Elektronik Seçim: Norveç'in İnternet Üzerinden Oylama Sistemi ve Kriptografik Altyapısı

Mehmet Sabır KİRAZ, Fatih BİRİNCİ, Uğur Kaşif BOYACI

***Özet*—Bu çalışmada internet tabanlı elektronik seçimi uygulayan iki ülkenin seçim protokolü anlatılacaktır: internet üzerinden e-Seçim'i ülke çapında ilk defa uygulayan ülke Estonya ve ikinci uygulayan ülke Norveç. Yazıda ayrıca genel olarak internet tabanlı elektronik seçimlerin güvenliğini analiz edeceğiz ve elektronik seçimler ile ilgili özgün bir risk analizi sunacağız. Sonuç bölümünde ise Türkiye için bazı tavsiyelerde bulunacağız.**

***Anahtar Kelimeler*—Elektronik seçim, Eşik şifreleme sistemleri, Homomorfik şifreleme**

***Abstract*—In this work, we present the Internet-based electronic voting protocols of two countries: Estonia, the first country that used internet based voting and Norway, the second country that used internet based voting for the local elections at the end of 2011. We discuss the security of an Internet based voting scheme in general and give a detailed risk analysis. We conclude this paper by giving some recommendations for Turkey.**

***Keywords*—Electronic voting, Threshold cryptosystems, Homomorphic encryption**

I. Elektronik Seçim ve Kriptografi Kullanımı

Oy verme ve/veya oy saymanın elektronik olarak yapıldığı seçimlere elektronik seçim ya da kısaca e-Seçim denir. Elektronik seçim sistemi bilgi güvenliğinden insan psikolojisine, kriptolojiden hukuka kadar birçok konuda çözüm gerektiren sorunlar barındırır [1], [2], [3], [4]. Kriptografi açısından birbirleri ile neredeyse zıt farklı isterler aranmaktadır. [1], [5]'de elektronik seçim sistemlerinin sağlaması beklenen güvenlik özellikleri hakkında detaylı bilgi bulabilirsiniz. Farklı güvenlik beklentileri, farklı ödünleşimler ve farklı kriptografik teknikler sayesinde çok farklı elektronik seçim mekanizmaları tasarlamak, hatta kağıt tabanlı seçimlerde sağlanmayan bazı özellikleri sağlayan sistemler bulmak mümkündür. [6], [7], [8], [9].

Bu yazıda internet üzerinden yapılan iki e-Seçim sistemi (i-Seçim) incelenecek, e-Seçim ile ilgili kapsamlı ve özgün bir risk analizi sunulacaktır.

A. İnternet tabanlı seçim sistemleri (i-Seçim)

İ-seçim sayesinde oyumuzu seçim zamanı süresince istediğimiz saatte, sıra beklemeden, istediğimiz yerden hatta yurtdışından kullanabiliriz. Sandık başına gelmesi çok müşkül engelli seçmenlerin oy kullanabilmeleri sağlanabilir. Diğer yandan, kullanıcılar alışkanlık kazandıkça seçim otoritelerinin yükü azalacak, oylar çok daha hızlı ve zahmetsiz sayılacak ve seçim maliyetleri tahminen çok düşecektir. [10] Bu yazımızda Estonya ve Norveç'in i-Seçim uygulamalarını inceleyeceğiz. Kullanılan kriptografik yöntemler kısaca anlatılacak ve sistemlerin analizleri verilecektir.

Bu çalışma kısmen Akıllı Kart Tabanlı Elektronik Kimlik Doğrulama Sistemi ve TC Kimlik Kartı Geliştirme Projesi tarafından desteklenmiştir.

M. S. Kiraz, F. Birinci ve U. K. Boyacı TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Ensistüsü'nde çalışmaktadır, e-posta: {m.kiraz, ukasif, fatih}@uekae.tubitak.gov.tr

II. Estonya'da İ-seçim

Estonya, nitelikli imza fonksiyonu içeren akıll vatandaşlık kartının mecburi olduğu ilk ülkedir ve kamu hizmetlerinin neredeyse tamamı internet üzerinden verilmektedir [11].

Estonya, 2005 yerel seçimleri ile birlikte internet yoluyla ülke çapında vatandaşlarına oy kullandıran ilk ülke oldu. 2011 genel seçimlerine kadar i-seçmen katılımcıların oranı ülke genelindeki her yeni seçimde artarak %2'lerden %24'lere vardı [12]. Estonya seçim protokolünün ana adımları aşağıda verilmiştir.

A. Estonya i-seçim sistemleri adımları

1) Seçmen, kurumsal bir e-seçim sitesine girer ve elektronik kimlik kartı vasıtasıyla kimliğini doğrulatır. İstemci uygulamasını siteden indirir.
2) İstemci uygulaması, seçmeni Oy Yönlendirme Sunucusu'na (OYS) bağlar.
3) OYS, kimlik doğrulamasının ardından seçmene aday listesini gönderir.
4) Seçmen, listeden bir aday seçer. İstemci uygulaması, OYS'nin açık anahtarını kullanarak seçmenin oyunu şifreler.
5) Seçmen, imza özel anahtarını kullanarak şifreli zarfı imzalar ve OYS'ye yollar.
6) OYS, seçmenin oyunu Oy Depolama Sunucusu'na (ODS) gönderir.
7) ODS, Açık Anahtar Altyapısı (AAA) sistemi ile iletişim kurar ve seçmen kimliğini doğrulatır. Oyu veritabanına kaydeder ve OYS'ye onay gönderir.
8) OYS, istemciye (seçmene) oyun başarılı olduğunu gösteren onay bilgisini gönderir.
9) Oy kullanma süresi bitiminde ODS oyları sıralar ve mükerrer oyları veya klasik yolla oy kullanan i-seçmenlerin oylarını iptal eder.

10) ODS, farklı kesimlerden gelen gözetmenlerin izlediği bir prosedürle oyların üzerindeki elektronik imzayı kaldırır.
11) ODS personeli, tüm şifreli oyları çevrimdışı bir kanaldan Oy Sayım Sunucusu'na (OSS) taşır.
12) OSS asimetrik şifreleme özel anahtarı daha önceden farklı yetkililere dağıtılmıştır. Özel anahtar eşik sır paylaşımı yoluyla tekrar oluşturulur. OSS, şifreli oyların şifresini çözer.
13) OSS yetkilileri açılan oyların sayımını yapar ve seçim sonucu üretir.
14) Sistemde anlık bilgi kayıtları tutulmaktadır. Kayıt bilgileri gözetmenler tarafından incelenerek güvenlik ihlalleri tespit edilir.

III. Norveç'te 2011'de Uygulanan İ-seçim Sistemi

Birçok kritere göre dünyanın en gelişmiş ülkelerinden biri olan 4,9 milyon nüfuslu Norveç'in nüfusun %95'i internet kullanmaktadır. Dolayısıyla i-Seçim'e en hazır ülkelerden biri olduğu söylenebilir. Yine de Avusturya gibi gelişmiş bir ülkede yaşanan olumsuz tecrübeler, Norveç hükümetini daha temkimli davranmaya yöneltmiştir.

A. Avusturya Deneyimi, Norveç e-Seçim Hazırlıkları

Avusturya'da sistemin kriptografik bazı detaylarının topluma açıklanmamasından dolayı medyada az sayıda kişi tarafından dile gettirilen fakat çok ses getiren eleştiriler yer almış ve halkın e-Seçim'e güveni azalmıştır. Avusturya hükümeti bunun üzerine sistem kaynak kodunu gönüllü katılımcı uzmanlardan oluşan bir gruba kısmen açmışsa da, toplumda oluşan güven eksikliğini gidererememiş ve akabinde e-Seçim projelerini rafa kaldırmak zorunda kalmıştır. Avusturya Federal Anayasa Mahkemesi 2009 yılında yapılan bir pilot uygulamann sonuçlarını geçersiz saymıştır [13]. Avusturya deneyimi e-Seçim'in benimsenmesinde açıklık ve şeffaflığın payını göstermesi açısından önemli bir örnek olmuştur.

Norveç Yerel Yönetimler ve Bölgesel Kalkınma Bakanlığı (KRD), e-Seçim'in uygulanabilirliği açısından halkın beklentilerinin önemli bir rol oynayacağının bilinciyle, 2004 ortasında bir çalışma komitesi atamıştır. Komite dört alt çalışma grubundan oluşmuştur: 1. e-Seçim teknikleri, 2. Ekonomik ve idari hususlar, 3. e-Seçim ve demokrasi 4. Hukuki durum. Bu çalısma gruplarının yanı sıra komite, genel toplantılar düzenlenmiş ve bulgularını hükümete sunmuştur [14]. 2009 yılında Norveç hükümeti, 2011 yerel seçimleri için elektronik seçim pilot projesini uluslararası bir ihale prosedürüyle başlatmıstır. 2017'deki milletvekili seçimlerinde uygulanacak i-seçimlere kadar milli açık anahtar altyapısı ve ulusal elektronik kimlik kartının hazır olacağı öngörülmüştür.

