



Nyílt kártyákkal játszottunk,
avagy mennyire biztonságos egy
RFID-kártyavár

Bemutakozás

Veres-Szentkirályi András

Silent Signal

IT biztonsági szakértő

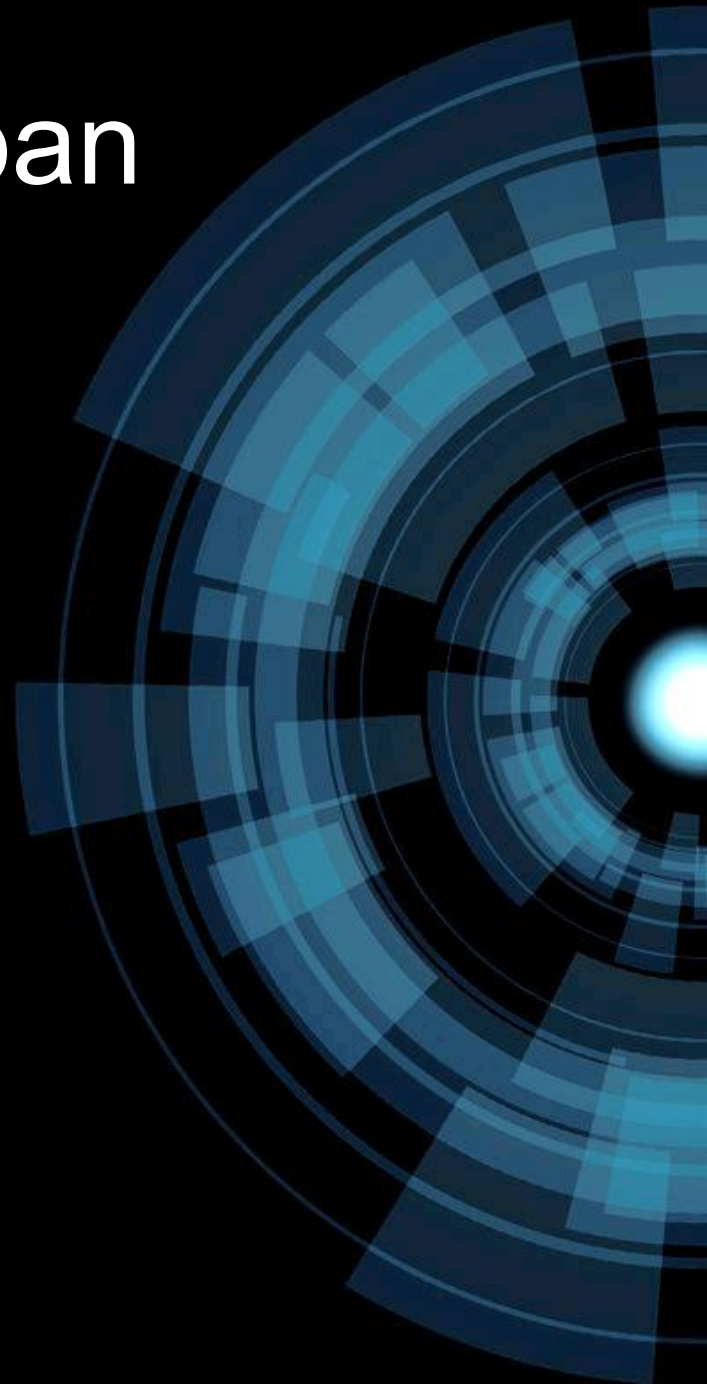
OSCP GWAPT

vsza@silentsignal.hu



Dráma egy felvonásban

- Bevezetés
 - Proxmark3, a „csodafegyver”
- Bonyodalom
 - Mifare Classic, az „áldozat”
- Cselekmény
 - Terepszemle és analízis
- Tetőpont
 - Támadás a rendszer ellen
- Megoldás
 - Hogyan védekezzünk?



