



İletişim Ağlarında Güvenlik

Burak DAYIOĞLU '98

Hacettepe Üniversitesi
Bilgi İşlem Dairesi Başkanlığı

burak@hacettepe.edu.tr



Sunum Planı

- Bilişim Güvenliđi ve Kapsamı
- Bilişim Güvenliđi'nin Önemi
- Saldırganlar ve Örnek Saldırı Teknikleri
- Korunma ve Güvenlik Arttırımı



Bilişim Güvenliđi Tanımı

- Bilişim Güvenliđi, bilişim teknolojisi ürünü cihazları ve bu cihazlar tarafından işlenen *bilgileri* korumayı amaçlayan çalışma alanıdır
 - Bilginin korunması ve gizliliđi genellikle ön planda olduğundan “Bilgi Güvenliđi” olarak da anılır
 - Mühendislik çalışması gerektirir



Güvenliğin Temel Eksenleri

- **Gizlilik ve Mahremiyet** (*Secrecy & Confidentiality*)
 - Depolanan ve taşınan bilgilere yetkisiz erişimlerin engellenmesi
 - Gizli bilgilerin korunması ve mahremiyetinin sağlanması
- **Güncellik ve Bütünlük** (*Accuracy & Integrity*)
 - Kullanıcılara bilgilerin en güncel halinin sunulması
 - Değişikliğe yönelik yetkisiz erişimlerin engellenmesi
- **Bulunurluk** (*Availability*)



Tehdit ve Tehdit Örnekleri

- Hasımların, doğal olayların ya da kazaların neden olabileceği, bir bilişim sistemine zarar verebilecek ve bu yolla kurumun işlevini aksatabilecek her türlü olay
 - Elektrik kesintisi, su baskını, deprem
 - Rakip firma, terörist, art niyetli personel
 - Cihaz arızası, operatör hatası
 - Virüsler
 - ...



B.T. Evrimi ve Güvenlik Boyutu

- Tek bilgisayar sistemi
 - Ardışık işletim
- Merkezi bilgisayar sistemi
 - Terminaller ve paralel işletim
- Dağıtık sistemler
 - Sunucular ve istemciler
- İnternet bilişimi
 - Alabildiğine girift yapı

