Sistem Güvenliği ?
BT Güvenliği ?
Bilgi Güvenliği ?

A.Levend Abay
MSc, MBA, CISM, 8211013

Mart 2014
Yıldız Teknik Üniversitesi

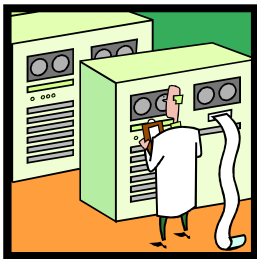
Levend Abay ?

Eğitim :
1986 - Yıldız Teknik Uni./ Bilgisayar Bilimleri ve Mühendisliği
1989 - Yıldız Teknik Uni./ Yüksek Lisans / Bilgisayar Mühendisliği
2008 - Istanbul Bilgi Uni./ MBA

Kariyer (1990 - .... Yapı Kredi)
1990 - DB2 Database Admin
1992 - MVS Sistem Programcısı
1998 – Disaster Recovery Yöneticisi
1999 – Değişiklik Yönetimi Müdürü
Kullanıcı Destek Yönetimi Müdürü
Test Yönetimi Müdürü
2002 – BT Güvenlik Yönetimi Müdürü
2010 CISM (Certified Information Security Manager)
2014 – BT Risk Kontrol ve Koordinasyon Müdürü

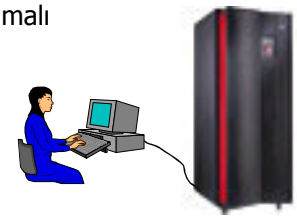
Güvenliğin Tarihçesi

- 1940 - 1950 :
  Tek makina (Güvenlik yok)
  - Bir oda kadar büyük
  - İçinde gezilebilen bilgisayar
  - Zarar vermek için fiziksel temas



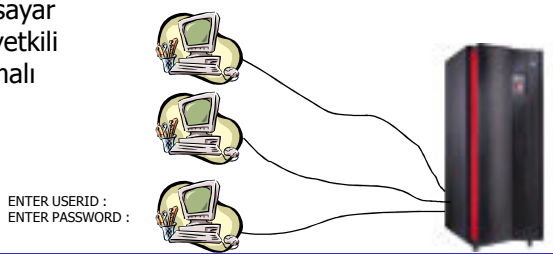
Güvenliğin Tarihçesi

- 1960 - :
  Mainframe, tek konsol
  - Aynı mekanda
  - Tek kullanıcılı bilgisayar
  - Zarar vermek için konsola ulaşılmalı



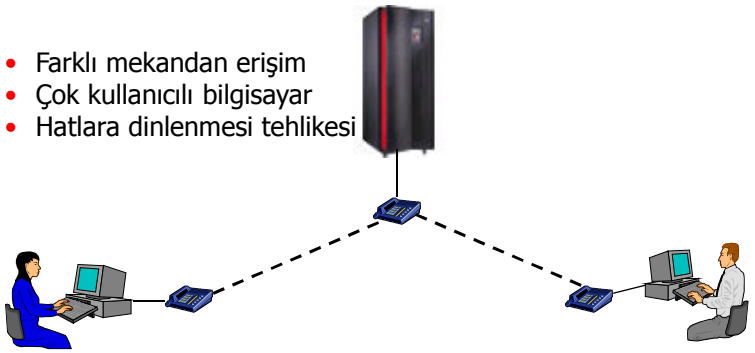
Güvenliğin Tarihçesi

- 1970 - :
  Dump terminaller, Password Control
  (Erişim Kontrol ve Veri Güvenliği)
  - Aynı mekanda
  - Çok kullanıcılı bilgisayar
  - Zarar vermek için yetkili kullanıcıya ulaşılmalı



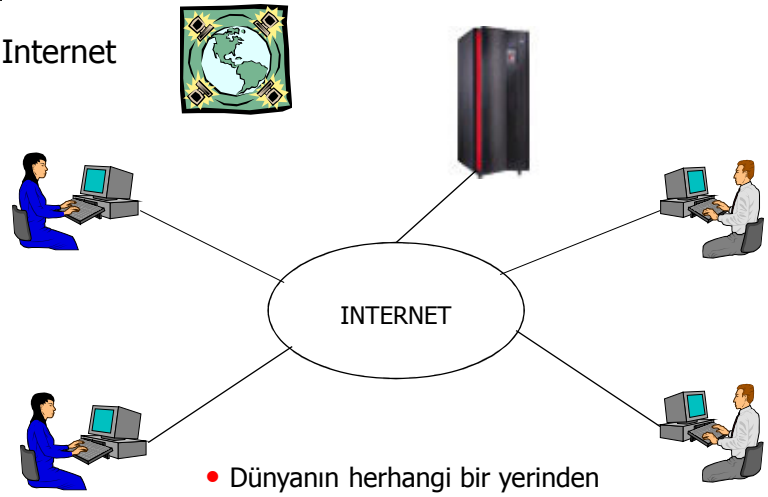
Güvenliğin Tarihçesi

- 1980 - :
  Telefon hatlarıyla erişim (Ağ Güvenliği)
  - Farklı mekandan erişim
  - Çok kullanıcılı bilgisayar
  - Hatlara dinlenmesi tehlikesi



