# Implementace OTP ve vybraném systému

Zpracoval: Bc. Petr Jajtner

INFONK 2017

# Obsah prezentace

- **Cíle práce**
- **Metodika**
- **Teoretická východiska**
- **Praktická část**
- **Diskuse a závěr**

# Cíle práce

- **Hlavní cíl**
  - **Implementace generátoru jednorázových hesel a integrace do stávajícího systému**
    - **Ověření uživatele pomocí přihlašovacích údajů a jednorázového hesla**
- **Dílčí cíle**
  - **Otestování implementace a integrace**
  - **Vývoj klientské aplikace pro OS Android**

# Metodika

- **Teorie jednorázových hesel a použité technologie**
  - **Seznámení se s jednorázovými hesly, názvoslovím a druhy generátorů**
  - **Známé pozitivní a negativní stránky tvorby a používání OTP**
  - **Útoky na jednorázová hesla a obrana**
  - **Popis značkovacích jazyků, HTML, CSS, PHP, MySQL**
  - **Popis zvoleného systému**
- **Praktická část**
  - **Detailní popis částí – návrh architektury generátorů, komponenty systému**
  - **Prototypová aplikace – otestování bazální funkčnosti implementace**
  - **Integrace do stávajícího systému a identifikace možných problémů**

# Teorie – klasická vs. jednorázová hesla

- **Přihlašování uživatele (autentizace), hesla**
  - **Bankomaty: posloupnost číslic**
  - **Informační systémy: typicky jméno a heslo (libovolná kombinace znaků)**

  } **forma dána systémem**
  - **Správné heslo – subjekt považován za oprávněného, silné heslo**
  - **Slabá místa – uchovávání, stejná hesla k různým systémům, nezabezpečený přenos, keyloggery**
- **One-time password**
  - **Platné pouze pro jedno přihlášení nebo jedinou transakci, smyslem je zvýšit bezpečnost systémů**
  - **Kombinací čísel nebo čísel a písmen, získáváno generátory – hardware (RSA SecurID), software (FreeOTP)**
- **Dvoufaktorová autentizace**
  - **klasický přístup (znalost) a jednorázová hesla (vlastnictví)**
- **Varianty**
  - **Technologie HMAC-base OTP (HOTP, též event-based) – RFC 4226**
  - **Time-based OTP – RFC 6238, využívá časové bloky a metodu HOTP**

# Praktická část

- **Vybraný systém – vlastní CMS**
  - **HTML(5), CSS(3), PHP, MySQL, Zend Framework**
- **Implementace**
  - **Vyzkoušení bazální funkčnosti HOTP a TOTP v prototypové aplikaci a FreeOTP**
  - **Přenos nastavení realizován pomocí pseudoprotokolu otpauth**
    - **otpauth://TYP/POPIS?PARAMETRY**
  - **Model pro OTP testován pomocí UnitTestů, kód 100% pokryt testy**
- **Integrace**
  - **Rozšíření databáze o nutné entity a atributy ve stávajícím systému**
  - **Doplnění kódu o potřebnou funkčnost**
  - **Kontrola na počty pokusů přihlášení**
  - **Nastavení softwarového generátoru**

# Diskuse a závěr

- **Cookies a blokování IP adres**
  - **Problém se SESSION, klientská cookies**
  - **Blokování konkrétního počítače – problém se získáváním identifikace**
    - **Blokovat IP?**
    - **Javascript?**
  - **Problémy se schováváním se za routery**
- **Softwarový vs. hardwarový generátor OTP**
  - **K dispozici pouze softwarový generátor**
- **Zabezpečení protokolu (HTTPS)**
  - **Let‘s Encrypt**
- **<u>Přidaná hodnota</u> – webová aplikace využívající dvoufaktorou autentizaci**
  - **Zvýšení bezpečnosti; generátor OTP, transformace BASE32 a OTPAuth protokol v jednom**