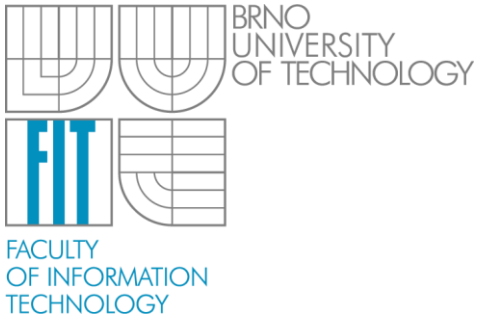
MPO TIP: NBASaaS - Výzkum a vývoj hardwarově akcelerovaného řešení pro detekci kybernetických hrozeb a anomálií v počítačových sítích

Jan Kořenek, Pavel Čeleda, Martin Žádník

Brno University of Technology
Faculty of Information Technology
Božetěchova 2, 612 66 Brno, CZ



INVESTMENTS IN EDUCATION DEVELOPMENT

Úvod

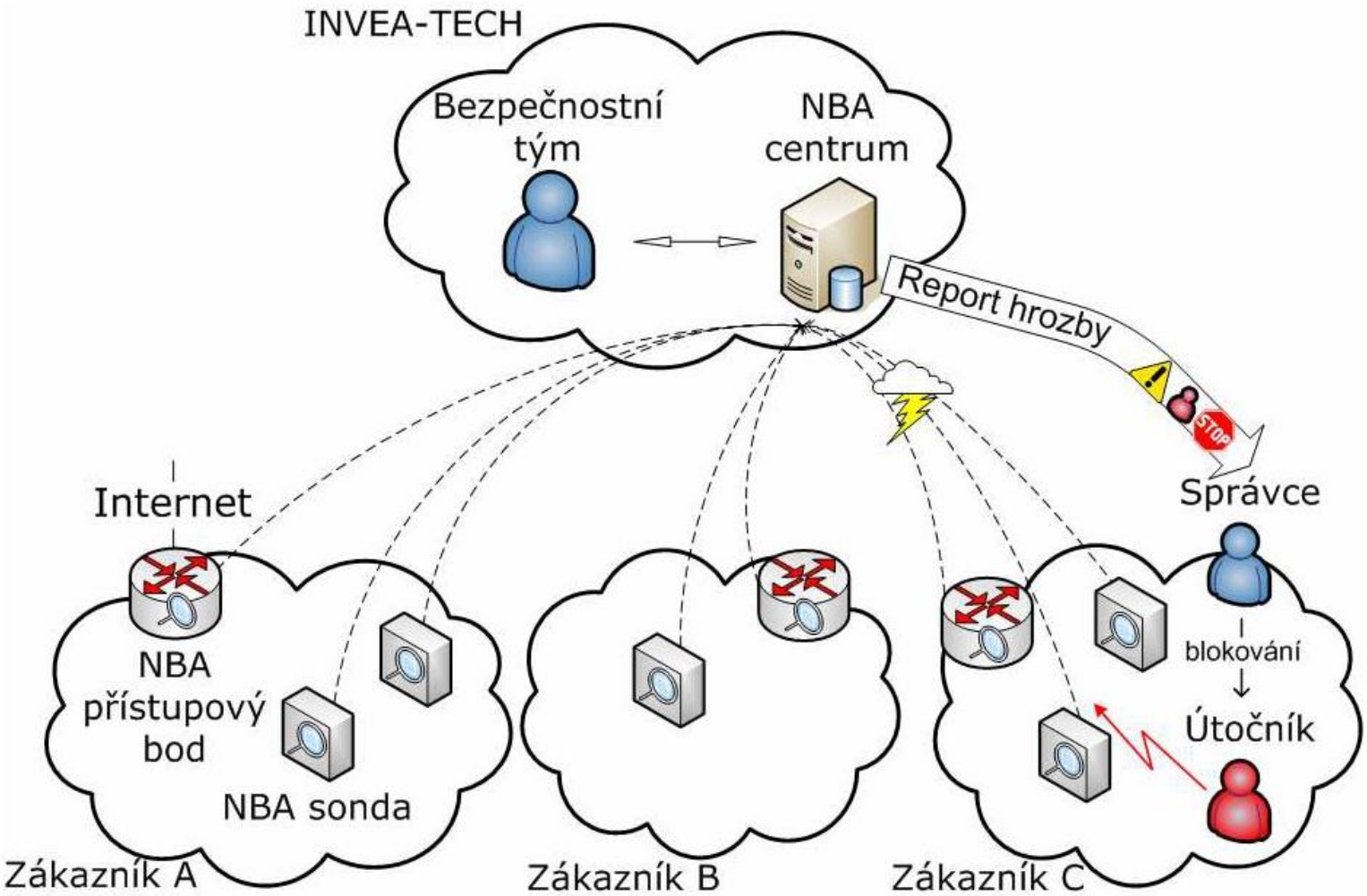
- MPO vyhlásilo TIP
  - Podpora aplik. výzkumu a vývoje inovací
  - Podpora spolupráce komerční a akademické sféry
- INVEA-TECH + FIT
- 29.8.2011 podán návrh
- 21.1.2012 výsledek schvalovacího řízení