Güvenliğin Tarihçesi

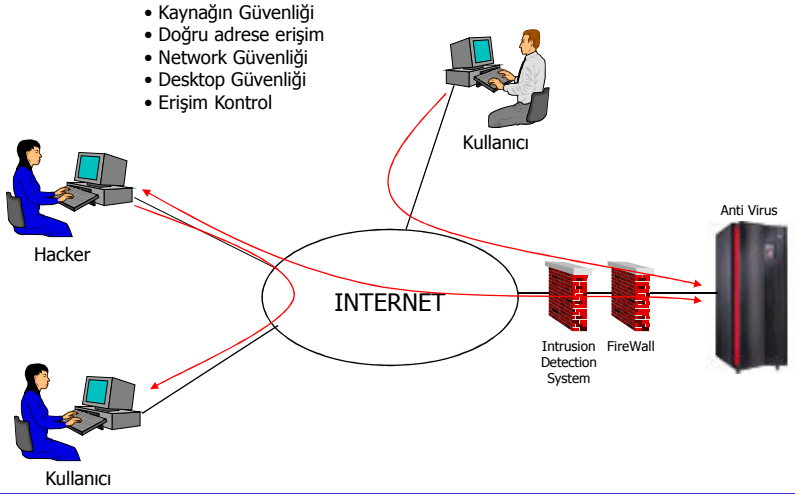
- Internet



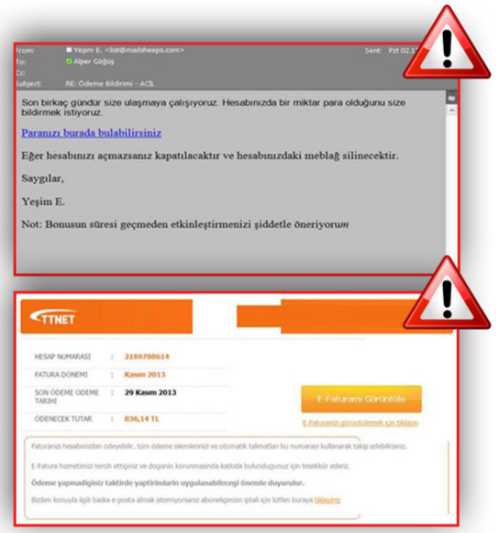
- Dünyanın herhangi bir yerinden

Internet Kullanıcıları

- Kaynağın Güvenliği
- Doğru adrese erişim
- Network Güvenliği
- Desktop Güvenliği
- Erişim Kontrol



Güncel Örnek : Phishing



Mobil cihazlar - BYOD

- Cep telefonları
- Tabletler
- Laptoplar

- Sadece bireyler değil, kurumlar için de mobil cihazlar tehdit
- Verilerimiz güvende mi?

Güvenlik Nedir?

TEHDİTLER NELERDİR?

VARLIKLARIN
ORTAMDAKİ TEHDİTLERDEN
ZARAR
GÖRMEDEN KULLANILABİLMESİDİR.

Tehditler Nelerdir?

Zararlı Programlar

- Virusler (Diskinize bulaşır, makinanıza zarar verir)
- Kurtçuklar (Makinadan makinaya atlayabilirler)
- Truva atları (Başka bir programın arkasına gizlenir)
- Casus programlar (Sizin hakkınızda başkasına bilgi gönderir)

Güvenliğin Temel İlkeleri

Confidentiality (Gizlilik)

Integrity (Bütünlük)

Availability (Süreklilik)

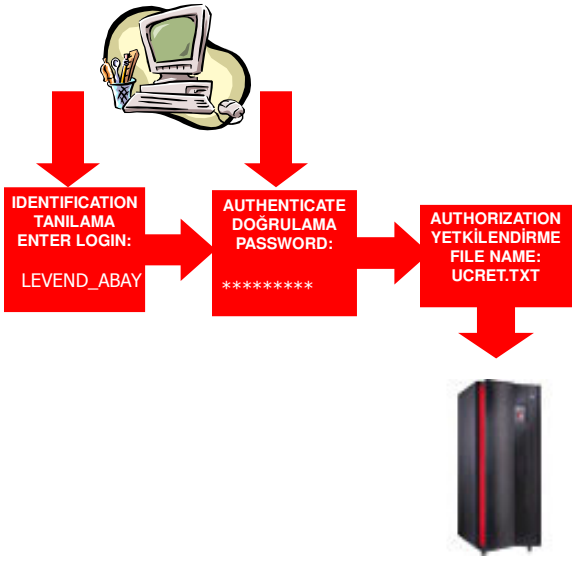
Ve Non-Repudiation (İnkaredilememe)

CONFIDENTIALITY - Gizlilik

Doğru kişinin bilgi kaynaklarına ulaştığından emin olmak.

