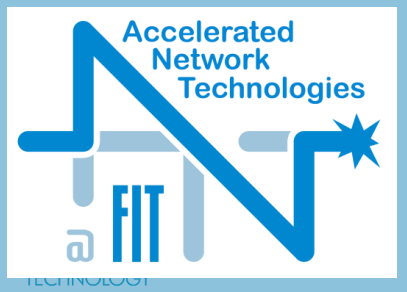
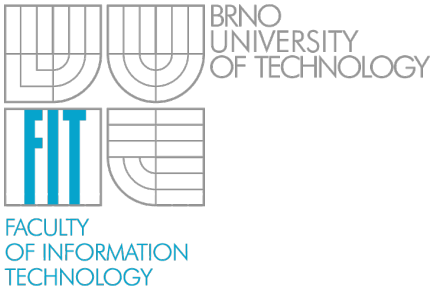
Accelerated Network Technologies
Research Group



Jan Kořenek, Martin Žádník

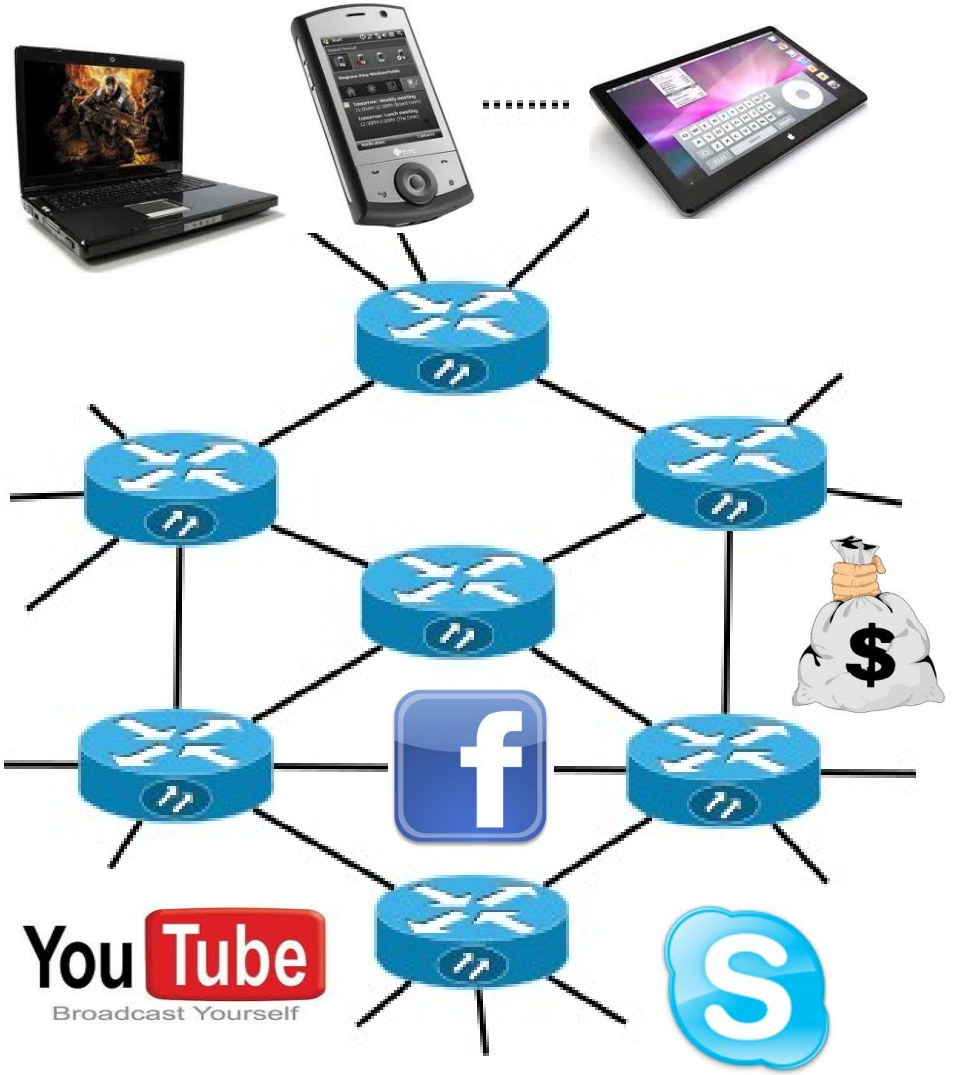
Brno University of Technology, Faculty of Information Technology
Bozetechova 2, 612 00 Brno, CZ
http://merlin.fit.vutbr.cz/ant/



