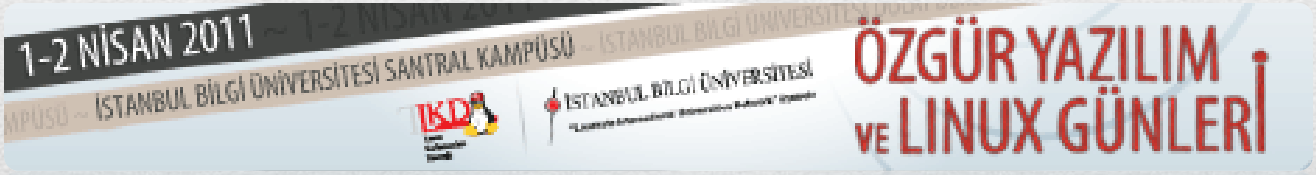
Mobil İstemcilere Yönelik Güvenlik Tehditleri ve Özgür Uygulamalarla Savunma



AFŞİN TAŞKIRAN

afsin@taskiran.org || afsin@enderunix.org

www.enderunix.org/afsin

Afşin Taşkıran ?

- http://www.linkedin.com/in/afsintaskiran
- Yüksek Elektrik-Elektronik Mühendisi
- Sektör Sertifikaları
  - CISSP® – Certified Information Systems Security Professional
  - EC-Council – CEH – Certified Ethical Hacker
  - CCSP-SND – Cisco Information Security Specialist
  - CCSA – Check Point Certified Security Administrator NGX
  - JNCIS-FWV – Juniper Networks Certified Internet Specialist
  - JNCIA-FWV – Juniper Networks Certified Internet Associate
  - CCNA – Cisco Certified Network Associate

Nelerden bahsedeceğiz ?

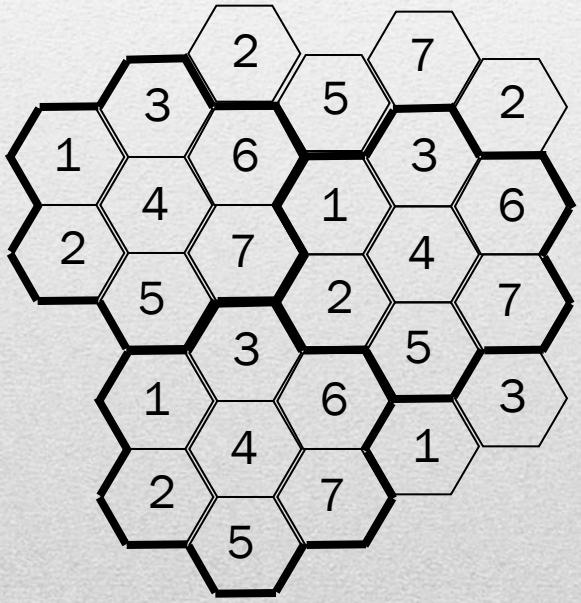
- Wireless ve GSM ağlarının genel mimarisi
- Kablosuz ve özellikle GSM veri ağlarında istemcilere yönelik tehditler.
- Linux terminallerdeki güvenlik önlemleri

Mobil Telefonlarla/Cihazlarla Ne Yapılır ?

- Sesli görüşme
- SMS/MMS göndermek
- Ofis dökümanları
- PDF Okumak
- GPS
- MP3 Player
- Kamera
- Veri Saklama
- Wi-Fi, Kablosuz Internet
- WAP
- Internet APN, Kurumsal APN ler

3G Networks

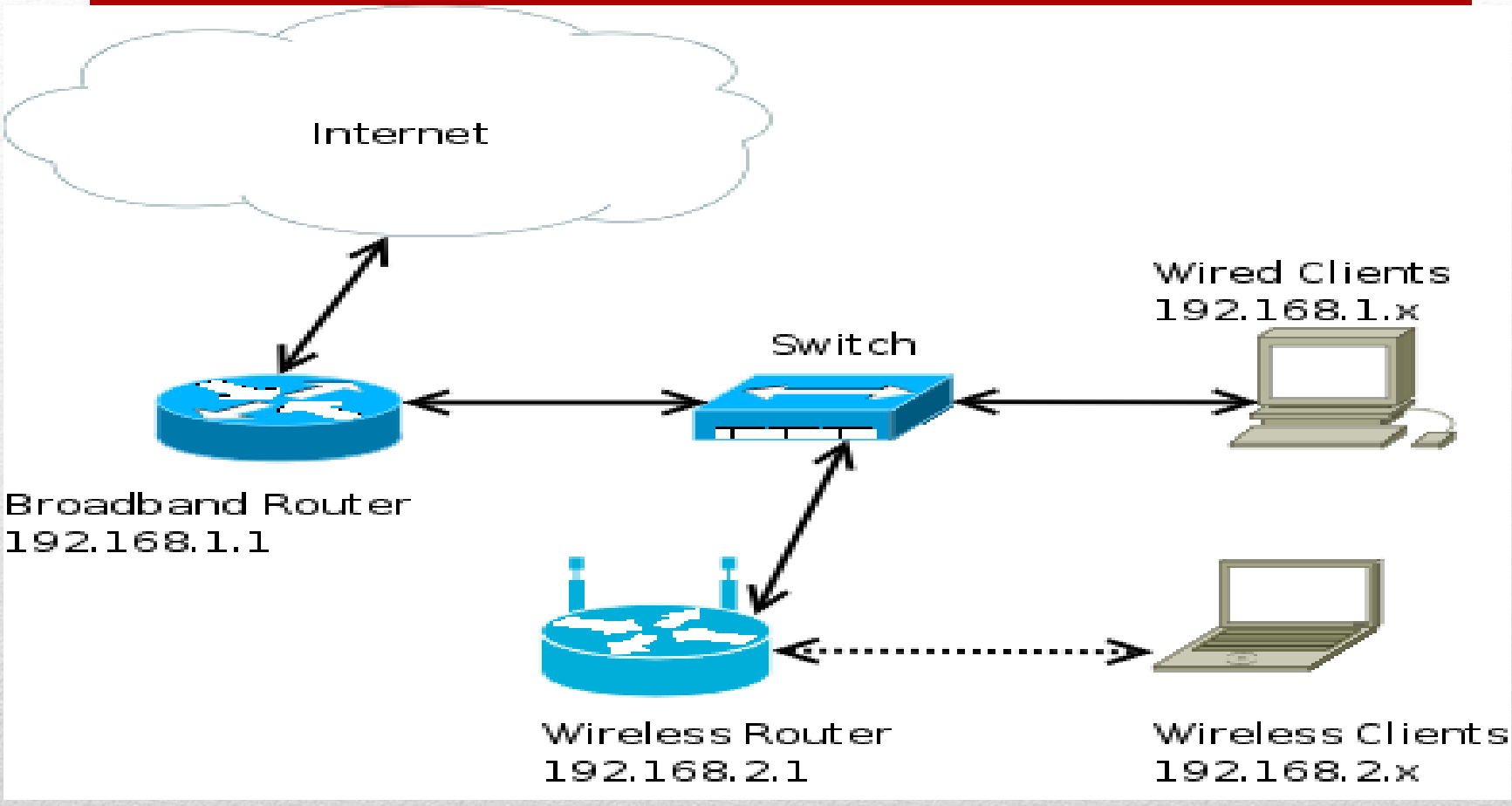
- 3G
- Mobil Operatör Yapıları
  - GPRS ve 3G Ağ Altpısı
- Mobil istemcinin Internet'e bağlanması?
- Veri ağlarındaki saldırı türleri

