümkün değildir. Benzer şekilde akıllı karta yapılacak bir kaba kuvvet saldırısında geçerli veri yapısının bilinmemesi nedeni ile akıllı karttan alınacak meydan okuma yanıtı uç birimi taklit eden sistem için bir anlam ifade etmeyecektir. İkinci aşamada akıllı karta gönderilecek komut ve bilgiler geçerli anahtar olmadan şifrelenmeye çalışılacağından, bu veriler akıllı kart için anlamsız bilgiler olarak ele alınacaktır. Bu açıdan geliştirilen sistemde hem uç birim hem de akıllı kart kaba kuvvet saldırısına karşı dayanıklıdır.

Bilinen açık metin saldırısında ise ilk olarak saldırgan akıllı karta yüklenecek veya düşülecek kontör/para miktarını bilmekte ve buradan yola çıkarak 3-DES ile şifrelenmiş veriyi kaba kuvvet saldırısı ile çözüp anahtarı elde etmeye çalışmaktadır. Ancak burada 256-bitlik veri yapısı bilinmediğinden hangi verilerin 3-DES ile şifrelenmiş veriler olduğunun anlaşılması mümkün değildir. Bu veri yapısı elde edilmesi mümkün olmamakla birlikte, olası böyle bir durumda anahtarların sabit kısımları bilinmediğinden 3-DES algoritmasının kırılması kaba kuvvet atağı ile oldukça zordur.

Başka bir bilinen açık metin saldırısı durumda ise saldırgan akılla karta kontör/para yükleme veya düşürme işini veri hattını dinleyip daha sonra taklit etmeye çalışabilir. Bu amaçla öncelikle uç birim tarafından yapılan meydan okumanın aşılması gerekmektedir. Sisteme dahil olmayan bir akıllı kartın yukarıda açıklandığı gibi meydan okumayı geçmesi mümkün değildir. Ancak böyle bir durumda bile 3-DES anahtarının belirli bazı bitleri her oturumda değiştiğinden bu şifreli verinin elde edilmesi bir anlam ifade etmemektedir. Çünkü bir sonraki oturumda uç birim ve akıllı kart tarafından rasgele üretilen 3-DES anahtarı ve üretilen diğer rasgele bilgiler aynı olmayacaktır. Dolayısıyla bu verinin elde edilmesi sistem açısından herhangi bir güvenlik açığı yaratmamaktadır.

Veri hattının dinlenerek uçbirim taklit edilmesi ise yine mümkün değildir. Çünkü oturum anahtarının belirli bir kısmı akıllı kart tarafından rasgele olarak üretilmektedir. Uç birim tarafından gönderilen meydan okuma verisi taklit edilse bile akıllı kartın meydan okumaya verdiği yanıttaki 3-DES anahtarının 24-bitlik kısmı değiştiğinden, uçbirim tarafından gönderilen kontör/para yükleme düşme bilgisi akıllı kart için herhangi bir anlam ifade etmeyecektir.

Yukarıda örneklerle açıklandığı gibi güvenli anahtar güncellemeli bu sistemin belirtilen saldırılarla aşılması olası görülmemektedir.

3. Sistemin Detayları

3-DES algoritmasında kullanılan anahtar aslında 56-bitlik üç anahtarın birleşimi ile oluşmaktadır. Anahtar güncelleme aşamasında her bir anahtarın farklı 16-bitlik kısmı rasgele olarak üretilmektedir. Böylece oluşturulan şifrelenmiş verinin 2^48=2.81e+14 farklı anahtarı üretebilmesi sağlanmış olur. Bu rasgele anahtarların üretilmesinde, uçbirimdeki mikrodenetleyicinin saat işaretine göre değeri değişen 8-bitlik ve 16-bitlik sayıcılar [8] ve her oturumda değeri belirli miktarda artan sayaçlar kullanılmıştır. Sayıcıların ve sayaçların değerleri her oturum sonrasında saklanarak sonraki oturumda sayıcıların kaldığı yerden başlaması sağlanmıştır. Böylelikle benzer anahtarların arka arkaya kullanılması olasılığı da oldukça azaltılmıştır. Anahtar üretiminde rasgele sayı üreteçleri kullanabilir ancak işlem yükü açısından sayıcıların ve sayaçların kullanılması tercih edilmiştir.

