

Çok Etki Alanlı Hareketli Ağlar için Formel Güvenlik Politikası Betimleme

Devrim ÜNAL¹, M. Ufuk ÇAĞLAYAN²

¹ Tübitak Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü, Kocaeli

² Boğaziçi Üniversitesi Bilgisayar Mühendisliği Bölümü, İstanbul

devrimu@uekae.tubitak.gov.tr, caglayan@boun.edu.tr

Özet: 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 yönetsel etki alanı, dolaşan kullanıcılar ve farklı güvenlik politikaları bulunmasıdır. Yetkilendirme politikalarının formel betimlemesiyle ilgilenilmektedir. Özellikle kullanıcıların etki alanları arasındaki etkileşimleri 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 tümeleşik 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 verişini demek olup, İnternet altyapısı ile sağlanmıştır. Diğer yetenek olan dolaşım kullanıcıların birden fazla yönetsel etki alanına ait ağlara bağlanabilmeleri demektir. Dolaşımda kullanıcının

birden çok kuruluş tarafından tek bir kimlikle tanınması ve hareket içerisinde birden çok yönetsel 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 kullanılmaktadır. Devam eden araştırmamızda, yöntemimizin bir otomatik teorem doğrulama aracındaki gerçekleşmesi üzerinde çalışmaktayız.

2. Problem Tanımı ve Çözümlemesi

Kullanıcıların farklı yönetimsel etki alanları arasında dolaşabildiği bir ortamdaki güvenlik politikalarının formel betimlemesi ve doğrulanmasıyla 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 nesnelere (veya sadece nesnelere) olarak adlandırılan pasif öğeler üzer-

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

Bir yönetimsel etki alanı alanı bir öğeler kümesi tanımlar. Eylemler bir özne tarafından bir etki alanında gerçekleştirilebilecek işlemleri 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. Sonuç

Çok etki alanlı hareketli ağlardaki güvenlik politikalarının formel olarak betimlenmesi ve doğrulanması için bir yöntem önermiş bulunuyoruz. Yaklaşımımızın 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., Maffei, 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
10. Charatonik W., Dal Zilio S., Gordon A.D., Mukhopadhyay S., Talbot J. M.: Model Checking Mobile Ambients, Proc. FOSSACS 2001, LNCS 2030, (2001) 152-167
11. Luca Cardelli, Andrew D. Gordon, Ambient Logic, Mathematical Structures in Computer Science, basılacak.