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Vývoj v počítačových sítích

- Neustále narůstá počet uživatelů a služeb na Internetu
- Zvyšuje se kapacita linek a tím i požadavky na výkonnost prvků síťové infrastruktury
- Počítačové sítě se stávají důležitou součástí k zajištění fungování společností a služeb
- Narůstá počítačová kriminalita snažící se ochromit síť nebo ji zneužít pro nelegální aktivity
- Je potřeba zajistit bezpečnost počítačových sítí



Botnet

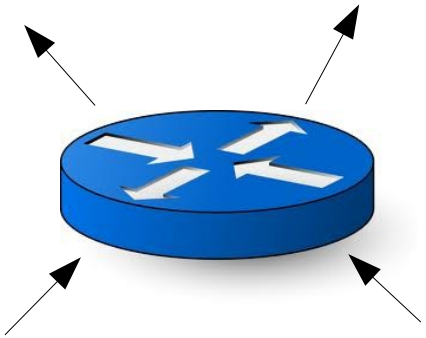
- Největší hrozbou Internetu jsou v současné době *botnety*
- **Botnet** – skupina počítačů pod kontrolou hackera
  - Zodpovědné za téměř veškeré DDoS útoky
  - Vytváří většinu současného spamu
  - Šíří spyware a získává hesla a jiné informace bez vědomí uživatele
- Získání botnetu je stále jednodušší
- Chování botnetů se neustále zdokonaluje (p2p, skypebot)
- Jedním z klíčových problémů současných sítí je detekce a následná eliminace botnetů

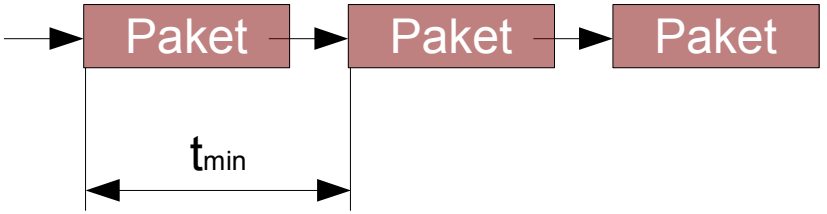
Boj proti botnetům

- ***Monitorování sítě***
  - ***Hledání signatur útoků***
  - ***Behaviorální analýza síťových toků***
  - ***Analýza DNS provozu***
  - ***Detekce anomálií***
- ***Detekce botnetů*** – modelování důvěryhodnosti uživatelů
- ***Eliminace nebo zmírnění následků botnetu***
  - Eliminace C&C serveru
  - ***Filtrování podezřelého provozu***
  - ***Zmírnění DDoS útoků***

Proč HW akcelerace?

- Rychlost zpracování dat na síti
  - Data jsou na síti přenášena prostřednictvím bloků dat – paketů
  - Je potřeba zpracovat každý příchozí paket – minimální délka paketu 64B





Počet cyklů procesoru pro frekvencí 3,6 GHz

1 Gb/s	500 ns	~	1 807	CPU clock cycles
10 Gb/s	50 ns	~	181	CPU clock cycles
40 Gb/s	12 ns	~	45	CPU clock cycles
100 Gb/s	5 ns	~	18	CPU clock cycles

Proč HW akcelerace?

- Časově kritické operace v počítačových sítích
  - ***Filtrace paketů*** - jak vybrat množinu pravidel nebo pravidlo, které odpovídá přijatému paketu?
  - ***Hledání útoků*** - Jak zajistit hledání tisíců regulárních výrazů v síťových tocích?
  - ***Analýza paketů*** - jak analyzovat hlavičky paketů a přesně určit umístění položek v hlavičce paketů?
  - ***Stavové zpracování síťového provozu*** - jak uchovat milióny záznamů o síťových tocích a zajistit vyhledání záznamu v konstantním čase?
- Výkonnost jednoho jádra procesoru Intel Xeon

Operace	Propustnost	1G	10G	40G	100G
Analýza paketů	14Gbps	✓	✓	STOP	STOP
Stavové zpracování prov.	6Gbps	✓	STOP	STOP	STOP
Filtrace paketů	1,3Gbps	✓	STOP	STOP	STOP
Hledání útoků (regexp)	18Mb/s	STOP	STOP	STOP	STOP

