TUSAŞ

AR-GE İŞBİRLİĞİ ÇAĞRISI

İşbirliği Çağrısı Kodu: 2020-ÜSİ-T2690-01

İşbirliği Çağrısı Başlığı: Aviyonik Sistemi Siber Saldırı Ağacı İçin Modelleme Algoritmasının Geliştirilmesi

Problem Tanımı: Havacılık ve savunma alanında belirlenmiş olan varlıklara (elektronik sistemler, arayüzler vb.) karşı oluşabilecek siber tehditlerin modellenmesi ve tehdit analizinin yapılması için saldırı ağaçları kullanılmaktadır. Saldırı ağaçları, varlıkların üzerindeki zafiyetlerin ve olası tehditlerin belirlenmesi ile bu zafiyetlere karşı ne tür önlemlerin alınacağının karar verilmesinde önemli rol oynamaktadır. Bu bağlamda, güncel tehditlerin açık kaynaklardan araştırılması, bu tehditlerin aviyonik sistemler üzerinde ne tür zafiyetlere sebebiyet vereceğinin tespit edilmesi ve gerekli önlemlerin alınması konularının analizi için saldırı ağacı modelleme sistemlerinin geliştirilmesine ihtiyaç duyulmaktadır.

Bu çağrı kapsamında, TUSAŞ bünyesinde geliştirilmesi devam eden bir aviyonik sistem projesinde kullanılmak üzere saldırı ağacı modelleme sisteminin geliştirilmesi beklenmektedir.

İzlenmesi Beklenen Yöntem: Proje kapsamında geliştirilecek olan sistemin, aviyonik sistemler güvenlik mimarisi standartları, protokolleri ve yazılım / donanımı (DO326A, DO-356A, NIST SP 800-53, NIST SP 800-30 vb.[1]) ile uyumlu olması beklenmektedir. Sistemin aşağıdaki çalışma yöntemleri izlenerek geliştirilmesi beklenmektedir.

1) Aviyonik Sistem Siber Saldırı Tespit Sistemi Geliştirilmesi:
Sistem ile uyumlu olacak biçimde ağ ve uç birim siber saldırı tespit sisteminin geliştirilmesi ve geliştirilen sistemin aşağıdaki özelliklere sahip olması beklenmektedir:

- Sistem kural tabanlı olmalı, geliştirilecek olan saldırı tespit sisteminde kullanılacak olan kurallar referanslarıyla birlikte belirtilmelidir.
- Belirlenen kurallara ek olarak yapay zekâ tabanlı (anomali tespiti) olarak da geliştirilmeli ve yeni kurallar üretmelidir.
- Açık kaynak kodlar kullanılarak geliştirme yapılabilir.

2) Aviyonik Sistem Siber Zafiyet Veri Tabanı ve İstihbarat Sistemi Geliştirilmesi:
Sistem ile ilgili zafiyetler için açık kaynaklardan derlenmiş ve özelleştirilmiş bir zafiyet veri tabanı geliştirilmesi ve geliştirilen sistemin aşağıdaki özelliklere sahip olması beklenmektedir:

- Geliştirilecek olan sistem, bahse konu olan aviyonik sistemle ilgili saldırı tekniklerini, taktiklerini ve istismarlarını açık kaynak verilerini tarayarak tespit etmeli, bu konuda uyarı vermeli ve bulguları bir veri tabanında saklamalıdır.
- Mevcut açık kaynak verilerini tarayacak yapıda olmalıdır.
- Güncelliğini koruması açısından ilgili açık kaynak veri tabanlarındaki güncellemeleri takip ederek uyarı vermeli, bulguları yeni bir veri tabanında saklamalıdır.

3) Aviyonik Sistem Siber Saldırı Ağacı Modelleme Sistemi Geliştirilmesi:
Saldırı tespit sistemi (1. madde) ve zafiyet veri tabanı (2. madde) girdileri kullanılarak aşağıda özellikleri belirtilen çok adımlı saldırı modelleme sistemi algoritmasının yazılması beklenmektedir:

[1] Çağrı sürecinde ücretli standartların paylaşılması planlanmamakta olup, ücretsiz standartlara internet taraması yapılarak ulaşılabilmektedir.

- Sistem, yukarıda ifade edilen 1. ve 2. adımlarda geliştirilecek olan sistem kullanılarak herhangi bir tehdit senaryosuna karşı saldırı projeksiyonu yapmalıdır.
- Saldırı kaynaklarına ilişkin geriye dönük saldırı ağacı modellemesi oluşturup gerekli raporlamayı yapmalıdır.
- Açık kaynak kodlar kullanılarak geliştirme yapılabilir.

Çalışma süresince, gelişen / değişen yeni siber tehditlerin de takip edilerek yazılıma adapte edilmesi amaçlanmalıdır.

Çağrıya Başvuru Koşulları: Çağrıya sadece üniversiteler başvuru yapabilecektir. Proje ekibinde, proje kapsamında lisansüstü tez çalışması yürütecek en az bir öğrenci bulunmalıdır.

Başvuru Yöntemi: Ar-Ge işbirliği çağrısı kapsamında proje önerilerinin EK'teki şablona uygun olarak doldurulması ve usi@tai.com.tr e-posta adresine gönderilmesi gerekmektedir.

Değerlendirme Süreci:

- Tüm başvurular, TUSAŞ içerisinde ilgili bölümlerle koordinasyon sağlanarak, proje çağrısı konusundaki uzmanlardan oluşturulan Değerlendirme Komitesi tarafından değerlendirilmektedir.
- Değerlendirme Komitesinin değerlendirmesi sonucu ihtiyaç olması durumunda, proje önerisi sahibi ile işbirliği toplantıları gerçekleştirilecektir.
- Projenin yürürlüğe alınmasına karar verilmesi durumunda, uygun model (Ar-Ge destekleri, Savunma Sanayi İçin Araştırmacı Yetiştirme Programı, TUSAŞ öz kaynak bütçesi vb.) proje önerisi sahibi ve ilgili TUSAŞ bölümleriyle birlikte değerlendirilecektir.

EK: TUSAŞ Ar-Ge İşbirliği Çağrısı Niyet Mektubu