



Bilgi Teknolojileri Güvenliđi **Geçmiři - Geleceđi**

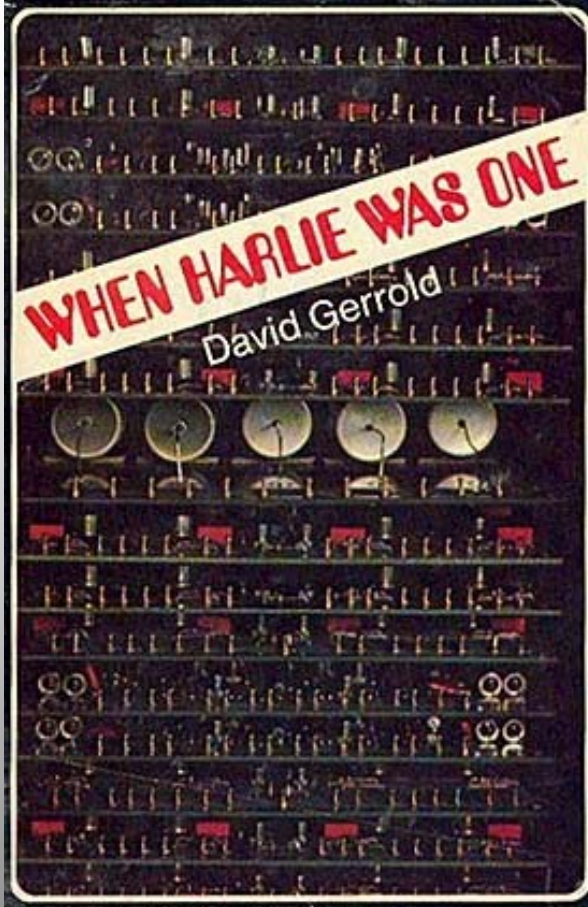
Mert ÜNERİ
Enstitü Müdür Yardımcısı
TÜBİTAK-UEKAE

- Bilgisayar Güvenlik Olayları Tarihçesi
- Günümüz Bilgisayar Güvenlik Olayları
- Gelecek Bilgisayar Güvenlik Olayları
- TÜBİTAK-UEKAE Bilgi Güvenliği Çalışmaları

Bilgisayar Güvenlik Olayları Tarihçesi

Güvenlikle İlgili İlk Problemler

İlk Virüs



- Bilgisayarlarla ilgili ilk bilinen virüs, 1972 yılında David Gerrold tarafından yazılan [When H.A.R.L.I.E. Was One](#) adlı bir bilim kurgu romanında geçmektedir.
- Kitap, "VIRUS" adında virüs şeklinde davranan hayali bir bilgisayar programından bahsetmektedir.
- "VIRUS" ile mücadele için "VACCINE" başka bir program kullanılmıştır.

İlk Virüsler – The CREEPER

- **The Creeper** virüsü ilk olarak ARPANET'te 1970'li yılların başında tespit edilmiştir.
- Tenex işletim sistemi yoluyla yayılmış ve bilgisayara bağlı modemi diğer bilgisayarlara bağlanmak ve onları enfekte etmek için kullanmıştır.
- "I'M THE CREEPER : CATCH ME IF YOU CAN." mesajını ekranda göstermiştir.
- Ardından ortaya çıkan ve Creeper'i temizleyen **Reaper** adlı programı da aynı kişinin yazdığı dedikodu olarak ortada dolaşmıştır.

İlk Virüsler - Elk Cloner

- **Elk Cloner** vahşi ortamda (yazıldığı bilgisayar sistemi veya laboratuvar dışında) yayılmış olan ilk bilgisayar virüsü olarak bilinir. Fakat bu doğru değildir.
- 1982'de [Apple II](#) sistemleri için 15 yaşında lise öğrencisi olan [Rich Skrenta](#) tarafından yazılmıştır.

