SecureFreePastry

Luboš Mátl

Cíle

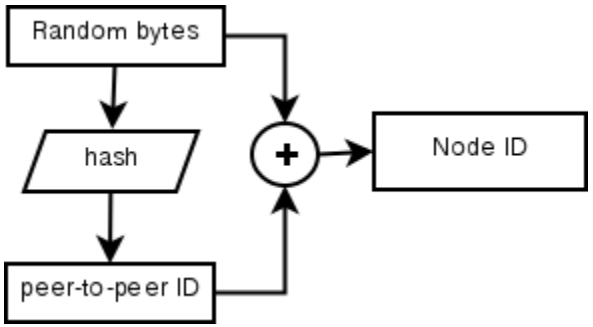
- P2P network Pastry

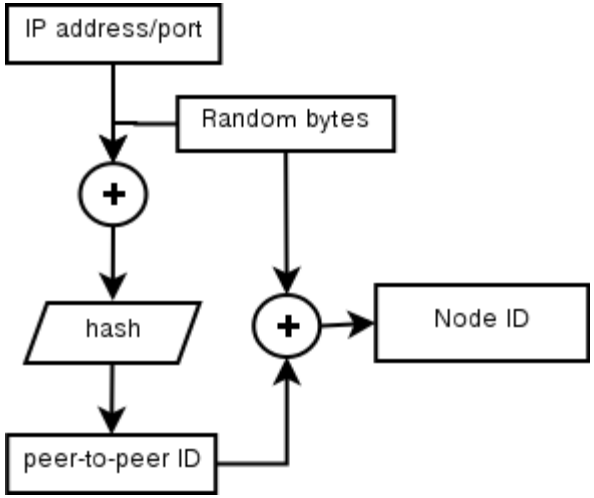
- odstranění možnosti útoku:
  - Sybil attack
    - obklopení uzlu

  - Eclipse attack
    - ukradení identity (změna směrovacích tabulek)

Řešení

- uzly generují ID samostatně ale pomocí hashovací funkce
- možnost volby hashovací funkce (defaultně SHA1)





Implementace

- problémy:
  - serializace - statická metoda ***serialize*** třídy ID
    - nemohl jsem přetížit
  - proto bylo nutné tuto třídu upravit
  - nutné zachovat původní funkcionalitu
    - bezpečnost se zapíná parametrem
    - nekompatibilita s původní verzí FreePastry, pokud je parametr zapnut
      - lze
        - security => security
        - no-security => no-security
      - nelze
        - no-security => security (logické)
        - security => no-security (omezení)

Výsledky

- výsledek byl otestován a je nasazen v projektu ELISA

- napsán článek, který secure ID rozebírá včetně testů
  - ISD 2012

Děkuji za pozornost

- tutoriál
  - https://github.com/matllubos/FreePastry/wiki
- repozitář
  - https://github.com/matllubos/FreePastry