Çok Etki Alanlı Hareketli Ağlar için Formel Güvenlik Politikası Betimleme

Devrim Ünal[1] ve M. Ufuk Çağlayan[2]

[1] Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli
devrimu@uekae.tubitak.gov.tr
[2] Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü, İstanbul
caglayan@boun.edu.tr

Özetçe. Bu makalede, dolaşan kullanıcılara sahip çok etki alanlı hareketli ağlarda güvenlik politikalarını betimlemek için bir formel betimleme yöntemi önerilmektedir. Çok etki alanlı hareketli ağların ayırt edici özellikleri, birden fazla yönetimsel etki alanı, dolaşan kullanıcılar ve farklı güvenlik politikaları bulunmasıdır. Yetkilendirme politikalarının formel betimlemesiyle ilgilenilmektedir. Özellikle kullanıcıların etki alanları arasındaki eylemleri konusuna odaklanılmıştır, örneğin etki alanları arasında dolaşım, erişim ve iletişim. Politika modelinde hareketlilik, hiyerarşi ve rol tabanlı yetkilendirme öğeleri kapsanmıştır. Bir formel etki alanı ve etki alanları arası politika modeli sunulmaktadır. Yaklaşımımız iki tümleşik öğeye dayanır: (i) formel sistem modeli, (ii) formel güvenlik politikası betimlemesi. Yöntemimizin yeni olan kısmı ambient mantığı formülleri kullanarak bir politika kuralının uygulanabilir olduğunu belirlemek amacıyla zaman ve konum gereklerinin betimlenebilmesidir.

Anahtar sözcükler: Güvenlik politikası, formel betimleme, ambient cebri, süreç cebri, çoklu etki alanı.

1. Giriş

Bir etki alanı bir güvenlik yöneticisi tarafından tanımlanır ve kullanıcılar ile bilgisayarları içerir, birbirine bağlı yerel veya geniş alan ağlar üzerinde yer alabilir. Bir etki alanının kullanıcısı olmak yalnızca bir bağlantı ile sağlanmayıp bir ağ konusundan çok bir güvenlik konusudur. Birçok ağda, güvenliğin ağ altyapısına fiziksel erişim ile ve ağa ilişkin bilgilerin bilinmesiyle sağlandığı varsayılmaktadır. Ancak hareketli kullanıcılar resme dahil oldukça bu varsayım da geçerliliğini yitirmektedir.

Çok etki alanlı ağlarda hareketlilik iki yetenek ile sağlanmaktadır. İlki, *arabağlantı*, birbirine bağlı ağlar arasında bilgi alış verişi demek olup, Internet altyapısı ile sağlanmıştır. Diğer yetenek olan *dolaşım* kullanıcıların

1 Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli
devrimu@uekae.tubitak.gov.tr
2 Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü, İstanbul
caglayan@boun.edu.tr

birden fazla yönetimsel etki alanına ait ağlara bağlanabilmeleri demektir. Dolaşımda kullanıcının birden çok kuruluş tarafından tek bir kimlikle tanınması ve hareket içerisinde birden çok yönetimsel etki alanının gezilmesi söz konusudur. Dolaşan bir kullanıcının bir *ev* etki alanı olduğu ve birden fazla *yabancı* etki alanlarında dolaşabildiğini varsaymaktayız. Kullanıcı genellikle ev etki alanında bulunmakta ve burada daha fazla erişim hakkına sahip olmaktadır. Kullanıcı bir yabancı etki alanına hareket ederek bağlandığında bu etki alanının bakış açısına göre bir *yabancı kullanıcı* olarak değerlendirilecektir.