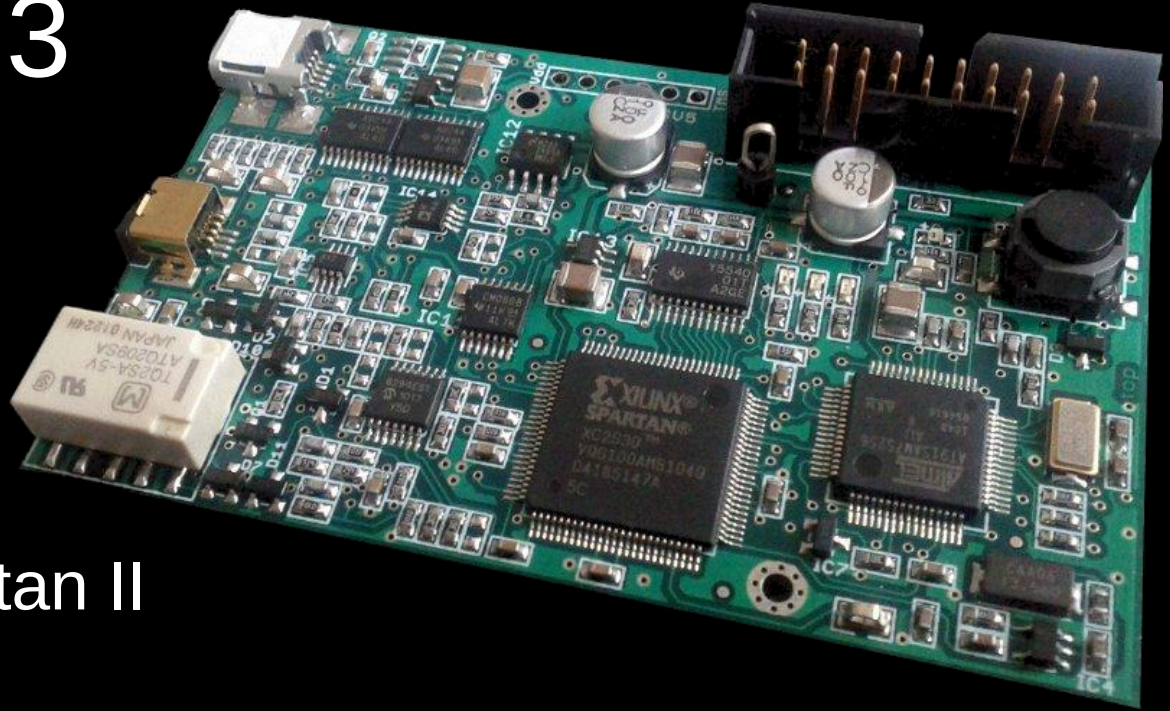
„Kötelező RFID slide”



Copyright 2005 UNDP-APDIP <http://www.iosn.net/events/wsis-2005>

Proxmark 3

- μC
 - ARM
- FPGA
 - Xilinx Spartan II
- ADC
- HF/LF antenna
- Jonathan Westhues, 2007, GPL



The background features a series of concentric circles and a grid pattern, primarily in shades of blue and red, set against a dark background. The circles are centered on the right side of the image, creating a sense of depth and movement. The grid pattern is composed of overlapping squares, some of which are highlighted in red, while others are in blue or dark grey. The overall effect is a complex, layered geometric design.