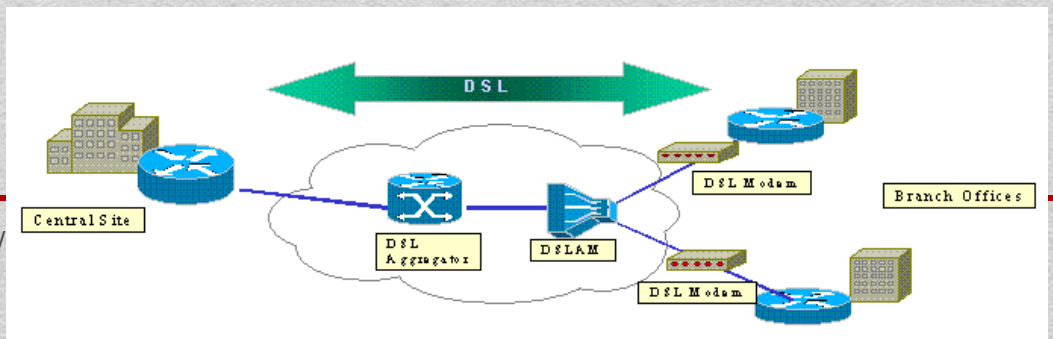


Neden 3G?

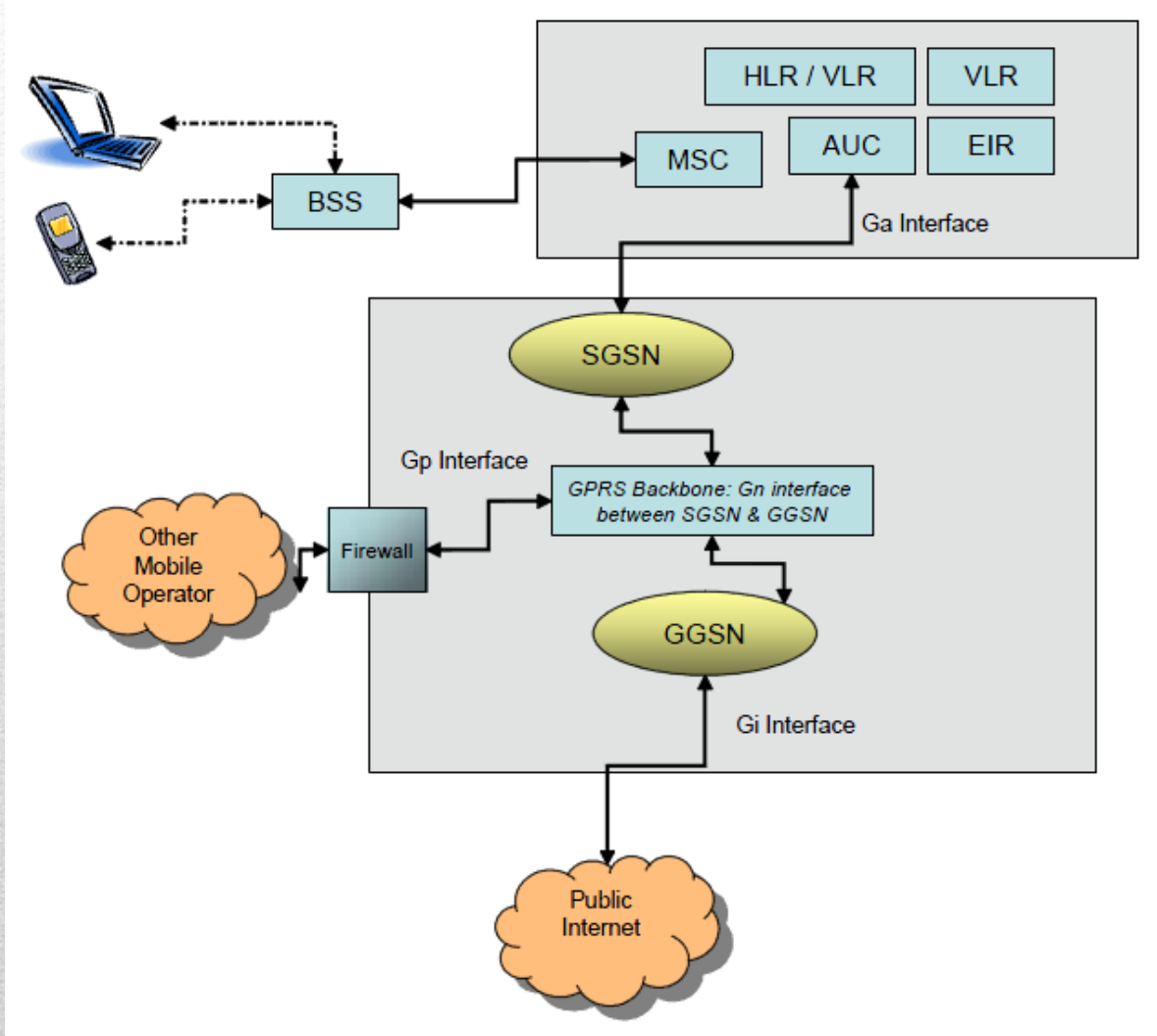
- Yeni uygulamalar için yüksek band genişliği ihtiyacı
- **Müşteriler İçin;**
  - Video streaming, TV broadcast
  - Video calls, video clips – Haber, müzik, spor
  - Güçlendirilmiş oyun, chat ve yer bulma servisleri
- **İş Dünyası İçin;**
  - Yüksek hızda teleworking / VPN erişimi
  - Satış otomasyonu
  - Araç takip sistemleri
  - Video konferans
  - Eş zamanlı finans çalışmaları