Güvenliği Sağlamak
Daha Kolay

Güvenliği Sağlamak
Daha Zor

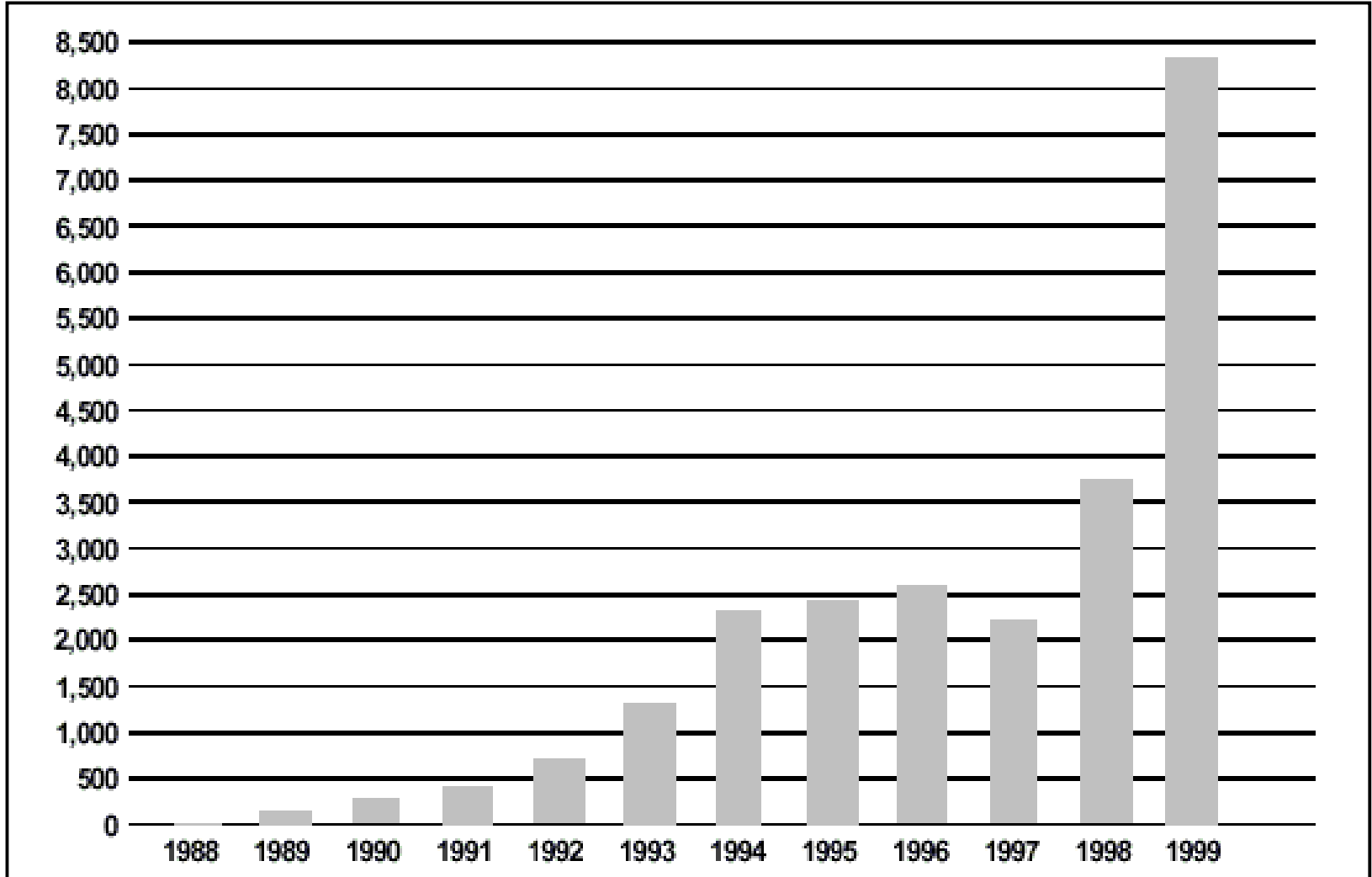


Bilişim Güvenliği'nde Bugün

- Geometrik biçimde artan saldırı sayıları
- Giderek karmaşıklaşan saldırılar
- "Sıradan saldırganlar"
- Konunun göz ardı edilmesi
- Eksik/yanlış bilgi
 - Boşa yapılan yatırımlar
 - Aldatıcı güvenlik hissi
 - Zan altında kalma



