Güvenli Uygulama Geliştirme Android

Bedirhan Urgun

- OWASP, www.owasp.org
- OWASP Turkey, www.webguvenligi.org
- Yazılım güvenliği farkındalığı
  - Projeler
  - Yarışmalar
  - İletişim
  - Etkinlikler
    - Uygulama Güvenliği Günü, 9 Haziran, Sultanahmet

Yazılım Öncelikleri

- İşlevsellik / Functionality
- Performans
- Güvenlik
- Kod Kalitesi
- Kullanılabilirlik / GUI

http://webguvenligi.org/mpoll

Primum non nocere

Önce, zarar verme

Convergence

The Next Big Thing

Startups

Social Networking

Business

Mobility

Web 2.0

Internet Enterpreneurs

Neden Güvenli Geliştirmeliyim?

- Şan/Şöhret kaybı
- Para kaybı
- Zorlayan standardlar
  - PCI, SOX, ISO-27001, HIPAA, v.b.
- Zorlayan kurumlar
  - BDDK, BTK, v.b.
  - Siyah şapka toplulukları

Güvenli Android Geliştirme

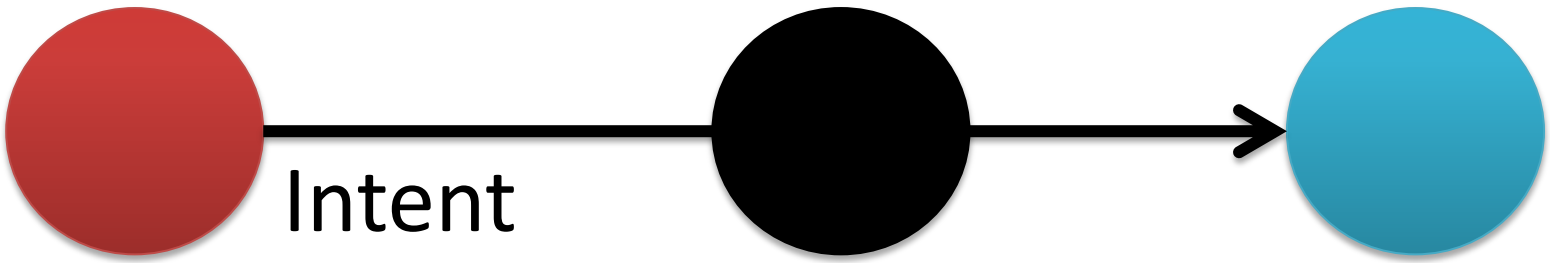
- Hassas Veriler ve Intent
- Hassas Veriler ve LogCat
- Girdi Denetimi
- Güvenli Depolama
- Bağlantı Güvenliği
- Bileşenler Arası Yetkilendirme

http://webguvenligi.org/belgeler

Hassas Veriler ve Intent

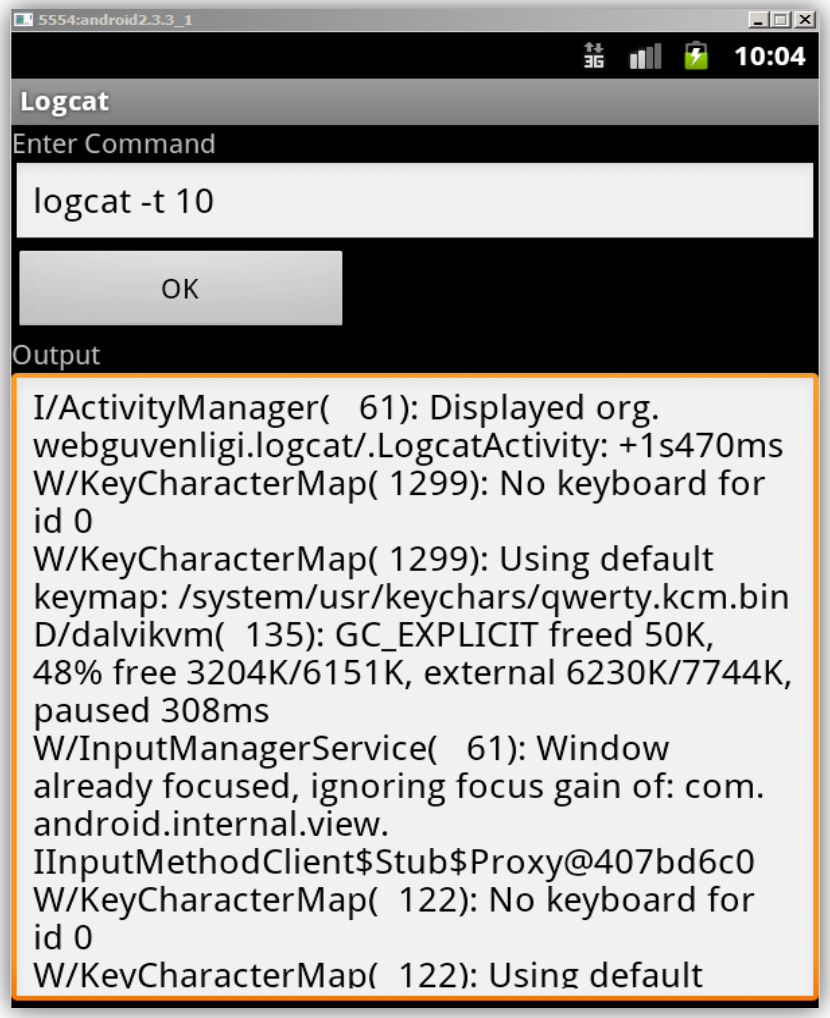
```
Intent registrationIntent = new
        Intent("com.google.android.c2dm.intent.REGISTER");

registrationIntent.putExtra("app",
        PendingIntent.getBroadcast(this, 0, new Intent(), 0));

registrationIntent.putExtra("sender","androidguvenligi@gmail.com");

startService(registrationIntent);
```

