Donanımsal Truva Atı Tespiti Etkinlik Analizi

M. Şahinoğlu, M. Öztemür ve B. Soysal

***Özet*—Bilgi güvenliğinin sağlanması tüm dünyada üzerinde çalışılan kritik bir konudur. Bu konuda ortaya çıkan en önemli tehditlerden birisi donanım yapıları üzerine truva atı yerleştirilmesidir. Sahip olduğu kritik önem nedeniyle tüm dünyada donanımsal truva atlarının tespitine yönelik çalışmalar yapılmaktadır. Bu kapsamda farklı yöntemler önerilmektedir. Bu yöntemlerin farklı açılardan birbirlerine karşı avantaj ve dezavantajları olabilir. Truva atı tespitinde başarıya ulaşılabilmesi için bu yöntemlerin güvenlik ihtiyacına bağlı olarak etkin bir şekilde kullanılması gerekmektedir. Bu makale kapsamında, literatürdeki truva atı tespit yöntemleri anlatılacak ve bir etkinlik analizi yapılacaktır.**

***Anahtar Kelimeler*—Truva atı, Arka kapı, Yan kanal analizi, Mantıksal davranış testi.**

***Abstract*—Information security is an important subject studied on all over the world. One of the most important threats encountered in this subject is placement of trojan horse on hardware. Studies regarding the detection of trojan horse on hardware have been carried out all over the world because of its critical importance. Different methods are advised on this field. These methods may have advantages and disadvantages to each other in some terms. These methods must be used efficiently for detecting the trojan horse depending on the need of security. In the scope of this article, trojan dedection methods in literature will be explained and an efficency analyze will be presented.**

***Keywords*—Trojan horse, Backdoor, Side channel analysis, Logic test.**

I. GİRİŞ

TRUVA atı, adını Troya kentini ele geçirmekte kullanılan efsanevi tahta truva atından alır. Bir armağan gibi gösterilen bu büyük at, aslında Troya surlarını geçip Troya kentini ele geçirecek Yunan askerlerini taşımıştır. Yaklaşık 10 yıl süren savaş ile ele geçirilemeyen şehir, yüksek güvenlik sağlayan surlarına rağmen bu at sayesinde fethedilmiştir.

Asırlar sonrasında ise teknoloji ilerlemiş; ancak güvenlik önlemlerini bertaraf etmek için insanoğlu yine benzer yöntemlere başvurmuştur. Troya atı durumuna benzer senaryolar teknoloji ürünleri üzerinde de uygulanmaya başlamıştır. IT sektöründe ilk karşılaşılan truva atı 1974 yılında oluşturulan "Pervade-Animal" isimli bir yazılımdır. Aslında güvenlik açıklığı oluşturmayı amaçlamayan bu yazılım, ticari üstünlük sağlamak amacıyla birçok bilgisayara sızmayı başarmıştır. Daha sonra 1980'li yıllarda güvenlik ihlalleri oluşturan truva atları da piyasada yayılmaya başlamıştır [1],[2].

M. Ş. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: muhammet.sahinoglu@ tubitak.gov.tr).

M. Ö. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: muhammet.oztemur@ tubitak.gov.tr).

B. S. TUBİTAK BİLGEM Siber Güvenlik Enstitüsü , Gebze, KOCAELİ 41470 TÜRKİYE (Telefon Nu: 0262 648 10 00; fax: 0262 648 11 00; e-posta: betul.soysal@ tubitak.gov.tr).

Truva atları ilk aşamada daha çok yazılıma özgü bir uygulama gibi dikkate alınmıştır. Ancak son yıllarda, donanım yapıları içinde truva atlarının ciddi bir tehdit oluşturabileceği bilinci ortaya çıkmıştır. Bu durum "donanımsal truva atı" teriminin ortaya çıkmasına ve bu alanda ciddi çalışmalar yapılmasına zemin oluşturmuştur.

Donanımsal Truva Atı, "*elektronik bir devrenin içerisine, kullanıcının isteği olmaksızın, kasıtlı olarak yerleştirilmiş kötücül devre yapısı"* olarak tanımlanmaktadır [3]. Bu yapı, devrenin normal işleyişi ya da boşta beklemesi esnasında devrenin işlevlerini değiştirebilir, ekstra bir işlem yapmasına sebep olabilir, hatta güvenlik mekanizmalarını devre dışı bırakabilir. Böylece, kritik verilerin işlenmesinde, iletiminde ya da saklanmasında kullanılan ürünün verileri istenmeyen taraflara sızdırması sağlanabilir. Ayrıca, devrelerin içerisine yerleştirilen truva atları ile kritik işlevlerde kullanılmak üzere tasarlanan ürünler planlanmayan ve öngörülemeyen bir şekilde servis dışı kalabilirler [3].

Truva atı kavramı ile bir arada değerlendirilen kavramların biri de arka kapı'dır. Backdoor olarak da yaygın şekilde bilinen arka kapı, *"bir programa, bir online sisteme veya bir bilgisayar sistemine erişmek için standart dokümanlarında belirtilmeyen bir özellik"* demektir [4]. Arka kapılar, yazılımı veya daha genel anlamda sistemi meydana getiren kişiler tarafından oluşturulurlar. Genelde sadece bu kişiler tarafından bilinirler [4]. Arka kapı, bir bakıma truva atı yapısının özel bir hali olarak ta düşünülebilir.

II. GERÇEK HAYATTA TRUVA ATI ÖRNEKLERI

Donanım yapıları içerisine truva atı ve arka kapı yerleştirme uygulamaları ABD-Rusya arası soğuk savaş dönemine dayanmaktadır [5]. Bu dönemde Rusya ve ABD donanımsal truva atı uygulamaları ile birbirlerinin sinyallerini gizlice dinlemeyi başarmışlardır. Daha sonraki yıllarda da Avrupa ülkelerinin Suriye tarafından kullanılan radarlar üzerindeki bir işlemciye, Suriye'nin İsrail'i izlemesini engellemek amaçlı donanımsal truva atı yerleştirdiğinden ve bu şekilde çalışmasını durdurduğundan şüphelenilmiştir [5].