İlk Virüsler - Elk Cloner

- Elk Cloner, Apple II'nin işletim sistemine enfekte olarak yayılmaktadır.
- Bilgisayar, enfekte bir floppy diskten başladığında virüsün bir kopyası otomatik olarak çalışmaya başlar ve ardından disk erişimini gözetler. Enfekte olmamış başka bir disk bilgisayara yerleştirildiğinde virüs kendisini o diske kopyalayacaktır.
- Diğer ilk virüsler gibi Elk Cloner da herhangi bir zarar vermiyordu. Kendisini sabit bir track bölgesine yazdığı için sadece DOS imajı içeren disketlere zarar verebilirdi.

İlk Virüsler - Elk Cloner

- Yaptığı şey enfekte olan diskette bilgisayarın 50'inci defa açılmasında şu kısa şiiri göstermekti:
 - Elk Cloner: The program with a personality
 - It will get on all your disks
 - It will infiltrate your chips
 - Yes it's Cloner!
 - It will stick to you like glue
 - It will modify RAM too
 - Send in the Cloner!
- Virüsün yazılış amacı rahatsızlık yaratmaktı.
- Yayılış sebebi ise Kullanıcıların sürücüde disk bulundurarak bilgisayarlarını başlatmamaları gerektiğini bilmemeleri ve o günlerde Virüs Tarayıcılarının olmamasıydı. Virüs bir miktar uğraşyla elle temizlenebiliyordu.

Morris Solucanı

- **Morris Solucanı** veya **Internet Solucanı**, Internet yoluyla yayılan ilk solucanlardan birisidir. İlk solucan olduğu tahmin edilmektedir. Basının ciddi miktarda dikkatini çekmiştir.
- Üniversitesinde öğrenci olan, [Robert Tappan Morris](#) tarafından yazılmış ve MIT'ten 2 Kasım, 1988 tarihinde Internet'e bırakılmıştır.
- Virüsün MIT'ten bırakılmasının sebebi solucanın Cornell'den geldiğinin anlaşılmaması içindir.

Solucanın Mimarisi

- Solucanın yazarına göre Morris solucanı zarar vermek amaçlı değil, Internet'in büyüklüğünü tahmin etmek amaçlıydı.
- Gözden kaçırılan bir bilgisayarın birçok kere enfekte olması ve her enfeksiyonun ayrı bir proses olarak çalışarak bilgisayarı çalışamayacak kadar yavaşlatmasıydı.
- **Morris solucanı**, Unix sendmail, Finger, rsh/rexec içindeki bilinen açıklıkları ve zayıf parolaları kullanarak yayılmıştır.

Hata

- Solucanı, zararsız bir bilgi toplama çalışmasından etkili bir servis dışı bırakma saldırısına çeviren hata yayılma mekanizmasındaydı.
- Solucan yeni bilgisayara saldırdığında bilgisayarın zaten enfekte olup olmadığına bakmıyordu.
- Zaten böyle bir mekanizma olsaydı; solucan enfekte etmek istediğinde solucanın bilgisayarda çalıştığını gösteren bir proses, solucana karşı koruma kolaylıkla sağlayabilirdi.

Solucanın Etkileri

- Solucan 6000 Unix makineye bulaştı. O günkü tahminlere göre Internet'e sadece 60,000 makine bağlıydı. Böylece Morris solucanı tüm Internetin yüzde onuna bulaşmış oldu.
- ABD, Genel Muhasebe Ofisine (GAO) göre zarar 10M–100M\$ arasındaydı.
- Gene Spafford, acil durum müdahale çalışmalarını koordine etmek için Phage ePosta listesini oluşturdu.
- 1986 Computer Fraud and Abuse Act'i ihlal ettiği gerekçesiyle 3 yıl gözaltı, 400 saat kamu servisi ve 10,050 \$ cezaya çarptırıldı.
- Morris solucanı, o günlerde hem Interneti büyük ölçüde servis dışı bıraktığı hem de psikolojik açıdan Internetin güvenliği ve güvenilirliği algısını yıktığı için "Büyük Solucan" olarak da adlandırılmaktadır.