Norveç hükümetinin internet üzerinden elektronik oylamaya yönelmesinin en temel nedenleri şunlardır:

- Sayım sürecini hızlandırmak. Tüm seçmenler elektronik oylama yoluyla oyunu kullanırsa, sayma işlemi potansiyel olarak sandık kapanışından kısa süre sonra sonuçlandırılabilir.
- Yenilik sayesinde katılım oranını artırmak. Özellikle genç seçmenlerde katılım oranının hissedilir oranda yükseleceği tahmin edilmektedir.
- Engelli vatandaşların daha rahat oy kullanmalarını sağlamak. Özellikle görme engelli vatandaşların sesli ekran okuyucular aracılığıyla başkalarının yardımı olmadan oy kullanabilmesi sağlanabilir.
- Elektronik seçimlerin orta vadede maliyet-etkinliğinden faydalanmak. i-Seçimlerin kurulum maliyeti nedeniyle kısa vadede olmasa da uzun vadede diğer seçim sistemlerine göre daha az zaman ve para gerektireceği kestirilmektedir.

B. Norveç sistemi

Norveç'in seçim mimarisi genel olarak Estonya seçim sistemi ile benzerlik taşımaktadır [15]. Estonya seçim sistemi ile en temel fark Norveç i-Seçim sisteminin açık ve şeffaf olmasıdır. Norveç hükümeti sistemin kriptografik mimarisi ve kaynak kodu dahil teknik konularla ilgili birçok belgeyi detaylarıyla yayınlamıştır. Norveç sisteminin kriptografik protokolü, İspanyol elektronik seçim şirketi Scytl tarafından tasarlanmış fakat ulusal ve uluslararası uzman danışmanlar tarafından pek çok değişikliğe uğramıştır. Scytl şirketi standart seçim çerçevesi ve iki farklı kanal mekanizması önermiştir. Önerilen standart seçim çerçevesi genel olarak bilinen standart kriptografik protokol ve mekanizmalarından oluşmaktadır [16].

Norveç sistemi iki önemli tehdit türüne karşı önlem almıştır:

- Seçmen bilgisayarlarına yönelik kötü amaçlı yazılım (malware), kurban saldırganlar ağı (botnet), palıkçılık (phishing) gibi tehditler,
- Zorlama (coercing) ve oy satma

Norveç sisteminin Estonya sisteminden bir diğer önemli farkı, seçmen bilgisayarındaki tehditlerin engellenmesi için internetin dışında, farklı ve bağımsız iletişim kanallarının kullanılmasıdır. Seçim öncesi ve seçim sonrası kullanılan bu iletişim kanallarına posta servisi ve kısa mesaj servisi (SMS) örnek gösterilebilir.

Norveç seçimlerinde de Estonya'da olduğu gibi, i-Seçim yoluyla seçmenler istedikleri kadar oy kullanabilmekte fakat varsa klasik seçim sistemi ile kulanılan oy, yoksa i-Seçim ile kullanılan en son oy sayılmaktadır.

i-Seçim sistemlerinde oy verme aşamasında homomorfik şifreleme yapılmakla birlikte, oy sayımı için genelde aşağıdaki iki yöntemden biri tercih edilir:

- Şifreli oyların hepsi çarpıldıktan sonra, ortaya çıkan şifre bir çeşit eşik sır paylaşımı yoluyla çözülür. Homomorfik şifrelemenin özelliği nedeniyle şifresi çözülen mesaj oy toplamlarıdır. Bu yöntem, basit ve küçük seçimler için uygulanabilir olmakla birlikte büyük ölçekli seçimlerde verimi tartışmalıdır.

- Karıştırıcı ağlar kullanılarak oylar anonimleştirilir, sonrasında şifreli oylar (eşik sır paylaşımı yoluyla) tek tek deşifre edilir. Oylar yetkili gözetmenler huzurunda toplanır [1].

Norveç seçimlerinde güvenlik seviyesi ve verimliliğinden dolayı homomorfik sistemler yerine, karıştırıcı ağlar tercih edilmiştir.

1) Zorlama ve Oy Satma: Evden oy kullanılabildiği için maalesef kriptografik yöntemler, zorlamayla oy kullanımını doğrudan engelleyemektedir fakat zorlama altında oyunu kullanan seçmen daha sonra internet üzerinden ya da klasik seçim yoluyla oyunu tekrar kullanabilir. Zorlamaya karşı alınan önlemler aynı zamanda oy satmayı da bir ölçüde engellemektedir. Bunun yanında, aşağıda bahsedileceği gibi, kanunlar bu tarz eylemleri yasadışı sayacak şekilde değiştirilmiştir.

C. Norveç: i-Seçim için değişikliğe uğrayan yasalar

Bir ülkede elektronik seçim ülke yasalarının müsaade ettiği çerçevede uygulanabilir. Norveç Anayasası'nda ve seçim ile ilgili birçok yasada ülkede elektronik seçim yapılabilmesi için düzenlemeye gidilmiştir. Anayasada yer alan elektronik seçimi ilgilendiren temel direktifler aşağıdaki gibidir:

- Oylama sonuçlarını bozmak veya değiştirmek yasadışıdır.
- Seçmeni oy vermeye zorlamaya veya zorla istediği birine oy verdirmek yasadışıdır.
- Oy satmak ve oy satın almak yasadışıdır.
- Oy sayımına etki edebilecek her türlü davranışta bulunmak yasaktır.

  Bunun yanında aşağıdaki hukuksal metinlerde düzenlemeler yapılmıştır: Seçim Mevzuatı, Elektronik İmza Mevzuatı, Gizliliğin Korunması hakkında Mevzuat, Elektronik İdare Yönetmeliği, Özgür ve Gizli Seçme Hakkı ve İlkeleri, Eşit Seçme Hakkı İlkesi, Evrensel Seçme Hakkı İlkesi, Seçim Uygulama Yönergesi, Ceza kanunu. Ayrıca, yapılan değişikliklerin İnsan Hakları Avrupa Sözleşmesi'ne uygunlugu incelenmiştir.

D. Norveç: i-Seçim akışı

Çift zarf yöntemini kullanan i-Seçim sistemi şu adımlardan oluşmaktadır:

1) Seçimlerden önce seçmenlerin adreslerine adayların isimlerini ve doğrulama kodlarını içeren bir posta ulaşır.
2) Seçmen oy kullanmak için seçim merkezinin web sayfasına bağlanır ve bilgisayarına seçim uygulamasını indirir.
3) Seçmen, seçim uygulamasını kullanarak ulusal kimlik kartı ile oy sunucusuna kimliğini doğrulatır.
4) Seçim uygulaması güvenli bir kanal üzerinden parti ve adayların listesini alır. Bu liste, aynı bölgedeki tüm seçmenler için aynıdır ve şifreli değildir.
5) Seçim uygulaması partileri rasgele bir şekilde (karışık olarak) görüntüler.
6) Seçmen oy vermek istediği partiyi seçer ve bir sonraki adıma geçer. Seçmen için boş oy seçeneği de mevcuttur.
7) Seçilen parti için aday listesi gösterilir ve seçmenlerin istediği adaylara oy vermesi sağlanır. Seçmene karar verdiği oya ait bir özet sunulur. Seçmen yaptığı seçimden memnun ise "İleri" butonunu tıklar. Yapılan seçime ait metin, oy sayım sunucusunun açık anahtarı ile şifrelenir.
8) Seçmen, imzalama özel anahtarı ile oyunu imzalar. Şifreli imzalı oy, elektronik sandığa gönderilir.
9) Oy kullanıldıktan sonra seçmenin cep telefonuna bir doğrulama kodu gönderilir: "Siz, [seçmen adı], [gün-ay-yıl] tarihinde saat [GMT+1]'te bir oy kullandınız. Onay kodunuz [kod]'dur".
10) Seçmen cep telefonuna gelen doğrulama kodunu posta yoluyla evine gelen kodla eşleştirerek kullandığı oyun başarılı bir şekilde kullanılıp kullanılmadığını kontrol edebilir. Seçmen SMS ile gelen bu mesajla posta yoluyla gelen mesajlardan farklı olduğu durumlarda, "Oy sandığı bulunamadı" gibi mesajlarda veya oy vermediği halde mesaj geldiği durumlarda itiraz eder. Bu durumda seçmen tekrar oy kullanır, ya da klasik şekilde oy verir.