Yetkilendirme mekanizmaları bir kullanıcının erişim haklarını güvenlik politikasına dayalı olarak belirlerler. Erişim denetimi mekanizmaları daha sonra kullanıcının kaynağa erişimini bu önceden belirlenmiş erişim haklarına dayalı olarak denetlerler. Böyle bir ortamdaki güvenlik yönetimi kullanıcıların dolaştığı tüm etki alanlarında tek bir kimlikle bilinmesini, ziyaret edilen etki alanındaki kaynaklara erişim sağlarken eylemlerinin ev ve ziyaret edilen etki alanları arasında karşılıklı olarak politikaya göre denetlenmesini gerekli kılar.

Güvenlik politikaları, ziyaretçi kullanıcıların ziyaret edilen etki alanlarındaki iç güven ilişkileri nedeniyle güvenlik mekanizmalarını geçerek güvenlik politikasını delmelerine engel olmak için formel olarak denetlenmelidir. Kullanıcıların olası eylemleri hem ev hem de ziyaret edilen etki alanlarındaki güvenlik politikalarına karşı denetlenmelidir.

Burada çok etki alanlı hareketli ağların güvenlik politikalarını betimlemek için bir yaklaşım önermekteyiz. Bu yaklaşım ambient cebri, ambient modal mantığı ve yüklem mantığı kullanmaktadır. Devam eden araştırmamızda, yöntemimizin bir otomatik teorem doğrulama aracındaki gerçeklemesi üzerinde çalışmaktayız.

2. Problem Tanımı ve Çözümlemesi

Kullanıcıların farklı yönetimsel etki alanları arasında dolaşabildiği bir ortamdaki güvenlik politikalarının formel betimlemesi ve doğrulamasıyla ilgilenilmektedir. Bu problem aşağıdaki soruya indirgenebilir: "Hareketli kullanıcıların işlemleri, içerisine geldikleri yönetimsel etki alanlarının güvenlik politikalarına ve etki alanları arasındaki güvenlik politikalarına uygun mudur?"

Bir *güvenlik politikası* etkin öğelerin pasif öğeler üzerinde gerçekleştirebilecekleri *eylemleri* ve bunların gerçekleştirilebileceği *koşulları* tanımlar. Etkin öğeler aynı zamanda güvenlik politikasında *yetkilendirme özneleri* (veya sadece *özneler*) olarak adlandırılır. Özneler *yetkilendirme nesneleri* (veya sadece *nesneler*) olarak adlandırılan pasif öğeler üzerinde

işlemler gerçekleştirebilirler. Özneler kullanıcılar, roller veya sunucu ya da istemci bilgisayarlar olabilir. Nesneler ağ kaynakları olup uygulamalar, dosyalar, veri tabanları veya mesajlar olabilir. Etki alanları ve bilgisayarlar aynı zamanda pasif öğeler şeklinde davranarak yetkilendirme nesneleri olabilirler.

Bir *yönetimsel etki alanı* alanı bir öğeler kümesi tanımlar. Eylemler bir özne tarafından bir etki alanında gerçekleştirilebilecek işlevleri tanımlar. Bir eyleme izin verilmesi için zaman, kimlik, rol üyeliği, kullanıcı grubu üyeliği, konum ve hareketlilik gibi koşullar olabilir. Tüm bu öğelere bağlı kurallar kümesi bir etki alanındaki güvenlik politikasını oluşturmaktadır.

Bu tanımların sonucu problem tanımını şu şekilde formalize edebiliriz: "Bir sistem modelinde, hareketli kullanıcılar farklı yönetimsel etki alanlarını gezmektedir. Etki alanı güvenlik politikaları ve etki alanları arasında bir güvenlik politikası mevcutken, kullanıcıların eylemleri bu güvenlik politikalarına uygun olup olmadığının ve bu güvenlik politikaları birbirleriyle uyumlu olup olmadığının formel olarak doğrulanması hedeflenmektedir."

3. İlgili Çalışmalar

Güvenlik politikalarının mantık tabanlı betimlenmesi evrensel yapıtaşlarına dayanır ve formel cebir yöntemlerini destekler. Mantık kullanımı aynı zamanda model doğrulama ve teorem ispatı yöntemleri için otomatik araç desteği sağlar.