Morris Solucanından Sonra

- Olaydan sonra, Internet üzerinde bilgisayar güvenlik olaylarına tepkinin nasıl iyileştirilebileceği konusunda bir toplantı düzenlendi.
- Toplantı sonucunda Internet güvenlik problemleri ile ilgili tek bir iletişim noktası olması gerektiğine ve bu noktanın güvenlik bilgileri için güvenilir bir kaynak olması önerildi.
- Öneriye karşılık CERT Coordination Center, Internet'te meydana gelen güvenlik olaylarına müdahale etmek amacıyla kuruldu.

Hacking Terimi

- Hacking, 1960 ve 1970'lerde MIT ve diğer bazı üniversitelerde ortaya konmuş bir terimdir.
- Hack: Sınırları zorlamak, olağan konsept, yapı ve kuralların dışına çıkmak
- Olağan "hacking" aktiviteleri
 - Bilgisayar programı yazmak,
 - Pratik şakalar,
 - Üniversitenin çatı ve tünellerini keşfetmek
- Bu aktiviteler o günlerde MIT bilgisayarlarında yeni yeni konulmaya başlanan güvenlik önlemlerini aşmayı da içermeye başlar.

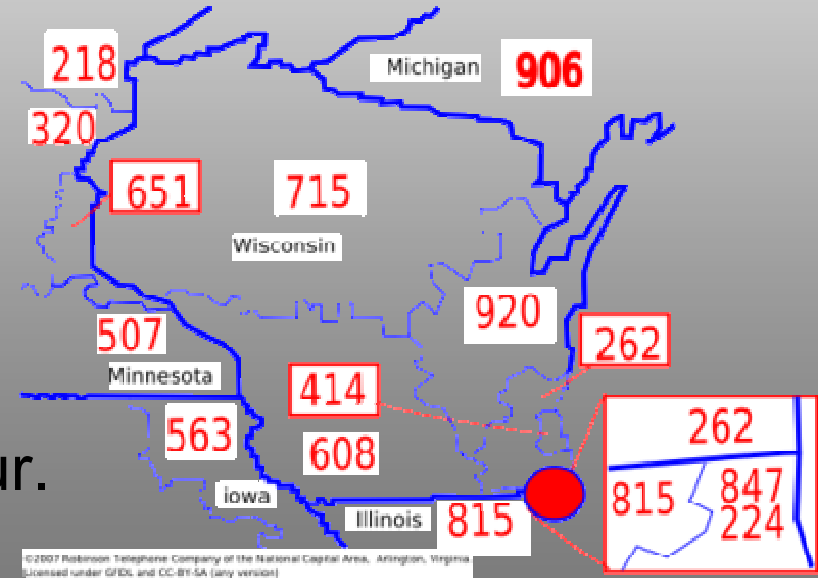
Hacking Tarihi - War Games



- **WarGames** 1983 yılı Amerikan yapımı bir film.
- Filmde bir lise öğrencisi, Askeri Bilgi Sistemlerine girerek füze ateşleme sistemine kadar erişir.
- Filmle birlikte Bilgisayar Güvenliği medyanın ve toplumun dikkatini çeker.

Hacking Tarihi – 414'ler

- Milwaukee, Wisconsin'de 414'ler adıyla bilinen genç cracker'lar
 - Los Alamos National Laboratory,
 - Sloan-Kettering Cancer Center ve
 - Security Pacific Bank da
 - dahil olmak üzere Kanada ve ABD'deki bilgisayar sistemlerine girdi.
- 414'ler adını yaşadıkları yerin telefon kodundan (Milwaukee) almışlardır.
- Bu şekilde Wargames'in sebep olduğu endişe gerçekleşmiş olur.