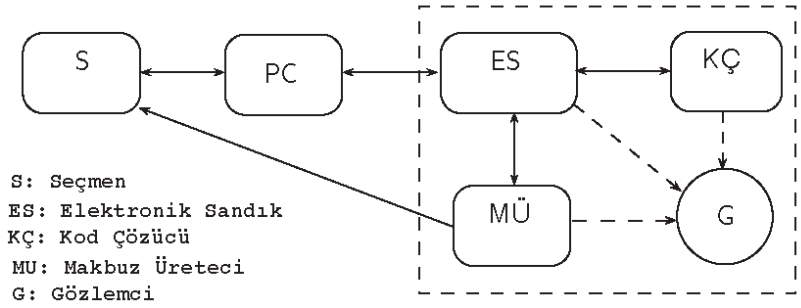
E. Oy kullanma protokolü

Uzaylar ve protokol katılımcıları: k_{max} toplam aday sayısını göstermek üzere, aday listesini $O = \{1, 2, 3, \ldots, k_{max}\}$ ile ifade edelim. $(v_1, \ldots, v_k)$ ise bir seçmenin oy verdiği adaylar olsun, öyle ki $v_i \in O$ $(k < k_{max})$.

- C Kodlama uzayı,
- F Fonksiyon uzayı,
- S Seçmen uzayı,
- PC Kişisel bilgisayar seçim uygulaması,
- ES Elektronik sandık,
- MÜ Makbuz Üreteci ,
- KÇ Kod Çözücüsü,
- SBP Sıfır bilgi protokolünü göstersin.

G, g elemanı tarafından üretilen (asal) q mertebeli bir çarpımsal grup olsun. C olarak ifade edilsin. S G'den C'ye (seçmene posta yoluyla gönderilen doğrulama kodlarının uzayı) giden sanki rassal fonksiyon uzayı F olsun. $f \in F$ bire-bir kodlama fonksiyonu, d buna ait kod çözme fonksiyonu olarak tanımlansın.

Anahtar üretimi: Anahtarların güvenli bir otorite (örneğin, Yüksek Seçim Kurulu) tarafından üretildiğini varsayılım . Bu anahtarlar eşik sır paylaşımı kriptografik yapı taşı kullanılarak üretilir [18]. Seçimden önce otorite tarafından a_1, a_2 ve a_3 parametreleri, $a_1 + a_2 = a_3 \pmod q$ olacak şekilde seçilir. a_1, a_2 ve a_3 anahtarları sırasıyla D, ES ve MÜ'ye dağıtılır. Açık anahtarlar ise şu şekilde hesaplanır: $y_1 = g^{a_1}, y_2 = g^{a_2}$ ve $y_3 = g^{a_3}$. Seçmen, oyunu bu açık anahtarları kullanarak şifreler ve ES'ye gönderir. ES ve MÜ özel anahtarları a_2 ve a_3'ü kullanır



Şekil 1. Norveç Protokolü iletişim kanalı [17]

ve çıkan sonucu D'ye gönderir. D ise özel anahtarı a_1'i kullanarak oyları sayar. Burada ES, MÜ ve D fiziksel ve organizasyonel olarak farklı olmak zorundadır, aksi takdirde farklı servisler olarak algılanmazlar. Bunun yanında, ES, MÜ, D ve gözetmenler arasındaki iletişim için güvenli bir kanal olması gerekmektedir. Bu amaçla standart internet güvenlik protokolleri, örneğin TLS veya IPSEC, kullanılabilir.

Makbuz üretimi: Makbuzlar seçimden önce şu şekilde oluşturulur: Her seçmen için $s_i \in_R \{0,\ldots,q\}$ ve $d \in_R F$ seçilir öyle ki $f : x \longmapsto x^{s_i}$ ve $r : O \longmapsto C$. f ve d fonksiyonlarının bileşke fonksiyonu $r(v) = d((f(v))^{s_i})$ olarak hesaplanır. Seçimden önce, $\{(v, r(v)) \,|v \in O\}$ ikilisi yani makbuz seçmene posta yoluyla gönderilir.

Protokol adımları:

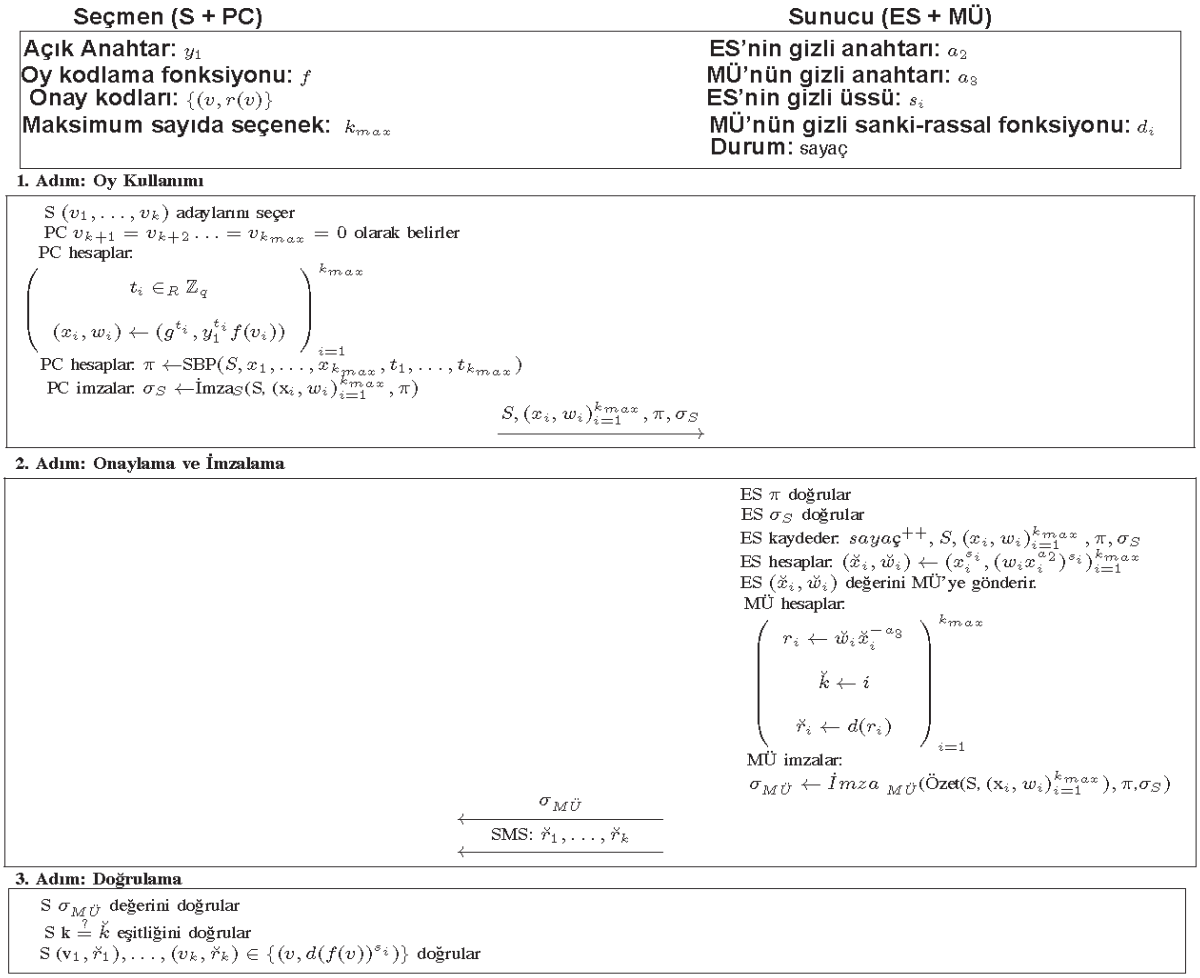
1) **Oy kullanımı:** Seçmen oylama esnasında O aday listesinden $(v_1,\ldots,v_k)$ seçeneklerine karar verir. PC, seçmenin yaptığı k seçiminden arta kalan adaylar için $v_{k+1} = v_{k+2} = \ldots = v_{k_{max}} = 0$ olarak belirler. Daha sonra PC her adayı $t_i \in_R \mathbb{Z}$, $(x_i, w_i) \leftarrow (g^{t_i}, y_1^{t_i} f(v_i))$ $\forall i = 1,\ldots,k_{max}$ homomorfik şifreler. PC yaptıklarının doğruluğunu ispatlamak için $\pi \leftarrow$SBP$(S, x_1,\ldots,x_{k_{max}}, t_1,\ldots,t_{k_{max}})$ sıfır bilgi protokol değerini hesaplar. Seçmen $\sigma_S \leftarrow$ İmza$_S(S,(x_i,w_i)_{i=1}^{k_{max}},\pi)$ imzaladıktan sonra ES'ye $S,(x_i,w_i)_{i=1}^{k_{max}},\pi,\sigma_S$ bilgilerini gönderir.
2) **Onaylama ve İmzalama:** ES, ilk olarak π'yi ve σ_S'yi doğrular. Daha sonra $sayaç^{++}, S,(x_i,w_i)_{i=1}^{k_{max}},\pi,\sigma_S$ bilgilerini kaydeder, $(\breve{x}_i,\breve{w}_i) \leftarrow (x_i^{s_i},(w_i x_i^{a_2})^{s_i})_{i=1}^{k_{max}}$ şeklinde hesaplar ve MÜ'ye gönderir.
MÜ $\forall i = 1,\ldots,k_{max}$ için şu hesapları yapar: $r_i \leftarrow \breve{w}_i \breve{x}_i^{-a_3}$, $\breve{k} \leftarrow i$, $\breve{r}_i \leftarrow d(r_i)$. Daha sonra $\sigma_{MÜ} \leftarrow İmza_{MÜ}(Özet(S,(x_i,w_i)_{i=1}^{k_{max}})),\pi,\sigma_S$ imzasını oluşturur ve PC'ye gönderir. C uzayından $SMS= \breve{r}_1,\ldots,\breve{r}_k$ makbuzunu üretir ve seçmene SMS yoluyla gönderir.
3) **Doğrulama:** Seçmen öncelikle $\sigma_{MÜ}$ değerini doğrular. $k \stackrel{?}{=} \breve{k}$ eşitliğini kontrol eder, eşit değilse oylama esnasında bir problem olduğu kabul edilir. SMS yoluyla gönderilen $(v_1,\breve{r}_1),\ldots,(v_k,\breve{r}_k)$ makbuzu ile posta yoluyla gelen $\{(v, d(f(v))^{s_i})\}$ makbuzunu karşılaştırır. Eğer farklı ise seçmenin oyu kötü amaçlı yazılım tarafından değiştirilmiş veya iletim esnasında bozulmuş olabilir.

