ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE
FAKULTA ELEKTROTECHNICKÁ
KATEDRA TELEKOMUNIKAČNÍ TECHNIKY

Jak se chovat v cyberprostoru

Ing. Pavel Bezpalec, Ph.D.

pavel.bezpalec@fel.cvut.cz

Agenda

- ČVUT v Praze a ITU CoE
- Pojmy cyber-…
- Zařízení používaná v kyberprostoru
- Aplikace IM – jejich stinné stránky
- Hesla – využití, použití, zneužití

České vysoké učení technické v Praze

- 8 fakult
  - Fakulta stavební (FSv)
  - Fakulta strojní (FS)
  - **Fakulta elektrotechnická** (**FEL**)
  - Fakulta jaderná a fyzikálně inženýrská (FJFI)
  - Fakulta architektury (FA)
  - Fakulta dopravní (FD)
  - Fakulta biomedicínského inženýrství (FBMI)
  - Fakulta informačních technologií (FIT)
- ~20 000 studentů
- Centrum Excelence ITU
    - *ITU Centre of Excellence*
  - od 1.1.2015
  - Zaměření: kybernetická bezpečnost
  - Výstavba laboratoře kybernetické bezpečnosti

Pojmy

- Kybernetický prostor
  - *Kyberprostor*, *Cyberspace*

    „Konsenzuální datová halucinace, vizualizovaná v podobě imaginárního prostoru, tvořeného počítačově zpracovanými daty a přístupná pouze vědomí uživatelů“
  - virtuální svět informací vzniklý propojením ICT (internet)

- Kybernetická bezpečnost
  - *Cybersecurity*
  - odvětví výpočetní techniky zabývající se ochranou informací a majetku před zneužitím za předpokladu zachování přístupnosti pro jeho uživatele

- Kyberkriminalita, kyberterorismus, kyberzločin, kyberválka, kyberarmáda, kyberútok …

Mobilní zařízení

- Notebook, netbook, tablet, phablet, smartphone …
- Víceúčelová zařízení, která umí i telefonovat
  - náhrada kalendáře, fotoaparátu, diktafonu, zápisníku, kalkulačky, slovníku …
  - mapy, navigace
  - úložiště hesel, přístupových údajů (EZS …)
  - přístup k internetu
  - e-maily, VPN, firemní internet
  - sociální sítě
    - FB, LinkedIn, Instagram, G+, Flicker, Lidé, Spolužáci …
  - NFC technologie ➔ peněženka
  - přístup k bankovním účtům

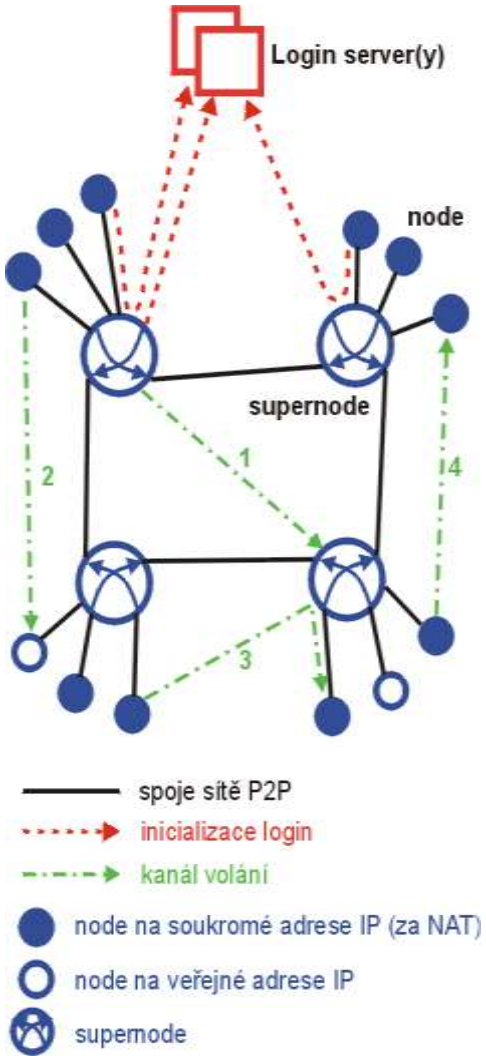
Mobilní uživatel a jeho data

- Vysoké riziko zneužitelnosti dat
  - i přes snahy zabezpečit komunikaci více kanálovým způsobem ➔ data + SMS
    - přístup k bankovním službám
    - EUROGRABBER …
  - sběr info o poloze
    - GPS data, Wifi sítě
      - Google, Microsoft, Nokia, Samsung …
  - instalace app bez autorizace !!!
    - možné trojské koně, viry

Mobilní komunikace

- Velká obliba IM
  - okamžitá odezva
  - „zdarma“
    - hovor, zprávy, obrázky, soubory
- Nejužívanější IM
  - Skype, WhatsApp, Viber
- Rizika používání IM?
  - P2P sítě
  - neprůhledná topologie
  - nestandardní komunikační protokol
- GSM/3G/LTE
  - není „zdarma“
    - hovor, zprávy (SMS), obrázky (MMS)
- Riziko používání
  - odposlech
  - šifrování hovoru
    - šifrování GSM, 3G, LTE
    - fallback
      - 3G → GSM
      - vynucení vypnutí šifrování
    - dodatečný sw pro šifrování
      - je opravdu kvalitní ?