DEMO

Mifare Classic





DEMO

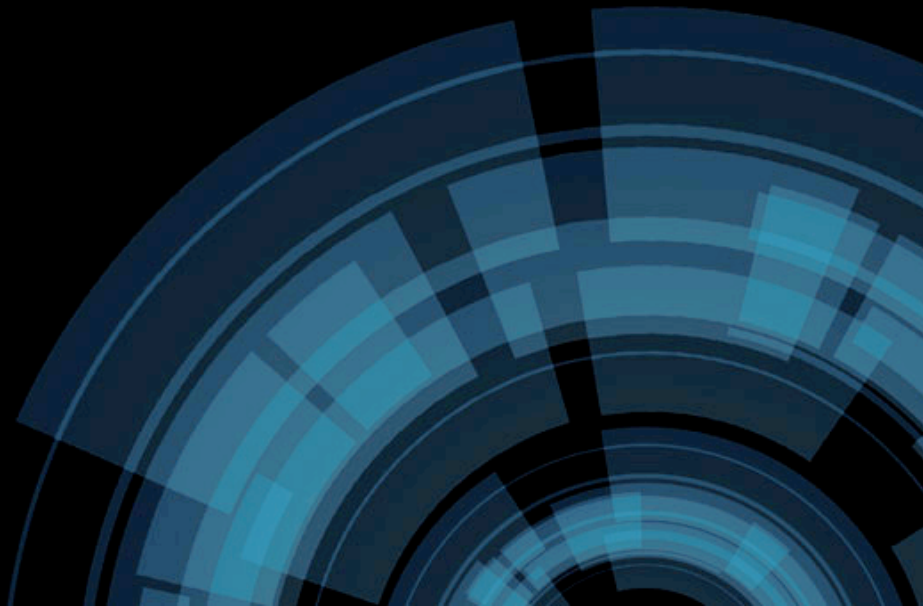
Nested támadás

- Szükséges egy ismert kulcsú blokk: ID
- Autentikálunk: N_t
- Még egyszer: N_t'
- Különbségből következtethetünk a nonce-ra
- ~10 perc PM3-mal



Android támogatás

```
Tag tagFromIntent =  
    intent.getParcelableExtra(NfcAdapter.EXTRA_TAG);  
MifareClassic mfc = MifareClassic.get(tagFromIntent);  
mfc.connect();  
if (mfc  
    .authenticateSectorWithKeyA(1,  
    new byte[] {XX, XX, XX,  
        9, 33, -35})) {  
    int bIndex =  
        mfc.sectorToBlock(1);  
    byte[] data =  
        mfc.readBlock(bIndex);  
}
```

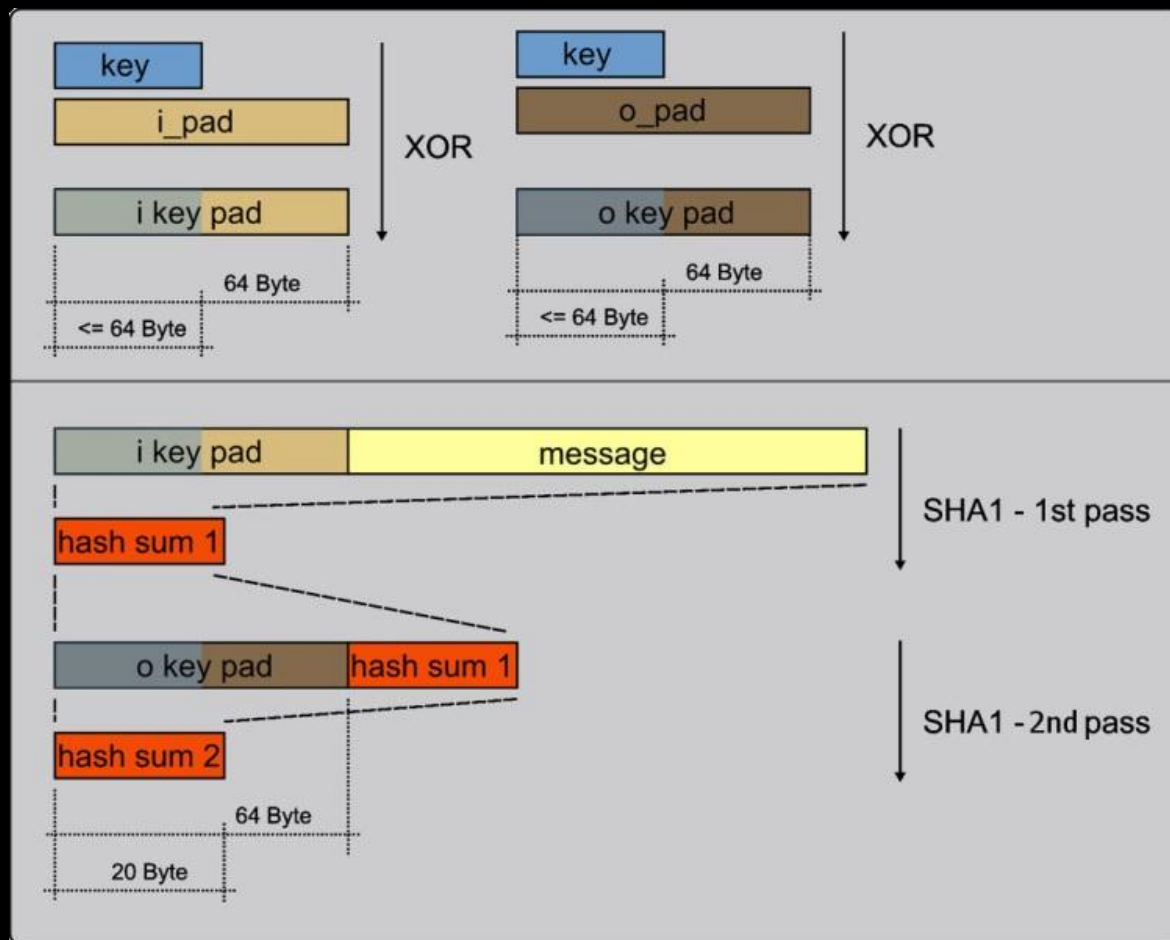
A decorative graphic in the bottom right corner consisting of several concentric, semi-circular arcs in various shades of blue, creating a stylized, modern look.