F. Oy sayma protokolü

1) **Gözetmen listeyi alır:** i-Seçmen listesi Li şu şekilde oluşturulur: En yüksek $sayaç$ değeri seçilir, $S,(x_i,w_i)_{i=1}^{k_{max}},\pi,\sigma_S$. $(x,w) \leftarrow \prod_{i=1}^{k_{max}}(x_i,w_i)$. Daha sonra $L \leftarrow L+$ ekle(x,w). Bütün i-seçmen listesi gözetmene gönderilir.
2) **Şifre çözülür ve oylar sayılır:** Gözetmen listenin doğruluğunu onaylar. $|L| = n$ olsun. D, $\forall i \in \{1,\ldots,n\}$ ve $s_i \in_R \mathbb{Z}_q$ değerleri için $(x'_i,w'_i) \leftarrow (x_{\prod(i)} g^{s_i}, w_{\prod(i)} y_1^{s_i})$ hesaplar. Sonrasında $\mu_i \leftarrow w'_i (x'_i)^{-a_1}$ hesaplar. $\pi_i \leftarrow$ SBP sıfır bilgi protokolunu kontrol eder ve şifre çözülür. En sonunda da $\forall i = 1,\ldots,n$ değerleri için $\pi' \leftarrow$ SBP Karıştırıcı işlemi yapılarak oylar karıştırılır. D, yapılan işlemleri gözetmene ispatlar. Oylar ϕ kod çözme fonksiyonu olmak üzere $\phi(\mu_1),\ldots,\phi(\mu_n)$ şeklinde ortaya çıkar.

IV. Norveç Seçim Protokolünün Bütünlüğü

Bir protokolün bütün olup olmadığının kontrolü dürüst modelde incelenir [18], yani bütün katılımcıların dürüst olduğu durumda protokolün doğru işlemi yaptığı kontrol edilir. Bu seçim protokolünde her dürüst katılımcı için şifreli oy doğru bir şekilde açılır. Seçmenin doğruladığı makbuz kodu hariç protokolün diğer kısımları bütündür. Seçmene gönderilen $(v_i,\breve{r}_i)$ (öyle ki, $\breve{r}_i = d(r_i)$) makbuz kodunun aynı olmasını gösterelim:



Şekil 2. Oy kullanma protokolü.

$$\begin{aligned} r_i &= \breve{w}_i \breve{x}_i^{-a_3} \\ &= w_i^{s_i} \breve{x}_i^{a_2 s_i} \breve{x}_i^{-a_3 s_i} \\ &= w_i^{s_i} \breve{x}_i^{(a_2 - a_3) s_i} \\ &= w_i^{s_i} x_i^{-a_1 s_i} \\ &= (w_i x_i^{-a_1})^{s_i} \\ &= (f(v))^{s_i} \end{aligned}$$

Böylece, eşik sır paylaşımı kriptografik yapıtaşı özelliğinden dolayı a_1, a_2 ve a_3 özel anahtarları kullanılarak $r_i = (f(v))^{s_i}$ değerinin sağlandığını ve bu sayede makbuz üretimi sürecinde gönderilen doğrulama kodlarının $\{v, r_i(v) | v \in O\}$ doğrulugunu göstermiş olduk.

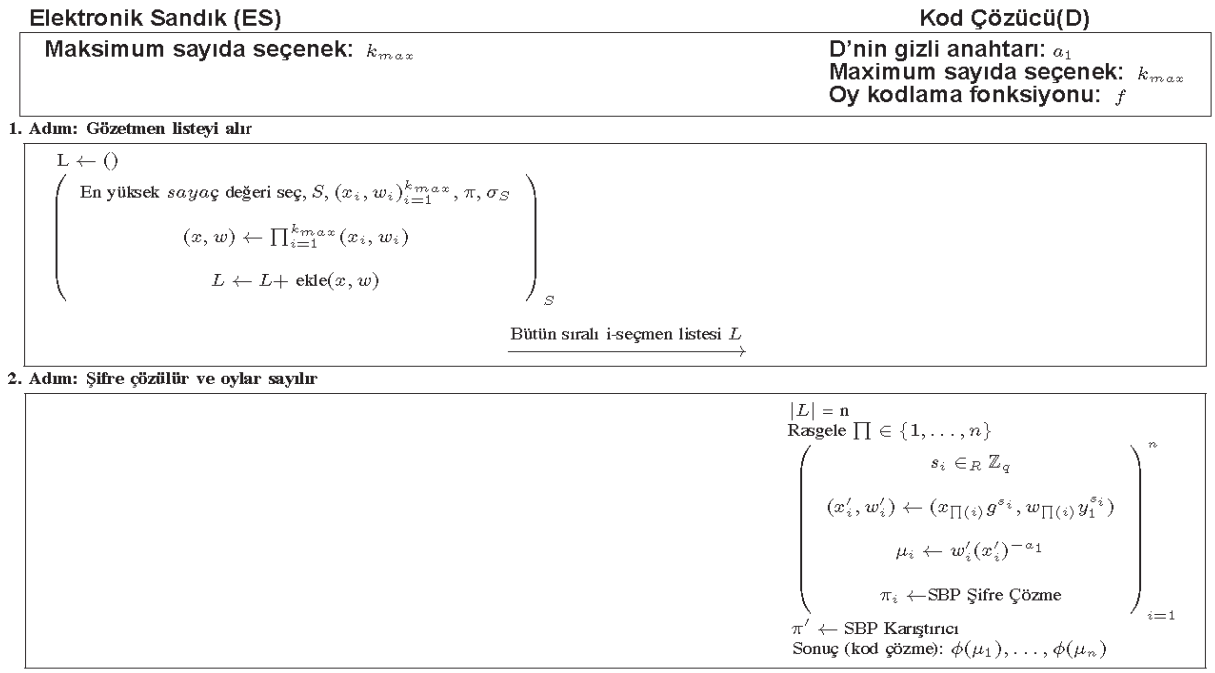
V. Norveç I-Seçim protokolü güvenlik analizi

Bu bölümde Norveç e-seçim sistemine yönelik özgün bir güvenlik analizi verilecektir. Mahremiyet ile ilgili baz potansiyel problemler için [19]'ye bakınız.

A. SMS saldırıları ve güvenlik problemleri

Estonya sisteminde mobil kimlik doğrulama için bir prosedür vardır fakat Norveç sisteminde SMS saldırıları, ayrı olarak ele alınmayı gerektiren ciddi bir açıklık kaynağı olarak göze çarpmaktadır. SMS göndermek için kullanıcı etkileşimi gerekli olmadığından bu tür saldırıları engellemek çok kolay görünmemektedir. SMS saldırılarından bazıları aşağıda listelenmiştir:

- SMS servis sağlayıcısının güvenlik duvarının olmaması
- SMS mesajlarını filtreleyen bir mekanizmanın eklenmemiş olması
- Bir mesajın orijinal biçiminde hedef telefona ulaşıp ulaşmadığının belirsiz olması (Standart SMS, kriptografik bütünlük korumadan yoksundur.)
- Cep telefonu operatörlerinin gönderilecek mesajları engellemesi



Şekil 3. Oy sayma protokolü.