DSL Ağlar


Internet
Wired Clients
192.168.1.x
Switch
Broadband Router
192.168.1.1
Wireless Router
192.168.2.1
Wireless Clients
192.168.2.x

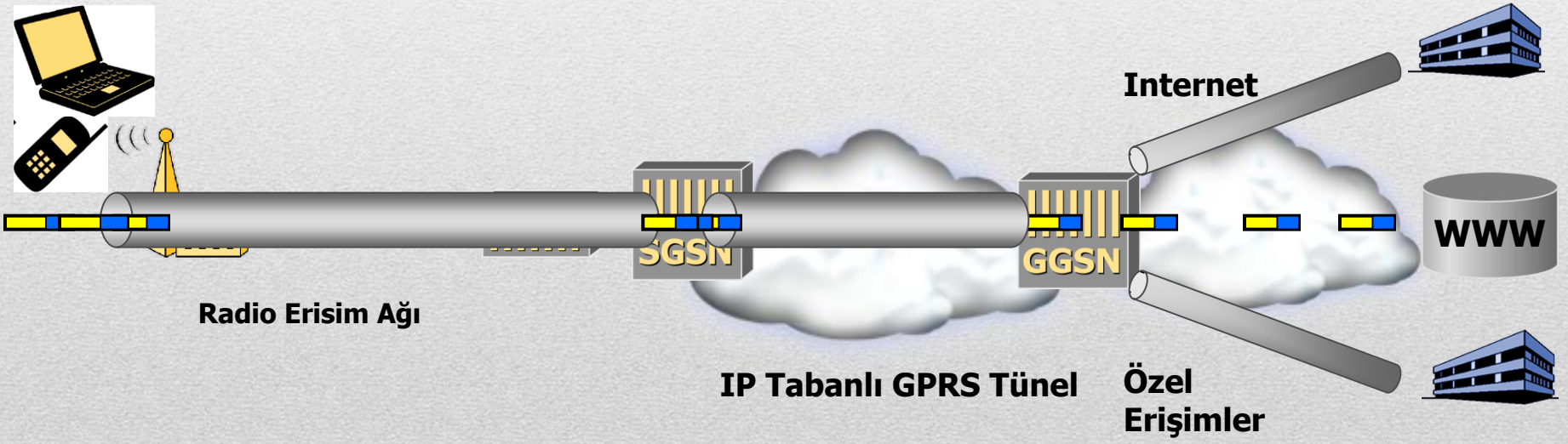

DSL
Central Site
DSL Aggregator
DSLAM
DSL Modem
DSL Modem
Branch Offices

Mobil Operatör Örnek GPRS Yapısı

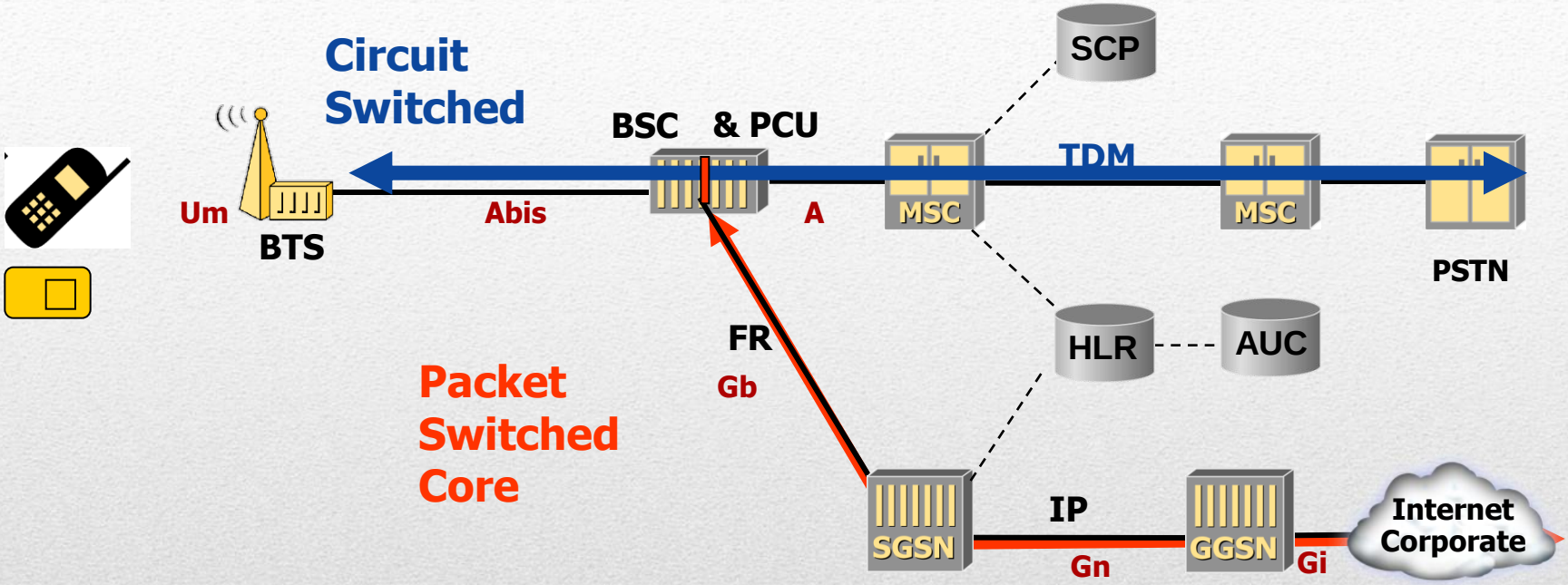


3G Ağ Yapısı

- Mobil cihazın aldığı IP adresi Internet' e ya da müşteri ağına yönlendirilir.
- IP adresini alan mobil her türlü uygulama işlemini gerçekleştirebilir.(MMS, WAP gateway, Web görüntüleme)



GPRS: General Packet Radio Service



Serving GPRS Support Node (SGSN)

Paket transferinin sağlanması

Kayıt, Kimlik doğrulama, mobility yönetimi, handover, CDR !

