MI-SP-SP-2 (MI-BPR.16) (přednáška 3 (+4))

# Přetečení bufferu, jeho druhy. Metody obrany, způsoby překonání obran.

- přepsání jednoho nebo více bytů na konci bufferu
  - přepis návratové hodnoty → stack smashing (stack)

- přetečení na heap také nebezpečné!
  - můžeme přepsat informace ukládání funkce

řešení:

DEP - Data execution prevention
- NX bit v položce tabulky stránek
- k přetečení může dojít, ale daná stránka nelze spustit
- dá se vypnout za běhu pomocí API
→ return oriented programming (exploit)

ASLR - Address space layout randomization
- program umístěn na náhodnou adresu
- (exploit) získ adresy pomocí nebezpečného printf()

kanárek - náhodná kontrolovaná hodnota (stack guard)

Safe structured exception handling
- výjimka (handler) se kontroluje proti seznamu známých handlerů
→ pokud není nalezen, chaoticky konec

(+ exploid unlink makra)

nepoužívat gets, ~~memcpy~~, strcpy, ...