Bilgi Güvenliği Eğitim/Öğretimi

İbrahim SOĞUKPINAR

Gebze Yüksek Teknoloji Enstitüsü

İçerik

- Bilgi Güvenliği Eğitim/Öğretimi
- Dünyadaki Örnekler
- Türkiye'deki Örnekler
- GYTE'de Bilgi Güvenliği Dersi
- Sonuç ve Öneriler

•Bilgi Güvenliği Eğitimi

- Bilgi Güvenliği Eğitimi/Öğretimi ve Önemi
- Öğrenim çıktıları
- Kapsamı

•Bilgi Güvenliği Eğitim/Öğretimi

- **Çıkıtılar/Beklentiler**
- **Bilgi güvenliğinin öneminin kavranması ve farkındalığının arttırılması**
- **Güvenlik politikaları, güvenlik modelleri ve güvenlik mekanizmalar gibi bilgi güvenliği ile ilgili temel kavramları vermek**
- **Düz metin, şifreli metin dahil olmak üzere uygulanan şifreleme ile ilgili kavramları açıklamak.**
- **Virüs, Truva atı ve solucanlara dahil olmak üzere kötü amaçlı kod kavramları, açıklamak.**
- **Genel bilgisayar zayıflıklarını bilgi güvenliği açısından açıklamak.**
- **Tanımlama ve kimlik doğrulama için gerekli şartları ve mekanizmaları anlatmak.**

•Bilgi Güvenliği Eğitim/Öğretimi

- **Sözlük saldırıları da dahil olmak üzere parola, parola kimlik doğrulaması ile ilgili konuları açıklamak.**
- **İşletim Sistemi güvenliğinin detaylarını açıklamak ve güvenli işletim sistemini tanımlamak.**
- **Veritabanı güvenliği için güvenlik gereksinimlerini açıklamak ve teknikleri öğretmek**
- **Ağlar için güvenlik tehditlerini tanımlamak ve ağ güvenliğinin sağlanması için gerekli teknikleri açıklamak.**
- **Güvenlik yönetimi için gerekli şartları ve teknikleri(politikaları, risk analizi ve fiziksel tehditler ve kontroller) üzere, açıklamak.**
- **Bütün bu problemlerin çözümü için bilgi ve beceri kazandırmak**

•Bilgi Güvenliği Eğitim/Öğretimi

•Kapsamı

- •Bilgi güvenliği kavramı, servisler mekanizmalar
- •Bilgi güvenliği gereksinimi
- •Verinin Gizliliği, Bütünlüğü ve Erişilebilirliği
- •Şifreleme temelleri ve yöntemleri
- •Kimlik doğrulama yöntemleri
- •Biyometrik kimlik doğrulama
- •İşletim sistemi güvenliği
- •Veritabanı güvenliği
- •Ağ güvenliği kavramı ve yöntemler
- •İletişim güvenliği kavramı ve yöntemler
- •Bilgi güvenliği yönetimi ve standartlar
- •Bilgi güvenliğinde gelecekteki eğilimler
- •Bilgi güvenliği projesi

Dünyadaki Örnekler, Univ of London

Dört mecburi ders(Inf. Sec MS.)
Güvenlik Yönetimi
Kriptografi ve Güvenlki mekanizmaalrına giriş
Ağ Güvenliği
Bilgisayar Güvenliği
Aşağıdaki derslerden ikisi seçmeli:
Güvenli Elektronik Ticaret ve Uygulamalar
Standartlar ve Değerlendirme Kriterleri
İleri Kriptografi
Veritabanı Güvenliği
Bilişim Suçları
Akıllı kart Güvenliği ve Uygulamaları
Sayısal Mahkemeler
İlave : Proje

•Dünyadaki Örnekler

CS155 Bilgisayar ve Ağ Güvenliği, Stanford University

Bölüm 1: Temeller:

Kontrol korsanlığı saldırıları: İfşaat ve savunmalar, ifşaat teknikleri ve açıklık analizi, Güvenli sistem tasarımı, erişim denetimi ve koruma, gürbüz uygulama kodu yazma araçları, kötü uygulama kodu yazmayla ilgilenme: kötü kodların izolasyonu, bilgisayar güvenliğinde kriptografinin kullanılması.

Bölüm 2: Web Güvenliği:

Temel web güvenliği modeli. Kullanıcı doğrulama ve oturum yönetimi, web uygulama güvenliği, HTTPS: amaçlar ve tuzaklar.

Bölüm 3: Ağ Güvenliği:

Ağ protokollerinde güvenlik problemleri: TCP, DNS, SMTP, ve ağ yönlendirme savunma araçları: Güvenlik duvarları, Sanal özel Ağlar(VPN), Sızma tespiti ve filtreler, Ağ güvenliği testi, Kötücül yazılımlar: Bilgisayar virüsleri, casus yazılımlar ce tuş kaydediciler, zombi-ağlar: saldırı ve savunmalar, İstenmeyen trafik: servis durdurma saldırıları

Part 4: Son Konu: Güvenli Hesaplama mimarisi

•Dünyadaki Örnekler

CSC 405 Bilgisayar Güvenliğine Giriş, NCSU

T1. Giriş (1 ders)
T2. Temel Kriptografi(1 ders)
T3. Gizli Anahtarlı Kriptografi(3 ders)
T4. Mesaj Özetleri(2 ders)
T5. Açık Anahtarlı Kriptografi(4 ders)
T6. Kimlik Doğrulama (5 ders)
T7. Güvenli Ortamlar(2 ders)
T8. Gerçek Zamanda iletişim Güvenliği(4 ders)
T9. Elektronik posta güvenliği (2 ders)
T10. Güvenlik Duvarları ve WEB Güvenliği(2 ders)
Özet(1 ders)