Günümüzde de, donanımsal ürünlerde truva atı ve arka kapı varlıkları konusunda medyada her gün yeni haberler çıkmaktadır. Örneğin, geçtiğimiz günlerde Avusturya Güvenlik Kurumu SEC Consult, Barracuda firmasına ait birçok üründe dokümante edilmeyen arka kapı bulunduğunu bildirmiştir. Firma, bunların üretim aşamasındaki deneysel çalışmalardan sonra unutulan özellikler olduğunu iddia etmiş olmakla beraber dolaylı bir şekilde bu arka kapıların varlığını kabul etmiştir. Cihazlara tasarımı esnasında gömülmüş olduğu iddia edilen bu arka kapılar, cihaz üzerinde kolayca aktif hale getirilebilen ek bir yönetici hesabı şeklinde tanımlanmıştır. Dolayısı ile bu yapılar, saldırganın uzaktan erişim ile yetkilendirilerek ağ üzerindeki hassas veriye erişmesine olanak sağlamaktadır [6],[7].

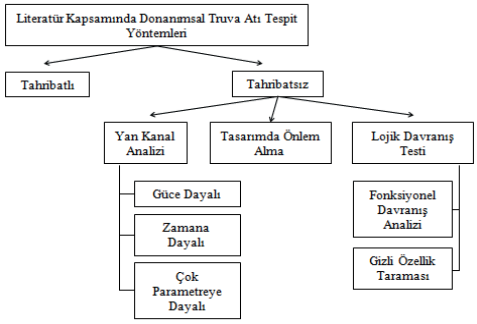
Benzer bir iddia da piyasada yaygın olarak kullanılan ZTE ve Huawei haberleşme cihazları için mevcuttur. Amerika, Çin menşeli ZTE ve Huawei haberleşme cihazlarının truva atı içermesi durumuna yönelik bir araştırma raporu yayınlamış ve bu cihazların kritik projeler içerisinde kullanılmasını engellemiştir [8].

Bu alanda ortaya çıkan en son gelişmelerden bir tanesi de HP firmasının yaygın olarak kullanılan depolama cihazlarında, kullanıcıların oluşturduğu hesaplar dışında, üretimden gelen dokümante edilmemiş erişim haklarının bulunduğunun itiraf etmesidir [9].

Donanım bazında, ilk arka kapı tespit edilmesi ise 2012 senesi yazında olmuştur. Sergei Scorobagatov bir askeri çip olan ACTEL FPGA üzerinde bulduğu arka kapıyı göstermiştir [10].

III. Donanımsal Truva Atı Tespit Yöntemleri

Donanımsal truva atları elektronik sistemlerin güvenliği için büyük bir tehdit oluşturduğundan bu yapıların tespiti için de yoğun bir çalışma yapılmaktadır. Bu çalışmalarda kullanılan yöntemler duruma göre farklılık göstermektedir. Donanımsal truva atlarının tespit edilmesine yönelik çalışmalar incelendiğinde, bu yöntemlerin Şekil 1'de görüldüğü gibi sınıflandırılabileceği değerlendirilmiştir.



Şekil 1. Donanım yapıları içinde truva atı tespiti için literatürde tanımlanmış yöntemlerinin sınıflandırması

A. Tahribatlı Yöntemle Truva Atı Tespiti

Truva atlarının tespit edilmesinde akla ilk gelen yöntemdir. Analiz edilecek olan elektronik devrenin öncelikle üst koruma katmanı açılır. Daha sonra gelişmiş cihazlar ve çeşitli kimyasallar kullanılarak aşama aşama tüm çip katmanları taranarak tersine mühendislik yapılır. Tersine mühendislikle elde edilen görüntüler birleştirerek, çipin en başta tasarlandığı şekilde üretildiğine karar verilir. Tersine mühendislik için en yaygın kullanılan teknik, elektron mikroskobu ile tarama ve light-induce voltage iteration tekniklerdir [14].

Tersine mühendislik yaparak truva atı aramak hem maliyet hemde zaman açısından çok zor bir uygulamadır. Çünkü donanımsal truva atları, bir mantıksal devre üzerinde az sayıda mantıksal kapının eklenmesi, kaldırılması veya modifiye edilmesi suretiyle gerçeklenebilir. Oysa modern bir elektronik devrede milyarlar düzeyinde bu şekilde kapının olması söz konusu olabilir. Bu kadar geniş bir yapı içerisinde truva atını tespit etmek samanlıkta iğne aramakla eşdeğer bir çalışma olabilir [3].

Bununla beraber, diğer bir çok truva atı tespit yöntemi için referans olarak ihtiyaç duyulan güvenilir devre (golden IC) [17] temini için tersine mühendislik yöntemi kullanılabilir.

B. Tahribatsız Yöntemle Truva Atı Tespiti

Tahribatlı devreler ile truva atı tespitinin büyük zorluk içermesi, tahribatsız yöntemlere yönelik çalışmalar yapılması ve bunların kullanılması sonucunu doğurmuştur. Tahribatsız truva atı tespit yöntemleri farklı gruplara ayrılmaktadır.

Mantıksal Davranış Testi

IC'lerin davranışsal yapılarının analiz edilmesi esasına dayanır. Fonksiyonel davranış analizi ve gizli özellik tarama olmak üzere iki grupta incelenir.

Fonksiyonel Davranış Analizi, bir elektronik devre girişine belli test vektörlerinin verilerek çıkışların izlenmesi ve beklenenin dışında bir çıkış elde edildiğinde bir anormalliğin var olduğunun tespit edilmesi esasına dayanır. Aslında bu yöntem, daha çok fonksiyonel hataların tespiti için geçerli bir uygulamadır [15]. Bununla beraber, parametrik truva atlarının (devrenin yapısını değiştirerek truva atı ekleme) tespiti için de kullanılabilir. Bu testlerde kullanılan otomatik test paternleri, normalde devrede olmayan bir fonksiyonu aktif etme yeteneğinde olmadıklarından (devreye ekleme/çıkarma yapılarak konulan) fonksiyonel truva atlarının (devreye ekleme/çıkarma yapılarak konulan) tespitinde kullanılamazlar [16].