BTS lerle lojik linkler ve GGSN lere tüneller

Gateway GPRS Support Node (GGSN)

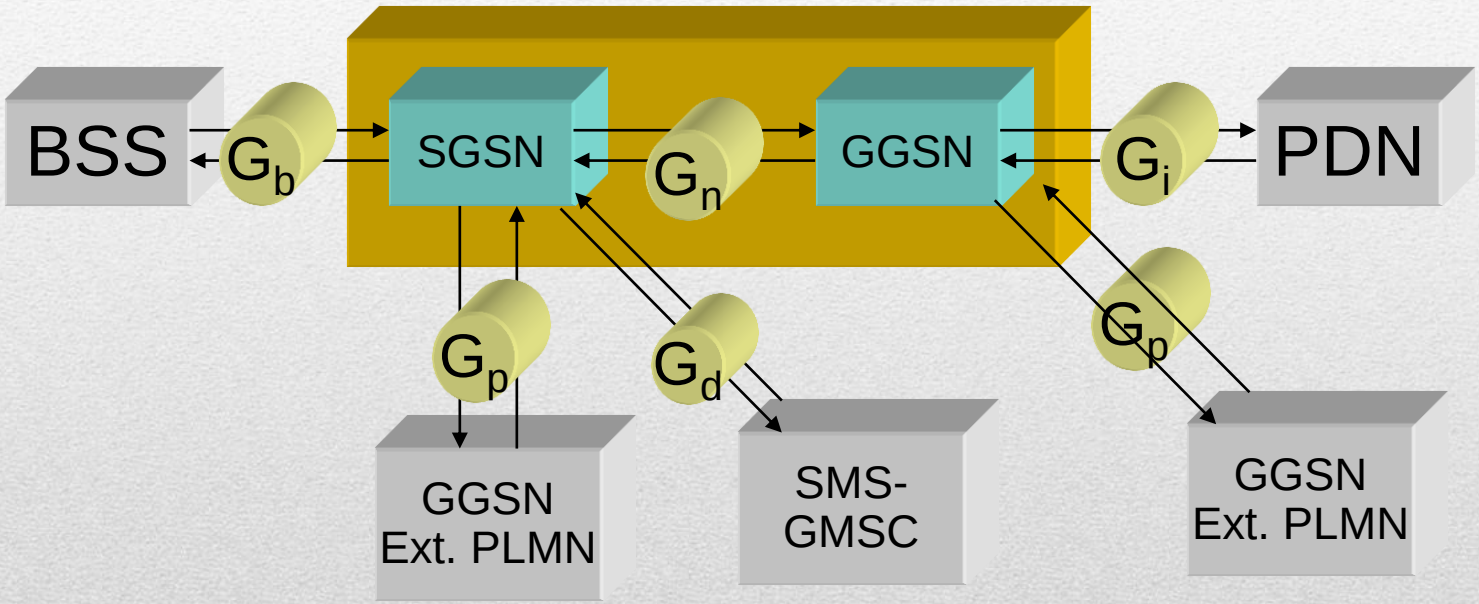
IP Ağına çıkış noktası

GPRS oturum yönetimi

AAA

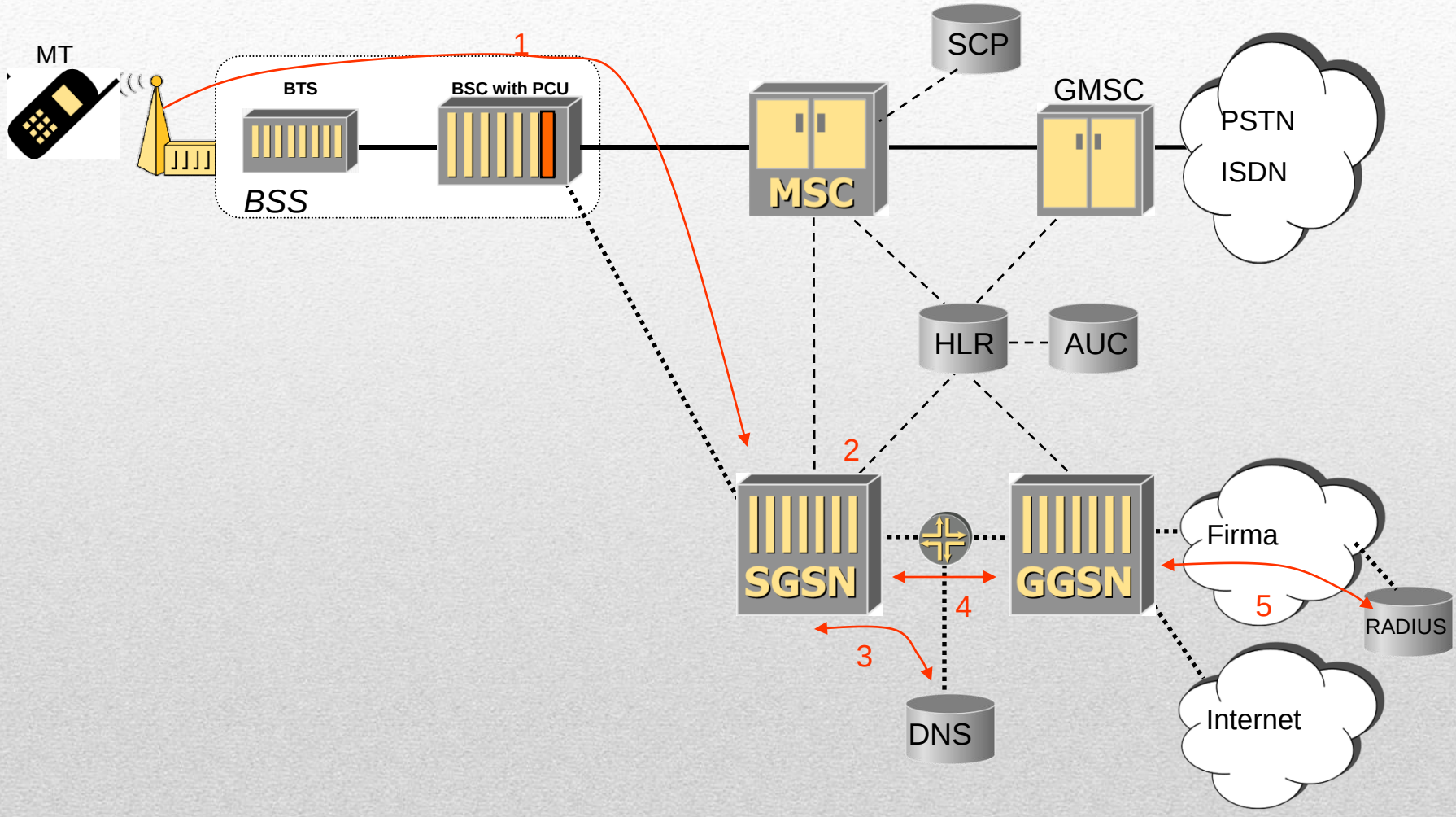
Ücretlendirme

GPRS Interface leri



PDP Context Aktivasyonu

“ 3G ile Internet’e Nasıl Bağlanırım ?”



