AKBİL ve GÜVENLİK

Oğuzhan Urhan

Elektronik ve Haberleşme Mühendisliği Bölümü
Kocaeli Üniversitesi
urhano@kou.edu.tr

ÖZET

Bu yazıda, Dallas Semiconductor/Maxim tarafından üretilen ve İstanbul Büyükşehir Belediyesi (İBB) tarafından AKıllı BİLet (AKBİL) uygulamasında kullanılan DS1991 ve DS1963s adlı donanımların güvenliği hakkında bilgi verilecektir. Hala kullanımda olan DS1991 modelinin önemli bir güvenlik açığından ve DS1963s ile buna karşı alınan önlemlerden bahsedilecektir. Son olarak DS1963s'yi kaba kuvvet atağı ile kırmanın maliyeti ele alınacaktır.

1. GİRİŞ

Paranın elektronik ortamda elektronik bir cüzdanda (e-purse) saklanması fikri üzerinde yıllardır çalışılmaktadır. Bu çabaların temel hedefi doğrudan para yerine geçebilecek fakat kullanımı daha kolay olan bir ödeme aracı geliştirebilmektir. Böylelikle hem hizmet sağlayanlar hem de hizmeti kullananlar için büyük kolaylıklar sağlanabilir. Örneğin bir ödeme çok kısa bir sürede gerçekleştirilebilir, bozuk para gibi sorunlarla karşılaşılmaz ve daha önemlisi sahte para/bilet kullanımının önüne geçilebilir. Ancak gerekli güvenlik önlemlerinin alınmaması durumunda paranın elektronik olarak kopyalanması fiziksel olarak kalpazanlık yoluyla kopyalanmasından daha kolaydır.

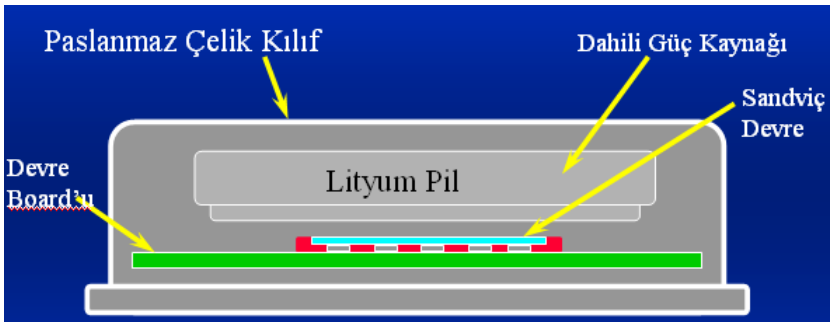
Elektronik cüzdan uygulamalarında genellikle akıllı kart adı verilen ve temel olarak içerisinde bir mikrodenetleyici barındıran kartlardan yararlanılmaktadır. Temaslı, temassız (contactless) ve karma (hybrid) olmak üzere üç tip akıllı karttan bahsedilebilir. Temaslı akıllı kartlarda veri aktarımı için okuyucu terminal ile kartın fiziksel teması gerekmektedir. Veri fiziksel bağlantı ile kurulan hat üzerinden aktarılır. Temassız kartlarda ise terminal ile kartın fiziksel temasına gerek bulunmamaktadır. Akıllı kartlara karşı farksal güç analizi ve basit güç analizi temelli saldırılar bulunmaktadır. Ayrıca bu tip kartların fiziksel saldırılara da açık olduğu ifade edilmektedir [1].

Temassız kartların bir diğer önemli açığı ise yeniden yönlendirme saldırısına karşı (relay attack) dayanıksız olmasıdır. Bu saldırıda amaçlanan başkasına ait bir kartı geçiş noktasında kart sahibinin haberi olmadan kullanmaktadır. Yeniden yönlendirme saldırısında temel olarak saldırıyı gerçekleştiren kişi, terminal ile akıllı kartmış gibi haberleşirken (konuşurken), akıllı kartla terminalmiş gibi haberleşmektedir. Bu saldırıda temassız akıllı kartların veri iletişimine geçmesi için gerekli enerjiyi terminalden almasından yararlanılmaktadır. Bu açık halihazırda İzmir, Manisa, Denizli ve Adana'da kullanımda olan Kentkart sisteminde kullanılan Mifare adlı kartlarda da bulunmaktadır [1].

Akıllı kartlar ayrıca fiziksel etkilere açık olduklarından dayanıklı oldukları söylenemez. Özellikle cüzdanda taşındıkları düşünüldüğünde bir akıllı kartın ortalama ömrünün birkaç yıl

olduğu söylenebilir. Kullanıcı sayısının yüksek olması durumunda kart maliyeti önemli bir sorun olmaktadır [2].