- Identification (Tanıma)
- Authentication (Doğrulama)
- Authorization (Yetkilendirme)
- Auditing (Denetleme)

Erişim Kontrol



Erişim Kontrol

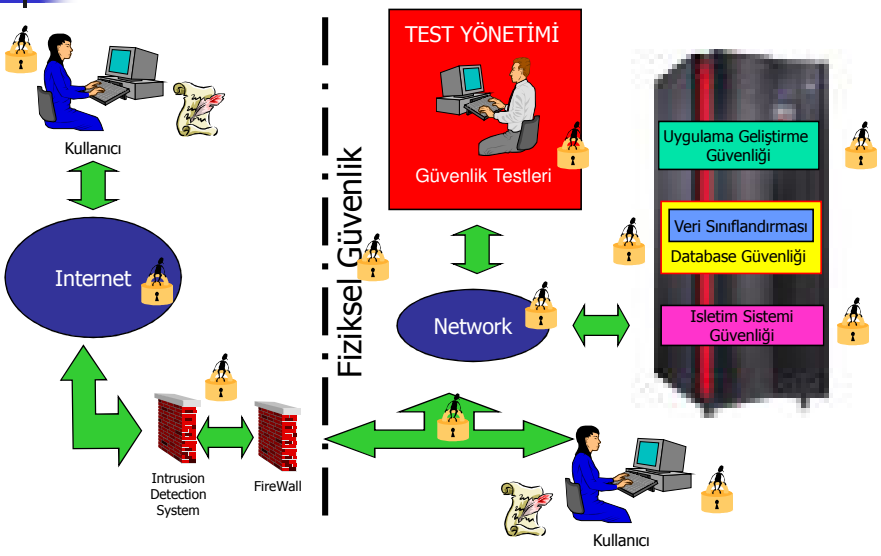
Erişenin tanınması ve doğrulanması için yöntemler

- Something you know - Userid/Şifre
- Something you have - Yaka kartı, Akıllı kart
- Something you are - Biometrics

En güvenliden en güvensize doğru sıralama (false positive'i fazla)

-Palm scan
-Hand geometry
-Iris scan
-Retina pattern
-Fingerprint
-Voice verification
-Facial recognition

CONFIDENTIALITY - Gizlilik



INTEGRITY - Bütünlük

Bilginin üç hali vardır;

KATI : Saklanan hali (Disk veya teyp gibi)
SIVI : İşlenen hali
GAZ : Network üzerindeki hali

Bilginin bu üç hali boyunca dışardan yetkisiz kişiler tarafından değiştirilmediğinin garanti edilmesi

INTEGRITY - Bütünlük

BİLGİNİN BÜTÜNLÜĞÜ, DOĞRULUĞU NASIL SAĞLANIR?

- **ENCRYPTION, HASHING (ÖĞÜTME)**
- **NETWORK GÜVENLİĞİ**
- **DATABASE GÜVENLİĞİ**
- **UYGULAMA GELİŞTİRME GÜVENLİĞİ**
- **ANTIVIRUS**

AVAILABILITY - Süreklilik

Hizmetin kesintiye uğramaması için bilgi kaynaklarının kesintisiz erişilebilir olmasının garantisi

AVAILABILITY - Süreklilik

BİLGİYE KESİNTİSİZ ERİŞİLEBİLİRLİK NASIL SAĞLANIR?

- **HİZMET ANLAŞMALARINA UYGUN TASARIM**
- **INTRUSION DETECTION**
- **İŞLETİM SİSTEMİ GÜVENLİĞİ**
- **UYGULAMA GELİŞTİRME GÜVENLİĞİ**
- **TEST YÖNETİMİ**
- **DEĞİŞİKLİK YÖNETİMİ**
- **FİZİKSEL GÜVENLİK**
- **İŞ SÜREKLİLİĞİ VE OLAĞANÜSTÜ DURUM PLANI**

Güvenlik Yönetimi

ISO 27001 - BGYS

A.05 Güvenlik politikası
A.06 Bilgi güvenliği organizasyonu
A0.7 Varlık yönetimi
A.08 İnsan kaynakları güvenliği
A.09 Fiziksel ve çevresel güvenlik
A.10 Haberleşme ve işletim yönetimi
A.11 Erişim kontrolü
A.12 Bilgi sistemleri edinim, geliştirme ve bakımı
A.13 Bilgi güvenliği ihlal olayı yönetimi
A.14 İş sürekliliği yönetimi
A.15 Uyum

İlginize
Teşekkür Ederim...

A.Levend Abay
Yapı Kredi Bankası AŞ
BT Risk Kontrol ve Koordinasyon Müdürü