Bilişim güvenliği

Gökdeniz Karadağ

Orta Doğu Teknik Üniversitesi

Bilgisayar Mühendisliği Bölümü

Araştırma Görevlisi ve Sistem Yöneticisi

12 Nisan 2008

Ana hatlar

- Güvenlik
- Kullanıcı Açısından
- Yönetici Açısından
- Yazılım Geliştirici Açısından

Güvenlik

- %100 Güvenlik imkansız
  - Ama yakınsayabiliriz
- Bir süreç
  - Geliştiriciden kullanıcıya herkes dahil olmalı
- Bir felsefe
  - Temelden tepeye kadar güvenlik göz önünde tutulmalı

Kullanıcı Açısından

- İstenmeyen sonuçlar
  - Özel bilgilerin çalınması
  - Parolaların çalınması
  - Kimlik hırsızlığı
  - Yavaşlayan bilgisayarlar
  - Artan faturalar

Kullanıcı Açısından

- Parolaların paylaşılmaması
- Parolaların açık bir şekilde iletiminin engellenmesi
- Güvenilmeyen kaynaklardan talimat veya yazılım alınmaması
- İşletim sistemine uygun korunma yazılımları kullanılması

Kullanıcı Açısından

- Şifreleme
  - http: https
  - telnet: ssh
- Paroladan daha güvenli araçlar
  - anahtar çiftleri
  - e-anahtar
  - tek kullanımlık parola

Kullanıcı Açısından

- Kullanıcılar için eğitim şart!

Yönetici Açısından

- İki tür yönetici
  - Şirket Yöneticisi
  - Sistem Yöneticisi
- İkisinin de sorumluluğu var

Yönetici Açısından

- Para kaybı
- Gizli bilgilerin Kaybı
- Verimlilik düşüşü
- Hizmetlerin kesintiye uğraması
- Müşteri güveninin sarsılması

Şirket Yöneticisi

- Şirket güvenlik politikalarının belirlenmesi
  - Uygulanabilir olmalı
  - Uygulanmalı!
- Çalışanlar haberdar olmalı
- Varsa güvenlik personeli takip etmeli
- “Şirket politikası” olduğu vurgulanmalı

Şirket + Sistem Yöneticisi

- Şirket için değerli varlıkların listesi
  - Sunucular, hizmetler, veri, çalışan makinaları
- Güvenliklerinin sağlanmasının bedeli
  - para/zaman/iş gücü
- Hangi varlıklar ne derece güvenliğe tabii olacak. Acil durumlarda izlenecek yöntemler
  - Şirket politikasında yer almalı

Sistem Yöneticisi

- Sunucular
  - Mümkün olan en az yazılım/servis
  - Güncellemeler düzenli olarak yapılmalı
  - Güvenlik duvarı ayarlanmış olmalı
  - Kayıtlar takip ediliyor olmalı
- Ağ güvenliği
  - Uygun detayda inceleme yapan yazılımlar
  - paket filtresi/içerik filtresi

Sistem Yöneticisi

- Çalışan bilgisayarları
  - Güncel tutulmalı
  - Güvenlik yazılımları bulunmalı
  - Belirlenen güvenlik seviyesine göre kısıtlanmış olmalı
- Dizüstü bilgisayarlar
  - Gizli veriler varsa çalınması kabus yaratabilir
- Bellek aygıtları
  - Politika ne diyor ? Ne derece uygulanabilir ?

Yazılım Geliştirici Açısından

- Güvenlik bir süreç ve bir felsefe
- Sonradan “elleyerek” yazılım güvenli hale getirilemez
- Tasarımın her aşamasında güvenlik ele alınmalı ve ihtiyaca göre güvenliğe önem verilmeli

Yazılım Geliştirici Açısından

- **Güvenlik sorunlarının ezici çoğunluğu; kullanıcıdan ya da karşıdaki sistemlerden gelen verilerin yeterince denetlenmemesinden kaynaklanmaktadır !!!**

Yazılım Geliştirici Açısından

- Tasarım hataları
  - Ör. WEP
- Buffer overflow
  - Dinamik diller; yama ama her şeye çözüm değil
- Öngörülemeyen koşullar