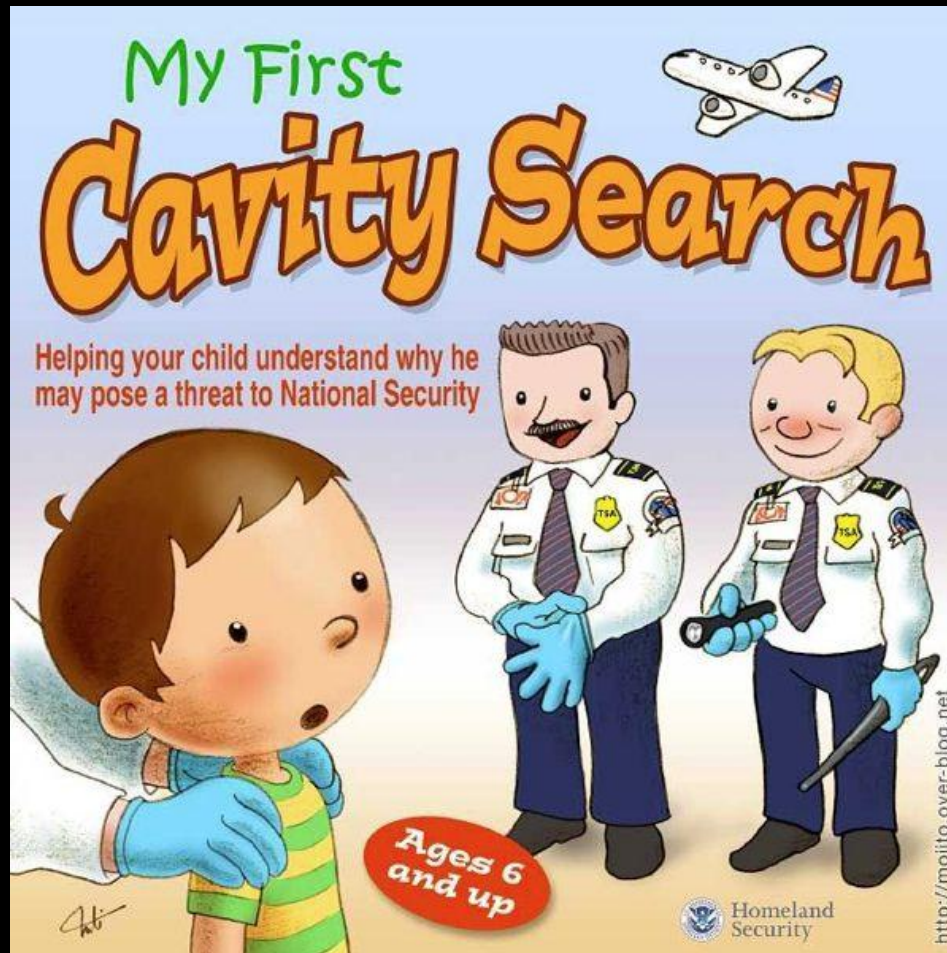
THAT AWKWARD MOMENT
WHEN YOU REALIZE

THAT THIS MASK
IS COPYRIGHTED
BY TIME WARNER INC.
(HUGE ACTA SUPPORTER).