Flexible Authorization Framework (FAF) [1], [2] yetkilendirme politikalarının tanımlanması, türetilmesi ve çelişkilerin çözülmesi için mantık programlamasına dayalı bir yöntemdir.

Mantığa dayalı olarak açık izin reddini, hiyerarşileri, politika çıkarımını ve çelişki çözümlemeyi destekleyen başka bir önemli çalışma [3]'tür. Woo ve Lam [4] yarı tutarlı bir formel dil ile yetkilendirmeleri mantıksal yapıtaşlarına dayalı olarak betimlemeyi seçmişlerdir. [5] çalışmasında deontik mantık kullanılarak *izin*, *zorunluluk* ve *yasaklama* unsurları sorumluluk, delegasyon ve zaman yapıları gibi yönetsel kavramları modellemek için kullanılmıştır. Küme ve fonksiyonlara dayalı bir güvenlik politikası dili [6]'da sunulmuştur.

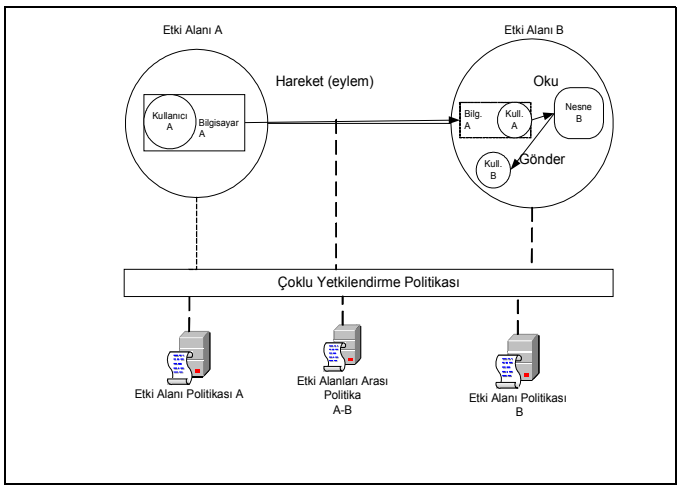
Her konumda kullanılabilecek uygulama katmanı güvenlik politikalarında uzaysal yapılandırmalarla ilgili çıkarımda bulunmak [7] çalışmasında göz önüne alınan konulardan biridir. Bu çalışmada ambient cebri ve ambient mantığının basitleştirilmiş bir sürümü bir güvenlik politikasındaki politika kurallarında kullanılmıştır. Süreç cebirlerinin güvenlik politikası betimlemesinde kullanımına bir örnek ise Sπ cebrinin formel dil olarak kullanıldığı ve gerçeklemede Datalog kullanılan [8]'dir.

Bunlara benzer olarak bizim yaklaşımımızda da süreç cebri ve onunla ilişkili modal mantık kullanılmaktadır. [8]'in aksine Ambient cebri [9] kullanılacak ve gerçeklemede bir otomatik teorem doğrulama aracı kullanılacaktır. [7]'nin aksine uygulama düzeyi politikalarından ziyade ağ düzeyi politikaları kapsanacak ve fiziksel konum değil, etki alanları ve bilgisayarlardan oluşan mantıksal konumlar göz önüne alınacaktır.

4. Modelleme Yaklaşımı

Tüm formel model aslında iki alt modelden oluşmaktadır. Bunlardan ilki dinamik bir sistem modeli, diğeri ise bir güvenlik politikası modelidir. Sistem modelinde sisteme özgü ve dinamik öğeler bulunmaktadır: etki alanları, ağ üzerindeki kullanıcılar ve kaynaklar ile kullanıcıların mümkün eylemleri. Güvenlik politikası yönetimsel yapıya özgü ve durağan öğeleri modeller: sistem tarafından sağlanması gereken kurallar ve kullanıcıların eylemleri üzerindeki kısıtlamalar. Birden çok yetkilendirme politikasından oluşan güvenlik politikası modeli, dinamik sistem modelindeki eylemler için bir denetleyici konumundadır.