Pro 10Gb linku je na zpracování jednoho paketu pouze 50 ns

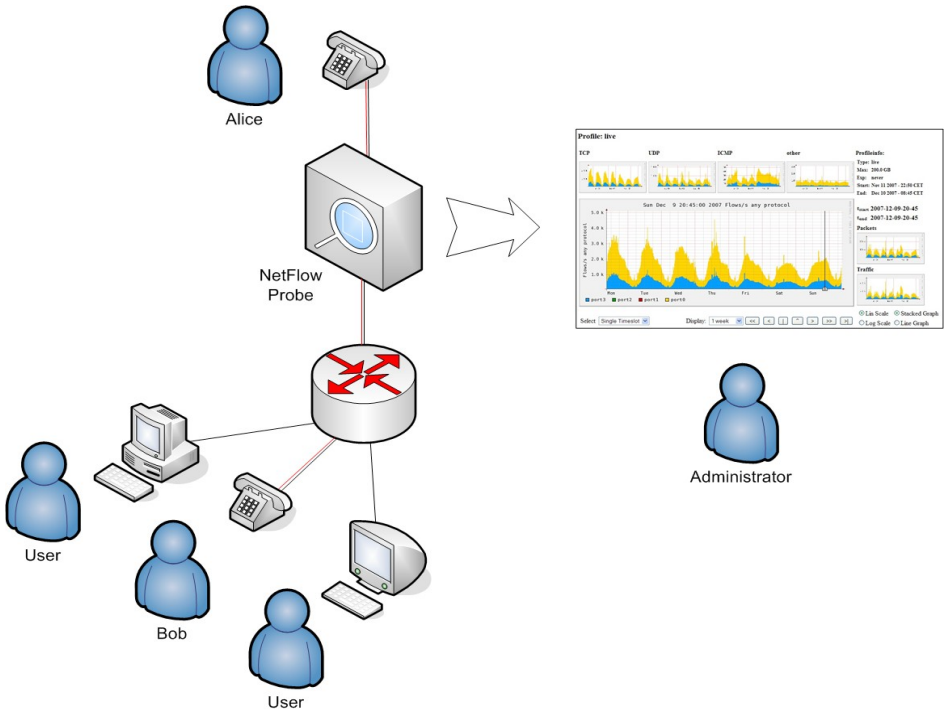
Zaměření výzkumného týmu

- Akcelerace algoritmů a architektur pro monitorování a bezpečnost vysokorychlostních sítí
  - *Algoritmy pro detekci anomálií*, útoků a jiných bezpečnostních incidentů
  - Vývoj zařízení pro monitorování a bezpečnost počítačových sítí
  - Využití technologie *MultiCORE* a *FPGA* pro 10, 40 a 100 Gb sítě

Realizované a vyvíjené prototypy

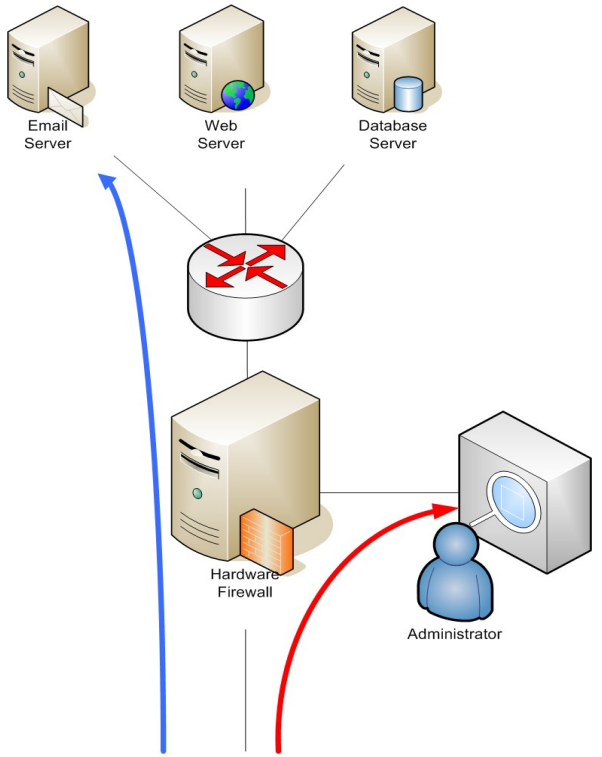
Monitorovací sondy

- ***Sledování provozu na síti***
  - Na rychlosti deset gigabitů a více
  - Vytváření statistik o síťovém provozu
  - Detekce anomálií a botnetů
  - Sledování kvality spojení



Filtrování provozu

- ***Filtrování a odposlech provozu***
  - Odposlech podezřelých aktivit
  - Filtrování škodlivého provozu



Reference a spolupráce

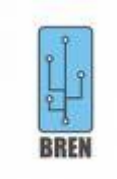
- Spolupráce s akademickými institucemi

Stanford University

Computer Laboratory

Czech NREN

- Nasazení vyvinuté technologie prostřednictvím spin-off společnosti INVEA-TECH



THE ACADEMY OF SCIENCES OF THE CZECH REPUBLIC

Připojte se k naší skupině

Research Group

Pojďte se za námi podívat do L310
nebo napište na korenek@fit.vutbr.cz