•Dünyadaki Örnekler

CS 467: Kriptografi ve Bilgisayar Güvenliği,Yale Univ

Güvenlik problemleri ve Sistemler: Bilgi çağında Gizlilik ve Güvenlik. Çok aşamalı problemler: Gizli mesaj iletimi, kimlik doğrulama, anahtar dağıtımı, sayısal imzalar, sertifikalı mesaj, anlaşma imzalama,vs. Pratik Sistemler: Kerberos, SSH, PGP, akıllı kartlar, SSL

Kriptografik primitifler ve özel gerçeklemeler. Primitifler:klasik konum ve eleman değiştirme şifreleyiciler, modern gizli ve açık anahtarlı şifreleme sistemleri, sayısal imzalar, mesaj özetleri, anahtar değişimi, anahtar paylaşımı rastgele sayı üretimi Gerçeklemeler: ES, DES, RSA, RC6, DSA, SHA,, MD5..

Kriptografi için matematik. Enformasyon teorisi, sayı teorisi, asal sayılar ve çarpanlara ayırma, ,sonlu alanlarda modüler aritmetik hesapları, ayrık logaritma problemi. Karmaşıklık teorisi. Dağıtık sistem teorisi .

Türkiye'deki Örnekler

BİL438 Bilgisayar ve Ağ Güvenliği (Hacettep Üniv.)

- Ağ güvenliğine giriş ve temel kavramlar.
- Risk değerlendirmesi, güvenlik politikası, tehditlerin sınıflandırılması.
- Parolalar, erişim izinleri.
- Şifreleme teknikleri, geleneksel yöntemler,
- Açık anahtar yöntemleri, asıllama, sayısal imza, protokollar, şifreleme yazılımları.
- TCP/IP protokol ve hizmetlerinde güvenlik
- Güvenlik duvarları
- Sanal özel ağlar.
- Saldırı tespit sistemleri

Türkiye'deki Örnekler

Kurumsal Bilgi Güvenliği, Gazi Üniv.

- Kurumsal Bilgi Güvenliğine Giriş
- Kurumsal Bilgi Güvenliğinin Temelleri
- İnsan ve Toplum Mühendisliği Güvenliği
- Yazılım Güvenliği ve Güvenli Yazılım Geliştirme
- Siber Güvenlik
- Bilgi Güvenliği Yönetim Sistemi
- Karşılaşılan Riskler ve Yönetimi
- Kurumsal Standartlar
- Kritik Altyapılar ve Güvenliği
- Bilgi Güvenliği ve Bilişim Hukuku
- Kurumsal Bilgi Güvenliğinde Sızma Testleri
- Araştırma ve Uygulama Projeleri

Türkiye'deki Örnekler

CE340 Kriptografi ve Ağ Güvenliği, İz.Eko.Üniv.

- Güvenlikte yaklaşımlar: OSI mimari model, saldırılar, sistemler, mekanizmalar ve modeller
- Simetrik algoritmalar: Klasik şifreleme teknikleri
- Blok şifreleme ve DES
- Sonlu alanlar: modular aritmetik Euclid algoritması, polinom aritmetiği
- Simetrik şifreleme ile bilgi gizliliğini sağlamak
- Sayı kuramı
- Açık anahtarlı şifreleme ve RSA
- Anahtar kotarma ve diğer kripto sistemler
- Mesaj doğrulama ve iz fonksiyonları
- Hash ve MAC algoritmaları
- Sayısal imza ve Kimlik doğrulama protokolleri
- Ağ güvenliği uygulamaları
- Proje sunumları

GYTE'de Bilgi Güvenliği Dersi

- BİL 673 Veri ve Ağ Güvenliği

- Veri ve Ağ Güvenliğine Giriş,
- Ağlar Niçin güvenli olmalıdır.
- Güvenlik gereksinimi ve Ne kadar güvenlik gerekir
- Ağ Sistemlerinin Çalışması ve Topoloji Güvenliği
- Yetkilendirme ve Kriptolama, Simetrik Şifreleme sistemleri
- Asimetrik Simetrik Şifreleme sistemleri
- Şifreleme ile Güvenlik, Sayısal İmzalar
- Güvenlik Duvarları ve tasarımı

GYTE'de Bilgi Güvenliği Dersi

- BİL 673 Veri ve Ağ Güvenliği

- Nüfuz Tespit Sistemleri
- Biyometrik Güvenlik Sistemlerine Giriş
- Biyometrik Güvenlik Sistemleri
- Sanal Özel Ağlar ile Güvenlik
- Yıkımdan Koruma ve Onarım
- Ağ Kullanım Politikaları
- Dönem projesi rapor ve sunumları

Sonuç ve Öneriler

2010'lu yıllarda yeni eğilimler

- Kötücül yazılımların hızlı yayılması(e-posta,anlık mesaj, web siteleri)
- Zombi ağların artarak anlaşılmalarını zorlaşması
- Kötü amaçlı güvenlik yazılımı ile saldırıların artması
- İstemci yazılımları üzerinden saldırıları
- Ransom saldırıları
- Sosyal ağ üzerinden yapılan saldırıların yaygınlaşması.
- Bulut bilişim üzerinden saldırılar
- Güvensiz Web uygulamaları
- Güvedlik personeli üzerinden saldırı
- Siber saldırılar ve siber güvenlik
- Kurumsal Bilgi güvenliği yönetişimi

Sonuç ve Öneriler

- Bilgi Güvenliğinin önemi ve bilişim suçları için bilirkişilik görevi
- Bilgi güvenliği Eğitim/Öğretimi için Bilgisayar müh .liği bölümlerine en azından seçmeli bir ders koyulması
- Bu dersi verecek öğretim elemanı için yetiştirme planı yapılması
- Bölümlerin bilgi alışverişinde bulunması