Hacking Tarihi – 414'ler

- Olay medyanın dikkatini çok çabuk şekilde çeker.
- Konu Newsweek Dergisinde kapak hikayesi olarak "Beware: Hackers at play" adıyla yer alır. Kapakta ise çetenin sözcüsü 17 yaşındaki Neal Patrick'in resmi yer almaktadır.
- Medyada hacker kelimesi ilk defa yer almış ve hacker sözcüğünün bu anlamda kullanılmıştır.

Hacker Toplulukları

- Organize çalışıyorlar.
- Aralarında iletişim çok güçlü.
- Kredi kartı bilgileri, henüz bilinmeyen açıkları, BotNet'leri kendi aralarında para gibi kullanıyorlar veya bunlar karşılığında para kazanıyorlar.

Günümüz Bilgisayar Güvenlik Olayları

Güncel Tehditler

Günümüz Güvenlik Tehditleri

- Genel tehditler
 - Virus, Worm, Trojan, Time Bomb, Logic Bomb, Rabbit, Bacterium, Spoofing, Scanning, Eavesdropping, Scavenging, Spamming, Tunneling, DoS, DDoS, ...
- İstemsiz tehditler
 - Donanım hataları, Yazılım hataları, Kullanım hataları, ...
- Fiziksel tehditler
 - Hırsızlık, Yangın, Su basması, Çalışma ortamı, Elektrik kesilmesi, Sosyal karmaşa, Vandalizm, Savaş, ...

Bazı arpıcı sonuçlar

- Sapphire/Slammer Worm (2003), internet üzerinde açıklıęa sahip olan bilgisayarların %90'ına 10 dakika içinde bulaşabildi.
- av-comperatives.org tarafından 8 adet polimorfik virüs için yayınlanan son deęerlendirmeye göre sektördeki 13 antivirüs yazılımından 8 tanesi en az 1 virüsün tespitinde başarısız oldu.
- Mali zararlar en ok virüsler, yetkisiz erişim, dizüstü bilgisayar hırsızlığı ve kişisel bilgi hırsızlığından kaynaklanmaktadır.

Siber Saldırı Motivasyon, Hedef ve Yöntemleri

	Motivasyon	Hedef	Yöntem
Siber Terör	Politik değişiklikler	Masum kullanıcılar	Bilgiayar-tabanlı şiddet ve yıkım
Hactivism	Politik değişiklikler	Karar vericiler	Saldırı
Cracking	Ego, Kişisel düşmanlık	Şahıslar, Firmalar, Kamu Sistemleri	Saldırı, Açıklık kullanımı
Siber Suç	Ekonomik fayda	Şahıslar, Firmalar	Sahtekarlık, ID çalma, Şantaj, Saldırı, Açıklık kullanımı
Siber Casusluk	Ekonomik fayda	Şahıslar, Firmalar, Kamu Sistemleri	Saldırı, Açıklık kullanımı
Devletler seviyesinde bilgi savaşları	Politik veya askeri fayda	Altyapı, Askeri bileşenler, Kamu sistemleri	Saldırı, Açıklık kullanımı, Fiziksel saldırılar

Estonya örneđi



Estonya'daki Bronz Asker heykeli



26 Nisan 2007 sonrası...

Estonya örneđi

- Heykelin kaldırılmasının Rusya tarafından kınanması (27 Nisan 2007) ardından Tallinn'de ayaklanmalar ve yağmalar başladı.
- 27-29 Nisan 2007 tarihleri arasında başlangıç seviyesi siber saldırılar
 - Bazı web sayfalarının ele geçirilmesi
 - Küçük DDOS saldırıları
 - Ulusal e-posta sunucular ve haber portallarına başlangıç seviyesi SPAM saldırıları

Estonya örneđi

- 30 Nisan-18 Mayıs tarihleri arasında daha organize saldırılar
 - Ulusal bilgi sistemleri, Internet hizmet sağlayıcıları ve bankalara yönelik daha geniş katılımlı ve koordineli DDOS saldırıları
 - Daha çok sayıda SPAM mesajları
- Ülkedeki internet sistemi çökme noktasına getirilmiştir.