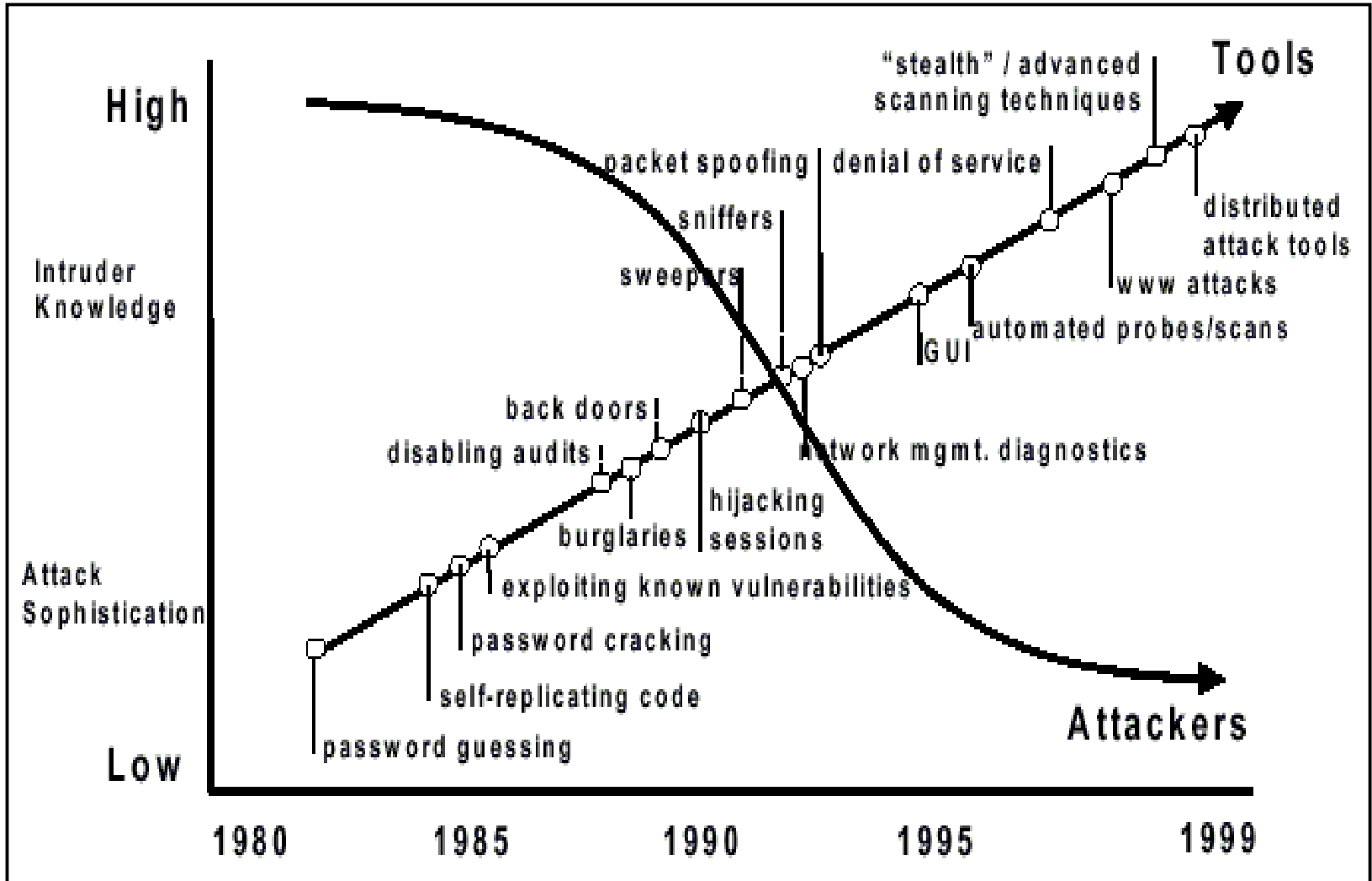
Artan Güvenlik Problemleri



CERT/CC'ye bildirilen saldırı sayısının yıllara göre değişimi



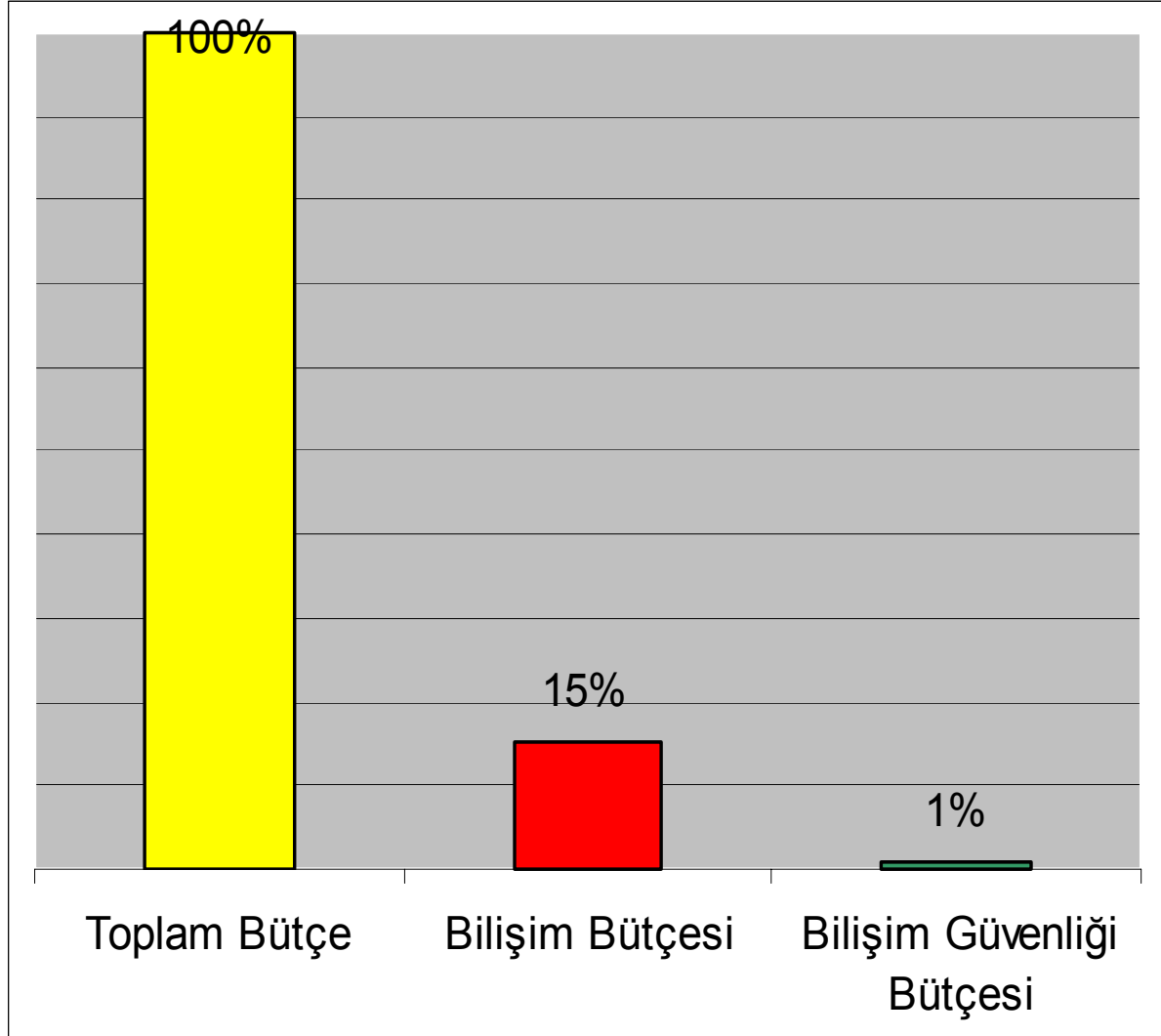
Saldırı Karmaşıklığı / Beceri Düzeyi



CERT/CC'nin saldırgan beceri düzeyi ve saldırı karmaşıklığı ilişkisi tablosu



Kurumsal B.T. Bütçesi ve Güvenlik





A.B.D.'de Durum

- 6 enstitü "NSA Mükemmellik Merkezi" olarak seçildi; dersler açıldı
- Savunma Bakanlığı yalnızca "Saldırı Tespiti" alanında 96 projeye sponsorluk yapıyor
- Gelecek savaşların B.T. temelli olması bekleniyor (*Information Warfare*)
 - Ekonomik sistemler, haberleşme ve yayıncılık tümüyle B.T. temelli



Bir Saldırının Anatomisi

- Bilgi Toplama ve Zayıflık Tespiti
 - Bilgisayarlar, bağlantı şemaları, hizmetler
- İzinsiz Giriş
 - Zayıflıklardan faydalanarak komut işletimi
- Hak Yükseltimi ve Tam Denetim
- Arka Kapı Hazırlama
 - Müteakip girişlerin kolaylaştırılması
- Veri Çalma/Değiştirme/Silme
- Başka Hedeflere Sıçrama



Elektronik Saldırı Örnekleri

- Ağ Taraması
- Truva Atları
- Web uygulamaları
- Alan taşıma
- Dağıtık Hizmet Aksatma (*DDOS*)



Ağ Taraması

- Bozuk TCP paketleri ile işletim sistemi tanımlama
 - İşletim sistemleri bozuk TCP paketleri için farklı yanıtlar üretiyor
- Hizmet taraması
 - “Yarım TCP bağlantıları” ile kayıt tutulmamasının sağlanması
 - Adres yanıtması ile birleştirildiğinde kaynağın tespiti güçleştirilebiliyor
- Nmap, queso ...



Truva Atları

- Programın içine gizlenmiş art niyetli ikincil program
- Çalıştırıldığı bilgisayarın tüm denetimi truva atının sahibine geçiyor
- E-posta mesaj ekleri ve web aracılığı ile dağıtılıyor
- Windows için son iki yılda 300+ truva atı yazılım üretildi
- Back Orifice, SubSeven, NetBus ...