Ülkemizde elektronik cüzdan amaçlı kullanılan diğer bir donanım ise İstanbul'da yaklaşık 3 milyon kişinin kullandığı AKBİL adı verilen "iButton"lardır. "iButton"lar güçlü bir dış kılıfa sahiptir ve bir kart gibi fiziksel hasarlara karşı korumasız değildir. Çarpma, su ile temas gibi olası durumlarından etkilenmez ve içindeki veriyi 10 yıldan fazla bir süre saklayabilir. Şekil 1'de "iButton"un fiziksel iç yapısı gösterilmektedir.



Şekil 1. Bir iButton'un fiziksel iç yapısı

İBB tarafından uygulanan AKBİL sisteminde DS1991 ve DS1963S model numaralı "iButton"lar kullanılmaktadır. Önceleri sadece DS1991 kullanılmaktayken sonrasında daha yüksek güvenlik için DS1963s kullanılmaya başlanmıştır [3]. Ancak güvenlik açığı içeren DS1991 hala kullanımdadır. İleriki bölümlerde DS1991'in güvenlik açıklarından bahsedilecek ve DS1963s ile bu açıkların nasıl kapatıldığına değinilecektir.

2. DS1991

DS1991 temel olarak "subkey" adı verilen 48 bayt'lık 3 adet hafıza bölgesi içermektedir. Bu hafıza bölgeleri veri saklama amaçlı kullanılabilir. 48 bayt'lık her hafıza bölgesi 8 bayt'lık bir şifre ile korunmaktadır. İstenilen bellek bölgesinin okunabilmesi için terminal tarafından DS1991'e doğru şifrenin iletilmesi gerekmektedir. Şifrenin DS1991 tarafından doğrulanması ile bu gizli veri terminale aktarılabilir. Şifrenin yanlış olması durumunda ise DS1991 "rasgele" bir sayı üretir. Böylelikle şifre tahmini engellenmeye çalışılmaktadır.

8 bayt'lık şifrenin kaba kuvvet atağı ile bütün olasılıklar denenerek kırılması hayli zordur. Bunun en temel nedeni ise DS1991 ile yapılacak haberleşme için en az 120ms gerekmesidir. Bu temel olarak DS1991'de kullanılan tek hatlı (1-wire) haberleşme protokolünün getirdiği bir sınırlamadır. Basit bir hesapla bütün olası şifreleri denemenin milyonlarca yıl zaman alacağı bulunabilir. Bu yaklaşımla DS1991'in güvenli olduğu düşünülebilir.

Yukarıda yanlış bir şifrenin DS1991'e iletilmesi durumunda, DS1991'in rasgele bir veri üreteceğinden bahsedilmişti. Ancak [4]'de üretilen sayının rasgele olmadığı ifade edilmektedir. Aslında basit bir yaklaşım kullanılarak rasgele sayı üretiliyor izlenimi sağlanmıştır. DS1991'in belleğinde 256 adet 48 baytlık sabit veri tutulmaktadır. Bu sabit veri "rasgele" olduğu ifade edilen verinin üretilmesine kullanılmaktadır. Denenen şifrenin her bir karakterine karşılık gelen 48 baylık veriler birer bayt kaydırılarak alt alta dizilmektedir. Sonrasında bu veriler özel-veya (EX-OR) işlemine tabii tutularak "rasgele" veri üretilmektedir. Ancak bu verinin rasgele olmayacağı açıktır. Bu önemli bir açığı beraberinde getirmektedir.Yani denenen şifre için, şifrenin yanlış olması durumunda DS1991'in vereceği

yanıt önceden hesaplanabilir. Böylelikle şifreler denenirken doğru şifrenin denenip denenmediği kolaylıkla tespit edilebilir. Ancak doğru şifrenin bulunması için yine kaba kuvvet atağının kullanılması zaman açısından mümkün değildir. Bu gibi durumlarda genellikle sözlük saldırısı (dictionary attack) adı verilen bir yöntem kullanılmaktadır. Yani binlerce aday şifreden oluşan bir sözlük kullanılarak bütün adayların sırasıyla denenmesi ile yaygın kullanılabilecek şifreler kolaylıkla bulunabilir. Bunun önüne geçmek için alınabilecek önlemlerden biri tahmin edilmesi güç bir şifre kullanmaktır.