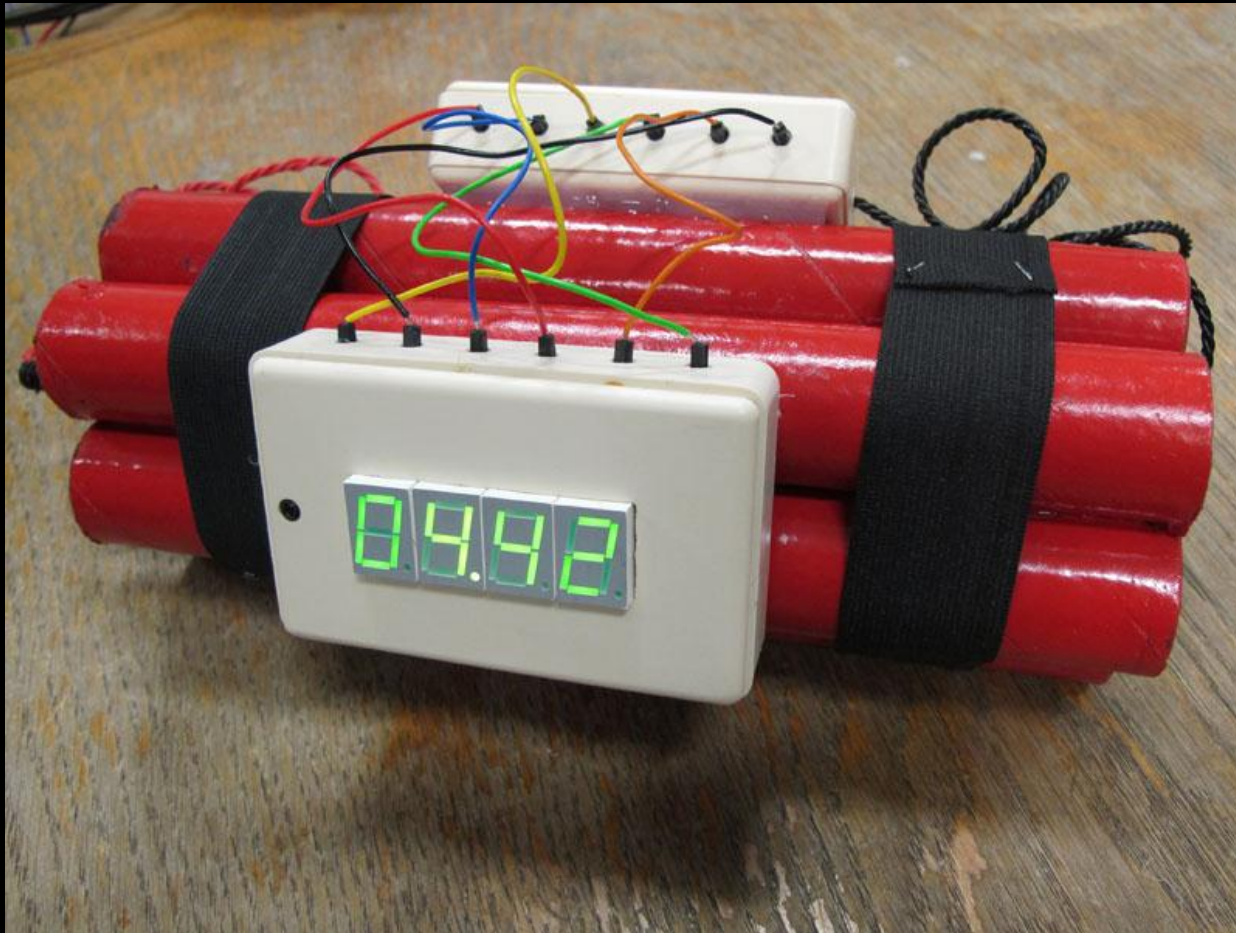
Kockázatcsökkentés: HMAC



Védekezés: on-line ellenőrzés

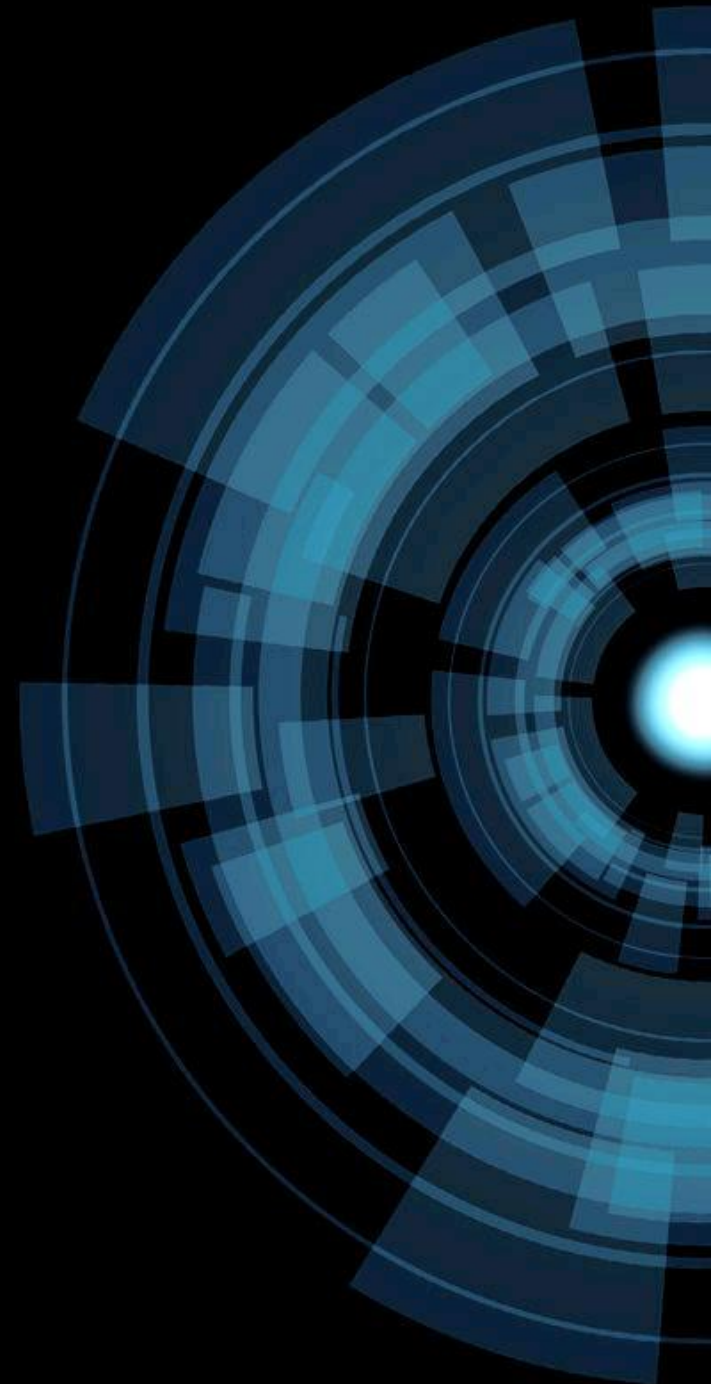