Hassas Veriler ve Intent




```
<intent-filter android:priority="999">
```

Hassas Veriler ve LogCat



Girdi Denetimi

```
Intent i = getIntent();
String url = i.getStringExtra("url");
// url whitelist kontrolünden geçirilmelidir.
```

Bağlantı Güvenliği

```
URL url = new URL("https://www.webguvenligi.org");

HttpsURLConnection con = (HttpsURLConnection)
                         url.openConnection();

readStream(con.getInputStream());
```

Güvenli Depolama

```
 try{
   FileOutputStream fos = openFileOutput("puanlar",
                                          MODE_PRIVATE);
   OutputStreamWriter out = new OutputStreamWriter(fos);
   out.append("oyuncu1#80\n");
   out.append("oyuncu2#34\n");
}
catch(FileNotFoundException fnfe){
...
```

Beni Hatırla

```
getSharedPreferences("MyPrefsFile",
                     MODE_PRIVATE)
        .edit()
        .putString("username", username)
        .putString("password", password)
        .commit();
```

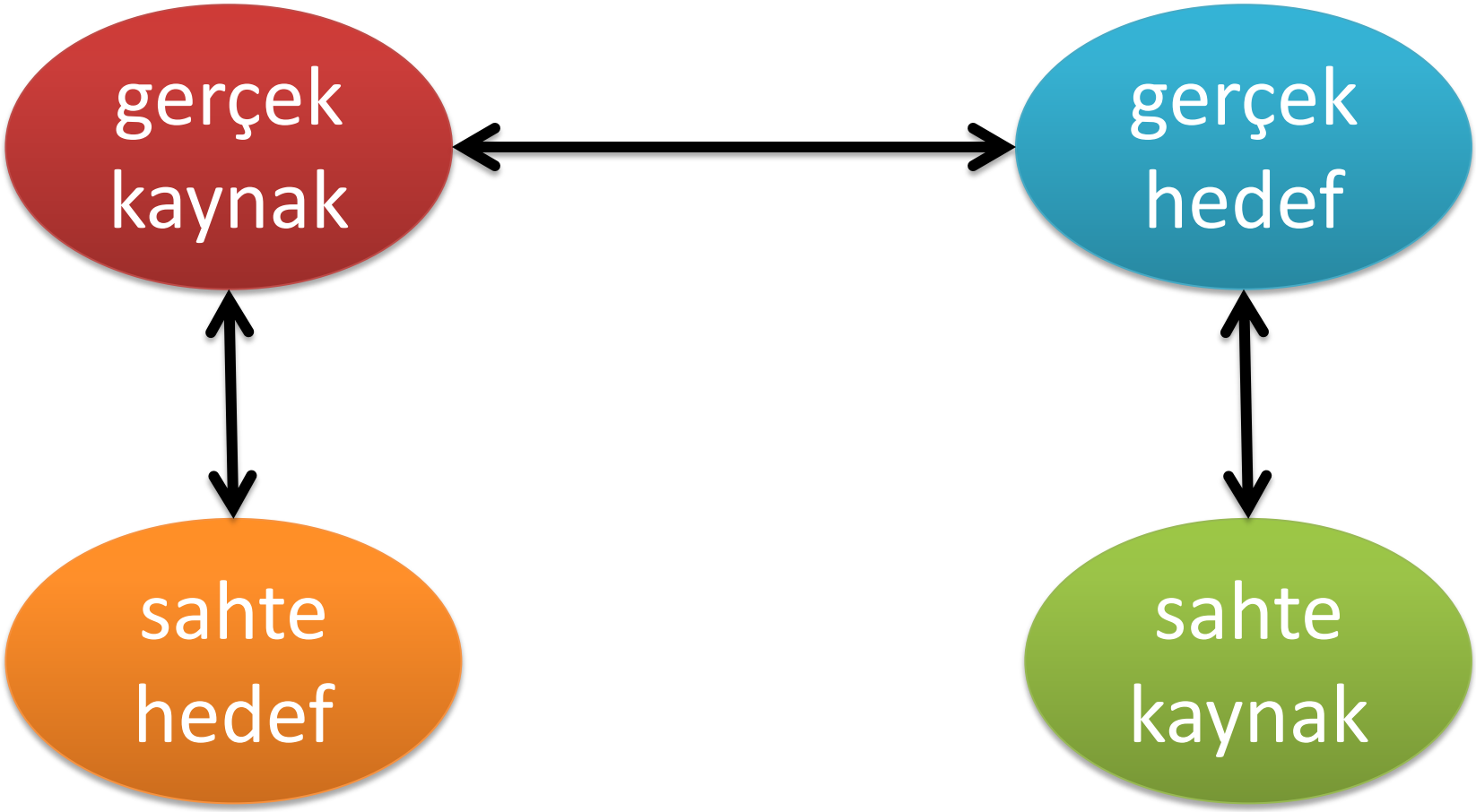
Beni Hatırla

```
String token = login(username, password);
getSharedPreferences("MyPrefsFile",
                                MODE_PRIVATE)
        .edit()
        .putString("token", token)
        .commit();
```