Dinamik ve sisteme özgü öğelerin durağan ve yönetimsel yapıya özgü öğelerden ayrılması daha etkin bir betimlemeye olanak tanımaktadır. Tüm olası sistem yapılandırmaları ve eylemlerin statik olarak doğrulanması gerekmez, yalnızca bir çoklu etki alanlı hareketli ağ modelinin belirli bir örneğinde ortaya çıkanların doğrulanması yeterlidir.



Şekil 1. Modelde sistem öğeleri, birden fazla politika ve kullanıcıların eylemleri vardır.

Şekil 1'de gösterilen örnekte, Etki Alanı A'daki Kullanıcı A, Bilgisayar A'ya oturum açmıştır. Daha sonra Etki Alanı B'ye hareket eder, bir dosya okur ve bunu Etki Alanı B'deki Kullanıcı B'ye gönderir. Bu türden bir senaryo Kullanıcı A'nın eylemlerinin birden çok politika uygulama noktasında denetlenmesini gerektirir. Bu uygulama noktalarındaki cihaza özgü güvenlik politikaları genellikle bir yönetici tarafından yönetimsel politikalara bağlı olarak yapılandırılır, örneğin etki alanı politikaları ve etki alanları arasındaki politikalar. Bu çalışmada, politika uygulama noktalarındaki politikalardan ziyade etki alanı ve etki alanları arasındaki politikaları modelleme ele alınmaktadır.

4. Sonuç

Çok etki alanlı hareketli ağlardaki güvenlik politikalarının formel olarak betimlenmesi ve doğrulanması için bir yöntem önermiş bulunuyoruz. Yaklaşımınızın kökünde ambient cebri ve mantık tabanlı yetkilendirme çerçeveleri bulunmaktadır. Bu çalışmanın katkıları şunlardır: (i) esnek süreç cebri tabanlı güvenlik politikası betimlemesi, (ii) bir formel etki alanları arası güvenlik politikası modeli, (iii) hareketlilik ve konum tabanlı güvenlik politikası betimlemesi.

Kaynakça

1. Jajodia, S., Samarati, P., Subrahmanian, V. S.: A Logical Language for Expressing Authorizations, Proceedings of the 1997 IEEE Symposium on Security and Privacy, IEEE (1997) 31-43
2. Jajodia, S.: "Flexible Support for Multiple Access Control Policies", ACM Trans. Database Systems, Vol. 26, No: 2, (2001) 214-260.
3. Bertino, E., Ferrari, E., Buccafurri, F., and Rullo, P: A Logical Framework for Reasoning on Data Access Control Policies. In Proceedings of the 1999 IEEE Computer Security Foundations Workshop. CSFW. IEEE Computer Society, Washington, DC, 175 (1999).
4. Woo T. Y. C. and Lam S. S.: Authorizations in distributed systems: A new approach. Journal of Computer Security, 2 (1993) 107--136.
5. Cuppens, F., Saurel,C.: Specifying a Security Policy: A Case Study, 9th IEEE Computer Security Foundations Workshop, Kenmare, Ireland, IEEE Computer Society Press, (1996) 123-134.

6. Ryutov, T., Neuman, C.: Representation and Evaluation of Security Policies for Distributed System Services, Proc. DARPA Information Survivability Conference, DARPA (2000)
7. Scott D.J., Abstracting application-level security policy for ubiquitous computing. UCAM-CL-TR-613, Cambridge University (2005)
8. Fournet, C., Gordon,A.D., Maffeis,S.: A Type Discipline for Authorization Policies, Lecture Notes in Computer Science, Volume 3444. Springer-Verlag,(2005) Pages 141 – 156
9. Cardelli, L., Gordon, A.D., Mobile Ambients, Theoretical Computer Science 240 (2000) 177-213