Mantıksal test ile truva atı aramanın en büyük problemi büyük elektronik devre yapıları nedeniyle taranması gereken uzayın çok geniş olmasıdır. Uzayın bu kadar geniş olması, test vektörleri ile tüm uzayı taramayı neredeyse imkansız hale getirmektedir. Örneğin; sadece 4 trigger noktası ve 1 payload noktası olan bir truva atı düşünülsün. 451 kapılı c880 tipinde küçük bir ISCAS-85 Benchmark devresinde bu truva atının yerleştirilmesi için 10^{11} muhtemel nokta mevcuttur ve truva atını tetiklemek için yaklaşık 10^{9} deneme yapılması gerekir [17].

Bu kısıtın aşılması için bazı metodlar önerilmiştir. Jha ve Jha bu durum için rastsallığa dayalı bir yöntem önermiştir [18]. Devrenin girişlerine değişik paternler uygulanmıştır. Devrenin bu girişlere verdiği cevaplara bağlı olarak devreye ait olasılıksal (probabilistic) bir imza tespit edilmiştir. Daha sonra aynı paternler, analiz edilen devrelere uygulanmıştır. Devrelerin davranışları daha önce elde edilen olasılıksal imza değeri ile karşılaştırılmıştır. Eğer bir farklılık varsa bu devrelerin truva atlı olduğu sonucuna varılmıştır.

Wolf ve arkadaşları truva atı tespiti için devre üzerinde nadir olarak aktif olan alanlara yoğunlaşmışlardır. Nadir olarak aktif olan bölgeleri tetikleyen test vektörleri üretilerek elektronik devrenin davranışı gözlemlenmiştir [19]. Chackraborty ve arkadaşları da benzer bir yöntemle truva atı tespitinin etkinliğini artırmaya çalışmışlardır [20].

Gizli Özellik Tarama, analiz edilen yapının tanımlı olmayan özelliklerinin tespit edilmesi esasına dayanır. Bu konu ile ilgili bir çalışma Skorobogatov ve Woods tarafından gerçeklenmiştir [10]. Bu çalışmanın literatürdeki diğer donanımsal truva atı tespiti çalışmalarından önemli bir farkı gerçek bir donanım üzerinde gerçekleştirilmiş olmasıdır. Analiz edilen eleman ACTEL firmasına ait ProAsic3 tipi FPGA elemanıdır. Çalışma kapsamında araştırmacılar, analiz edilen FPGA elemanının JTAG arayüzüne yoğunlaşmışlardır. Bu arayüz aracılığı ile FPGA'e ürün dokümanında tanımlı olmayan komutlar

göndererek aynı zamanda elemanın çektiği gücü dinlemişlerdir. Çekilen gücün analizinden, JTAG arayüzünde tanımlı olmayan bazı başka komutların varlığını tespit etmişlerdir. Bu komutların birinin kullanılmak için 128 bit uzunluğunda bir veri talep ettiğini tespit etmişlerdir. Gelişmiş yan kanal analiz teknikleri kullanarak 128 bit uzunluğundaki bu değer elde edilmiştir. Bu anahtar kullanıldığında çipte tanımlı olmadığı belirtilen geri okunma özelliğinin aktif olduğu tespit edilmiştir. Ayrıca çip özelliklerinde "değişmez" olarak belirtilen bazı konfigürasyon bölgelerinin programlanabilir hale geldiği tespit edilmiştir.

Yan Kanal Analizi

Truva atının tespit edilmesinde, devrelerin çalışması esnasında istemsiz olarak yaydıkları yan kanal bilgilerinden faydalanılır. Bu yan kanal bilgisi devrenin güç-akım tüketimi, elektromagnetik yayınımı, çalışma frekansı, çalışma zamanı değerleri olabilir. Yan kanal analizi ile truva atı tespitinde temel yaklaşım olarak, güvenilir devreye ait yukarıda örnekleri verilen yan kanal verileri ölçülerek bir karakteristik çıkarılır. Daha sonra analiz edilecek devrelerin yan kanal bilgilerine bağlı karaktreristikleri orjinal devre ile karşılaştırılarak truva atının olup olmadığına karar verilir.

Yan kanal analizi ile yapılan truva atı tespit çalışmaları, kullanılan yan kanal parametresine göre sınıflandırılabilir.

Güç Tabanlı Analiz, truva atı tespitinde yan kanal parametresi olarak gücü kullanır.

Agrawal ve arkadaşlarının yaptıkları çalışma, truva atı tespitinde gücü ve dolayısıyla yan kanal bilgisini kullanan ilk çalışmadır [11]. Çalışmada öncelikle, rastgele seçilmiş bir grup elektronik devreye rastgele giriş verileri verilmiş ve devrelerin güç ölçümleri alınmıştır. Bu güç tüketimi değerleri bir imza değeri (fingerprint) olarak kabul edilmiştir. Geride kalan devrelere aynı rastgele veriler uygulanarak güç ölçümü almışlardır. Elde edilen değerleri, güvenilir devreye ait imza değeri ile karşılaştırmışlardır.

Yan kanal analizi ile truva atı tespitinde en önemli problemlerden biri, üretim saçılmasından kaynaklanan işlem gürültülerinin (process variation) devredeki yan kanal parametrelerini etkilemesidir. Bu parametrelerde yaşanan değişimler, truva atlarının devreye katacağı yan kanal değerlerinin maskelenmesine neden olmaktadır [26]. Bu da özellikle küçük truva atlarının tespit edilmesine engel oluşturmaktadır. Rad ve arkadaşları tarafından, process değişkenlerinin devreye etkisini azaltmak için devreye bölge tabanlı "transient power signal analizi" yapılması önerilmiştir [22].