Şekil 3: Tasarımlanan ön-ödemli sistemde kullanılan uç birim

Uçbirim ile akıllı kart arasında yapılan veri transferi 256-bitlik paketler haline yapılmaktadır.256-bitlik bu bilgiler uç birim ve akıllı kart tarafından bilinen belirli bir sıra ile iletilmektedir.

3.1. Kullanılan Uç Birim ve Akıllı Kart Donanımı

Daha önce de belirtildiği uç birim ve akıllı kartta Microchip firması tarafından geliştirilen PIC16F877 mikrodenetleyicisi kullanılmaktadır. Şekil-3'de görüldüğü gibi uç birimde PIC16F877 mikrodenetleyicisi ve LCD kullanılmıştır.

Akıllı kartta bu mikrodenetleyiciye ek olarak 64kbitlik bir EEPROM bulunmaktadır. Bu EEPROM'a genel kullanıma açık kimlik bilgileri yüklenmiş ve bu bilgiler kartın terminale sokulduğu ilk anda şifresiz şekilde uçbirime gönderilmiştir. Geliştirilen sistemde kullanılan akıllı kartın dış görünüşü Şekil-4'de verilmektedir.

Uç birim üzerinde bilgisayar türü sunuculara veri aktarımı için RS-232 seri port bağlantısı da mevcuttur. Böylelikle birkaç yüz metre alan içerisinde bir ana bilgisayara veri aktarımı mümkündür. Ancak bu durumda bir ana bilgisayara aynı anda birden fazla uç birim bağlanmaz. Bu sorunu aşmak için RS-485 protokolü kullanılabilir. Böylelikle birden fazla uçbirim bir ana bilgisayara aynı anda bağlanabilir.

Şekil 4: Kullanılan akıllı kartın dış görünümü

Uç birimler ana bilgisayara sürekli veri göndermesinin gerekmediği durumlar için uç birimlerin yazılımına çevrim-içi (on-line) ve çevrim-dışı (off-line) çalışma seçenekleri eklenebilir. Böylelikle normal şartlarda çevrim dışı çalışan terminal verileri aktarması gerektiğinde ana bilgisayara bağlanır.

4. Sonuç ve İleriki Çalışmalar

Bu çalışmada, 3-DES algoritması kullanılan ön ödemeli bir sistem, kullanılan akıllı kartlar ve tasarımlanan uç birim donanımı ile oldukça düşük bir maliyetle gerçekleştirilmiştir. Geliştirilen sistemde kullanılan kırılması hayli zor olan 3-DES algoritmasının saldırılara karşı dayanıklılığını artırmak için anahtar güncellemesi önerilmiştir. Anahtar güncellemesine ek olarak kartın sisteme dahil olup olmadığının belirlenmesi de sistemin güvenliğini artırmaktadır. Tasarımlanan uçbirimin donanımsal maliyeti 20$'ın altında, bir akıllı kartın maliyeti ise birkaç dolar civarındadır. 2 sn civarı süren oturumun 1sn'nin altında gerçekleştirebilmesi için kaynak kodunun optimizasyonu üzerinde çalışılmaktadır.

5. Kaynakça

[1] Maxim/Dallas Firmasının Web Sitesi : www.maxim-ic.com

[2] Business Wire, Oct 25, 2000. http://www.findarticles.com/p/articles/mi_m0EIN/is_2000_Oct_25/ai_66321793

[3] ST Microelectornics, Smartcard Solutions, E-Purse References, http://www.st.com

[4] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", John Wiley & Sons Inc., 1994.

[5] A. Menezes, P. Van Oorschot, and S. Vanstone, **Handbook of Applied Cryptography**, CRC Press, 1996.

[6] B. Schneier, "A Hardware DES Cracker", Crypto-Gram Newsletter, 15 August 1998.

[7] O. Urhan, F. Zengin ve M. Şanlı, "DES Algoritması Kullanılan Akıllı Kart ile Güvenlik Sistemi Tasarımı ve Uygulaması", Otomasyon Dergisi, pp. 84-88, Eylül 2004.

[8] O. Urhan ve M.K. Güllü, "Her Yönüyle PIC16F628", Birsen Yayınevi, İstanbul, 2004.