SignOut ile beraber

Android Yetki Yönetimi

Gerçek – Sahte Ayrımı



Yetkilendirme Yapıları

- permission tanımı

```
<permission
android:name="org.webguvenligi.permission" />
```

- permission isteği

```
<uses-permission
android:name="org.webguvenligi.permission" />
```

Yetkilendirme Yapıları - Devam

- permission zorunluluğu

```
<receiver
android:permission="org.webguvenligi.permission">

<activity
android:permission="org.webguvenligi.permission">

<service
android:permission="org.webguvenligi.permission">

<provider
android:permission="org.webguvenligi.permission">
```

Yetkilendirme Yapıları - Devam

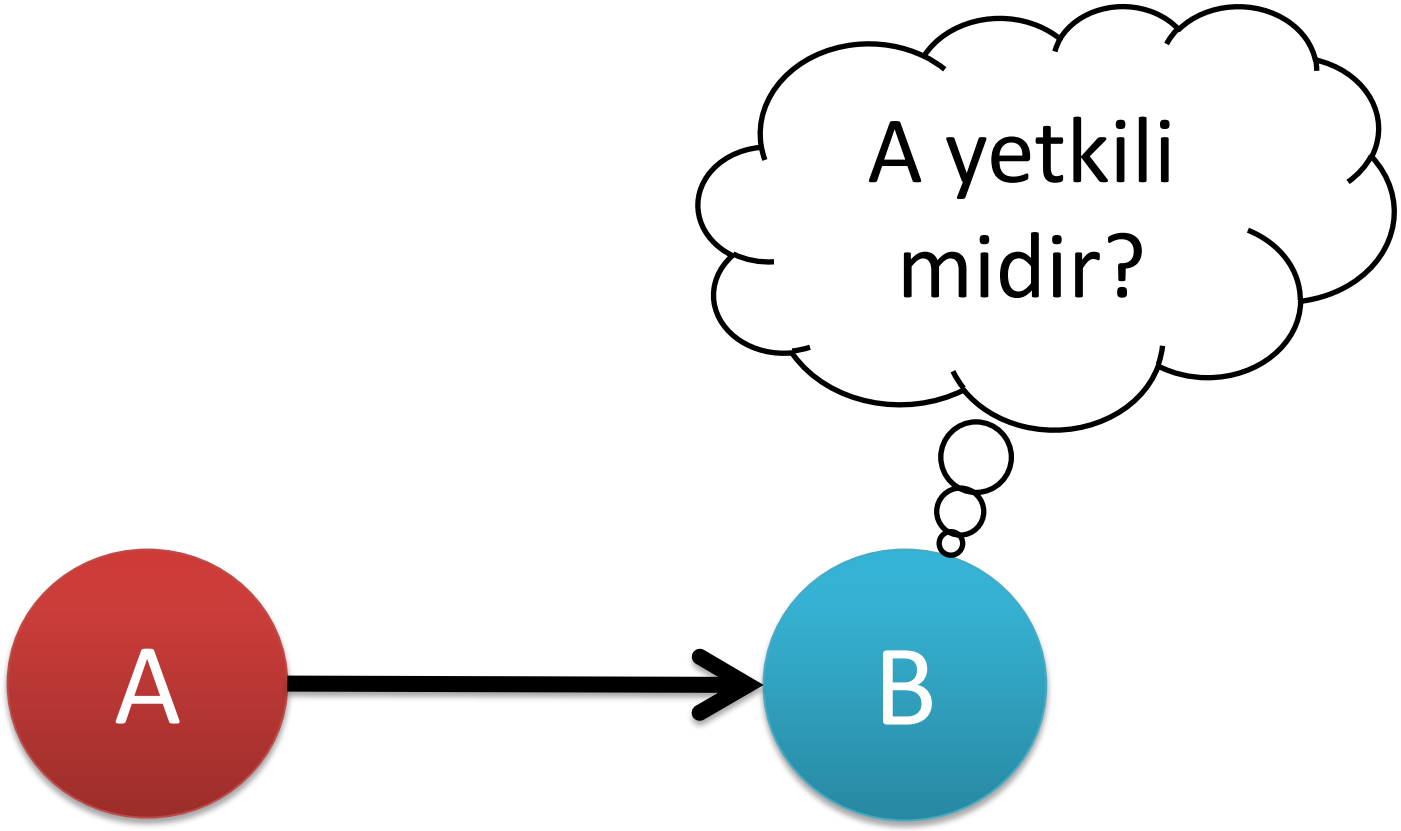
- permission zorunluluğu

```
sendBroadcast(intent, "org.webguvenligi.permission")
```