Banga ve Hsiao [24]'de truva atının harcadığı gücün devrenin toplam güç tüketiminde fark edilebilir hale gelmesini sağlamak için bölge tabanlı truva atı tespit yöntemini önermiştir. Yine Banga ve Hsiao [25]'da truva atının harcadığı gücün devrenin toplam güç tüketiminde fark edilebilir hale gelmesini sağlamak için geçiş sayısı minimizasyonu (toggle minimization) yöntemini önermiştir. Geçiş sayısı minimizasyon yönteminde truva atının çektiği güç sabit kalırken devrenin çektiği toplam gücü azaltmak hedeflenmiştir.

Alkabani [26]'da truva atının tespitinin hassasiyetini artırmak için tutarlılık tabanlı kapı seviyesi karakterizasyonu yöntemini önermiştir. Alkabani çalışmasında tutarlılık metriği olarak devrenin gerçek güç ölçümleri ile simülasyon yoluyla elde edilmiş güç ölçümlerinin ölçekleme değerinin arasındaki farkı kullanmıştır. Ölçekleme değeri; kapının gerçek güç ölçüm değerini hesaplarken matematiksel işlemlerle elde edilen güç ölçümünün işlem (process) gürültüsünden kaynaklı çarpılması gereken sabit değeridir.

Reece, yan kanal analizi ile Truva atı tespitinde yaygın olarak ihtiyaç duyulan güvenilir devre kullanılmadan Truva atı tespiti yapan bir yapı önermiştir [29],[30]. Elektronik devre tasarımında kullanılan, Process Development Kit ile elektronik devrenin işlem gürültüsü (process variation) ile etkilenmeyecek parametreleri için devreye ait bir imza çıkarılmıştır. Bunun için elektronik devreye farklı voltaj beslemeleri verilirken elektronik devre üzerinde iki nokta arasında oluşan akım değerleri dikkate alınmıştır.

Güç analizi ile Truva atı tespitinde, sonuç alınması için, devreden alınan güç işaretlerinin işlenmesi önem kazanmaktadır. Literatürde bu kapsamda aşağıdaki gibi çalışmalar yapılmıştır.

Baktir ve arkadaşları, simülasyon ortamında gerçekledikleri 16 devreden 8 tanesine Truva atı yerleştirmişlerdir [31]. Daha sonra Truva atı olmayan devreler için elde edilen güç işaretleri ile truva atı içeren devreler için elde edilen güç işaretlerini karşılaştırmışlardır. Güç işaretleri için klasik yöntemle zaman uzayında karşılaştırma yapıldığında sonuç alınamamıştır. Bununla beraber, Discrete Waveleth Transform, Spektogram ve Neural Network kullanılarak işaretler işlendiğinde truva atlarının tespit edildiği gösterilmiştir.

L.Gwon ve arkadaşları DISTROY adını verdikleri bir test ortamıyla etkin sinyal analizi içeren bir yöntem önermişlerdir [33],[34]. Çalışmalarında genel olarak simülasyon ortamından elde ettikleri güç ölçümleri ile gerçek devreden aldıkları güç ölçümlerini karşılaştırarak truva atını tespit etmişlerdir. Ölçümlerin karşılaştırılması öncesinde güç ölçümlerinin işaretin farklı özellikler baz alınarak sıkıştırılması esasına dayanan "compressive sensing" işlemini uygulamışlardır. "Compressive sensing" yöntemi ile yöntemin kullanılmadığı sisteme oranla 10 kat daha hızlı ve 1000 kat daha az ölçüm analiz edilerek truva atı tespit edilmiştir.

ASIC sistemler için yapılan çalışmalar için ASIC modüllerini temin etme zorluğu, araştırmacıları simülasyon üzerinde çalışmaya yöneltmiştir. Oysa bu çalışmaların başarısının değerlendirilmesi için gerçek devreler üzerinde uygulamalar yapılması önemlidir. Bu durum araştırmacıları ASIC yapısının bir benzeri olarak kabul edilen FPGA elemanları üzerinde çalışmalar yapmaya yöneltmiştir.

Wang ve Luo, Spartan3E FPGA üzerinde DES algoritması gerçekleyerek pratik olarak Truva atı yerleştirme ve bulma çalışması yapmışlardır [35].

Zaman Tabanlı Analiz ile truva atı tespiti yapılmasında, yukarıda anlatılan güç tüketimi yerine zaman gecikmeleri kullanılır.

Jin ve Markis, çip üzerinde yer alan kapılar arası gecikmeleri ölçerek truva atı tespiti yöntemi önermişlerdir [36]. Önerdikleri yöntemde, öncelikle güvenilir tasarım üzerinden kapı gecikmeleri ölçülerek bu değerler bir imza (fingerprint) olarak kabul edilmiştir. Aynı yöntemle, değerlendirilen her bir devre için karakteristik çıkarılmıştır. Değerlendirilen devrelerin karakteristikleri, güvenilir devre

ile karşılaştırılarak truva atı olup olmadığına karar verilmiştir.

Wei ve arkadaşları, truva atı tespit etmek için zaman gecikmelerini kullanan yöntemlerin en büyük sıkıntısı olan paralel yollar probleminin çözümünüde içeren bir yöntem önermişlerdir [37]. Zira zaman gecikmesine bakılacak kısmın girişi ile çıkışı arasında birden fazla yol olabilmektedir (reconvergent path). Çalışmada, bu yollara test noktası (D Flip flop) eklenerek ve oradan zaman gecikmesini ölçerek paralel yol problemi ortadan kaldırılmıştır.

Yan kanal analizi ile truva atı tespitinde kullanılan bir yöntem de, birden fazla yan kanal parametresinin birlikte kullanılmasıdır. Çok Parametreli Analiz olarak bilinen bu yöntem kapsamında aşağıdaki çalışmalar yapılmıştır.