“3G ile Internet’e Nasıl Bağlanırım ?”

- Kullanıcı hangi ağa bağlanacağını seçer.
  - Ya da otomatik seçilir. (internet)
- APN = ***Access Point Name*** = Bağlanılacak ağın adını belirtir.

  internet
  sirketiminagi
- PDP Context (Packet Data Protocol) mesajlaşmasıyla GGSN ile mobil arasında oturum kurulur. Bu oturum sonunda mobil cihaz bir IP adresine kavuşur.

Olası Saldırılar

- Worm, Virus, SMS/MMS Virusleri, Trojanlar
- Ücret Aşımı Saldırıları - Overbilling
- Abonelere kullanmadığı trafik için bedel yansıması
- Protokol anormalliklerine ilişkin saldırılar
- Şüpheli yada bozuk paketlerle abonenin oturumlarına müdahaleler
- Taklit edilmiş PDP içerik saldırıları
- Altyapıya yönelik saldırılar
- Kısıtlanmış sistemlere örneğin GGSN'e yapılan yetkisiz bağlantı denemeleri
- Sinyalleşme seviyesindeki saldırılar (VOIP – SIP)
- Servis kesintisi saldırıları (DOS)
- DNS cache poisoning

Mobil Tehditler ?

- Muhtemel saldırılara açık API ler
- Mobil OS'un servis bağlantıları, internet, wap, sms, mms, mail vb.
- Mobil Malware ler
  - Mobil ağlara ve Internet'e olan ağ bağlantısı
  - SMS
  - Bluetooth
  - Wireless
  - MMS
  - USB Cihazlar
  - Infrared

Tehditler

- Mobil Malware'lerin yayılması;
  - Malware'ler Internet üzerinden PC lere bulaşır.
  - Malware li PC'den akıllı telefonlara bulaşır.
    - Kızılötesi
    - Bluetooth
  - Malware li akıllı telefon ile wireless gibi methotlarla diğer akıllı telefonlara bulaşır.
- DDoS Saldırıları;
  - Botnet üyesi mobil cihazlar, merkezden emir bekler.
  - Gelen emirle ana şebekeye doğru saldırı gerçekleştirilir.
  - Sonuç olarak çağrılarda ve veri iletiminde problemler ortaya çıkar.

Hacker'lar Gözüyle

- Casusluk ?
- Telefonundaki bilgileri çalabilirler.
- Hesabındaki paraşarı transfer edebilirler.
- Virus/Trojan bırakabilirler.
- SMS/MMS kutularına erişebilirler.

Telefonlardaki Güvenlik Zaafiyetleri

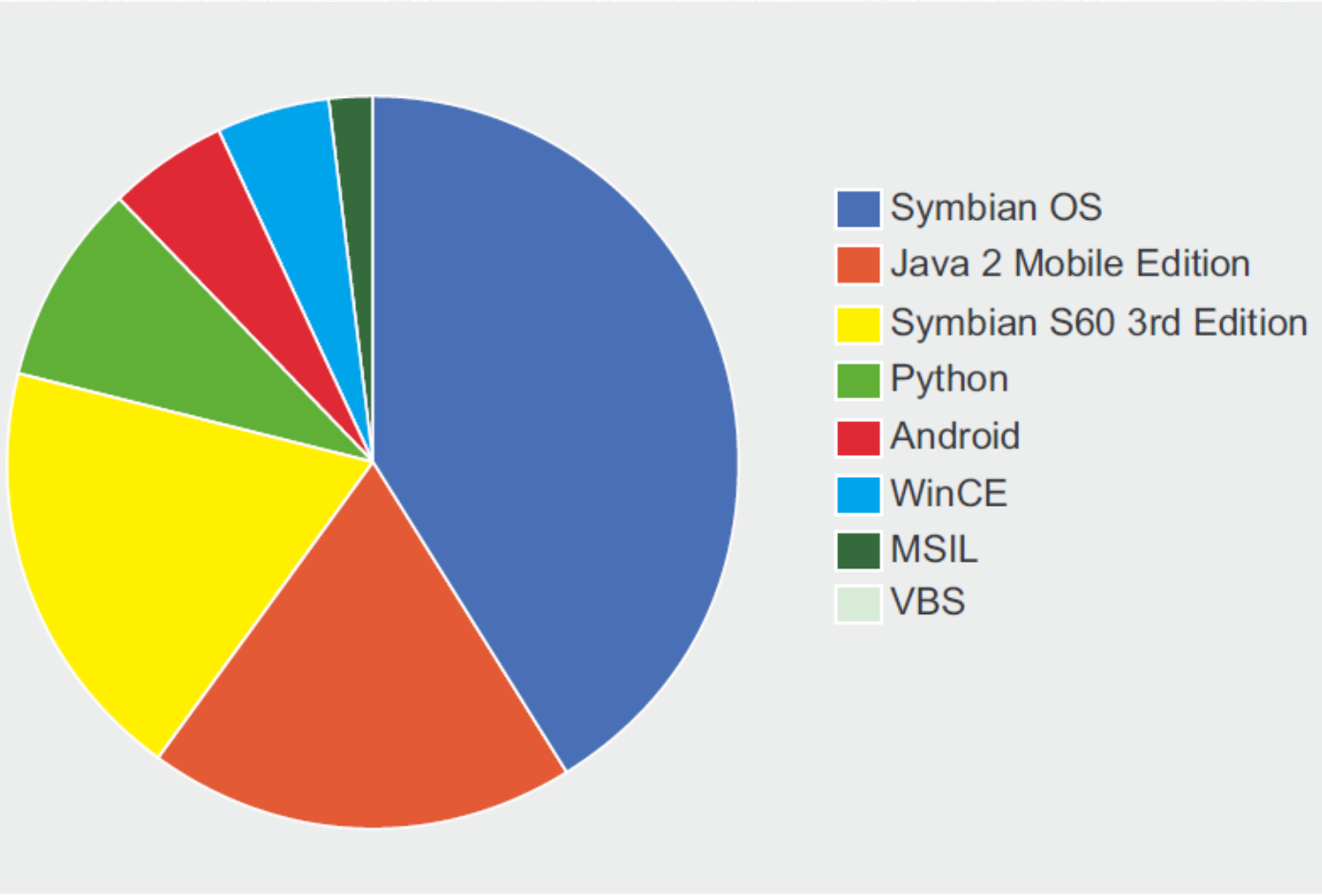
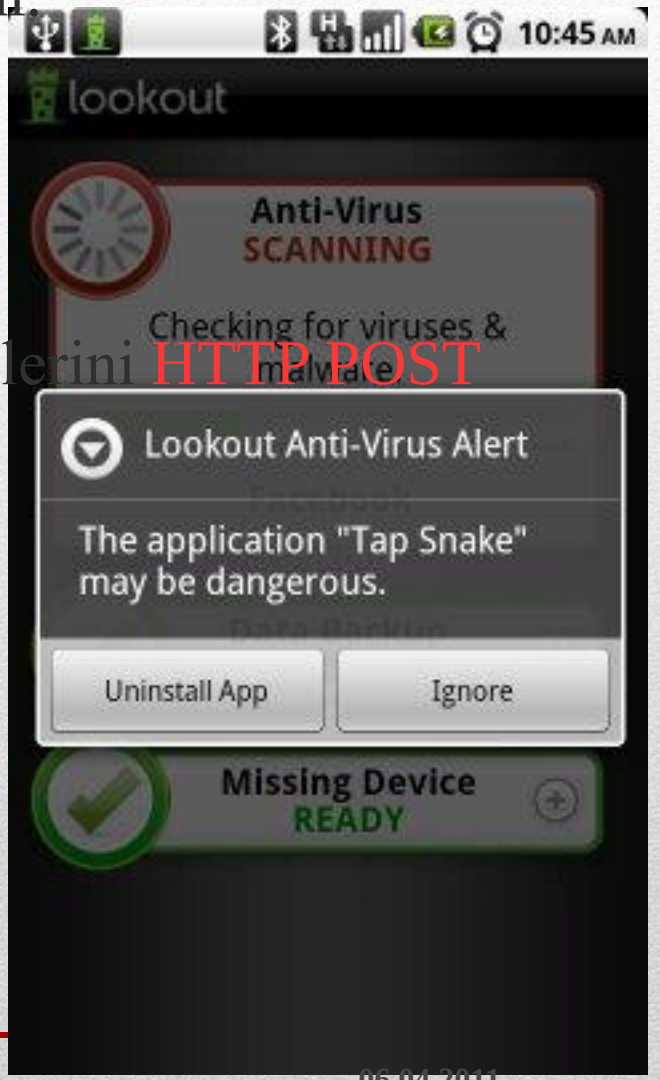