Web Uygulamaları

- Girdi verileri üzerinde yetersiz denetim
 - <http://www.kurbansite.com/cgi-bin/phf?Name=burak;/bin/cat%20/etc/passwd>
 - Son derece yaygın bir zayıflık ve saldırı türü
- Web sitesi kullanıcıları için akış denetimi öngörülerini
 - Kimlik doğrulama sayfasının çevresinden dolaşma



Alan Taşıırma

- Bir uygulama yazılımında tanımlanmış küçük bir alana büyük bir veri yüklemeye çalışırsanız ne olur?
 - Uygulama çakılır
 - Bazı durumlarda, uygulamanın "istenmedik" komutları işletmesi sağlanabilir



Programlama Örneği

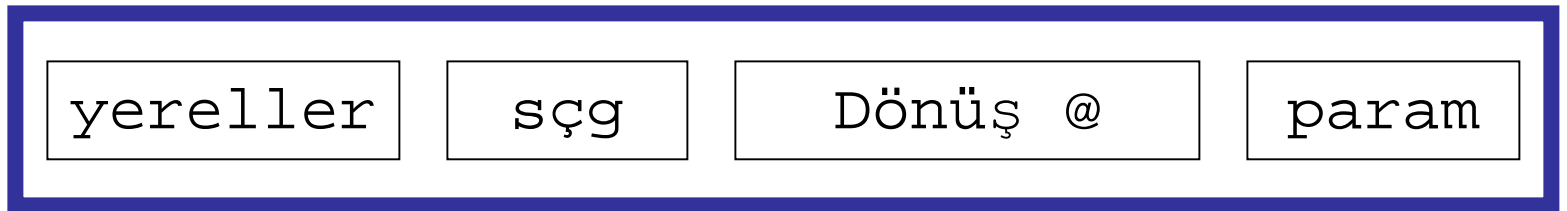
```
void kurban(char *param) {  
    char yerelalan[16];  
    strcpy(yerelalan,param);  
    ...  
}
```

```
int saldirgan(void) {  
    char buyuk_katar[256];  
    int i;  
    for(i=0;i<255;i++)  
        buyuk_katar[i]='A';  
    kurban(buyuk_katar);  
}
```