Narasinham ve arkadaşları simülasyon ortamında ve sonrasında FPGA kullanarak dinamik akım (I_{DDT}) ve çalışma frekansının maksimum değerini (F_{max}) birlikte kullanarak truva atı tespit etme yöntemini önermişlerdir [12]. I_{DDT} ve F_{max} için bir eğri oluşturulmuş ve eğriden farklılaşan değerler için truva atı tespit edilmiştir. Narasimham ve arkadaşları [13]'te de aynı yöntemle truva atı tespiti üzerinde çalışmışlardır. Ancak bu yöntemde, ek olarak truva atını tespit etme hassasiyetini artırmak için "power gating ve operand isolation" yöntemini kullanmışlardır. Bu yöntem, devrenin analiz edilen kısmı aktif iken geriye kalan kısımlarının pasif hale getirilmesi esasına dayanır.

Potkonjak ve arkadaşları, Kapı seviyesi karekterizasyonu (Gate Level Characterization) ile truva atı tespitini önermişlerdir [27]. Karakterizasyonun çıkarılmasında, statik güç tüketimi ve zaman gecikmesini kullanmışlardır.

Devrenin kontrol edilebilir kapı sayısını artırmak ve karakteristiği çıkarılan kapı sayısını artırmak için Wei [28]'de sıcaklık iyileştirmesini önermiştir. Bir kapının sıcaklığını artırmak için dışarıdan bir sistem ile ısıtmak yerine kapıların 0-1 geçişleri ile doğal yoldan sağlanan sıcaklık artımını kullanmıştır.

Tasarımda Eklenen Yapılar İle Truva Atı Tespiti

Bu yöntemle Truva atı tespitinde, elektronik devrenin üretilmesinden önce devreye truva atı eklenmesi durumunda bunu anlayan bir yapı eklenir. Bu yapı çoğu zaman bir devre veya devre parçasıdır. Literatürde "Design for Hadware Trust" olarak da bilinir. Bu yöntemin tasarıma hakim olunması durumunda uygulanabilen bir yöntem olduğu söylenebilir. Dolayısıyla ASIC devreler üzerinde uygulanabilir. Ancak araştırma çalışmalarında, ASIC üretmenin zorluğu nedeniyle, deneysel olarak FPGA üzerinde de uygulandığı görülmektedir.

Chacraboty ve arkadaşları, mantıksal test kullanarak truva atının eklenmesini tespit eden bir yapı önermişlerdir [38]. Bunun için devreye bir test lojiği ve I/O portları eklenir. Çip normal mod ve saydam mod (transparent mod) olmak üzere 2 modu içerir. Çipin saydam modda olduğu durumlarda devrenin bir imza değeri üreterek çıkışına vermesi sağlanır. Test işlemi, daha önce tanımlanmış anahtar benzeri bir paternin devreye verilmesi ile başlar. Truva atlarının devrelerin en az aktif olan kısımlarına yerleştirileceği varsayımından hareketle, truva atının tespitini sağlayan kontrol devrelerinin de devrelerin en az aktif olan bu kısımlarını gözlemlemesi gerekir. Verilen başlangıç değeri ile kontrol devresinin gözlemlediği değerlerde beklenen değerlerden (imza) farklı bir değer tespit edilmesi halinde truva atının varlığı tespit edilir. Bu yöntemde, devreye kontrol devreleri nedeniyle ek tasarım alanı ve karmaşıklığı oluşması en önemli dezavantajdır.

Bu yapıdan daha karmaşık ancak daha etkin bir önleyici truva atı tespit yöntemi Abromici ve Bradaley tarafından önerilmiştir [39]. Elektronik devre içine, devrenin çalışması esnasında gerçek zamanlı kontrol yaparak truva atını tespit eden bir kontrol lojiği eklenmektedir. DEFENCE (DEsign-For_ENabling-Security) mantıksal olarak da bilinen yapının en önemli özelliği, elektronik devrenin üretilmesinden sonra programlanabilme esnekliğine sahip olmasıdır.

Selmani ve arkadaşları [15] ve [40]'de, fonksiyonel Truva atı devrelerindeki geçiş olaylarının olasılığının artırılmasına dayanan bir yöntem önermişlerdir. Daha sonra bu geçişlerin üretilme zamanları analiz edilmiştir. Yöntemde, öncelikle geometrik dağılım yöntemiyle devre üzerindeki yollarda geçiş olasılıkları hesaplanır [40]. Daha sonra belli bir eşik değeri altında geçiş olasılığı olan yollar üzerine dummy flip floplar yerleştirilir. Bu yöntemle, truva atlarının saklanma ihtimalinin yüksek olduğu devrenin az aktif olan bölgelerinde aktivasyon oranının artırılması hedeflenmiştir.

Bu metodun daha uygulanabilir bir benzeri Li ve Lach tarafından önerilmiştir [41]. Bu metotta çipe yazmaçlar ve kapılar eklenerek, yazmaçtan yazmaca gecikmeler ölçülmüştür.

Reece ve arkadaşları [29] ve [32]'de, FPGA üzerinde belli noktalara ring osilatörler koyarak, ek bir müdahaleyapıldığında bu osilatörlerin frekanslarındaki değişime göre Truva atı tespiti yapan bir yöntem önermişlerdir.

Zhang ve Tehranipoor bu fikri daha ileri düzeyde uygulayan bir çalışma yapmışlardır [42]. Elektronik devre üzerine birbirleri ile bağlı ring osilatör networkü koyup, muhtemel bir trojeni bu osilatörlerdeki değişimden tespit etmeye çalışmışlardır.

Ferraiuolo ve arkadaşları [43]'de aynı yöntemi, 90 nm tenolojisinde gerçeklenmiş ASIC devreler üzerinde analiz etmiştir.

Banga ve Hsiao, elektronik devre üzerinde yer alan mantıksal kapıların başka kapılar ile gerçeklenebilme avantajından faydalanan bir yöntem önermiştir [44]. Bu yöntemde de amaç, truva atlarının daha az aktif olan noktalara konulması varsayımına karşın bu noktalardaki aktivasyon oranını yükseltmektir. Bu amaçla girişlerindeki değişimden daha az etkilenen mantıksal kapılar daha fazla etkilenen mantıksal kapılarla değiştirilmiştir.