Figure 1. *Mobile Threats by Platform, 2009-2010*
Reference: McAfee Threats Report Q4 2010 (c)

Android'de Güvenlik İhlalleri: TapSnake

- TapSnake (Trojan), Android leri etkiledi.
- 24 Ağustos 2010
- Zararlı uygulama, spyware
- Yılan oyunu
- Kullanıcının konum bilgisini, GPS verilerini HTTP POST ile bir adrese gönderiyordu.
- End-user license agreement (EULA)



Android'de Güvenlik İhlalleri

- 1 Mart 2011
- Android marketteki Kingmall2010, we20090202, ve Myournet kullanıcıları
- Android Malware: DroidDream
- IMEI ve IMSI lerin Fremont, CA deki bir adrese gönderildiği tespit edildi.
  - http://184.105.245.17:8080/GMServer/GMServlet,
- 50'den fazla uygulamaya bulaşma
- Android Market Security Tool

https://market.android.com/support/bin/answer.py?answer=1207928

android market

Search Help

Android Market Help

Help articles

Developers

Users

Help forum

Nexus One Help Center

Android Market › Help articles › Users › Troubleshooting › March 2011 Security Issue

March 2011 Security Issue

Share Comment Print

On March 1 2011, the Android team removed a number of malicious apps published to Android Market.

⚠ If your device has been affected, you will receive an email from android-market-support@google.com. You will also receive a notification on your device that "Android Market Security Tool March 2011" has been installed. You may also receive notification(s) on your device that an application has been removed.

You are not required to take any action from there, the update will automatically undo the exploit. Within 24 hours of the exploit being undone, you will receive a second email.

Didn't receive the security update? Check these tips. **Please keep in mind that only impacted users will receive this update.**

The malware apps took advantage of known vulnerabilities which don't affect Android versions 2.2.2 or higher. For affected devices, we believe that the only information the attacker(s) were able to gather was device-specific (IMEI/IMSI, unique codes which are used to identify mobile devices, and the version of Android running on your device). But given the nature of the exploits, the attacker(s) could access other data, which is why we've taken a number of steps to protect those who downloaded a malicious app:

1. We removed the malicious applications from Android Market, suspended the associated developer accounts, and contacted law enforcement about the attack.
2. We are remotely removing the malicious applications from affected devices. This remote application removal feature is one of many security controls the Android team can use to help protect you from malicious applications.
3. We are pushing an Android Market security update to all affected devices that undoes the exploits to prevent the attacker(s) from accessing any more information from affected devices.
4. We are adding a number of measures to help prevent additional malicious applications using similar exploits from being distributed through Android Market and are working with our partners to provide the fix for the underlying security issues.

A user can determine if their device has been affected by visiting Settings > Applications > Running services and look for "DownloadManageService" in the list of running services.

We always encourage you to check the list of permissions when installing an application from Android Market. The Android team takes security very seriously and we're committed to building new safeguards to prevent these kinds of attacks from happening in the future.

Guitar : Solo Lite

Coding Caveman

★★★★★
(41,563 ratings)

INSTALL

OVERVIEW | USER REVIEWS (3038) | WHAT'S NEW | PERMISSIONS

MORE FROM DEVELOPER

Solo
CODING CAVEMAN / ENTERTA
★★★★½ (2,106)
UK£2.49 (about $4.01)

RELATED

RockOut - Guitar
ACTIVE FREQUENCY / MEDIA
★★★½☆ (2,443)
Free

Robotic Guitarist Free
PEDRO J. ESTÉBANEZ / MUSIC
★★★★½ (5,055)
Free

DESCRIPTION

Get Solo, Android's most popular pocket guitar played by Eric Clapton on TV!
Solo is Android's most popular virtual guitar. Use it to play to your favourite songs, or create some of your own...