- SMS servisinin güvenilir bir hizmet olmaması, (Mesajlar gecikebilir ya da hiç ulaşmayabilir.)
- Hizmet engelleme (DoS) saldırıları
- Telefona özgü SMS sorunları (Örneğin bazı telefonlara gelen özel formatlı mesajlar telefonun SMS servis hizmetini bozabilir ve telefonu hizmet dışı bıraktırılabilir [20]).
- Yeni nesil akıllı telefonların SMS virüslerine karşı daha savunmasız olması [20]'da Nokia, iPhone ve Android platformları için çok sayıda yeni SMS virüsleri rapor edilmiştir.
- Truva Atı benzeri programlar sayesinde cep telefonlarından istenmeyen e-posta/mesajlar gönderilmesi.
- Kötü niyetli kişiler cep telefon numaralarını bir veritabanına kaydedebilir ve seçim zamanı mesaj bu telefonlara gereksiz mesaj yağdırabilir.

VI. Estonya ve Norveç İ-seçim sistemlerinin karşılaştırılması

Norveç e-Seçim sisteminin Estonya sistemine göre daha güvenli olduğu düşülmektedir. Norveç sisteminde, kötü niyetli seçmen bilgisayarlarına karşı önlemler geliştirilmiştir ve gözetim sistemi daha iyi organize edilmiştir.

- Seçmenin oyundan emin olması: Estonya sisteminde seçmen sadece oyunun "Oy Depolama Sunucusu"'da depolanmış olup olmadığını bilir. Diğer yandan, Norveç sisteminde seçmen oyunun kime verildiğini bilir.
- Seçmen bilgisayarına ynelik tehditler: Estonya sisteminde savunmasız seçmen bilgisayarına karşı seçmen oyunu korumak için bir mekanizma geliştirilmemiştir. Norveç sisteminde bulunan iki farklı kanal mekanizması seçmen bilgisayarına yönelik saldırılara karşı kullanılır. Hatta bilgisayar, seçmen oyunu bozmaya kalkışsa dahi seçmen gelen makbuz sayesinde oyunun değiştirildiğini anlayabilir.
- Verilen oy işlemleri için karıştırıcı ağlar yöntemi kullanma [1]: Daha verimli ve sağlam olması için Norveç sistemininde karıştırıcı ağlar kullanılmaktadır.
- Mobil kimlik doğrulama sistemi: Norveç sisteminde mobil kimlik doğrulama uygulaması yoktur. Ancak, Estonya sisteminde seçmen mobil kimliği ile kayıt olabilir.
- Matbaa: Seçim öncesi ve sonrası olan iletişimlerde, seçim öncesinde her bir seçmenin adresine yazılı bir kod gönderileceğini belirtmiştik. Seçim otoritesi her vatandaşa bu kodu göndermek zorundadır. Bu yüzden baskı hacmi büyük olacaktır. Matbaalarda çalışanları bu kodları çalabilir ve seçmen mahremiyetini ihlal edebilir. Kötü niyetli kişiler, matbaanın bilgisayar altyapısını hack'leyerek kodları ele geçirebilir.

Bilinen bazı potansiyel açıklıklara rağmen, ne Estonya'da yapılan birçok seçimde ne de Norveç 2011 seçimlerinde i-Seçim ile ilgili herhangi bir güvenlik ihlali vakası ihbar edilmemiştir.

VII. E-SEÇIM SISTEMLERİNİN AÇIK KAYNAK KODLU OLMASININ ÖNEMİ

Seçmenlerin seçim sistemine olan güvenlerini arttırmak için kullanılabilecek bir yöntem, sistemin tüm detaylarını ve kaynak kodlarını yayınlamaktır. Norveç bu yolu tercih etmiştir. Diğer yandan, seçim sisteminin detaylarının açıklanmasının getireceği avantaj ve dezavantajların çok iyi incelenmesi gerekmektedir.

Açık kaynak kodlu sistemlerin detaylarını bir çok kişinin incelediği ve açıklıkların uzmanlar tarafından tespit edilerek sistemin iyileştirilebileceği ve nihai sistemin çok az açık içereceği, bu nedenle seçmenlerin sisteme daha çok güven duyacağı düşünülür.

Sistemin açık kaynak kodlu olmasının en büyük dezavantajı, kötü niyetli kişilerin ve bilgisayar korsanlarının da sistemin detaylarına ve kaynak kodlarına erişebilecek olmasıdır. Bu kişiler buldukları zayıflıkları topluma açıklamayıp saldırı yapabilme amacıyla kullanmak isteyeceklerdir.

Açık kaynak kodlu olmayan sistemlerde bile istemci (seçmen) tarafında çalışan yazılımlar saldırganlar tarafından kaynak koda dönüştürülebilir. Kaynak kodun derlenmeden önce perdelenmesi (obfuscation) bu işi sadece biraz zorlaştıracaktır. e-Seçim sürecinin uzun olduğu düşünüldüğünde (Norveç'te bu süreç üç ay sürmektedir) perdeleme işleminin getireceği yarar tartışılabilir. Dolayısıyla, sistemin açık kaynak kodlu olması daha çok sunucu güvenliğini ilgilendirmektedir. Sistemin açık kaynak kodlu olması sonucunda saldırganlar sunucu tarafındaki detaylara ve kodlara da sahip olacaklardır [21].

Bir sonraki bölümde internet tabanlı sistemler için yapılan tehdit analizlerini incelemeye çalışacağız.

VIII. İ-SEÇİM TEHDİT ANALİZİ

Tehdit analizinde saldırganın e-Seçim sistemine gizlilik, bütünlük, erişim denetimi ve kullanılabilirlik yönlerinden yapabileceği saldırılar incelenecektir [20], [22]. Bu saldırıların yapılabilmesi için saldırganın sahip olması gereken bilgi düzeyi ve kaynak miktarı da dikkate alınmalıdır. Bu tehditlerin önlenmesi için alınabilecek önlemler konusunda fikir verilmeye çalışılacaktır. Farklı uzmanlar i-Seçim'in başlangıçta %5'lik kısmında uygulanmasını veya öncelikle yurtdışındaki seçmenlerin kullanabilmesini tavsiye etmişlerdir. Bu yolla zorlama gibi engellenmesi güç problemlerin çözülmesinden önce, kullanılabirlik analizi, ölçeklenebilirlik gibi konularda sahadan geribesleme alınabilir.

Tehdit analizi tablolarındaki sütunlar hakkında kısa bilgi aşağıda verilmiştir.

1) Tehdit: Güvenliği etkileyebilecek olay ve durumlardır. Seçim sistemine yapılabilecek bazı saldırılar basit tekniklerle çok nitelikli olmayan saldırganlar tarafından gerçekleştirilebilirken, bazılarını yapmak için bilgi birikimi, kaynak gereksinimi veya seçim sistemindeki cihazlara erişim gerekebilecektir. Kaynak gereksinimi içerden ve dışarıdan olmak üzere iki sınıfa ayrılır. İçeriden olan kaynaklar, seçim sistemindeki cihazlara veya iç ağa belirli seviyede erişimi olan kişi veya gruplardır. İnternet tabanlı seçim için tehdit kaynağı aşağıda verilmiştir:
   - Sistem içi tehdit kaynakları: i. Seçmen: Seçim sistemine sınırlı erişim imkanları vardır. Her bir seçmen, kayıt olmak, oy vermek ve seçim sonrası doğrulama amaçları için seçim sistemi ile etkileşim içinde olacaktır. ii. Seçim Görevlisi: Seçim sistemine ve verilerine kullanıcı düzeyinde erişim imkanları vardır. Fakat sistem operatörleri gibi yönetimsel hakları yoktur. iii. Sistem Yöneticisi: Seçim sisteminde yönetimsel düzeyde erişim imkanları vardır ve sistemin düzgün işlemesinden ve hata durumunda müdahale edilmesinden sorumlulardır. iv. Diğerleri: 1. Seçim sisteminin üreticileri, geliştiricileri 2. Sistemin entegrasyonunu yapanlar 3. Destek/Bakım elemanları 4. Doğrulama kodlarının üretildiği yerler(matbaa veya cep telefonu operatörleri)
   - Sistem dışı tehdit kaynakları: i. Kötü niyetli kişiler: Seçim sisteminin zayıf yönlerinden yararlanmak isteyen kişilerdir. ii. Kötü niyetli gruplar: Bu saldırılar hacking, organize suç veya terör faaliyeti için biraraya gelmiş olabilir. Kötü niyetli kişilerden iş gücü ve teknik kaynak miktarı açısından daha güçlülerdir.
2) Tehdit Sonucu: Saldırının sisteme, yapılan seçime ve/veya seçmenlere vereceği zararlar.
3) Tehdit Seviyesi: Tehdidin gerçekleşmesi durumunda oluşacak etkinin büyüklüğü.
4) Alınabilecek Güvenlik Önlemleri: Saldırıları önleme ya da etkisini azaltmak için alınabilecek önlemler.

A. Kriptografik yönüyle tehdit analizi

Bu bölümde kriptografik hizmetler açısından genel bir tehdit analizi yapılacaktır, detaylar için Şekil 4 bakınız.

B. e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi

Bu bölümde yer alan tehditler, genellikle seçmen tarafına (verilen oya ya da mahremiyete) yönelik ciddi tehditlerdir, detaylar için Şekil 5 bakınız..

