

TRUSTWORTHY HARDWARE: IDENTIFYING AND CLASSIFYING HARDWARE TROJANS

Ekonomi nedeniyle güvenilmeyen fabrikalarda üretilen IC sistemler çoğalmıştı. 2005'te yapılan araştırmada ABD bu IC sistemlerin en çok talep edildiği yeri buna karşılık sahte ürünlerin satıldığı siteler, açık artırmalar vb. gibi durumların söz konusu olduğu belirlendi. Bu satış siteleri orjinal ürünlerin satıldığı sitelere sızarak kullanıcıları kendi ağına düşürüyorlardı. Bu durumun nelere yol açabileceğini bilen yetkililer alıcıların özel hayatlarına bile müdahale edebileceğini, hatta bir bomba gibi patlayabileceklerini biliyordu. Bir başka kötü yanı ise kullanıcılar durumların farkında olmayacaklardı çünkü yalnızca tasarımcının ulaşabileceği gizli kanallar sayesinde bilgi sızdırıyordu. Bu bilgiyi sızdıran Truva Atları, adeta bir multiplexer gibi çalışıp, kendi şifreli verileri sayesinde çipin işlevselliğini bozarak kullanıcıya çıkış göstermez. Güvenilir tasarımlar hataya karşı dayanıklıyken, güvenilir olmayan tasarımlar sistemi hataya odaklayabilir ve birçok kazaya neden olabilir. Bu nedenle insan hayatına mal olabilecek sistemleri tasarlarırken birçok test algoritması geliştirilmiştir. DTF bu hataların konumunu tasarımcılara bildirip düzenlenmesi için kısa yol oluştururken, ATPG ise üretim aşamasından kaynaklanan hataları test eder. Truva Atları diğer hatalar gibi çalışmadığı için bu testlerden geçmeyi başarabilirler. Öyle ki örneğin bir işlemcinin dalga formunu izleyip, analiz edip bilgi sızdırabilirler. Her ne kadar bu duruma karşı geliştirilen donanımlar olsa da donanıma sadık kalınmadığı durumlarda sistem sızıntıya karşı gelemmez ve Truva Atı sistemi kontrolü altına alabilir. Truva Atları kontrol ettikleri her birimin verilerine ve hatta güvenlik anahtarlarına ulaşabilir. Bunları önlemek ancak tasarım sırasında mümkün olmaktadır çünkü tasarımı güvenilir olmayan sistemlerde filigranlar yetersiz ve tersine mühendislik bu işlemleri gerçekleştirmeyi süresinden dolayı uygun görmez. Yani sistemi gerçekten korumak isteniyorsa herşey tasarım aşamasında güvenilir donanım sağlamakla olur. Truva Atlarından kurtulmak için gerçekleşen sanal ortam deneyleri bize gösteriyor ki, truva atları sınıflandırılmalı ve özelliklerine göre ayırt edilmelidir. Truva atları tasarıma yardımcı olabilecek herhangi bir bileşende bulunabilirler. İmalat yapılırken kullanılan maskeleye sayesinde birçok şey değiştirilebilir ve test aşamasında test edilir. Test aşamasında Truva Atı yerleştirilemez bu nedenle diğer aşamalara göre daha güvenilirdir. Montaj aşamasında test edilen kart monte edilir ve birbiriyle iletişime geçen iki farklı birim Truva atı oluşturabilir bu nedenle bağlantı yaparken yüksek dikkat gereklidir. Gittikçe daha fazla dikkat gerektiren bu işlemler bir klavyenin sahip olduğu ASCII kodlarının değişimi sayesinde bile ortaya çıkabilir. Yapılan geliştirmeler sırasında yazılıma ait olan Truva atı donanım Truva atlarını maskeleyebilir. RTL tasarımında her modül sinyal ve boolean cebiri olarak ifade edildiğinden dolayı Truva atı burada kendine çok daha rahat yer bulacaktır. Örneğin Truva atı XOR kapılarından oluşan bir karşılaştırmacı devresi bile olabilir. Hatta birkaç transistör kullanılarak yapılmış olan xor kapısından istenilen sayıda transistör ekleyerek ya da çıkararak devre parametrelerini değiştirebilir. Truva atlarının bir diğer özellikleri de tetiklenene kadar tetiklenecekleri anı bekleyip durdurulana kadar hatta belki de sonsuza kadar çalışabilmeleridir. Truva atları hedef sistemin algılarını anlaşılmayacak derecede değiştirebilir ve istenmeyen yazılımların onaylanması sonucu sistemin birçok noktasına erişim sağlayabilir. Erişim sağladıkları sistemde birden fazla noktaya yayılabilir veya grup halinde hareket edebilirler. Xilinx'in sponsor olduğu New York Üniversitesi Politeknik Enstitüsü'nde düzenlenen yarışmada katılımcılar Truva atlarını sergilemeye çalıştılar. Bu yarışmadan sonra sınıflandırılan Truva atlarının bazıları kullanıcıdan kaynaklı, her zaman açık ve saatli bomba şeklindeydi ve yapılan incelemelerde bu Truva atlarının büyük çoğunluğu sistem işlevini değiştirirken bir kısmı da bilgi sızdırdı. Bu şekilde gerçekleşen araştırmalar sayesinde Truva atları sınıflandırılmış, neler yapabildiği hakkında deneysel veriler elde edilmiştir.

Muhammet Fatih KESKİN