Yığıt Düzeni

Belleğin Başı → Belleğin Sonu

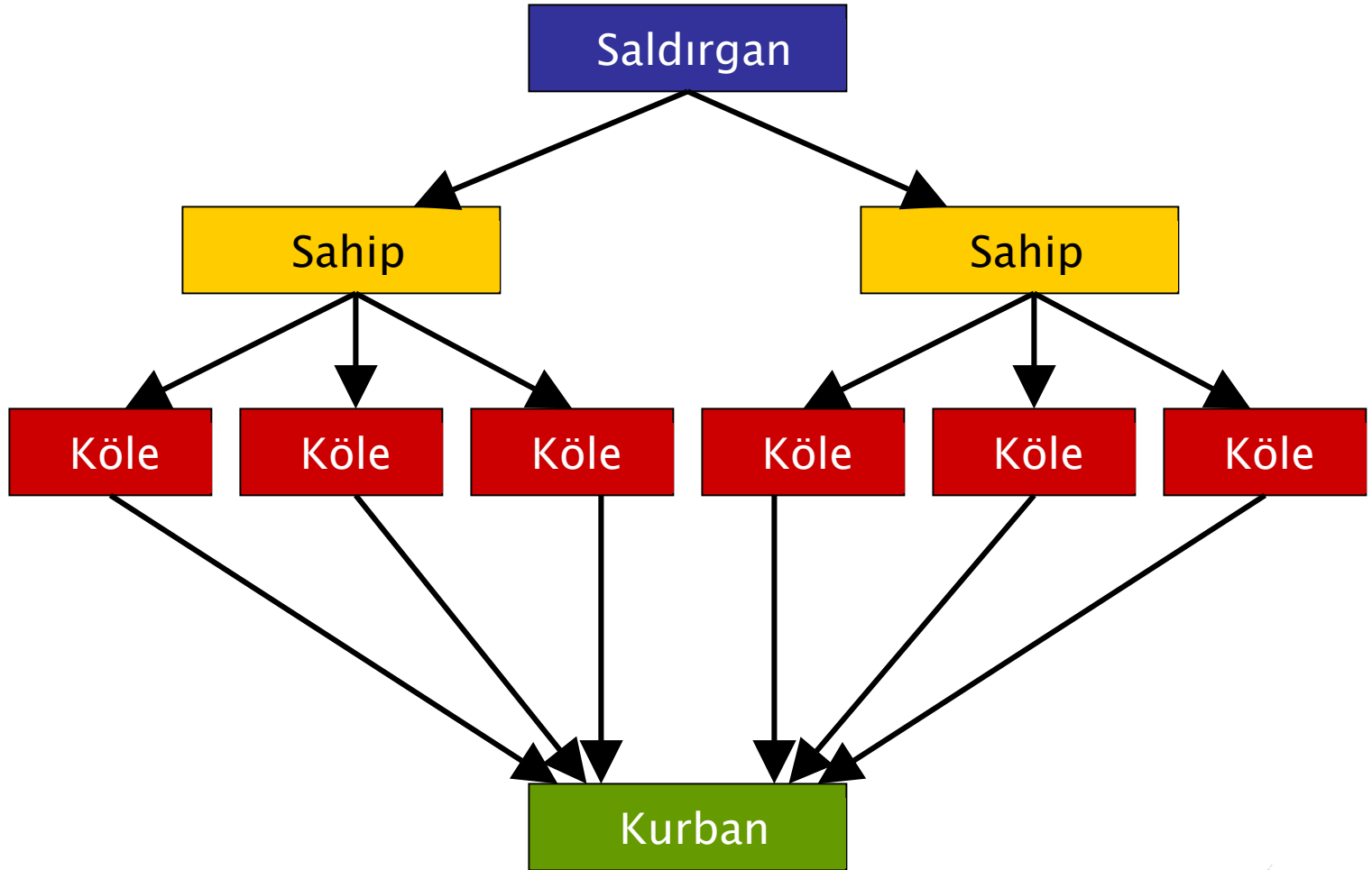


Yığıtın Üstü ← Yığıtın Altı

```
void kurban(char *param) {  
    char yerelalan[16];  
    strcpy(yerelalan, param);  
    ...  
}
```



Dağıtık Hizmet Aksatma





Güvenlik Arttırımı ve Korunma

- Risk Yönetimi ve kurumsal güvenlik politikalarının belirlenmesi
- Bilinçlendirme
- Minimalist yaklaşım
- Teknolojik çözümlerden faydalanılması
 - Güvenlik duvarları, Saldırı tespit sistemleri, sayısal sertifikalar, anti-virüs yazılımları, sanal özel ağlar, güvenlik analizi yazılımları
 - ...



Risk Yönetimi





Kurumsal Güvenlik Politikaları

- Güvenlik politikası kabaca neye izin verilip neye izin verilmediğini tanımlar
- Detaylı prosedürlerden ziyade genel konulara yer verilir
 - Kabul edilebilir bilgisayar kullanım politikası
 - Ağ bağlantı politikası
 - İhlal yönetim politikası
- İnsanlar üzerindeki etkisi
 - Esneklik, üretkenlik, "büyük birader etkisi", değişikliğe direnç



İnsanların Bilinçlendirilmesi

- Bilişim güvenliği ile ilgili çalışmaların en çok atlanan adımlarından birisidir
- Düzenli ve kısa süreli eğitimler
 - Güvenlik politikasının gerekçeli sunumu
 - Güvenliğin değil, bireysel tehditlerin ve risklerin vurgulandığı anlatımlar