C. İletişim kanalları yönüyle olası tehdit analizi

Bu bölümde, alternatif kanalların güvenlik sorunundan kaynaklanan tehditler de yer almaktadır, detaylar için Şekil 6 bakınız.

Kriptografik yönüyle tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Erişim Denetimi, Kimlik ve Kaynak Doğruluğunun Düzgün Yapılmaması	Kayıtlı olmayan kişilerin oy vermesi, Kayıtlı seçmenlerin yerine oy verme, Oyların değiştirilmesi, Birden fazla oy verme	Yüksek	Parola tabanlı erişim denetimi, Sayısal imza, Güçlü kriptografik kimlik doğrulama yöntemleri
2	Seçmenlerin kime oy verdiğinin ortaya çıkması	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Ara sonuçların öğrenilmesi, Zorlama	Yüksek	Ağ katmanında Şifreleme, Uygulama katmanında Şifreleme (uçtan uca şifreleme)
3	Oyların Bütünlüğünün Sağlanması	Oyların değiştirilmesi	Yüksek	Mesaj Doğulama Kodu Kullanımı, Sayısal İmza
4	İmzalı ve Şifreli Oyların Ele Geçmesi	Anahtar uzunluklarına bağlı olarak oy gizliliğinin ihlali, Saldırganın seçim sonrasında (örn, yıllar boyu kriptanalizle) belirli seçmenlerin kime oy verdiğini ortaya çıkarması	Orta	Anahtarların yeterince uzun olması veya anahtar uzunluğundan bağımsız olarak güvenlik sağlanması [1], Anahtarların korunması, Sistemdeki şifreli verilere eşik sır paylaşımı ile erişilmesi
5	Seçim Sisteminin Özel Anahtarının Korunamaması	Oy gizliliğinin ihlali, Ara sonuçların öğrenilmesi, Zorlama, Servis Dışı Bırakma	Yüksek	Basit Erişim Denetimi, Sır Paylaşımı
6	İmzasız ve Şifreli Oyların Ele Geçmesi	Anahtar ortaya çıkmadığı takdirde tehdit oluşturmamaktadır	Düşük	-
7	Oyların Anonimliğinin Sağlanamaması	Oy gizliliğinin ihlali, Zorlama, Ara sonuçların öğrenilmesi	Yüksek	Şifreleme/ Deşifreleme, Karıştırıcı Ağlar, Homomorfik Sayım
8	Denetlemenin Güvenilir Olmaması	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Zorlama, Birden fazla oy verme	Yüksek	Standart Kayıt (Log), Değiştirilemez, Kayıt (immutable log), Standart Makbuz, Bireysel Doğrulanabilirlik, (seçmenin niyeti oya doğru şekilde yansıdı), Bireysel Doğrulanabilirlik, (oylar doğru sayıldı), Evrensel Doğrulanabilirlik

Şekil 4. Kriptografik yönüyle tehdit analizi

D. Sunucu güvenliği

i-Seçim sistemlerinde Oy Sayım Sunucusu, Oy Yönlendirme Sunucusu, Oy Depolama Sunucusu ve benzeri sunucular bulunmaktadır. Bu sunucuların güvenliği genel anlamda bu başlık altında incelenecektir, detaylar için Şekil 7 bakınız.

IX. Sonuç ve Ülkemiz için Ön Değerlendirmeler

Bu yazıda Estonya (internet kanalıyla elektronik seçimi ilk uygulayan ülke) ile Norveç i-seçim sistemlerini inceledik. Bahsi geçen ülkelerdeki göreceli başarıda, pek çok faktörün etkili olduğu görülmektedir. Kullanıcı profili özellikle internet okur-yazarlığı oranı, internet ve cep telefonu erişim ağının yaygınlığı, seçim sistemine duyulan güven bu etmenlerin başlıcalarıdır. Elektronik seçim sistemi hakkında topluma genel bilgiler sağlamak ve güvenilir bir otoritenin bu sistemi resmi olarak nitelikli hale getirmesi toplumda güven duyulmasını artıracaktır. e-Seçim projesinin analiz edilebilirliği çok önemlidir, Avusturya e-seçim projesinin rafa kaldırılması buna güzel bir karşı örnektir.

Diğer yandan, i-Seçim'in seçmen demokratik katılımıa ne kadar tesir ettiği tartışılır. Örneğin i-seçmen oranı artsa da, Estonya seçimlerinde hissedilir bir seçmen artışı olmamıştır. Diğer yandan özellikle genç seçmenlerde oy verme şekli değişmektedir. Ülkemizde, özellikle e-kimlik kartının yaygınlaştırılmaya başladığı şu günlerde, demografik yapının genç ağırlıklı olduğu da göz önüne alınırsa, muhtemel bir e-seçim uygulamasında i-seçmen oranı azımsanmayacak oranda çıkabilir. Üstelik Türkiye'de elektronik okur-yazarlık konusunda potansiyel olarak büyük gelişmelerin devam edeceği öngörülmektedir. (Okullara tablet PC

e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Seçmen bilgisayarındaki kötü amaçlı kodların (örneğin, Truva atı) seçmenin oyunu öğrenmesi, silmesi değiştirmesi veya seçmen yerine oy vermesi	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçmenin haberi dışında oy kullanma, Oy verememe, Sunucuya saldırı amaçlı kullanım	Yüksek	Seçmen bilgisayarından tehdit gelmeyeceğinin garanti edilmesi farklı ve bağımsız iletişim kanallar kullanılması (örn., posta, SMS), Virüs, Truva atı, Casus yazılımlara karşı kullanılan programlarını güncel olması; Seçmenin bilgisayar başında bulunduğunun kanıtlanması (Kart, Parola, PIN, Parmak izi kullanımı vb.)
2	Seçmenin başka siteye yönlendirilmesi	Oy gizliliğinin ihlali , Oyların değiştirilmesi, Oy verememe	Yüksek	Virüs, Truva atı, Casus yazılımlar, vs. güncel olmalıdır.Seçmenler yapılabilecek saldırılar konusunda bilgilendirilmelidir.
3	Zorlama	Oyların değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir. Seçmen fiziksel olarak oy sandığına ulaşamayacağı bir noktadan i-Seçim bitmesine yakın kullandığında cebine mesaj gelir. Mesaj geldiğinde ne zaman oy kullandığı bilinecektir. Seçim sonrası tekrar oy kullanamayacağına ve fiziksel olarak da oy sandığına gidemeyeceğine göre oy satışı veya zorlama gerçeklenebilir.
4	Aile bireyleri evinden oy kullanırken baskı altında kalabilirler (Bu probleme literatürde Aile Oylaması denilir).	Seçmenlerin kendi inisiyatifleri doğrultusunda oy kullanamaması	Yüksek	Aile oylamasını uzaktan seçim uygulandığı müddetçe engellemek pek mümkün değildir.
5	Oy Satma	Seçim sonucunun değiştirilmesi	Yüksek	Seçmenlerin seçim sonuna kadar oylarını değiştirmesine müsaade edilebilir.
6	Seçmen doğru olduğu halde bazı işlemlerin yanlış gerçekleştiğini iddia edebilir (örn. SMS kontrolü)	Seçime olan güvenin azalması	Düşük (kişisel olursa), Orta (büyük grup olursa)	Bunu iddia eden kişilerin klasik seçime yönlendirilmesi, Kötü niyetli bir seçmen kasten telefonuna yanlış kod gönderildiğini iddia ederse, onun yanlış veya yalan söylediğini doğrulayan anlık bir mekanizma yoktur. Bir grup insan bu senaryoyu kasıtlı olarak uygularsa bu durum vatandaşlar arasında güvensizlik oluşturabilecektir. Bu teknik bir saldırı değildir fakat vatandaşlar arasında yanlış kanı doğurabileceğinden önemlidir.

Şekil 5. e-Seçim'in bilgisayar ve ağ güvenliği yönüyle olası tehdit analizi

dağıtılması, cep operatörlerinin akıllı telefon kampanyaları vb.) Ülkemizde engellilerin seçim sandığına ulaşma imkanları da bahsi geçen ülkelere kıyasla yeterli olduğu söylenemez. i-Seçimin engelli vatandaşların seçime katılıma katkısı farklı olacaktır. Bu ve benzer nedenlerle, yakın ya da orta vadede, ülkemizde e-Seçim'in gerekliliği tartışılmaya başlanacaktır. Çeşitli e-Seçim teknikleri şimdiden bazı bilim kurumlarında teorik olarak araştırılmaya başlanmıştır. Ne var ki, e-Seçim uygulamasına geçilmeden önce detaylı bir fayda-maliyet analizi yapılmalı ve öngörü ve kestirimler yapabilmek adına bazı temel sorular hakkında bilgi toplanması gereklidir.

