Mobilappok támadó szemmel

Vida Zsolt, hwsw konferencia, 2017. november 29.

vida.zsolt@gmail.com

A pentestről

- Mi a pentest? Hogy zajlik?
- Etikus vs. blackhat
- Mit fog kérni a tesztelő mobilappok esetén?
  - Bináris (nem obfuszkált)
  - Tesztfelhasználók
  - API végponthoz hozzáférés
  - API leírás

Kitérő: emulátor vagy eszköz?

Emulátor	
pro	**kontra**
"egyszerű"	mégsem real life
sokféle eszköz emulálható	

Eszköz	
pro	**kontra**
real life	brickelés veszély
	tipikusan kevés eszköz kéznél

Android Studio
Xcode

"alpine"

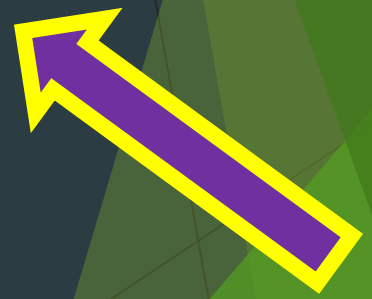
Mi ellen védekezünk?

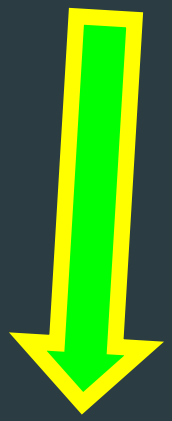
- Rosszindulatú felhasználó
  - API támadások
- Man in the middle
- Lopás
  - Személyes/céges adatok
  - Hozzáférések
- Ezen meg lehet sértődni, de attól még támadni fogják ☺