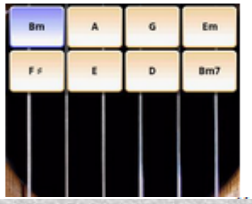
It's ideal for jamming sessions when you don't have your guitar with you, or an excellent reference for when you do!

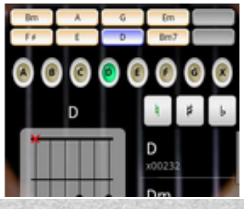
This is a free demo version and includes:
* Great, authentic sounding acoustic guitar
* The same huge chord library available in the full version

MORE

Visit Developer's Website ›

APP SCREENSHOTS





Tweet

ABOUT THIS APP

RATING:
★★★★½
(41,563)

UPDATED:
January 3, 2011

CURRENT VERSION:
1.32

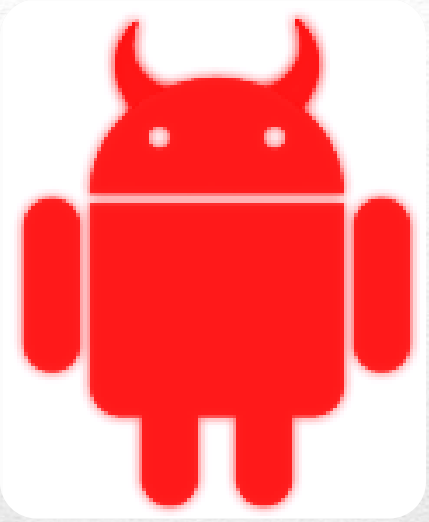
REQUIRES ANDROID:
1.5 and up

CATEGORY:
Entertainment

INSTALLS:
5,000,000 - 10,000,000

SIZE:
1.6M

PRICE:
Free

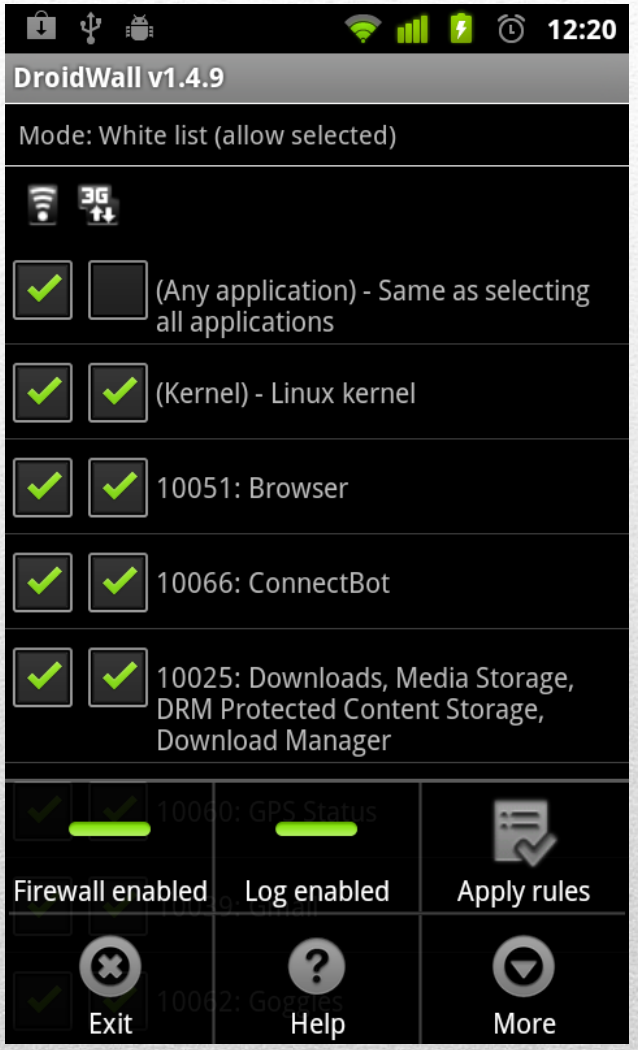


Adroid ve Güvenlik Uygulamaları

Afşin Taşkıran // afsin@taskiran.org

06.04.2011

droidwall

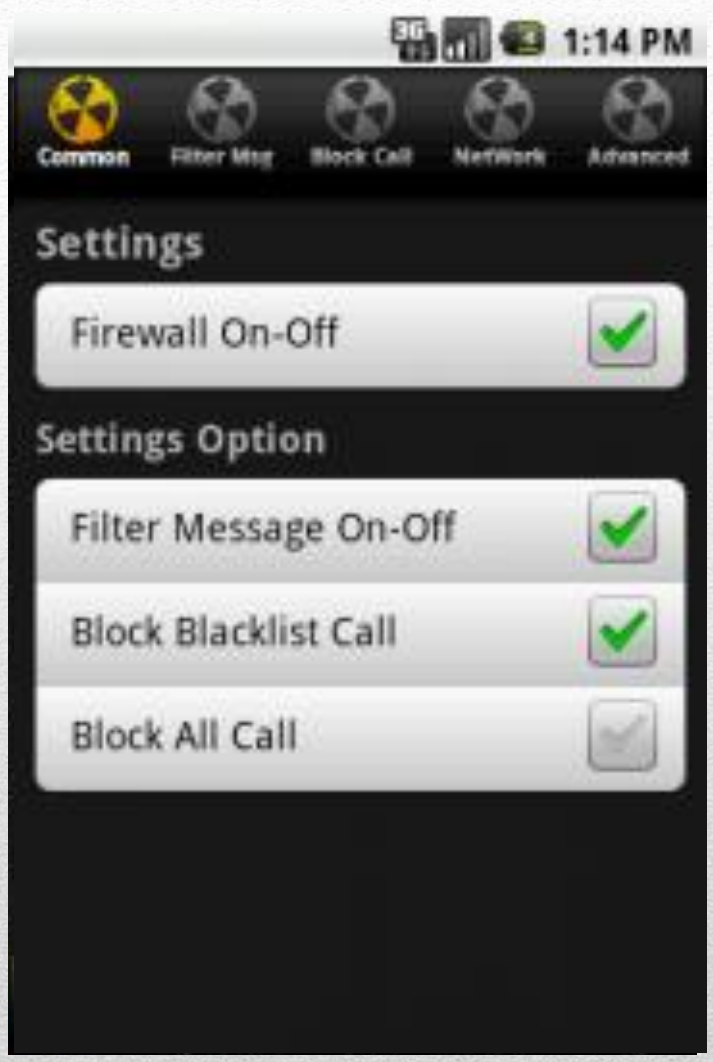


- iptables Linux Firewall kullanır.
- 2G/3G/Wi-Fi da çalışır.
- http://code.google.com/p/droidwall/

AndFire v1.2

- Andbox ailesindendir.
- Özellikleri:
  - message filter
  - block calls
  - app firewall
  - ftp pop3 smtp block
  - virus firewall.You can block some network application software to help you save flow!