DS1991 ile ilgili aslında daha büyük bir sorun bulunmaktadır. Bu sorun DS1991'den verinin okunması için ilgili şifrenin hatta basılması gereğinden kaynaklanmaktadır. Terminal ile DS1991 arasından gerçekleşen iletişimi dinleyen biri şifreyi kolaylıkla ele geçirebilir. Böylelikle en azından daha önce "iButton"a yüklenen parayı defalarca yükleyebilir. Bu DS1991'in yapısından kaynaklanan ve bir çözümü bulunmayan bir açıktır.

3. DS1993

DS1963s, Türkiye'deki AKBİL projesi başta olmak üzere Arjantin ve Brezilya gibi birçok ülkede de e-cüzdan amaçlı çeşitli uygulamalarda kullanılmaktadır. Sağladığı yüksek güvenlik bir çok özel şirket bu iButton'u erişim kontrolü amacı ile de kullanmaktadır. DS1963s'nin temel özellikleri aşağıda listelenmektedir [5].

- Kimlik ve veri doğrulama amaçlı kullanılacak dahili SHA-1 (Secure Hashing Algorithm) birimi içerir.
- 7 farklı uygulamaya aynı anda hizmet verebilir.
- Saldırılardan korunmak üzere üstün güvenlik mekanizmalarına sahiptir.

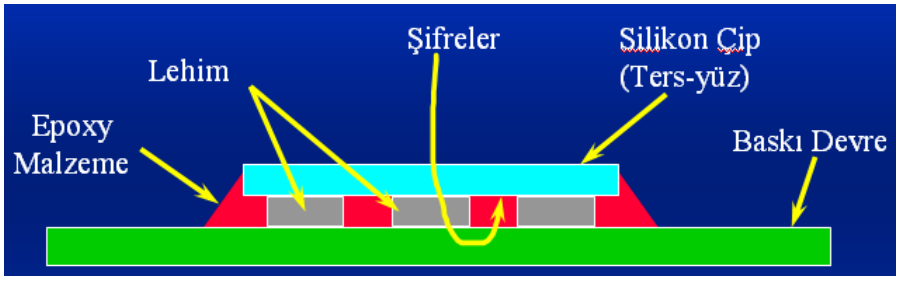
Bu noktada DS1963s'nin sağladığı üstün güvenlik mekanizmaları aşama aşama ele alınarak yapılacak bütün olası saldırılara karşı ne şekilde yanıt verileceğinden bahsedilecektir. DS1963s'in DS1991'den en büyük farklarından biri veri okuma/yazma işlemi sırasında hatta kesinlikle şifrenin kullanılmamasıdır.

E-cüzdan uygulamasının başlangıç aşamasında öncelikle kullanılan DS1963s'nin sistem dahil olup olmadığının güvenli şekilde kontrol edilmesi gerekmektedir. Kimlik doğrulama amaçlı kullanılabilecek en temel yol, kimliğini doğrulatmak isteyen kişiye önceden belirlenen bir şifreyi sormaktadır. Eğer kişi sistem dahilse şifreyi söyler ve böylelikle sisteme dahil olduğu anlaşılır. Ancak bu durumda şifrenin başkaları tarafından da dinlenmesi ve ele geçirilmesi mümkündür. Dolayısıyla doğrudan şifre sorularak kimlik doğrulaması yapmak güvenli bir yol değildir.

Sisteme dahil olup olmama durumlarını kontrol etmek amacı ile kriptolojide (şifreleme-bilimi), "**meydan okuma ve meydan okumaya yanıt**" (challenge&response) adı verilen bir yöntem yaygın olarak kullanılmaktadır. Bu kimlik doğrulama yönteminde karşı tarafa rasgele bir sayı gönderilmekte ve önceden belirlenen bir işlemi yapıp, sonucunu geri bildirmesi istenmektedir. Bu esnada kimliği kontrol etmek isteyen taraf da aynı işlemi yapar ve karşı taraftan yanıt beklemeye başlar. Eğer karşı taraf yapılacak işlemi biliyorsa bu işlemi yapıp sonucu söyler, sonuç tutuyorsa kişinin sisteme dahil olduğu anlaşılır. Bu durumda birisi konuşulanları "dinliyor" olsa bile, kimlik doğrulamak isteyen kişi her seferinde farklı bir rasgele sayıyı göre işlem yapılmasını isterse dinlediği verilerin anlamı olmayacaktır. Yani sadece yapılan bu "**özel işlemi**" bilen kişilerin kimliği doğrulabilir.