AZ ESZKÖZ NEM MEGBÍZHATÓ

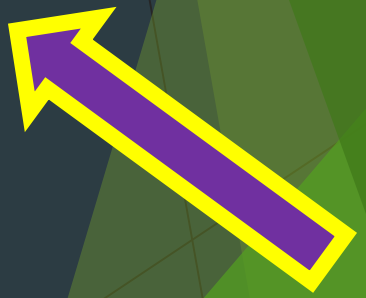
AZ ESZKÖZ NEM MEGBÍZHATÓ

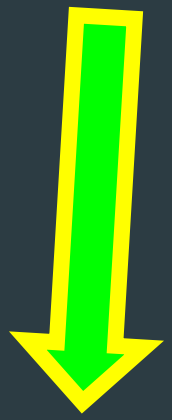
AZ ESZKÖZ NEM MEGBÍZHATÓ



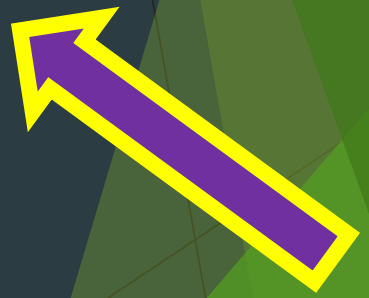


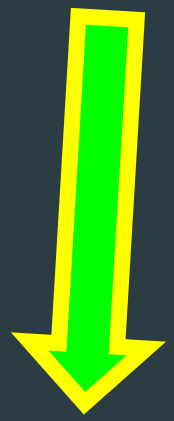
AZ ESZKÖZ NEM MEGBÍZHATÓ



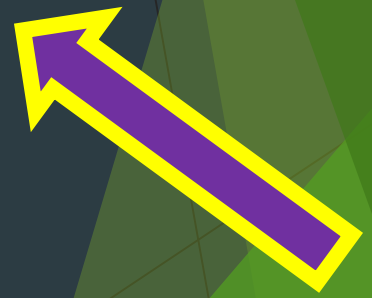


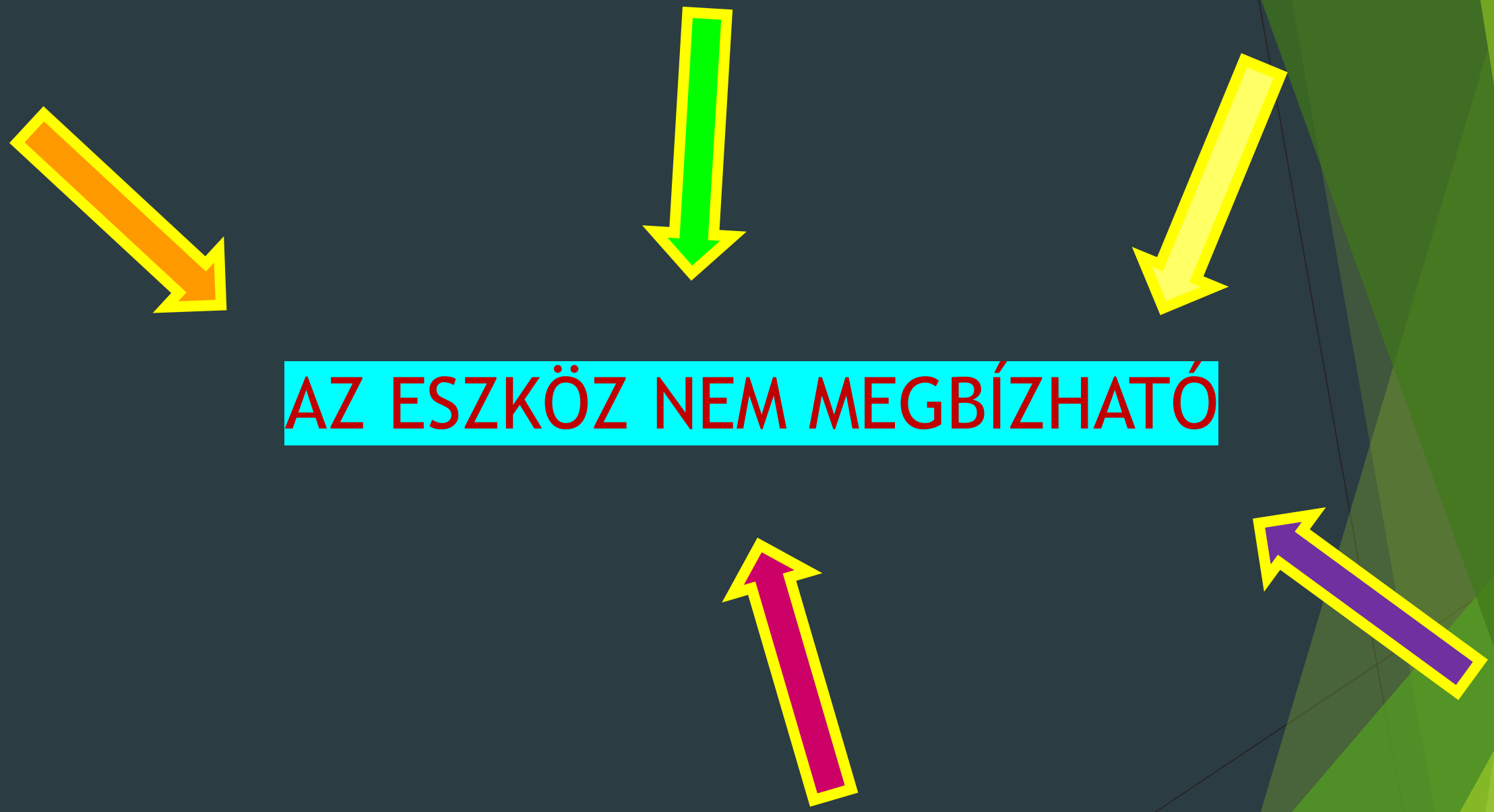
AZ ESZKÖZ NEM MEGBÍZHATÓ

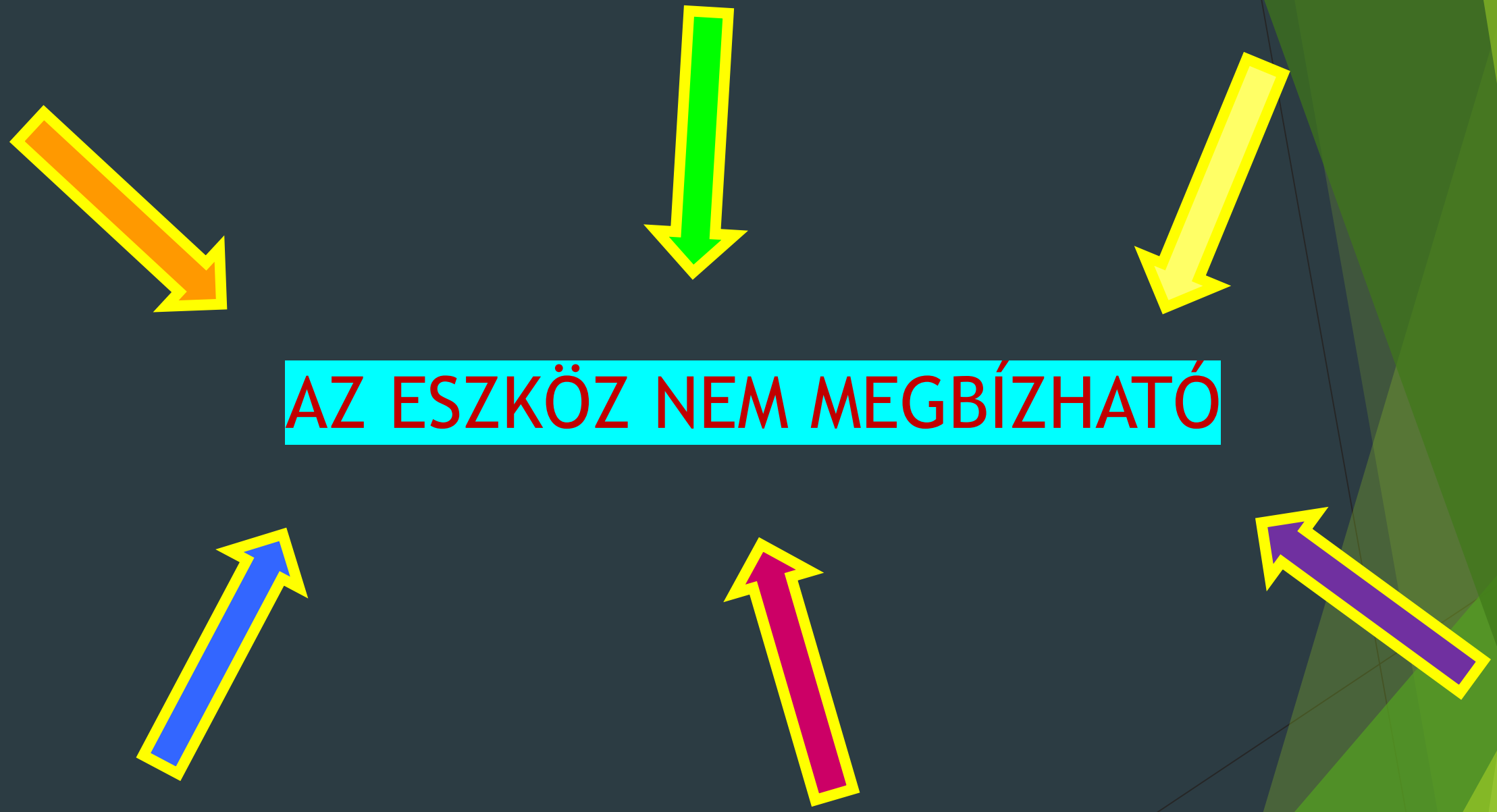


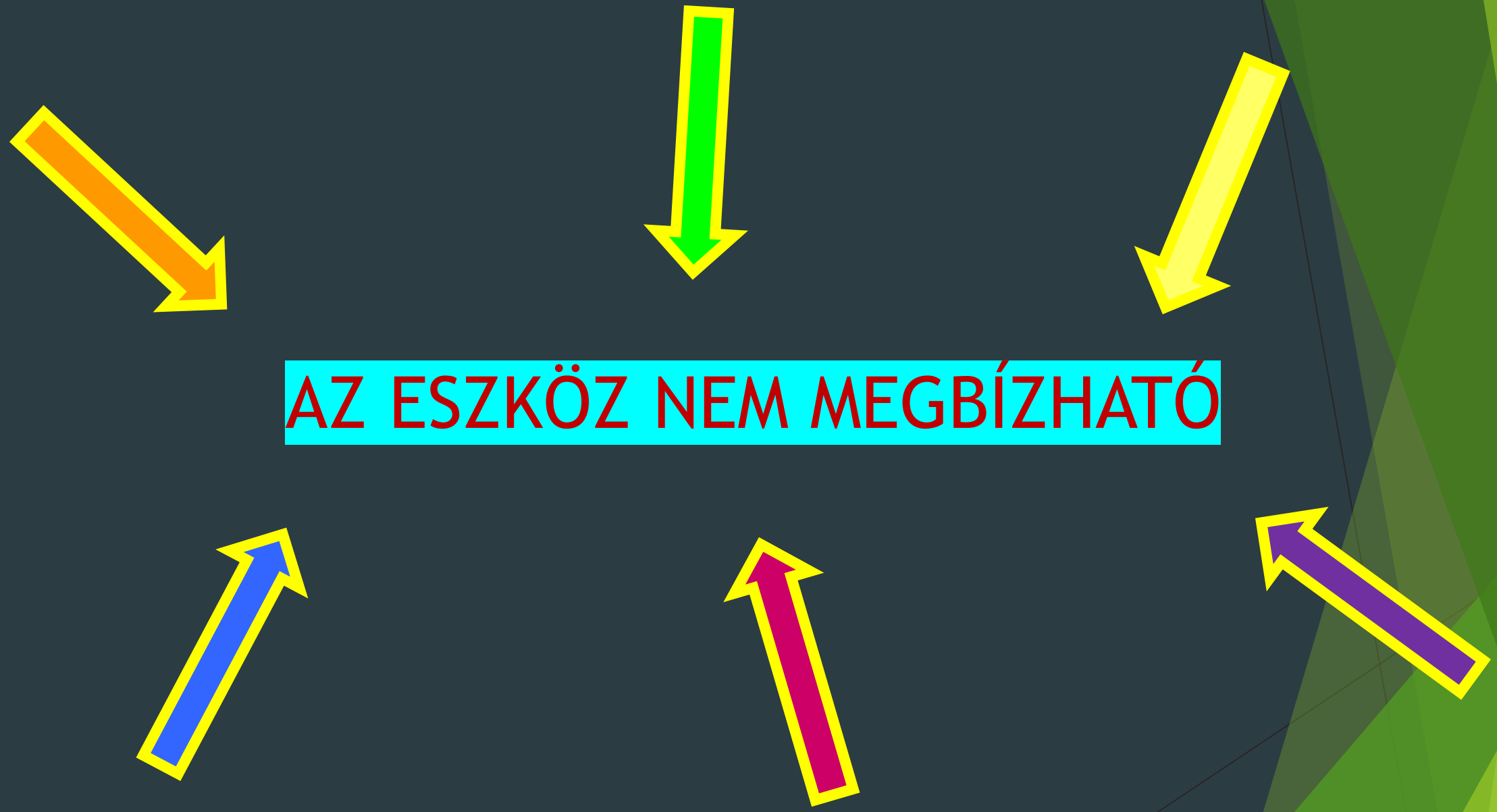



AZ ESZKÖZ NEM MEGBÍZHATÓ


AZ ESZKÖZ NEM MEGBÍZHATÓ


AZ ESZKÖZ NEM MEGBÍZHATÓ