Benzer mantıksal temele dayanan bir çalışma Alkabani tarafından gerçekleştirilmiştir [45]. Truva atını tespit etmek için devrenin dual'iyle (aynı devrenin eş değerinin diğer mantıksal kapılarla gerçeklenmiş hali) beraber değerlendirmesinden yola çıkmışlardır. Ayrıca, genellikle truva atı eklenen bir devrede truva atının tetiklenmesi için nadir gerçekleşen bir giriş değerinin seçileceği varsayımıda temel alınmıştır. Bu amaçla, truva atı tespiti için devrenin nadir aktif olan bölgeleri için kapılar seviyesinde duali alınmıştır. Bu şekilde Truva atlarına ait giriş nadir gerçekleşme durumu sık gerçekleşme durumuna dönmüş olmaktadır. Böylelikle truva atı tespit için truva atının çoğu

giriş vektörünün devreye girdiği bir devre elde edilmiş olmaktadır.

Lamech ve arkadaşları, yol gecikmelerinden truva atını tespit etmek için REBEL (Regional Delay Bevavior) isimli gömülü test yapısını önermişlerdir [46]. Truva atı olarak yollara kapasite ya da kapı yerleştirmişlerdir.

IV. SONUÇ

Literatürde donanımsal truva atlarının tespitine yönelik uylanan yöntemler etkinlik açısından farklılık göstermektedir. Uygulanan yöntemler ve bunların etkinliği Tablo-1'de özetlenmiştir. Tabloda yöntemlere ilişkin tüm alt kırılımların gösterilmesi yerine etkinlik açısından birbiriyle farklılık oluşturacak kadar üst seviye olan başlıklar gösterilmiştir. Yöntemlerin etkinlikleri; altyapı ihtiyacı, maliyet, uygulama zamanı, başarı şansı ve uygulanabilecek ürün kapsamları dikkate alınarak incelenmektedir.

TABLO I
TESPIT YÖNTEMLERI ETKINLIK ANALIZI

		Altyapı İhtiyacı	Gerçekleme Kolaylığı	Zaman	Başarı Oranı	Tekrarlama Kolaylığı	Uygulanabilecek Kapsamı	Toplam Etkinlik
Tahribatlı	Tersine Müh.	Çok Gelişmiş	Çok Zor	Çok Uzun	Yüksek	Çok Zor	Dar	Düşük
	Tasarımda Önlem	Gelişmiş	Zor	Uzun	Yüksek	Zor	Dar	Orta
Tahribatsız	Mantıksal Davranış	Orta	Kolay	Orta	Düşük	Orta	Çok Geniş	Orta
	Yan Kanal Analizi	Orta	Orta	Orta	Orta	Orta	Geniş	Yüksek

Tahribatlı yöntemle donanımsal truva atı tespiti her ne kadar başarı şansı yüksek olsa da (tespit sonunda somut bir kanıta ulaşılmış olsa da) bir çok dezavantaj içermektedir. Bu yöntem için ihtiyaç duyulan; altyapı, zaman ve maliyet çok fazladır ve geliştirilen altyapı ve kazanılan yetenek ile çalışmayı tekrarlamak her seferinde yeniden yüksek maliyet ve zaman gerektirecektir. Ayrıca tersine mühendislik çalışması ancak bir referans noktası olarak serim (layout) bilgisi gibi kritik tasarım verilerine sahip olan ASIC uygulamalar için gerçeklenmeye uygundur. Bu nedenlerden dolayı literatürde etkin bir donanımsal truva atı tespit yöntemi olarak önerilmemektedir.

Tahribatsız yöntemlerin etkinliğini farklı alt başlıklar altında incelemek uygun olacaktır. Tasarımda kontrol devresi ekleyerek truva atının tespit edilmesi de tahribatlı tersine mühendislik yöntemi kadar olmasa da altyapı, zaman ve maliyet açısından dezavantaja sahiptir. Her devre için yeniden tasarım yapılması gerekeceği ve yine kontrol devresinin yer kaplaması sorunu tekrar edeceği için bu yöntemin yetenek kazanımı sonrasında yine zorluğu devam etmektedir. Uygulama alanıda, ASIC yapıları ile sınırlıdır. Yöntemin getirdiği yüklerin tahripli yöntem kadar fazla olmaması ve ASIC yapıları için başarı şansının yüksek olması, bu yöntemin literatürde, özellikle ASIC yapıları için etkin sayılabilecek bir yöntem olarak kabul edilmesini sağlamıştır.

Mantıksal davranış testi; alt yapı, zaman ve maliyet açısından avantajlı bir sistemdir. Aslında fonksiyonel bozukluklar için özelleşmiş bu yöntemin başarı şansının da düşük olduğu görülmektedir. Bu durum truva atlarının fonksiyon bozuklukları ile kolayca farkedilemeyeceği varsayımına dayanmaktadır. Ancak bu yöntemin diğer tüm yöntemlere göre çok büyük bir avantajı mevcuttur. Diğer yöntemlerin hiçbirinin çalışmadığı noktalarda bu tespit yöntemine ihtiyaç duyulmaktadır. Örneğin, hakkında hiçbir ön bilgi bulunmayan bir elektronik bileşen veya son ürün üzerinde truva atı aranmasına ilk olarak mantıksal davranış testi ile başlanabilir. Bu geniş kapsamı nedeniyle mantıksal davranış testinin etkin bir yöntem olduğu değerlendirilmektedir.

Yan kanal analizi yöntemi altyapı, zaman ve maliyet açısından avantajlı bir sistemdir. Uygulama kapsamı olarak da bir çok yapı için kapsayıcı durumdadır. Ayrıca mantıksal davranış testi ve tasarımda önlem alma yöntemleri için de yardımcı bir analiz türüdür. Tüm bunlarla beraber başarı şansının da düşük olmaması, bu yöntemi şu an litaratürde tanımlı donanımsal truva atı tespit yöntemleri arasında en etkin yöntem haline getirmiştir.