DS1963s kimlik doğrulama amacı ile içerisinde dahili olarak bulunan SHA-1 birimini kullanmaktadır. Güçlü bir özetleme (hashing) yöntemi olan SHA-1, özellikle "elektronik imza" uygulamalarında gönderilen bilginin gerçekten o kişi tarafından gönderilip gönderilmediğini kontrol etmek amacı ile yaygın olarak kullanılmaktadır. SHA-1 temel olarak kendisine giriş olarak verilen büyük miktardaki verilerin kısa bir özetini çıkartmaktadır. Bu özet giriş verisindeki küçük bir değişiklik durumunda bile aşırı miktarda değişmektedir. SHA-1'in ayrıca farklı veriler için aynı özetin oluşturulma ihtimali de yok denecek kadar azdır (collision resistant). Bu nedenle veri özetleme için güvenle kullanılmaktadır.

DS1963s ile kimlik doğrulama için terminalden iButton'a rasgele bir sayı gönderilir. Sistem dahil olan iButton'nun gönderilen rasgele sayıyı, yüklü olan veri (para) ve kendisine daha önceden yüklenen şifreyle birlikte özetleyip geri göndermesi beklenir. Bu sırada terminal de o iButton'a özel oluşturduğu şifre ile özetle işlemini gerçekleştirir (Terminal DS193s'nin ROM–ID bilgisini kullanarak onun kullandığı kimlik doğrulama şifresini elde etmektedir). Eğer iButton tarafından gönderilen özet, terminalin hesapladığı özet ile aynı ise buradan o iButton'un kimlik doğrulama şifresini bildiği ve sisteme dahil olduğu kararı verilmektedir. Şifreyi bilmeyen bir iButton özetleme işlemini doğru yapamayacağı için kimlik doğrulama aşamasını geçemeyecektir. Bu noktada DS1963s'de bulunan şifrenin güvenli şekilde saklanması oldukça önemlidir. Bu şifrelerin fiziksel olarak güvenli şekilde saklanması için Şekil 2'de gösterilen sandviç devre yapısı kullanılmaktadır. Ayrıca RAM'de tutulan bu şifrelerin bulunduğu bellek gözleri sadece yazılabilir özelliktedir. Böylelikle şifrenin dışarıdan okunmasının da önüne geçilerek güvenlik bir kimlik doğrulaması gerçekleştirilmiştir.



Şekil 5. Sandviç devre yapısı

Kimlik doğrulaması ile sisteme dahil olmayan kullanıcıların sistemi kullanması engellenmiştir. Ancak sisteme dahil olan kullanıcılar (yani AKBİL/iButton sahipleri), sahip oldukları iButton'a illegal yollardan veri (para) yüklemeye çalışabilir. DS1963s'nin veri saklama amaçlı bellek bölgeleri, okumaya ve yazmaya açık olduğundan kötü niyetli kişiler bu bölgelerdeki verileri değiştirebilirler. Bu nedenle sadece kimlik doğrulması ile birlikte önceden sistem tarafından yüklenen paranın değişmediğinin doğrulanması da gerekmektedir. Bu işlemin yapılmaması durumunda sisteme dahil bir iButton'daki veri diğer iButton'lara yüklenip, sistemde açığa neden olunabilir. Bunu engellemek üzere DS1963s'nin bazı bellek bölgelerinde yazma sayacı (write counter) bulunmaktadır. Veri (para) bu bellek bölgelerine yazılmakta ve bu yazma sayacı kimlik doğrulama aşamasında kullanılan verinin içerisine dahil edilmektedir. Böylelikle bu veriden çıkarılacak özetle hem kimlik doğrulaması yapılmakta hem de iButton içerisindeki verinin sistem dışından başka biri tarafından değiştirilmediği garanti altına alınmaktadır. Veri bütünlüğünün bozulmadığını kontrol etmek için yazma sayaçlarına kullanıldığından bu sayaçların sadece okunabilir olması gerekmektedir. 32-bitlik bu sayaçlar ile 2 milyar üzerinde işlem yapılabilir. 32-bitlik sayma sonucu sayaçlar yeniden sıfıra dönmediğinden, paranın değiştirilmesi anında sayaçtaki veri

tekrar aynı değeri alamaz. Dolayısıyla verinin sistem dışından değiştirilmesi durumunda bu kolaylıkla anlaşılabilir.