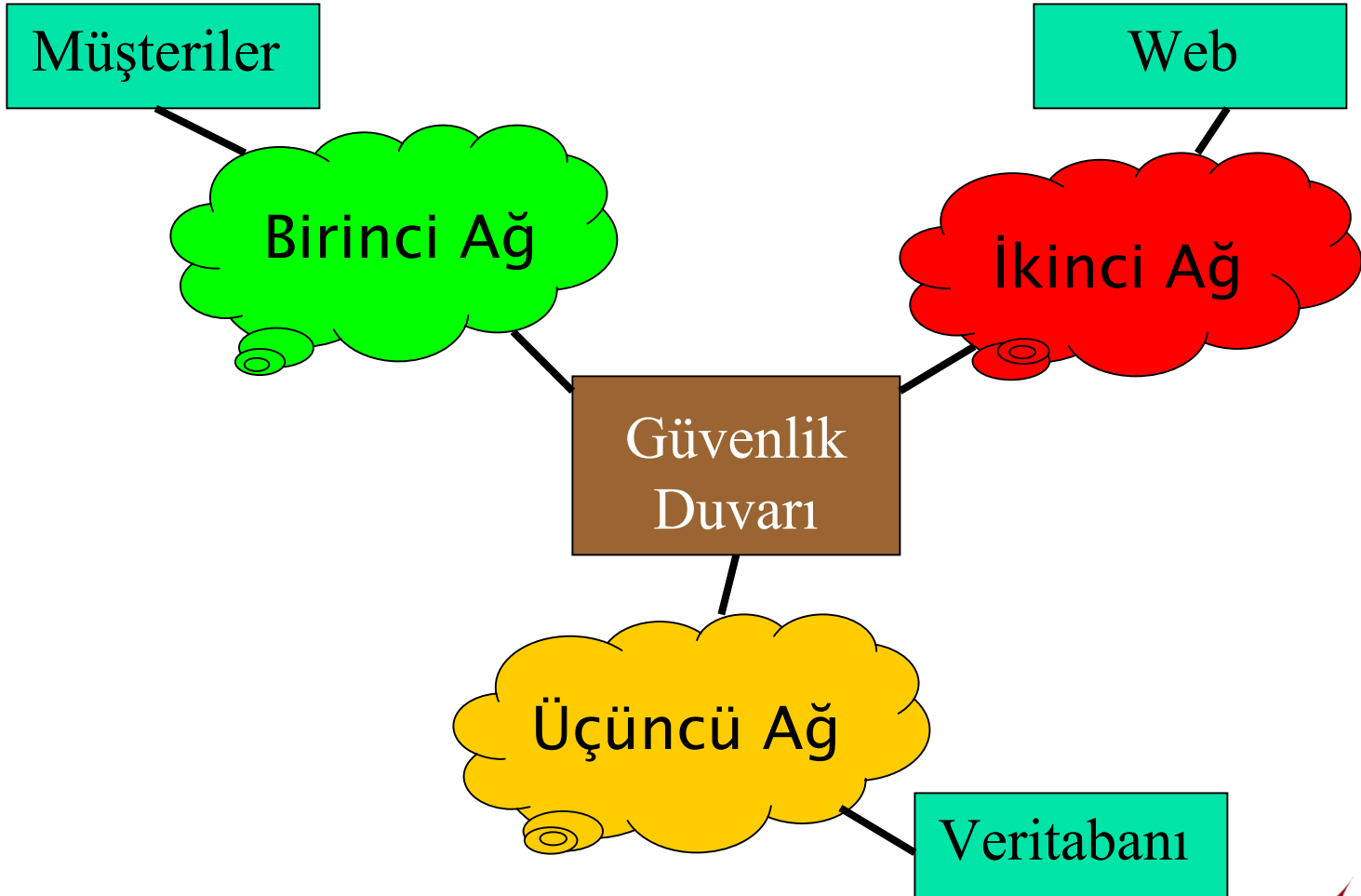


Minimalist Yaklaşım

- Kimseye gerektiğinden fazla erişim hakkı tanımama
- Kimseye gerektiğinden fazla bilgi vermeme
- Gerekmeyen hiç bir yazılımı yüklememe
- Gerekmeyen hiç bir hizmeti sunmama
- Yüklenen küçük yazılım kümesinin güncelliğinin sağlanması