KAYNAKLAR

[1] K. Jurgen : Selbstreproduktion bei programmen' (VX heavens) Vx.netlux.org. http://vx.netlux.org/lib/mjk00.html. Retrieved 2010-07-10.,

[2] "Fred Cohen 1984 "Computer Viruses – Theory and Experiments". Eecs.umich.edu. 1983-11-03. http://www.eecs.umich.edu/%7Eaprakash/eecs588/handouts/cohen-viruses.html. Retrieved 2012-03-29., Communication of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763.

[3] M. Beaumont, B. Hopkins, Newby T.: Hardware Trojans – Prevention, Detection, Countermeasures (A Literature Review), Defence Science and Technology Organisation (2011)

[4] http://www.webopedia.com/TERM/B/backdoor.html

[5] T. Huffmire, C. Irvine, T. D. Nguyen , T. Levin, R. Kastner: Handbook of FPGA Design Security, Springer (2010).

[6] http://isc.sans.edu/diary/Barracuda+Back+Door+/15004

[7] https://www.seconsult.com/fxdata/seccons/prod/temedia/advisories_txt/20130124-0_Barracuda_Appliances_Backdoor_wo_poc_v10.txt

[8] http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/Huawei-ZTE%20Investigative%20Report%20(FINAL).pdf

[9] http://www.theregister.co.uk/2013/07/11/hp_prepping_fix_for_latest_storage_vuln/

[10] S. Skorobogatov, C. Woods : Breakthrough silicon scanning discovers backdoor in military chip. Cryptographic Hardware and Embedded Systems Workshop - CHESS (2012).

[11] D. Agrawal, S. Baktir, D. Karakoyunlu, P. Rohatgi, B. Sunar: Trojan detection using ic fingerprinting. IEEE Symposium on Security and Privacy. (2007).

[12] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff : Multiple-Parameter Side-Channel Analysis: A Non-Invasive Hardware Trojan Detection Approach. IEEE (2010)

[13] S. Narasimhan, D. Du, R. S. Chakraborty, S. Paul, F. Wolff, C. Papachristou, K. Roy, S. Bhunia: Hardware Trojan Detection by Multiple-Parameter Side-Channel Analysis. IEEE Transaction on Computers. (2012)

[14] B. Sanno: Detecting Hardware Trojans. Ruhr-University Bochum, Germany. (2009).

[15] H. Salmani, M.Tehranipoor, J. Plusquellic: A Novel Technique for Improving Hardware Trojan Detection and Reducing Trojan Activation Time. IEEE Transaction on very large Scale Integration (VLSI) Systems, VOL. 20, NO. 1. (2012).

[16] X. Wang, M. Tehranipoor, J. Plusquellic: Detect-ing Malicious Inclusions in Secure Hardware, Challenges and Solutions. 1st IEEE International Workshop on Hardware-Oriented Security and Trust - HOST'08. (2008).

[17] R. S. Chakraborty, S. Narasimhan, S. Bhunia: Hardware trojan: Threats and emerging solutions. (2010).

[18] S. Jha, S. K. Jha: Randomization based probabilistic approach to detect trojan circuits. High-Assurance Systems Engineering, IEEE International Symposium on 0, 117–124. (2008).

[19] F. Wolff, C. Papachristou, S. Bhunia, R. S. Chakraborty: Towards Trojan-Free Trustedelektronik devres: Problem Analysis and Detection Scheme. European Design and Automation Association - EDAA. (2008).

[20] R. S. Chakraborty, F. G. Wollf, S. Paul, C. A. Papachristou, S. Bhunia: Mero: A statistical approach for hardware trojan detection. Cryptographic Hardware and Embedded Systems Workshop - CHESS (2009).