Motivace

- Flow Network Behavioral Analysis
- Bezpečnost sítě
- Řešení síťových problémů a incidentů
- Současný stav
- UTM – Unified Threat Management
  - Drahé
  - Vyžaduje expertní znalost
  - Zahltí administrátora
  - Výsledek: hnije to ve skříni

Myšlenka

- Stěžejní myšlenka projektu: SaaS – Security as a Service
- Poskytneme zajištění síťové bezpečnosti formou služby



Výhody

- Outsourcing bezpečnosti a sledování sítě z pohledu zákazníka
  - Nízké náklady
  - Řešení problémů expertním týmem
  - Komplexní spektrum služeb

- Z pohledu INVEA-TECH
  - Rozložení nákladů mezi zákazníky
  - Získávání expertní znalosti od více zákazníků
  - Nové hrozby a problémy = rozvoj služeb

- Výsledky:
  - NBA centrum (funkční vzor)
  - NBA sonda (funkční vzor)
  - NBA přístupový bod (funkční vzor)
  - Programová knihovna algoritmů pro detekci hrozeb (software)
  - Publikace nových metod pro detekci kybernetických hrozeb a anomálií, nových algoritmů pro efektivní sběr dat ze sítě a nových architektur pro hardwarovou akceleraci detekčních metod.

Plán vývoje

- Výzkum a vývoj rozdělen do 12 fází
  - Analýza kybernetických hrozeb, stávajících metod a ekonomických dopadů, návrh koncepce systému
  - Experimentální ověření existujících metod a systémů vhodných pro SaaS
  - Výzkum a vývoj algoritmů pro detekci kybernetických hrozeb a architektur pro sběr dat ze sítě
  - Návrh a vývoj architektury sběrného a vyhodnocovacího místa a bodů pro získávání dat
  - Experimentální ověření navržených algoritmů a optimalizace
  - Návrh a vývoj efektivní metody pro validaci bezpečnostní politiky a metody pro eskalaci bezpečnostních událostí

Plán vývoje

- Experimentální ověření metody validace, ladění a optimalizace s cílem minimalizovat falešné poplachy
- Výzkum a vývoj efektivních metod pro detekci neznámých kybernetických hrozeb
- Integrace navržených metod do systému NBA spolu s experimentálním ověřením vlastností systému nad síťovými daty
- Změření výkonnosti NBA centra a identifikace časově kritických částí vhodných pro HW akceleraci
- Výzkum a vývoj nových algoritmů a architektur pro hardwarovou akceleraci časově kritických úloh
- Provoz a finalizace systému NBA v prostředí SaaS

Závěr

- SaaS
- Výzkum a vývoj kompletního systému dohledu sítě
- Včetně akcelerace kritických částí

- Při přijetí
  - Začátek – únor 2012
  - Trvání projektu 4 roky
  - 4 úvazky INVEA-TECH
  - 3 úvazky FIT

- Držte palce