Yazılım Geliştirici Açısından

- Gelen verinin kontrolü
- SQL injection
  - “SELECT * FROM .. WHERE isim=' ” +
    $_POST['isim'] + “ ' ;”
  - ali' OR 1=1; --
- Cross site scripting (XSS)
  - İsminiz: Ali Veli <script>patlat()</script>

Yazılım Geliştirici Açısından

- Kesinlikle sadece web ile sınırlı değil
- Command injection
  - rm -rf /tmp/$1
  - ./dosya.sh “parametre ; rm -rf /”
- Veritabanı bağlantısı kuran, başka sistemlere komut yollayan her kod bu şekilde açıklar içerebilir

Yazılım Geliştirici Açısından

- **Gelen her veri, kullanılmadan ve diğer sistemlere gönderilmeden önce kontrolden geçirilmeli, gereken kaçış karakterleri eklenmeli**

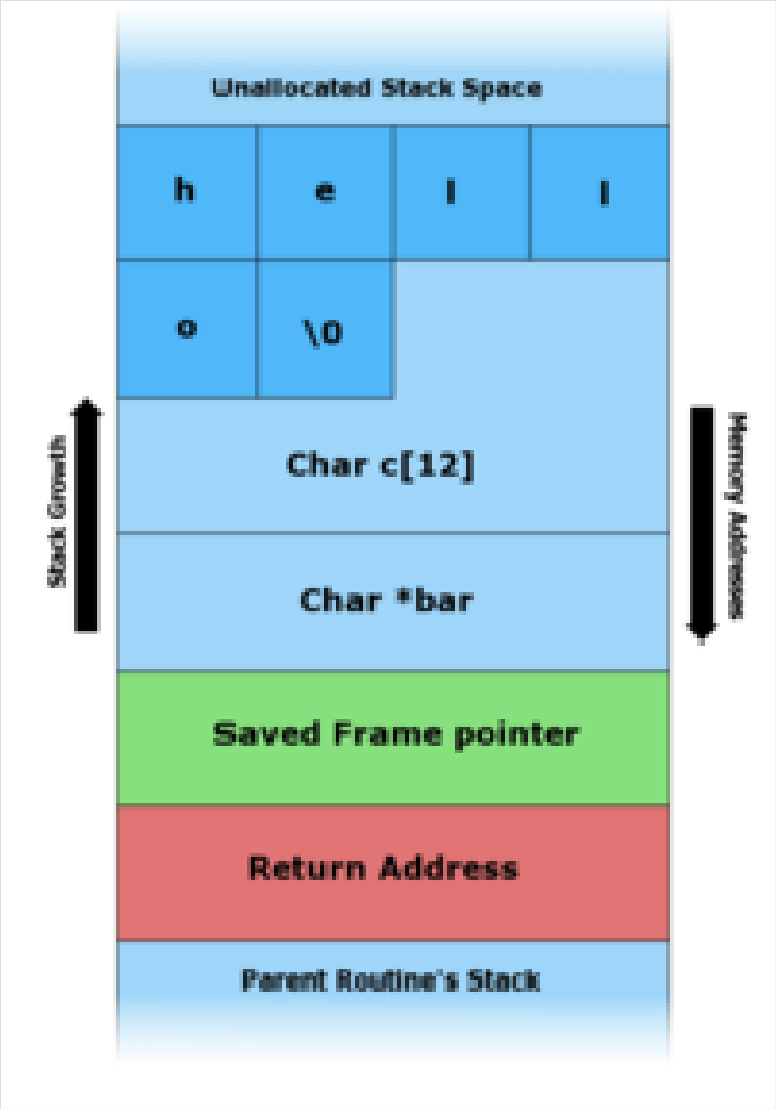
Yazılım Geliştirici Açısından

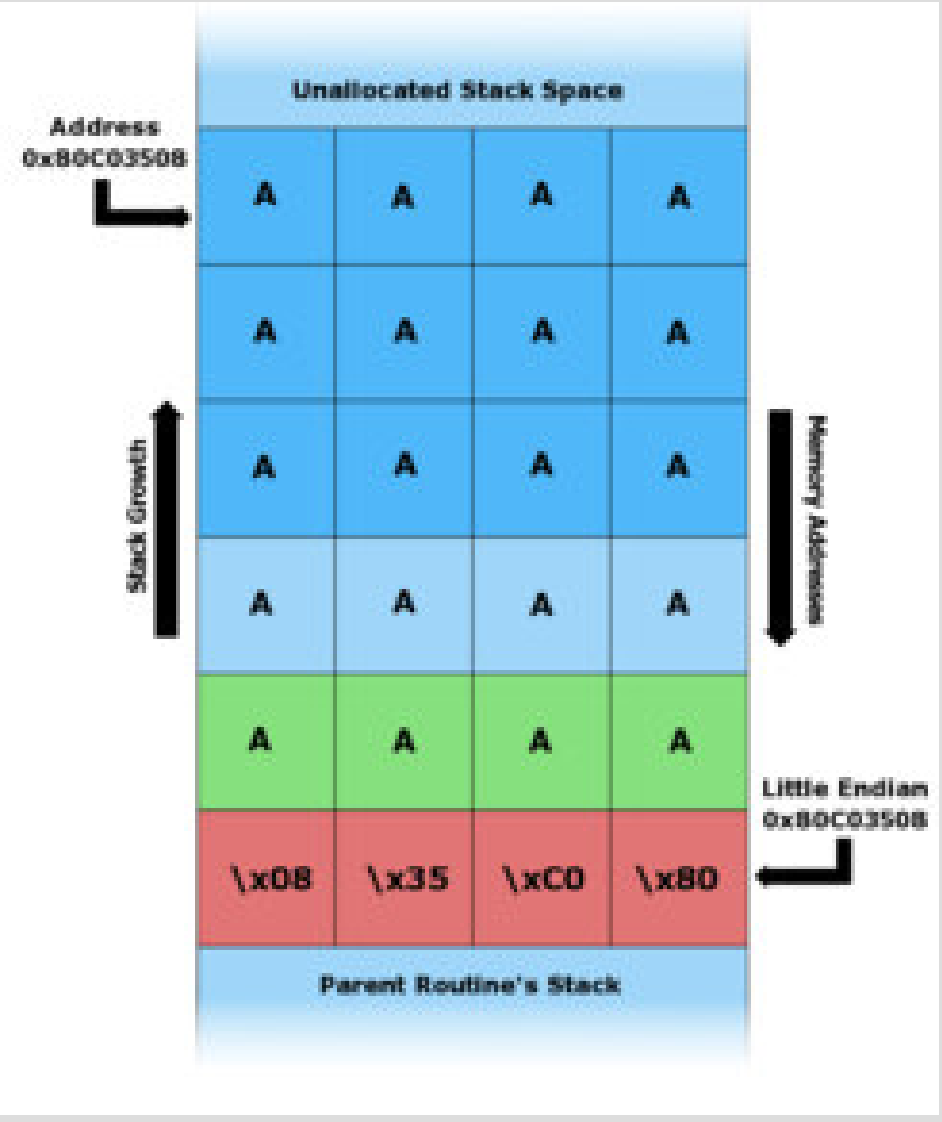
- PHP için;
  - strip_tags(), htmlentites()
  - Prepared statements
  - escapeshellcmd()
- Diğer diller için ilgili kaçış(escape) mekanizmaları bulunmalı, bilinmeli, kullanılmalı

Yazılım Geliştirici Açısından

- Buffer overflow
  - Stack(Yığıt)'ta değişken için ayrılan yer sınırlı
  - Bunu aşan bir girdi yığıttaki diğer verilerin üstüne yazabilir
  - Fonksiyonun dönüş adresini değiştirirsek kendi kodumuzu çalıştırabiliriz.

Yazılım Geliştirici Açısından





Yazılım Geliştirici Açısından

- Kullanılan algoritmaların güvenliği
  - Kolay tahmin edilebilen “rastgele” sayılar
  - Kolay kırılabilir şifreler (WEP)
- Yazılımın bileşenleri arasındaki güven
  - imzalanmış mesajlar
  - OpenSSL vb. kütüphaneler

Özet

- Eğitim şart!
- Politika gerekli
- Güvenlik bilinci gerekli
- Tüm sürece yedirilmeli