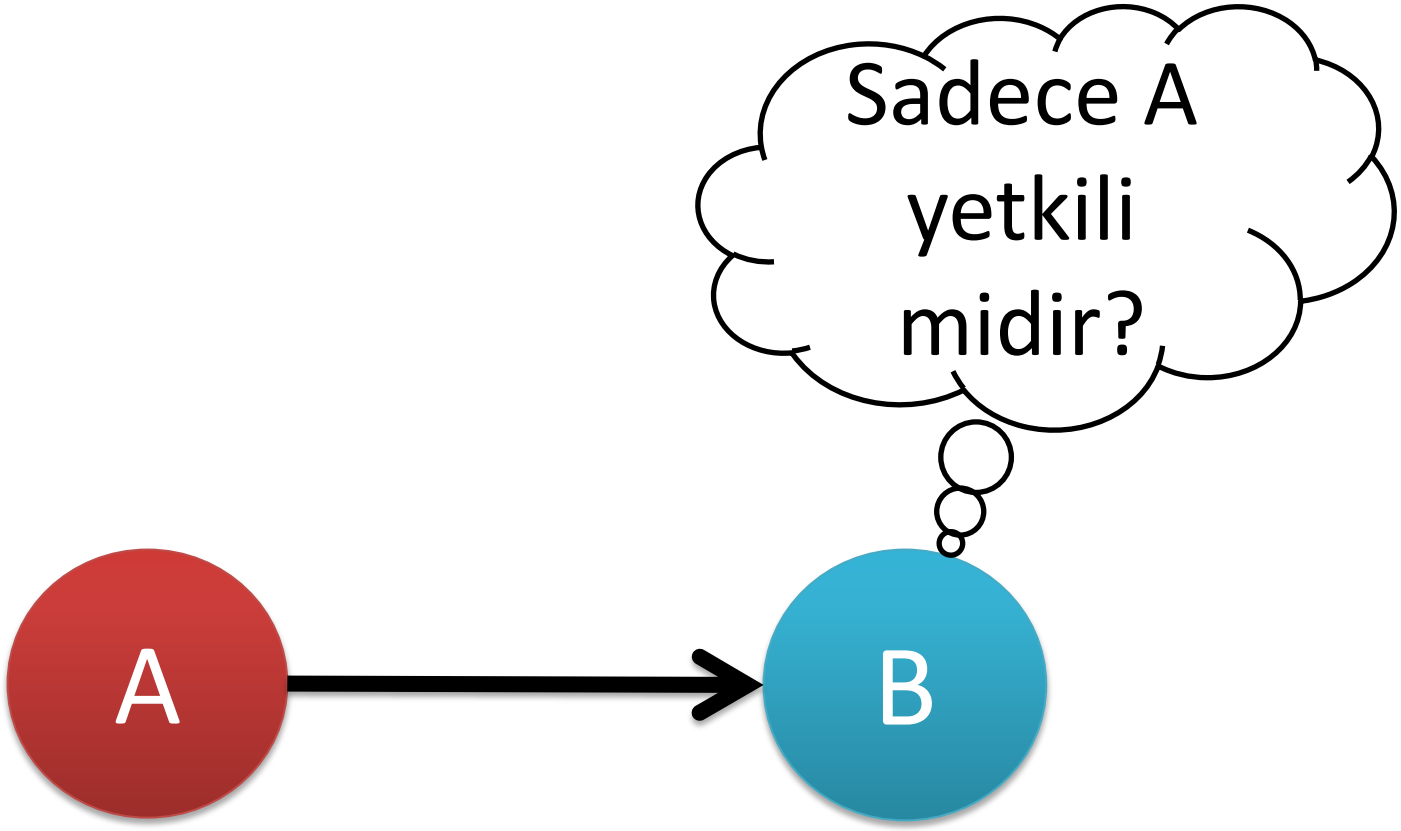
```
checkCallingPermission("org.webguvenligi.permission")
```

```
PackageManager pm = context.getPackageManager();
pm.checkPermission("org.webguvenligi.permission",
                                        pkgName);
```