Neden bu kadar önemli ?

- Estonya nüfus 1.3 Milyon.
 - 1 milyondan fazla digital kimlik kartı mevcut
 - Mayıs 2007'den itibaren cep telefonlarında digital kimlik tutulmaktadır.
- Nüfusun %66 oranında İnternet'i yoğun olarak kullanmaktadır.
- Evlerin %55 inde kişisel bilgisayar (PC) bulunmaktadır.
- Vergi beyanları %80 oranında İnternet üzerinden yapılmaktadır.
- Bankacılık işlemleri %97 oranında İnternet üzerinden yapılmaktadır.
- Sağlık kayıtları %100 oranında dijital ortamda taşınmaktadır.
- Ülke çapında hemen her yerde kablosuz İnternet hizmeti sunulmaktadır ve bu erişim genel olarak şifresizdir.
- Kurulan her 4 yeni şirketten 1 tanesi İnternet üzerinde kurulmaktadır.

Bu saldırılarla İnternet sistemi değil Estonya zarar görmüştür!

Ayrıca...

- Yağmalara katılan vatandaşların fotoğrafları polis tarafından web sayfasında isimleriyle teşhir edildi. Bu fotoğraflar hem haksız rekabet(reklam) hem de kişisel gizlilik açısından hükümeti zora soktu.



Gelecek Bilgisayar Güvenlik Olayları

Olası Tehditler

Günümüzden geleceğe...

- Zararlı yazılımlar daha gelişmiş kriptografik ve polimorfik özelliklere sahip olacak.
 - Tespitleri daha zor olacak.
- Dostunuza düşman, düşmanınıza dost olabilirsiniz! (Botnet)
- Siber saldırılar Türkiye'yi daha çok etkileyecek.
 - İnternet şirketlerinin oranı bugünden çok daha fazla olacak.
 - Kamu hizmetlerinin büyük kısmı İnternet ortamına taşınacak.

Günümüzden geleceğe...

- 70'li yıllarda bilim-kurgu romanlarına konu olan virüsler 80'li yıllarda tehdit olmaya başladı.
 - Bugünün hayalleri yakında gerçek olacak.
- Çok uzak olmayan gelecekte ülkelerin siber savaş yapan “daha büyük” düzenli siber orduları olacak. (küçük çapta var)
- Kablosuz ve Hücresel sistem kullanımlarının artmasıyla izole sistem kalmayacak.
 - Siber saldırılar evimizdeki eşyalara kadar girecek. (başladı ama yaygınlaşmadı)

Günümüzden geleceğe...

- Günümüzde güvenli sayılan güvenlik algoritmalarının eksponansiyel kırılma süreleri zaman içerisinde polinom zamana düşecek.
- Ulusal güvenlik ürünleri ve ulusal güvenlik değerlendirmelerinin yapılması çok daha önemli olacak.

TÜBİTAK UEKAE

Bilgi Güvenliđi alıřmaları

- Ağ Güvenliği
- Kriptografik Analiz ve Tasarım
- Milli Kripto Cihazları (Hat, Ses, ISDN, IP)
- Milli Açık Anahtar Altyapısı (PKI)
- EMC (Elektromanyetik Uyumluluk)
- TEMPEST
- Adli Analiz Cihazları

Ağ Güvenliği - OKTEM

- Güvenli Sistem Tasarımı ve Kurulumu
- Güvenlik Testleri ve Denetlemeleri
- Bilgi Güvenliği Eğitimleri
- Bilgisayar Güvenlik Olaylarına Müdahale (CERT)
- Bilgi Güvenliği Yönetim Sistemleri
 - ISO/IEC 27001, CoBIT, ITIL
- Risk Yönetimi
- Penetrasyon Testleri
- Kod Analizi
- İş Sürekliliği Yönetim Sistemleri
- Ortak Kriterler Değerlendirmeleri
- Haberleşme Güvenliği (COMSEC) Değerlendirmeleri





Sorularınız...?