AZ ESZKÖZ NEM MEGBÍZHATÓ

Mit vizsgálunk egy mobil pentest során?

- Telefon-szerver kommunikáció
- Mit művel az alkalmazás a telefonon
- Alkalmazáslogika
- Bináris elemzése

Telefon-szerver kommunikáció

- Beproxyzás
- A forgalom általában http(s)
- A szerveroldali sérülékenységek hasonlók a webalkalmazásokhoz
- Man in the middle támadások
  - Ha nem vagy biztos abban, hogy a kapcsolat biztonságos, inkább dobd el

Az app lokális viselkedése

- Milyen adatokat és hogyan tárol?
  - Lokális tárolók (keychain, plist)
  - Cache fájlok
  - Temp fájlok
  - Logok

Alkalmazáslogika

- Automatikus szoftverekkel legtöbbször nem felderíthetők
- Néhány példa:
  - Session id generálás
  - Userek egymást szerkeszthetik
  - Süti érték/disabled paraméter átírása
  - A kliensoldal csak elfed funkciókat
  - Fix jelszóváltoztatás url

A bináris elemzése

- APK, IPA: lényegében zip fájlok
  - Akár a forráskód is visszafejthető
- Beégetett jelszavak, connection stringek
- Tesztuserek, tesztszerverek kommentezve
- Nem dokumentált API hívások

Összefoglalás

AZ ESZKÖZ NEM MEGBÍZHATÓ

Köszönöm a figyelmet!