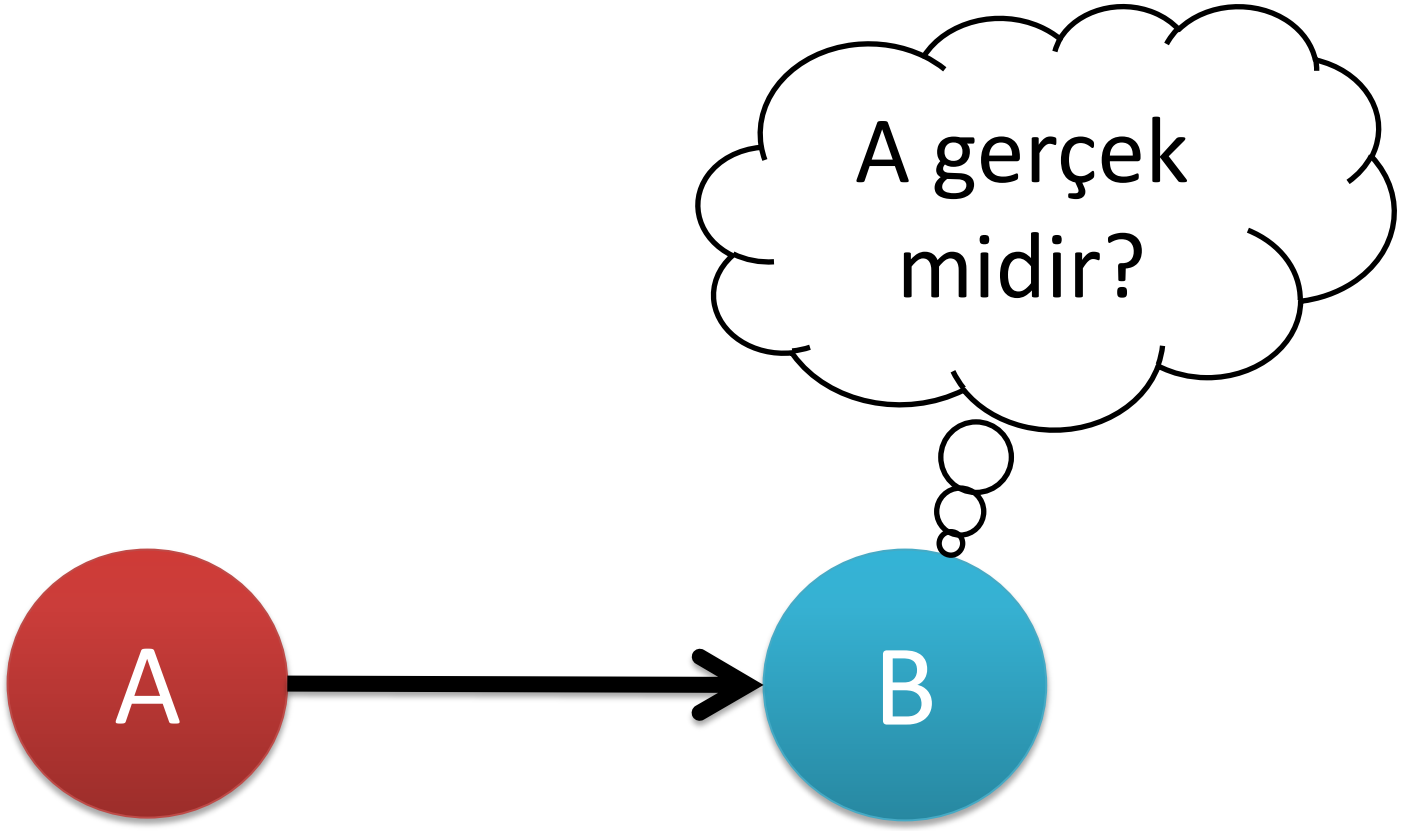
Yetkilendirme – Senaryo 1



Yetkilendirme – Senaryo 2



Yetkilendirme – Senaryo 3

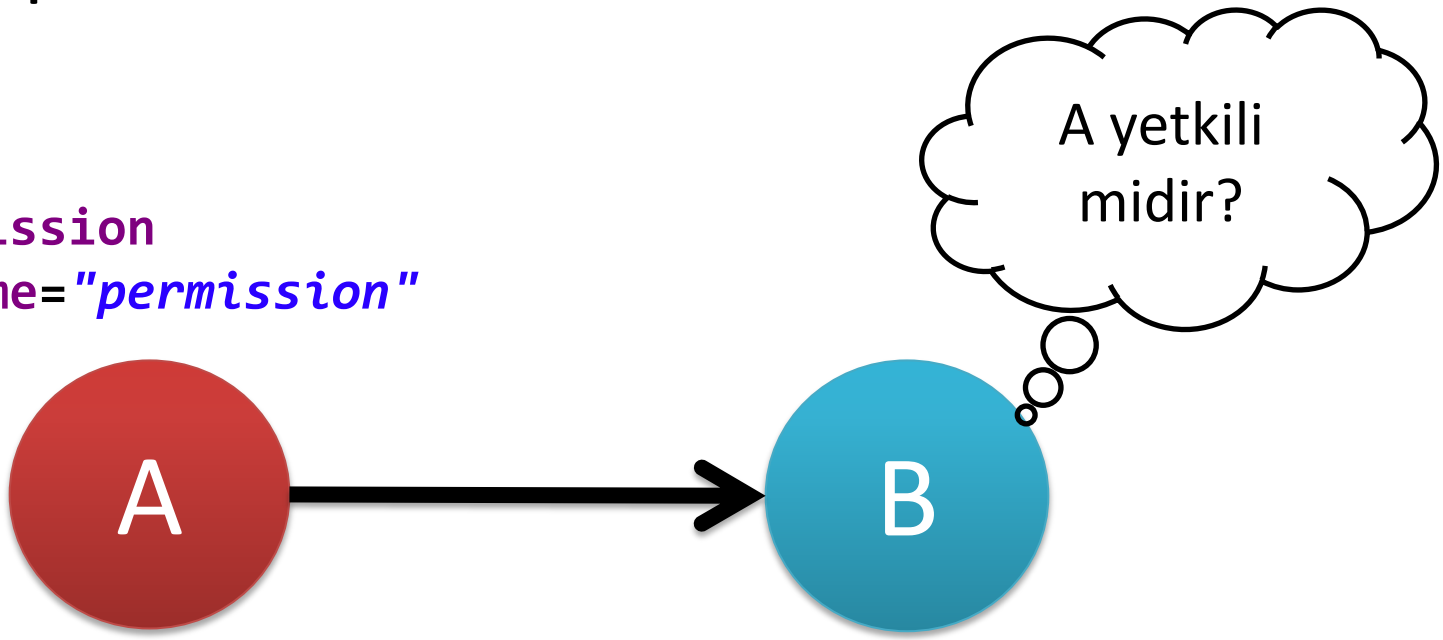


Yetkilendirme - İpucu 1

- normal permission kontrolü