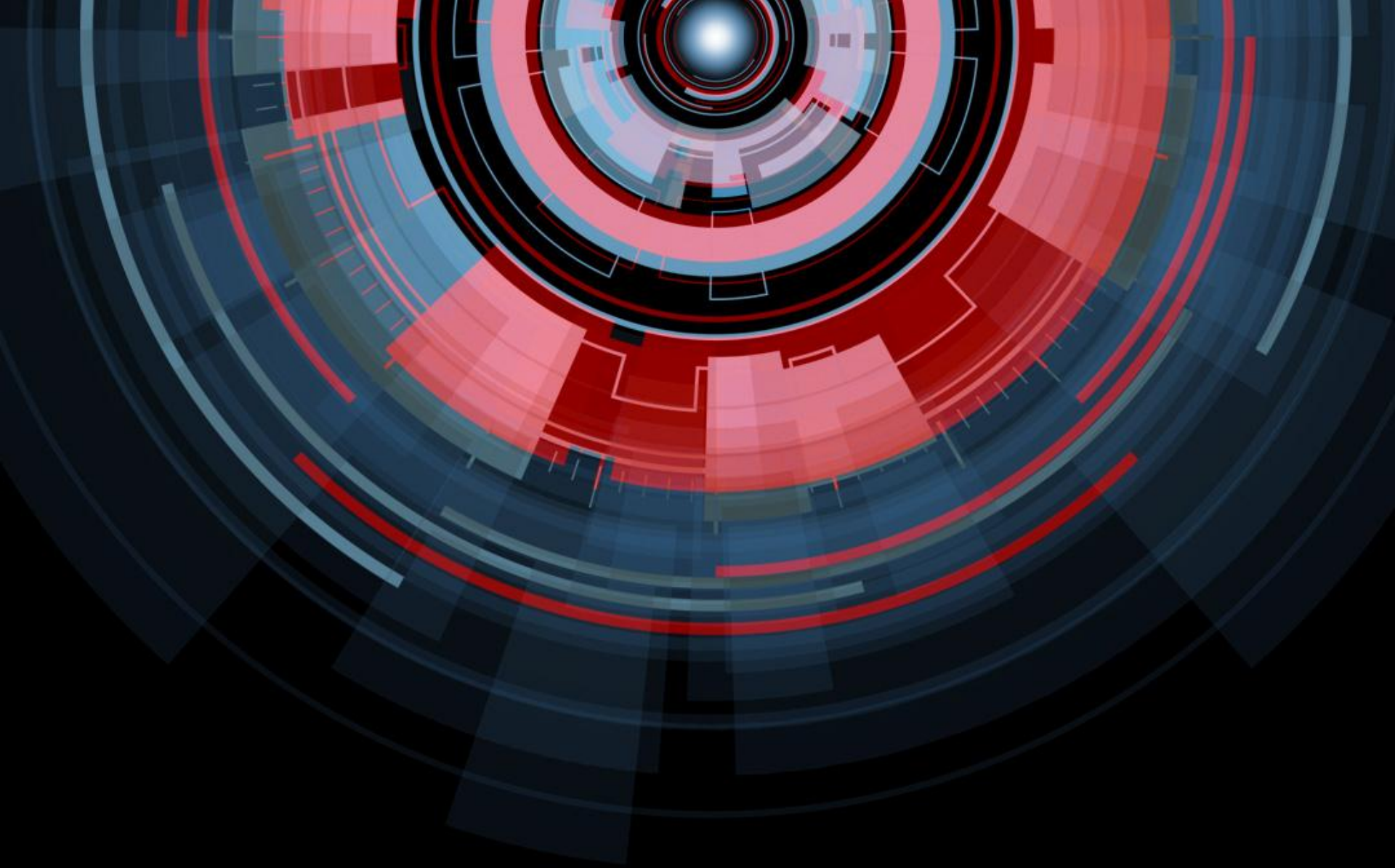
Megoldás (?): counter



Összefoglalás

- Hardverbe vetett hit...
 - Ne legyen vakhit!
 - Olvassunk utána!
 - Próbáljuk ki!
- Usability vs. security
 - Nehéz egyensúlyozni
 - Kevesebb nyűg, ha már fejlesztéskor gondolunk rá





Köszönöm a figyelmet!