- Mevcut sistemin olası sorunları ve riskleri
- Kullanılacak yeni teknolojinin faydaları
- e-Seçim teknolojisinden beklenen hedefler
- Kullanılacak e-Seçim sisteminin belirlenmesi: i-Seçim, elektronik oy kayıt sistemleri (örneğin DRE), görsel e-Seçim sistemleri (örneğin "Prêt à Voter") ya da ülkemize has özgün tasarım kullanılabilir.
- Yeni teknoloji kullanımı ile beraber olası yeni problemler ve yeni riskler
- Kullanılacak yeni teknoloji ve seçim sürecinin

İletişim kanalları yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	İnternet ortamının güvensizliği nedeniyle seçmen bilgisayarı ve sunucu arasındaki iletişimin içeriğinin öğrenilmesi, değiştirilmesi, engellenmesi	Oy kullanılamaması, Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Bölüm 6.1 Kriptogafik yönüyle tehdit analizi, Bknz. 6.2 Bilgisayar ve ağ güvenliği yönleriyle tehdit analizi
2	Posta sisteminin zaafiyetlerinden dolayı postanın seçmenin eline geçmemesi (postanın dağıtılmaması, başkası tarafından kasıtlı olarak alınması) veya seçmenden habersiz içeriğinin öğrenilmesi	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Düşük	Posta yanlışlıklarına sık rastlanılması seçmenler arasında huzursuzluk doğurabilir. Bunun yanında sistemin doğru çalışıp çalışmadığının anlaşılması için bütün seçmenlerin bu doğrulamayı yapmasına gerek yoktur. Belirli oranda seçmenin bu doğrulamayı yapması yeterlidir.
3	Kötü niyetli kişiler cep telefonu altyapısına veya bireysel cep telefonuna saldırı yaparak servis vermesini/almasını engelleyebilir. (Servis dışı bırakma, SMS virüsleri, SMS enjeksiyon gibi farklı saldırı türleri olabilmektedir.)	Seçmen güvenli ve güvenilir bir şekilde oy verdiğini doğrulayamaz	Orta	Bu tür saldırılar seçmenin farkına varabileceği türlerdendir. Seçmen herhangi bir saldırı altında kaldığını hissederse tereddüt etmeden klasik seçimde oyunu kullanabilir.

Şekil 6. İletişim kanalları yönüyle olası tehdit analizi

demokrasi bilinci ve kurumların şeffaflığına etkileri
- Yeni teknoloji ile ilgili donanım, yazılım ve altyapı için gerekli iletişim, ulaşım, personel, danışmanlar, bakım ve güncellemeler ilgili tüm masraf kestirimleri
- Yeni teknolojinin uygulanması için detaylı bir zaman çizelgesi
- Kullanılacak sisteme bağlı olarak gerekli hukuki altyapının hazır olması adına gerekli düzenlemeler
- Uygulanan yeni teknoloji başarısız olursa ilgili maliyet tahmini
- Sistemi işletenlerin ve seçmenlerin sistem çalışması hakkında eğitim ve bilgilendirilmesi için gerekli planlamanın yapılması

Yukarıda saydığımız genel hususların yanı sıra, e-Seçim sistemi tasarlarken e-güvenlik açısından yapılacak çalışmaların aşağıdaki ilkeler çerçevesinde olması beklenir:
- Sistemin güvenlik gerekleri kesin olarak belirlenmelidir [2].
- Biçimsel (formel)analiz ve sistemin güvenilirliğinin ispatı uzman ulusal ve uluslararası yetkililer veya danışmanlar tarafından yapılmalıdır.
- Tehditler yapılandırılmalıdır ve sınıflandırılmadır.
- Tehdit önleme stratejileri geliştirilmelidir.
- Muhtemel hata işleme, yönetme ve kurtarma senaryoları çıkarılmalıdır.
- Sosyo-teknik sistem analizi geliştirilmelidir.
- Küçük ölçekli prototip seçimlerle (birçok ülkede saygın bir üniversitenin bilgisayar bölümü ilk pilot bölge seçilir) ara tasarımlar denenmeli, geri beslemeler ışığında olası güvenlik açıkları kapatıacak ve kullanıcı kolaylığını artırıcak değişikliklerle sistem geliştirilmelidir.

Elektronik seçimin birçok avantajının olmasına rağmen hala problemlerinin olduğu görülmektedir. Ancak zaman içerisinde edinilen bilgi birikimi ve tecrübe ile beraber bu problemler azaltılabilmiştir. Estonya'da 2005, 2007 ve 2009 yılında başarılı uygulaması Norveç hükümeti için bir ilham kaynağı olmuş bu başarıyı kendi ülkelerinde de uygulamak istemişlerdir. ABD yurtdışındaki vatandaşlarının oy kullanabilmesi için bir çalışma yürütmektedir [23]. İngiltere, ABD, Belçika, Estonya ve Norveç başta olmak üzere gelişmiş ülkeler

e-Seçim'in sunucu güvenliği yönüyle olası tehdit analizi				
	Tehdit	Tehdit Sonucu	Tehdit Seviyesi	Alınabilecek Güvenlik Önlemi
1	Kullanılmış oy pusulalarının bazı kısımlarına yetkili personel tarafından erişilmesi (okuma, silme veya değiştirme).	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Yüksek	Bknz. Resim-18, Bölüm 6.1 e-Seçim'in kriptografik yönüyle olası tehdit analizi (Örneğin, Kimlik Doğrulama, Oyların Bütünlüğünün Sağlanması Deşifrelemede Oyların Anonimletirilmesi)
2	Kullanılmış oy pusulalarının bazı kısımlarına yetkisiz personel tarafından eriilir (okuma, silme veya değitirme).	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Düşük	Eriim denetiminde ve kimlik doğrulamada güçlü kriptografik yapılar kullanılması (Bknz. Tablo-18, Bölüm 6.1 Kriptogafik Yönden Tehdit Analizi)
3	Yetkisiz personelin sunuculara uzaktan erierek kullanılmış oy pusulalarını okuması, silmesi veya değitirmesi.	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Düşük	Sunuculara uzaktan eriimin zorunlu olduğu durumlarda güçlü eriim denetim ve kimlik doğrulama mekanizmalarının kullanımı
4	Sunuculardaki kötü amaçlı kodların (örneğin, Truva atı, Casus Yazılım) seçmenin oyunu öğrenmesi, silmesi veya değitirmesi	Oy gizliliğinin ihlali, Oyların değitirilmesi, Seçimin sonucunun değitirilmesi	Orta	Virüs, Truva Atı, casus yazılımlar, vs. programları güvenilir ve güncel olmalıdır.
5	Sunucu yazılımındaki hatalar nedeniyle seçmen oylarının yanlış kaydedilmesi	Seçim sonucunun seçmenlerin niyetini yansıtmaması	Orta	Yazılımın geliştirilmesinde endüstri standartlarına uyum, Sistemin ve yazılımı sertifikasyonun yapılması, Kaynak kodların açıklanması
6	Seçmenlerin yanlış bir sunucuya yönlendirilmesi (Örneğin, Phishing yoluyla)	Oy gizliliğinin ihlali, Oyların değiştirilmesi, Oy verememe	Yüksek	Seçmenlerin saldırı yöntemleri konusunda bilgilendirilmesi, Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi.
7	DNS sistemine yapılan bir saldırı sonucunda seçmenlerin yanlış sunucuya yönlendirilmesi	Oy gizliliğinin ihlali, Seçmenlerin oy kullanamaması, Oyların değiştirilmesi	Düşük	DNS güvenlik önlemleri alınmalıdır. Kriptografik yöntemlerle sunucunun taklit edilmesinin önüne geçilmesi. Siber saldırılar için acil müdahale ekibinin bulundurulması
8	Sunuculara yönelik servis dışı bırakma saldırısında bulunulması	İ-seçimde oy kullanmanın engellenmesi, İ-seçimin sabote edilmesi	Orta	Birden Fazla Seçim Kanalı, Kiosk (DRE) kullanımı, Siber saldırılar için acil müdahale ekibinin bulundurulması
9	Sunucuların normal seçim trafiğini kaldırabilecek altyapıda olmaması	Seçmenlerin i-Seçim'de oy kullanılamaması	Düşük	Planlamanın iyi yapılması, Sistemin sertifikasyonunun yapılması
10	Doğal afetler veya acil durumlar	Seçmenlerin i-Seçim'de oy kullanılamaması	Düşük	Seçimin tekrarlanması veya Seçmenlerin klasik seçime yönlendirilmesi

11	Başarısızlıklar veya istemci uygulamasının kalitesi sorunları	Seçmenlerin oy kullanamaması	Orta	Tekrar oy kullanabilme imkanı verilmesi
12	Oy Yönlendirme Sunucusuna servis dışı bırakma saldırısı da düzenlenebilir.	Seçmenlerin oy kullanamaması	Orta	Sunucuların yedeklemesi, Siber saldırılar için acil müdahale ekibinin bulundurulması.
13	Açık Anahtar Altyapısı ile Oy Depolama Sunucusu arasında da bir saldırı gerçekleşebilir.	Seçmenlerin oy kullanamaması	Orta	Sunucuların yedeklemesi, Siber saldırılar için acil müdahale ekibinin bulundurulması
14	Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu aynı anda saldırı altında olması	Oy gizliliğinin ihlali	Orta	Her ne durumda olursa olsun Oy Yönlendirme Sunucusu ve Oy Sayım Sunucusu birlikte işbirliği yapamayacağının prosedürel yöntemlerle garanti altına alınması gerekmektedir. Bu sunucular bağımsız merkezlerin sorumluluğun altında olması gerekmektedir.
15	Oy Sayım Sunucusuna içeriden gelen saldırılar (dışarıya bağlantısı olmadığından dışarıdan saldırı beklenmemektedir)	Oyların değiştirilmesi, Seçimin sonucunun değiştirilmesi	Düşük	Oy Sayım Sunucusu diğer sunuculara nispeten en güvenli sistemdir, çünkü hatta bağlı değildir. Bu yüzden sadece içeriden tehdit gelebilir. Bunların engellenmesi için de Eşik Sır Paylaşımı kriptografik yöntemleri kullanılabilir. Ayrıca bu işlemler gözetmenler tarafından yapılmalıdır. Bireysel ve evrensel doğrulanabilir yöntemleriyle ve sunucuda kötü niyetli kod olmadığı anlaşılabilir.