3

```
<uses-permission
android:name="permission"
```



1
```
<permission
android:name="permission" />
```

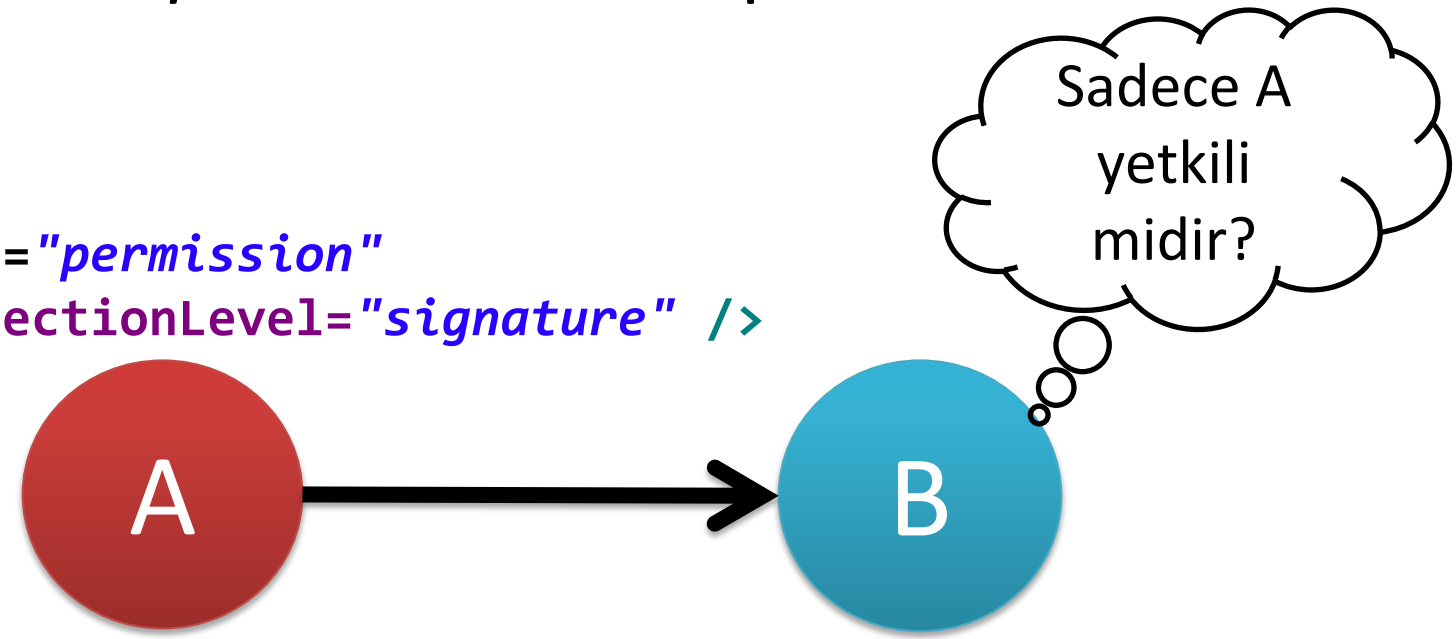
2
```
<receiver
android:permission="permission"
```