Bu aşamadan sonra hizmet karşılığı olan paranın iButton'dan düşülmesi ve kalan paranın tekrar iButton'a yazılması gerekmektedir. Terminal kimlik doğrulama aşamasında aynı zamanda paranın da değiştirilmediğini doğruladığından artık iButton'da yüklü olan paraya güvenip, o para üzerinden işlem yapabilir. Bu noktada okunan para üzerinden hizmet bedeli düşülür ve bu yeni para miktarına göre yeniden özetleme yapılır. Elde edilen özet de orijinal veri (para) ile birlikte iButton'a yazılır. Ancak bu noktada veri yazılmadan önce iButton okuma yuvasında kasıtlı olarak veya yanlışlıkla çekilebilir. Verinin iButton'a doğru şekilde yazıldığını doğrulamak için bu kez iButton'dan yeni yazılan veriyi kendine özel şifresi ile özetleyip göndermesi istenir. Eğer bu özet de doğruysa veri (kalan para) iButton'a sorunsuz şekilde yazılmış demektedir. Böylelikle sisteme dahil olan iButton'dan hizmet bedeli güvenli şekilde düşülüp, kalan para miktarı yine güvenli ve sistem dışından herhangi bir şekilde değiştirilemeyecek biçimde tekrar iButton'a yazılmış olur.

2005 yılı başlarında Bruce Schneier, Çinli bir araştırma grubunun SHA-1 özetleme yöntemini kırıldığını duyurup [6] ve artık daha güvenli özetleme yöntemlerinin kullanılması gerektiğini ifade etmiştir [7]. Aslında Çinli araştırmacı grubun yaptığı farklı metinlerin benzer bir özet çıkarabileceğinin kaba kuvvet atağından daha kısa sürede gerçekleştirilebileceğini gösterilmesidir [8]. Yani bu açık sayesinde özet veriden orijinal verinin geri elde edilmesi mümkün değildir.

DS1963'de özetleme işlemi için SHA-1 kullandığı için bu açıktan etkilenebileceği düşünülebilir. Dallas Semiconductor/Maxim kısa bir süre sonra bu açıkla ilgili bir uygulama notu yayınladı [9]. Bu uygulama notunda açıkça ifade edildiği gibi bunun tek yolu kullanılan şifrenin bilinmesidir. Bu şifre yukarıda bahsedildiği gibi yüksek güvenlikle korunduğundan SHA-1'in bu açığının DS1963s'i etkilemeyeceği açıktır.

Kaba kuvvet atağı ile 819 gigaflops (floating point operations per second) işlem güçüne sahip 64 işlemcili Cray X1 süper bilgisayarı bu şifreyi yaklaşık 12.5 yılda elde edebildiği üretici Dallas firması tarafından ifade edilmektedir [9]. Standart bir Intel Xeon işlemci 5-6 gigaflops işlem gücüne sahiptir ancak yakın zamanda İngiliz ClearSpeed Technology firması tarafından geliştirilen ve PCI-X slota takılan bir kart ile standart bir PC'nin işlem gücü 50gigaflops artırılabilmektedir [10]. Bir kartın maliyetinin en fazla 10.000$ olacağı öngörülmektedir. Bu durumda en fazla yaklaşık 2 milyon dolarlık bir yatırımla DS1963s'in kaba kuvvet atağı ile 1 yılda kırılabileceği kolaylıkla hesaplanabilir. Dolayısıyla DS196s adlı "iButton"ların da yakın gelecekte artık çok güvenli olmadığı söylenebilir.

4.SONUÇ

Bu yazıda AKBİL sisteminde kullanılan DS1991 ve DS1963s adlı "iButton"ların güvenlik analizi yapılmıştır. AKBİL sisteminde halen kullanımda olan DS1991'in önemli güvenlik açıklarına değinilmiş ve DS1963s'de buna karşı alınan önlemlerden bahsedilmiştir. Ayrıca yakın zamanda güvenliğinden şüphe duyulmaya başlanan SHA-1 özetleme tekniğinin "iButton"lar üzerindeki etkisi değerlendirilmiştir. Son olarak kaba kuvvet atağı ile DS1963s'in güvenliğinin aşılmasının maliyeti ele alınmıştır.

KAYNAKLAR

[1] O. Urhan, "Temassız Akıllı Kartlara Pratik Bir Saldırı," Otomasyon Dergisi, pp. 116-119, Ocak 2006.
[2] http://en.wikipedia.org/wiki/Smart_card
[3] http://www.belbim.com.tr/
[4] http://www.grandideastudio.com/files/security/tokens/ds1991_ibutton_advisory.txt
[5] http://pdfserv.maxim-ic.com/en/ds/DS1963S.pdf
[6] http://www.schneier.com/blog/archives/2005/02/sha1_broken.html
[7] http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html
[8] http://theory.csail.mit.edu/~yiqun/shanote.pdf
[9] White Paper 9: Are SHA-1 Devices Still Secure Enough? http://www.maxim-ic.com/appnotes.cfm/appnote_number/3522
[10] "A Desktop Super Computer", IEEE Spectrum Magazine, pp. 52, January 2006. http://www.spectrum.ieee.org/jan06/2594/4