[21] M. Tehranipoor, F. Koushanfar: A survey of hardware trojan taxonomy and detection, IEEE Design and Test of Computers 27, 10–25. (2010)
[22] R. Rad, J. Plusquellic, M. Tehranipoor: Sensitivity analysis to hardware trojans using power supply transient signals. IEEE International Symposium on HardwareOriented Security and Trust. (2008)
[23] R. M. Rad, X. Wang, M. Tehranipoor, J. Plusquellic: Power Supply Signal Calibration Techniques for Improving Detection Resolution to Hardware Trojans. IEEE (2008)
[24] M. Banga, M. Hsiao: A Region Based Approach for the Identification of Hardware Trojans. Proc. IEEE Int'l Workshop Hardware-Oriented Security and Trust - HOST (2008)
[25] M. Banga, M. Hsiao: A Novel Sustained Vector Technique for the Detection of Hardware Trojans. Proc. 22nd Int'l Conf. VLSI Design, IEEE CS Press, pp. 327-332. (2009)
[26] Y. Alkabani, F. Koushanfar: Consistency-Based Characterization for IC Trojan Detection. Proc. IEEE/ ACM Int'l Conf. Computer-Aided Design - ICCAD (2009)
[27] M. Potkonjak, A. Nahapetian, M. Nelson, T. Massey: 'Hardware Trojan Horse Detection Using Gate-Level Characterization. Proc. 46th Design Automation Conf - DAC (2009)
[28] S. Wei, S. Meguerdichian, M. Potkonjak: Malicious Circuitry Detection Using Thermal Conditioning. IEEE Transaction on very large Scale Integration (VLSI) Systems. VOL. 6, NO. 3. (2011)
[29] T. Reece: Detection of Malicious Hardware Integrated Circuits and Field Programmable Gate Arrays. Submitted to the Faculty of the Graduate School of Vanderbilt University. (2009)
[30] T. Reece, W. H. Robinson, B. L. Bhuva: Signature-based detection of hardware trojans with voltage stepping. Governmental Microcircuit Applications and Critical Technology - GOMACTech (2010)
[31] S. Baktir, T. Güçlüoğlu, A. Özmen: Detection of Trojans in Integrated Circuits. IEEE (2012)
[32] T. Reece, W. H. Robinson: Hardware Trojans: The Defense and Attack of Integrated Circuits. IEEE (2011)
[33] Y. L. Gwon, H. T. Kung, D. Vlah: DISTROY: Detecting Integrated Circuit Trojans with Compressive Measurements. Harvard University. (2011)
[34] Y. Tsaiy, K. Huangy, H. T. Kung, D. Vlah, Y. L. Gwon, L. Cheny: A Chip Architecture for Compressive Sensing Based Detection of IC Trojans. Harvard University. (2012).
[35] L. Wang, H. Luo: A Power Analysis Based Approach to Detect Trojan Circuits. IEEE (2011)
[36] Y. Jin, Y. Makris: Hardware trojan detection using path delay fingerprint. IEEE International Symposium on Hardware-Oriented Security and Trust. (2008)
[37] S. Weiy, K. Liz, F. Koushanfarz, M. Potkonjaky: Provably Complete Hardware Trojan Detection Using Test Point Insertion. IEEE/ACM International Conference on Computer-Aided Design - ICCAD (2012)
[38] R. S. Chakraborty, S. Paul, S. Bhunia: On Demand Transparency for Improving Hardware Trojan Detectability. Proc. IEEE Int'l Workshop Hardware Oriented Security and Trust - HOST (2008).
[39] M. Abramovici, P. Bradley: Integrated Circuit Security: New Threats and Solutions. Proc. 5th Ann. Workshop Cyber Security and Information Intelligence Research: Cyber Security and Information Challenges and Strategies - CSIIRW (2009).
[40] H. Salmani, M. Tehranipoor, J. Plusquellic: New Design Strategy for Improving Hardware Trojan Detection and Reducing Trojan Activation Time. IEEE (2009)
[41] J. Li, J. Lach: At-speed delay characterization for ic authentication and trojan horse detection. Hardware-Oriented Security and Trust - HOST (2008).
[42] X. Zhang, M. Tehranipoor: RON: An On-Chip Ring Oscillator Network for Hardware Trojan Detection. European Design and Automation Association - EDAA. (2011)
[43] A. Ferraiuolo, X. Zhang, M. Tehranipoor: Experimental Analysis of a Ring Oscillator Network for Hardware Trojan Detection in a 90nm ASIC
[44] M. Banga, M. Hsiao: VITAMIN: Voltage InversionTechnique to Ascertain Malicious Insertion in ICs. Proc. 2nd IEEE Int'l Workshop Hardware-Oriented Security and Trust - HOST (2009)
[45] Y. Alkabani: Trojan Immune Circuits Using Duality. 15th Euromicro Conference on Digital System Design. (2012)
[46] C. Lamech, J. Plusquellic: Trojan detection based on delay variations measured using a high-precision, low-overhead embedded test structure. Univercity of New Mexico. (2012)

M. Sahinoglu Isparta'nın Senirkent ilçesinde 1983 yılında dünyaya geldi. 2001'de Isparta Fen Lisesi'nden mezun oldu. 2006 ve 2009'da İstanbul Teknik Üniversitesi Elektronik Mühendisliği bölümünden lisans ve yüksek lisans derecelerini aldı. 2009'dan itibaren Gebze Yüksek Teknoloji Enstitüsünde Elektronik Mühendisliği bölümünde Doktora programına devam etmektedir. Genel çalışma alanı kriptoloji olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir.
Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde TRT Radyo (Harbiye - İSTANBUL), NETAŞ (Ümraniye - İSTANBUL) ve ARÇELİK A.Ş'de (Çayırova - KOCAELİ) yapmıştır. Yüksek Lisans tez çalışmaları sırasında İ.T.Ü'de 2006-2008 yılları arasında araştırma personeli olarak çalışmıştır. 2008 yılından itibaren TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.

M. Öztemür Samsun'un Çarşamba ilçesinde 1985 yılında dünyaya geldi. 2001'de Samsun Bafra Lisesi'nden mezun oldu. 2007 ve 2011'de Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği bölümünden lisans ve yüksek lisans derecelerini aldı. Genel çalışma alanı ürün güvenliği ve gömülü sistemler olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir.
Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde Siemens (Kartal - İSTANBUL), AKBİL Otomasyon (Ümraniye - İSTANBUL) yapmıştır. TÜBİTAK bünyesinde çalışmaua başlamadan önce 2009 yılında bir dönem NETAŞ'ta donanım tasarım mühendisi olarak çalışmıştır. 2009 yılından itibaren TÜBİTAK-BİLGEM Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.

B. Soysal Ankara'da 1983 yılında doğdu. 2001'de Çankırı Fen Lisesi'nden mezun oldu. 2006'da Ortadoğu Teknik Üniversitesi ve 2010'da Boğaziçi Üniversitesi Elektrik Elektronik Mühendisliğinden lisans ve yüksek lisans derecelerini aldı. 2010'dan itibaren Boğaziçi Üniversitesi Elektrik Elektronik Mühendisliği bölümünde Doktora programına devam etmektedir. Genel çalışma alanı kriptoloji olmakla birlikte özel çalışma alanı kriptografik sistemlere yapılan güvenlik değerlendirmeleridir. Lisans öğrenimi sırasında sırası ile stajlarını 1 ay sürecek şekilde TÜBİTAK-BİLTEN (ODTÜ - ANAKRA), ASELSAN (Macunköy - ANAKRA) ve Turkcell A.Ş'de (Söğütözü - ANAKRA) yapmıştır. 2005 yılından itibaren ASELSAN A. Ş.'de önce 1 yıl süre ile aday mühendis olarak daha sonra da 6 ay süre ile mühendis olarak çalışmıştır. 2007'den beri Siber Güvenlik Enstitüsünde (Gebze - KOCAELİ) çalışmaktadır.