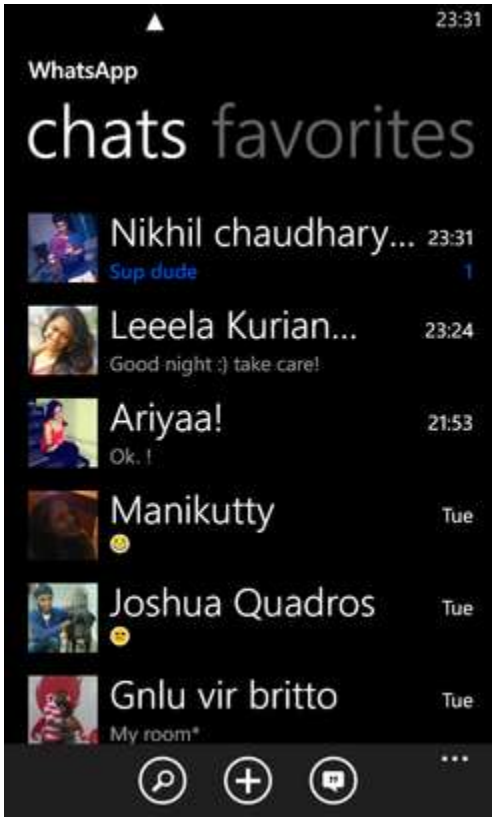
SKYPE



- Neveřejná architektura
  ? protokoly ? šifrování ?
- Peer-to-peer síť umožňuje
  - (video)hovor
  - přenos souborů a zpráv
- Dříve
  - parazit na PC uživatele
  - node, supernode
- Nyní
    - Po převzetí Microsoftem
  - Centralizovaná architektura

WhatsApp

- nezávislost na platformě
  - Android, iOS, BlackBerry, WinPhone, Symbian
- 2009 WhatsApp
  - ➔ Facebook
- ID = telefonní číslo
- upload a akualizace telefonního seznamu
- vyhledávání „přátel“
  - kontakty vašich kontaktů



Viber

- nezávislost na platformě
  - Android, iOS, BlackBerry, WinPhone, Symbian, Bada …
  - Win, Mac, Linux
- hlavní tahák pro lidi
  - sdílení: textové zprávy, obrázky, čmáranice, GPS pozice, videa
- ID = telefonní číslo
- upload telefonního seznamu
  - cloud Amazon AWS
- vyhledávání „přátel“
  - kontakty vašich kontaktů
- úplná a **skrytá** integrace do systému telefonu
- až do 04/2014 **bez šifrování** dat posílaných do cloudu
  - obrázky, videa

http://s3.amazonaws.com/staticphotos/eac09a37d51979ccf13e3d9e595ec98520fed44e6f83ac10cf5d8cf628f7f470.jpg

HESLA, hesla, hesla

- Politika hesel
  - změna defaultního hesla
- Životní cyklus hesel
  - stáří a obnova
- Tvorba a ochrana hesla
  - papírek na monitoru ?
  - na krabici na kapesníky ?
- Množství hesel
  - intranet, e-mail, banky, škola, obědy, obchody,

www.howsecureismypassword.net

Dobré heslo

- nepředpověditelné
- jedinečné
- snadno zapamatovatelné pro lidi
  - rozumně dlouhé
    - Dobrojeprisjetitisedaprividnopravputpremaciljupredstavljaustvaripravodlivokrivudanje
  - jednoduše napsatelné
- nesnadno uhodnutelné pro stroje
    - S0bJK7BYqlmSeQ4QB4rwG8pVgLg5WXOU
- „často“ měněno

Nejhorší hesla roku 2014

- **123456**
- password
- 12345
- 12345678
- qwerty
- 1234567890
- 1234
- baseball
- dragon
- football
- 1234567
- monkey
- letmein
- abc123
- 111111
- mustang
- access
- shadow
- master
- michael
- superman
- 696969
- 123123
- batman
- trustno1

http://www.cnet.com/news/worst-passwords-of-2014-are-just-as-awful-as-you-can-imagine/

Děkuji za pozornost, diskuse