Yetkilendirme - İpucu 2

- permission *protectionLevel* ipucu

1

```
<permission
android:name="permission"
android:protectionLevel="signature" />
```

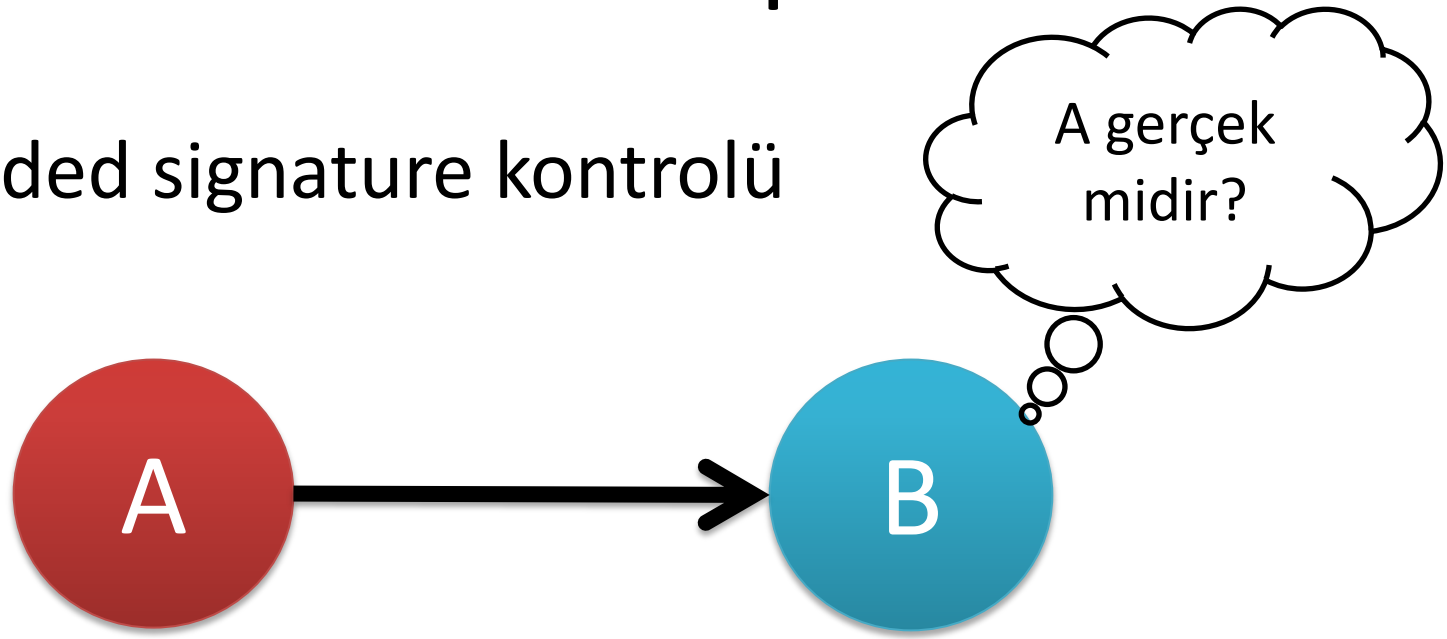


2

```
<receiver
android:permission="permission"
```

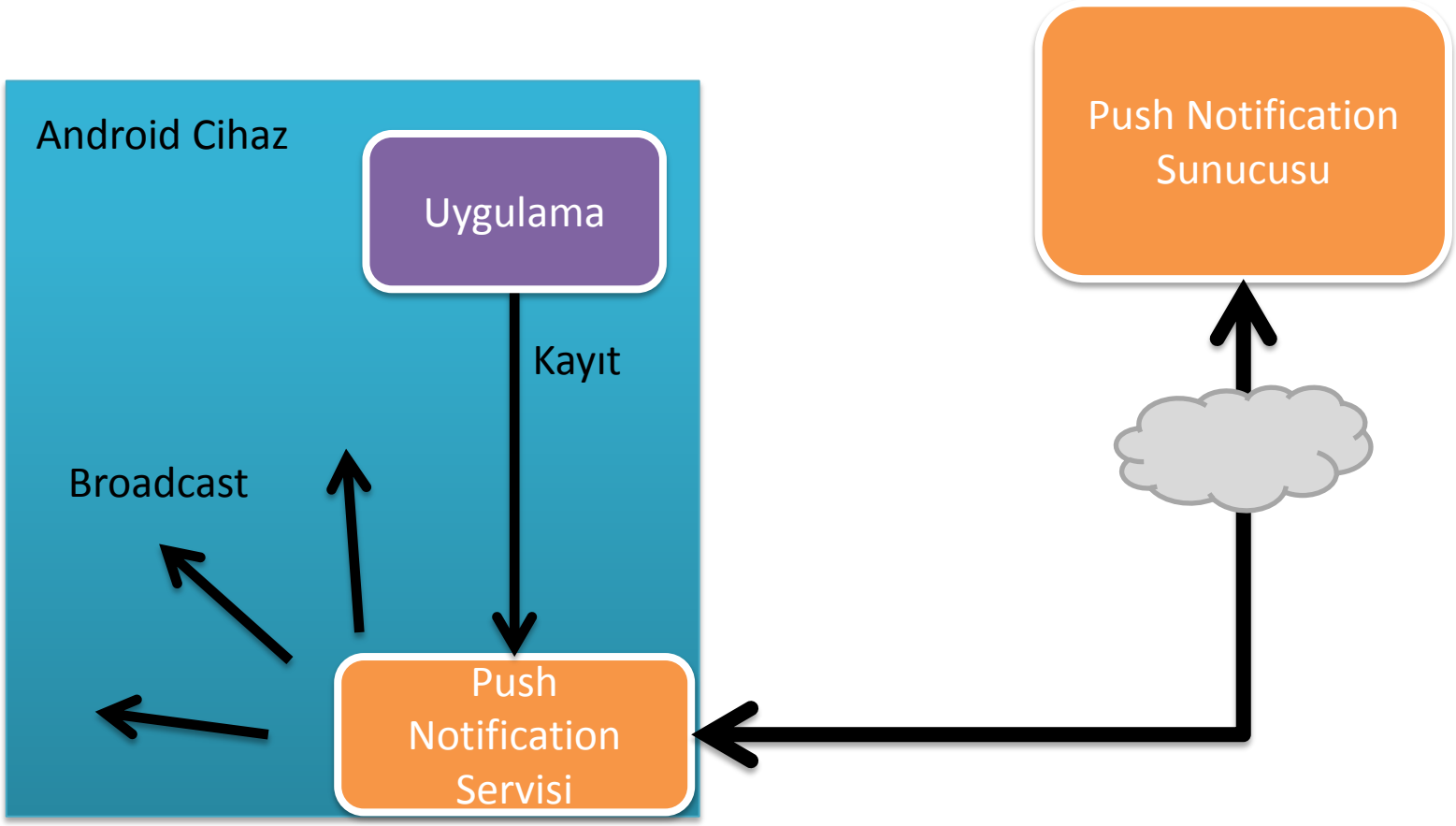
Yetkilendirme - İpucu 3

- hardcoded signature kontrolü




```
packageInfo = pm.getPackageInfo(A_PkgName,
                PackageManager.GET_SIGNATURES);

String A_SIGNATURE = "308202...";

for (Signature signature : packageInfo.signatures)
   if (signature.toCharsString().equals(A_SIGNATURE)) {
   }
```

Tehdit Modelleme - Push Notification



Doğrulama Eğilimi

n, 2n, 2n+2

Üçlü	Doğru/Yanlış	Emin Olma Yüzdesi %
7, 14, 16	**Doğru**	**% 60**
5, 10, 12	**Doğru**	**% 80**
8, 16, 18	**Doğru**	**% 100**

Doğru Formül: **a < b < c**

Yanlışlama Eğilimi

n, 2n, 2n+2

Üçlü	Doğru/Yanlış	Emin Olma Yüzdesi %
7, 14, 16	Doğru	% 60
6, 12, 13	Doğru	% 0

Teşekkürler

owasp turkey mailing list