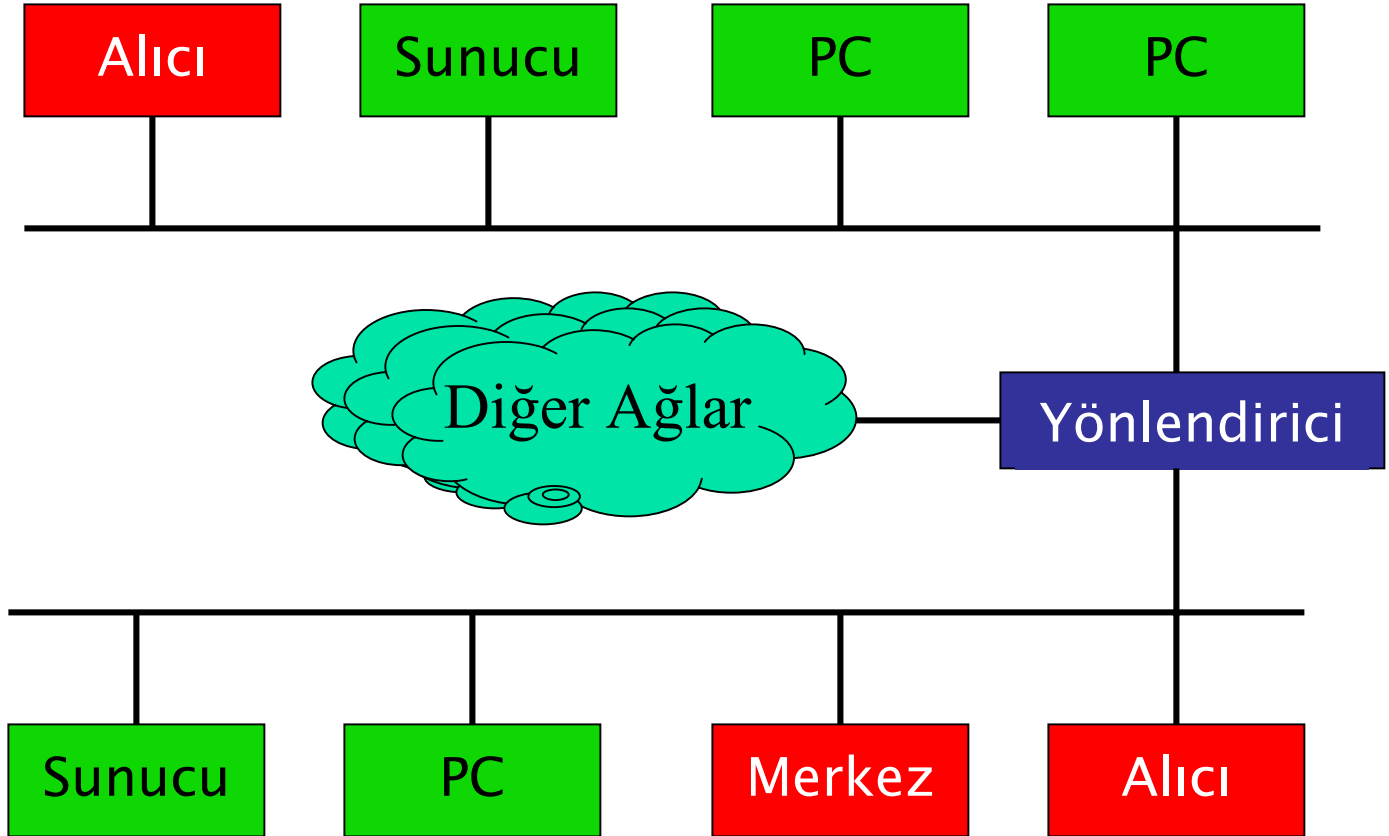


Güvenlik Duvarları





Saldırı Tespit Sistemleri





Güvenlik Analizi Yazılımları

- Sistemleri inceleyerek zayıflıkları tespit etmeye çalışan yazılımlar
 - Anti-virüs yazılımlarının “virüs veritabanı” benzeri “zayıflık veritabanı”
 - Yeni bir teknoloji
 - Anti-virüs olgunluđuna eriřmesi için 1-2 sene gerekiyor



Sonuç

- Bilişim güvenliği konusu hızla önem kazanıyor
- Güvenlik probleminin “teknik” kısmı küçük, sosyal kısmı büyük
- Türkiye’de durum çok “tehlikeli”
 - Kamu’nun güvenlik problemleri
 - Güvenlik’siz e-ticaret



İletişim Ağlarında Güvenlik

Burak DAYIOĞLU '98

Hacettepe Üniversitesi
Bilgi İşlem Dairesi Başkanlığı

burak@hacettepe.edu.tr