Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky

Operativní forenzní analyzátor

Průběžná zpráva - 2008

Róbert Lórencz
Tomáš Zahradnický, Jiří Buček
ČVUT Praha, FEL
Katedra počítačů

Personální obsazení

- doc. Ing. Róbert Lórencz, CSc. – zodpovědný vedoucí
- Ing. Jiří Buček – řešitel
- Ing. Tomáš Zahradnický – řešitel
- Ing. Petr Kurtin – řešitel
- Jan Cílek – student, člen studentského řešitelského týmu
- Josef Nouzák - student, člen studentského řešitelského týmu

Akce 2008

- výjezdní porada Červená nad Vltavou (19.-21.3.)
  - Prezentace částečných výsledků řešení OFA a diskuse
- Schůzka s experty s KÚP (25. 4.)
  - Diskuse o vlastnostech OFA
- Konference EurOpen – Rožmberk (18.-21.)
  - Příspěvek: R. Lórencz, T. Zahradnický, J. Buček „Forenzní analyzátor pro operativní analýzu“

Forenzní analyzátor – změny vlastností

- Důraz na
  - práci v národním prostředí – čeština,
  - jednoduchost,
  - přenositelnost,
  - minimalizaci paměťových nároků.
- Boot na počítači vyšetřovatele – „čistý systém“
- Specifikace:
  - Co analyzovat, jak postupovat …
  - Hledání, třídění, náhledů, statistik …
  - Reportů (uložení)

Forenzní analyzátor – systémové změny

- Možnost spouštění z paměťového média
  - Přepsané výkonné jádro analyzátoru
  - Nezávislost na OS vyšetřovatele
  - Změna implementační báze z Windows na Linux
  - Čtení libovolného FS s podporou modulů FS
- Zabudovaná SQL databáze
  - Rychlé hledání v názvech a typech souborů
- Podpora připojování externích nosičů dat v režimu pouze pro čtení

Forenzní analyzátor - architektura

- Spuštění z bootovatelného CD, DVD nebo USB klíčenky
  - na fyzický disk se nic nezapisuje
- Minimální nároky na paměť
- Podpora přes 35 různých filesystémů
  - FAT32, NTFS, ext2, ext3, HFS, …
  - poradí si se všemi systémy Windows, Linux, Mac, …
- Možnost práce s konzolí
  - spouštění dalších utilit (zálohování disků, ...)

Forenzní analyzátor - GUI

- Prvotní nástin vzhledu a rozvržení aplikace
  - dále se podřídí potřebám aplikace, přehlednosti, zpětné reakci uživatelů
- Prozatím náhledy pouze obrázků
  - rozšíření na více než 500 různých typů souborů
- Panel rychlého hledání
  - vzhledem k použití SQL databáze je hledání podle názvu nebo typu souboru velmi rychlé i s řádově stovkami tisíc souborů

Forenzní analyzátor – další vývoj

- Vývoj uživatelského rozhraní
  - Možnosti filtrace
  - Prohlížení, …
- Vývoj systémové podpory
  - Připojování zkoumaných médií
  - Optimalizace paměťových nároků a swapování
- Vývoj aplikační vrstvy
  - Statistika
  - Reporty
  - Zpracování metadat souborů