Şekil 7. e-Seçim'in sunucu güvenliği yönüyle olası tehdit analizi

elektronik seçim uygulamadan önce geniş yelpazeli konsorsiyumlar oluşturmuştur. [24], [25], [26], [15] Ülkemizde de geniş çaplı bir konsorsiyum e-seçimin teknik özelliklerinden sosyo-ekonomik etkilerine, yapılması gereken hukuki değişikliklerden maliyet analizine kadar değişik yönlerden tartışmalı ve geniş anlamda bir rapor hazırlamalıdır. Konsorsiyum bulguları ve bilimsel toplantılar ışığında ülkemiz için bir yol haritası çıkarılmalıdır.

KAYNAKLAR

[1] Fatih Birinci and Mehmet Sabır Kiraz, "Elektronik Seçim: İleri Düzey Kriptografinin Yapı Taşları ve Uygulamaları", Available online at http://www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 5, 84–101, 2011.

[2] Mehmet Sabır Kiraz, Fatih Birinci, and Umut Uludağ, "Elektronik Seçim: Yöntemler, Uygulamalar, Kriptoloji Altyapısı ve Ülkemizdeki Geleceği", Available online at http://www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 4, 76–87, 2011.

[3] "Electronic Voting and Electronic Counting of Votes- A Status Report", Available at http://www.eca.gov.au/reports/electronic_voting.pdf, 2012.

[4] Sokratis Katsikas Lilian Mitrou, Dimitris Gritzalis and Gerald Quirchmayr, "Electronic Voting: Constitutional and Legal Requirements, and Their Technical Implications. The Role of Trust, Participation and Identity in the Propensity to e- and i-vote", Electronic Voting 2010: 65-78. Advances in Information Security, Volume 7, Part I, 2010.

[5] O. Çetinkaya, "Verifiability and Receipt-freeness in Cryptographic Voting Systems", PhD Thesis, Department of Cryptography, Institute of Applied Mathematics, Middle East Technical University, Ankara, Turkey, 2007.

[6] "Punchscan", Available at http://www.punchscan.org/, 2012.

[7] "Scantegrity", Available at http://scantegrity.org/, 2012.

[8] "Prêt à Voter", Available at http://www.pretavoter.com/, 2012.

[9] Ronald L. Rivest, "The ThreeBallot Voting System", Available at http://people.csail.mit.edu/rivest/Rivest-TheThreeBallotVotingSystem.pdf, 2012.

[10] Act, "Uniformed and Overseas Citizens Absentee Voting", Available at http://www.fvap.gov/reference/laws/uocava.html, 2012.

[11] Indrajit Basu, "Estonia Becomes E-stonia", Available at http://www.govtech.com/e-government/Estonia-Becomes-E-stonia.html, 2008.

[12] "Statistics about Internet Voting in Estonia", Available at http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics/, 2008.

[13] "E-Voting Pilot in Austria Cancelled by Constitutional Court", Available at http://www.wu.ac.at/evoting/en/news, 2012.

[14] "E-Vote 2011- Pilot Project in Norway", Available at http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658, 2012.

[15] Ministry of Local Government and Regional Development, "The report: Electronic voting - challenges and opportunities", Available at http://www.regjeringen.no/en/dep/krd/prosjekter/e-valg-2011-prosjektet/omprosjektet/Forprosjektrapport-2006.html?id=604417, 2006.

[16] Uğur Kaşif Boyacı, "Günümüzde Kriptoloji", Available online at www.uekae.tubitak.gov.tr/dergi, BİLGEM Dergisi, Sayı 1, 34–43, 2009.

[17] Mehmet Sabir Kiraz, Süleyman Kardas, Muhammed Ali Bingöl, and Fatih Birinci, "An improved internet voting protocol", *IACR Cryptology ePrint Archive*, 2011.

[18] Berry Schoenmakers, "Lecture Notes. Part 1 Cryptographic Protocols.", Available online at http://www.win.tue.nl/ berry/2WC13/LectureNotes.pdf, 2012.

[19] Véronique Cortier and Cyrille Wiedling, "A formal analysis of the Norwegian e-voting protocol", in *Proceedings of the 1st International Conference on Principles of Security and Trust*

(POST'12). Mar. 2012, Lecture Notes in Computer Science, Springer, To appear.
[20] Collin Mulliner and Charlie Miller, "Injecting SMS messages into smart phones for security analysis", WOOT'09 Proceedings of the 3rd USENIX conference on Offensive Technologies. USENIX Association, Berkeley, USA, 2009.
[21] Arne Ansper, Sven Heiberg, Helger Lipmaa, Tom André Øverland, and Filip van Laenen, "Security and Trust for the Norwegian E-voting Pilot Project E-valg 2011", vol. 5838, pp. 207–222, Springer-Verlag.
[22] "A Threat Analysis on UOCAVA Voting Systems", Available at http://www.nist.gov/itl/vote/upload/uocava-threatanalysis-final.pdf, 2012.
[23] Act, "Uniformed and Overseas Citizens Absentee Voting", Available at http://www.fvap.gov/reference/laws/uocava.html, 2012.
[24] "Workshop on UOCAVA Voting Systems", Available at http://www.nist.gov/itl/csd/ct/uocava-2010-workshop-agenda.cfm, 2012.
[25] D. Wagner D. Rubin Jefferson, B. A. Simons, "A security analysis of the Secure Electronic Registration and Voting Experiment (SERVE)", Available at http://www.servesecurityreport.org, 2004.
[26] UCL KUL ULg UA et UG) Consortium of Belgian universities (ULB, VUB, "BeVoting study of electronic voting systems Part 1 and 2", Available online at http://www.epractice.eu/en/library/281715, 2008.

Dr. Mehmet Sabır Kiraz Orta Doğu Teknik Üniversitesi Matematik Bölümü'nden (ODTÜ) 2000 yılında mezun oldu. Haziran 2000 - Ekim 2002 yılları arasında Pamukbank ve Yapı Kredi Bankası bilgi işlem bölümlerinde çalıştı. 2003 yılında yüksek lisans derecesini Almanya'da Max-Planck Enstitüsü Bilgisayar Bilimleri Bölümü'nden aldı. Doktorasını 2008 yılında Hollanda'da Eindhoven Teknik Üniversitesi Matematik ve Bilgisayar Bilimleri Bölümü'nden aldı. 2008-2010 yılları arasında Amsterdam'da TOMTOM ve Eindhoven'da PHILIPS Research şirketlerinde çalıştı. 2010 yılından itibaren TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde araştırmacı olarak çalışmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Mahremiyet, Anahtar Yönetimi, Güvenli Fonksiyonel Hesaplamalar, Elektronik Seçim, RFID.

Fatih Birinci ODTÜ Matematik Bölümü'nden 1995 yılında mezun oldu. 1998 yılında ODTÜ Matematik Bölümü'nden, 2002 yılında Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü'nden Yüksek Lisans derecesi aldı. TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde toplam 12 yıldır çalşmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Dizi Şifreleme, Anahtar Yönetimi, Formal Analiz, Elektronik Seçim.

Uğur Kaşif Boyacı ODTÜ Matematik Eğitim ve Matematik Lisans (Çift Anadal Programı) bölümlerinden 1994 yılında mezun oldu. 2003 yılında Yıldız Teknik Üniversitesi Matematik Mühendisliği'nden Yüksek Lisans derecesi aldı. 1999 yılından itibaren TÜBİTAK BİLGEM Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'nde araştırmacı olarak çalışmaktadır. İlgi alanları Kriptoloji, Kriptografik Protokoller, Açk Anahtar Altyapısı, Anahtar Yönetimi, Yapay Sinir Ağları.