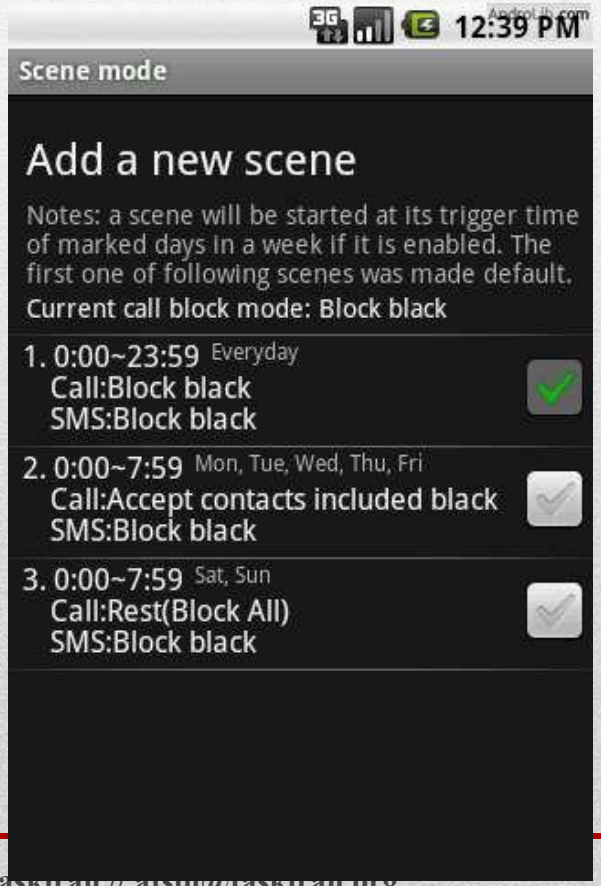
AndFire v1.2

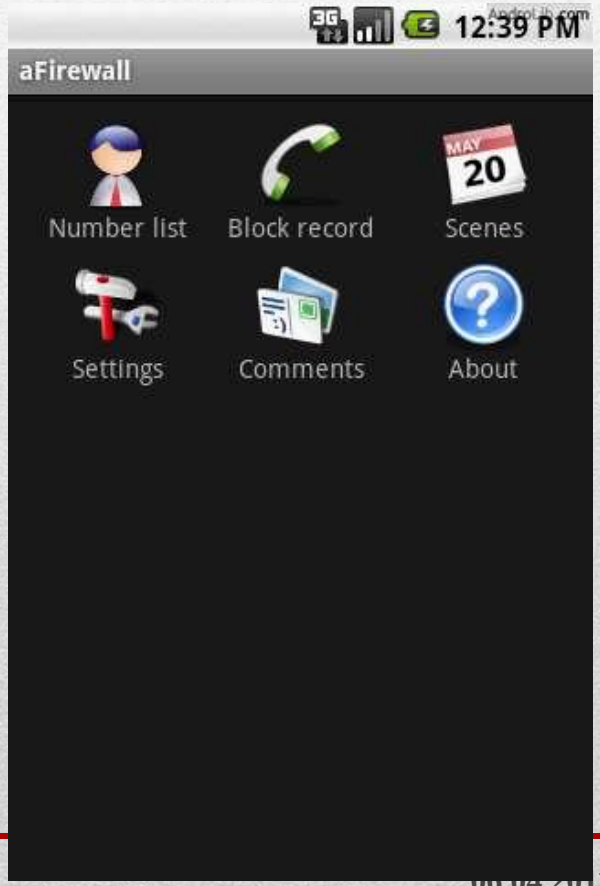

1:14 PM
Common
Filter Msg
Block Call
NetWork
Advanced
Settings
Firewall On-Off
Settings Option
Filter Message On-Off
Block Blacklist Call
Block All Call


1:13 PM
Common
Filter Msg
Block Call
NetWork
Advanced
Virus Firewall
Prevent virus attack
Virus Firewall On-Off

aFirewall

- http://www.androlib.com/android.application.com-lianyun-firewall-qmmA.aspx
- Çağrı bazlı kontrol yapabilirsiniz.



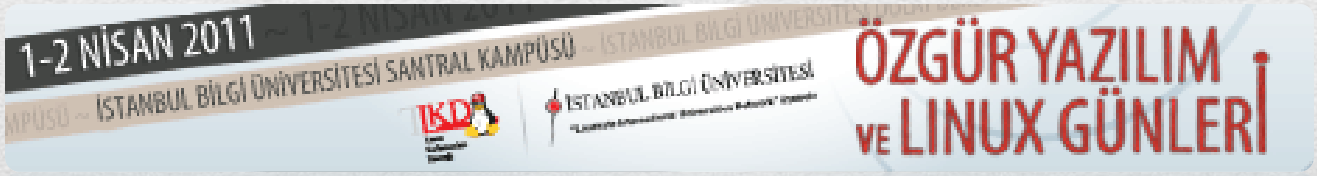


Güvenlik Önerileri

- Antivirus kullanın
- Düzenli olarak sisteminizi kötücül yazılımlara karşı (trojan/malware) taramadan geçirin.
- Firewall kullanın
- Bluetooth'u kullanmadığınızda kapalı tutun.
- Bilmediğiniz, özellikle .jar ve .sis uzantılı dosyalardan uzak durun.
- Kurduğunuz yazılımların güvenilirliğinden emin olun.
- Cihazınıza girişte şifre kullanın ve 2 ayda bir değiştirin.
- Internet browser geçmişini silin
- Sistem/network/kurulum cache lerini silin
- Okuduğunuz SMS/MMS/E-mail leri silin

Mobil İstemcilere Yönelik Güvenlik Tehditleri ve Özgür Uygulamalarla Savunma

TEŞEKKÜRLER



AFŞİN TAŞKIRAN

afsin@taskiran.org || afsin@enderunix.org

www.enderunix.org/afsin